KUPNÍ SMLOUVA

níže uvedeného dne, měsíce a roku uzavřeli

1. **Kupující:** **Nemocnice Pelhřimov, příspěvková organizace**
   se sídlem: Slovanského bratrství 710, 393 01 Pelhřimov
   IČ: 00511951
   DIČ: CZ00511951
   zastoupená: Ing. Radimem Hoškem, ředitelem
   se sídlem: Slovanského bratrství 710, 393 01 Pelhřimov
   IČ: 00511951
   (dále jen "**Kupující**")

a

2. **Prodávající:** **IXPERTA s.r.o.**
   se sídlem: Lihovarská 1060/12, Libeň, 190 00 Praha 9
   zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, sp.zn. C 117991
   zastoupená: Pavlem Šiprem, jednatelem
   IČ: 27599523
   DIČ: CZ 27599523
   Bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.
   Číslo účtu: 513686001/2700
   (dále jen "**Prodávající**")

(Kupující a Prodávající společně též jen „**Smluvní strany**“ nebo jednotlivě „**Smluvní strana**“)

tuto kupní smlouvu (dále jen „**Smlouva**“)
podle ust. § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „Občanský zákoník“)

Preambule

1. Smluvní strany uzavírají tuto Smlouvu na základě zadávacího řízení níže uvedené veřejné zakázky, za účelem vymezení práv a povinností Smluvních stran při realizaci veřejné zakázky s názvem **„Kybernetická bezpečnost Nemocnice Pelhřimov - 2**“ vedené ve Věstníku veřejných zakázek pod ev. č. Z2024-040058 a u Kupujícího pod ev.č. 03/24/VZ zadávané v nadlimitním režimu v otevřeném řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů a jeho prováděcími předpisy (dále jen „ZZVZ“).
2. Smluvní strany prohlašují, že veškeré podmínky uvedené v Zadávací dokumentaci k předmětnému zadávacímu řízení, jakož i v nabídce Prodávajícího, jsou platné i pro plnění této Smlouvy.
3. Prodávající prohlašuje, že je oprávněný a odborně způsobilý k plnění předmětu této Smlouvy a zavazuje se v maximální míře chránit zájmy Kupujícího.

4. Smluvní strany vzájemně deklarují vůli vynaložit veškeré spravedlivě očekávatelné úsilí k dosažení účelu a předmětu této Smlouvy, k zachování dobrého jména druhé Smluvní strany jakož i k eliminaci či minimalizaci jakýchkoli škodlivých následků vzniklých při plnění povinností z této Smlouvy.

5. Smluvní strany si sjednaly, že smluvní vztah touto Smlouvou založený bude vykládán výhradně podle obsahu Smlouvy, bez přihlédnutí k jakékoli skutečnosti, která nastala a/nebo byla sdělena, jednou Smluvní stranou druhé Smluvní straně před uzavřením Smlouvy.

6. Předmět této Smlouvy bude spolufinancován z Evropského fondu pro regionální rozvoj - Integrovaného regionálního operačního programu (IROP) - 4. výzvy IROP - Kybernetická bezpečnost - SC 1.1 (PR) v rámci projektu Kupujícího: „**„Kybernetická bezpečnost Nemocnice Pelhřimov**“ registrovaného pod č. CZ.06.01.01/00/22_004/0000177.

7. Prodávající prohlašuje, že si je vědom skutečnosti, že Kupující má zájem realizovat předmět této Smlouvy v souladu se zásadami odpovědného zadávání veřejných zakázek stanovenými v § 6 odst. 4 ZZVZ. Odpovědné zadávání veřejných zakázek kromě důrazu na čistě ekonomické parametry zohledňuje také související dopady zejména v oblasti zaměstnanosti, sociálních a pracovních práv a také životního prostředí.

8. Kupující proto klade důraz na to, aby Prodávající při své podnikatelské činnosti v maximální možné míře naplňoval požadavky z usnesení vlády České republiky ze dne 24. července 2017 č. 531, o Pravidlech uplatňování odpovědného přístupu při zadávání veřejných zakázek a nákupech státní správy a samosprávy, které zohledňuje sociální, resp. širší společenské a zejména také environmentální aspekty směřující k prospěchu pro společnost a ekonomiku a minimalizaci negativních dopadů na životní prostředí. Aspekty odpovědného zadávání veřejných zakázek jsou zohledněny dále v textu této Smlouvy.

I. Předmět smlouvy

1.1 Předmětem Smlouvy je dodávka hardware a software IT infrastruktury včetně montáže, instalace a jejich implementace Prodávajícím Kupujícímu v rozsahu a způsobem, jak je věcně a technicky specifikováno v technických specifikacích, které tvoří Přílohy č. 2 a č. 3 této Smlouvy. Součástí předmětu Smlouvy jsou i veškeré související dodávky, služby a činnosti nezbytné pro realizaci předmětu Smlouvy podle této Smlouvy a jejích příloh (dále také souhrnně „Předmět Smlouvy nebo Předmět koupě“). Spolu s převodem vlastnického práva k HW položkám Předmětu koupě a užívacího práva (vlastnictví licencí) k SW položkám Předmětu koupě se převádí i vlastnické právo k veškerému věcnému příslušenství Předmětu koupě a poskytuje licence na použití všech práv duševního vlastnictví k software, jak vyplývá z Technické specifikace uvedené v Příloze č. 2 této Smlouvy. Prodávající prohlašuje, že Předmět koupě je věcí novou, nerepasovanou a bez vad.

1.2 Prodávající se zavazuje realizovat a předat Předmětem koupě, Kupujícímu řádně a v termínu dohodnutém v této Smlouvě a umožnit Kupujícímu nabýt vlastnické právo k HW položkám Předmětu koupě a nabýt užívacích práv (vlastnictví licencí) k SW položkám Předmětu koupě. Řádně a včas odevzdaný Předmět koupě se Kupující zavazuje převzít a zaplatit za něj cenu dle čl. IV. této Smlouvy, na základě dohodnutých platebních podmínek.

1.3 Předmět Smlouvy je dán:

a) touto Smlouvou a jejími přílohami,
b) Zadávací dokumentací k výše uvedené veřejné zakázce,
c) nabídkou Prodávajícího, podanou v rámci zadávacího řízení výše uvedené veřejné zakázky.

1.4 Prodávající se zavazuje realizovat Předmět Smlouvy v rozsahu a termínech dle této Smlouvy a jejích příloh. Harmonogram realizace Předmětu Smlouvy bude obsahovat i Detailní realizační projekt, zpracovaný Prodávajícím v rozsahu a v termínu dle požadavků Kupujícího uvedených v příloze č. 2 této Smlouvy.

1.5 Prodávající se zavazuje odevzdat Kupujícímu Předmět koupě ve smluveném množství, jakosti, provedení, termínu a za stanovenou kupní cenu. Předmět koupě musí splňovat požadavky dané legislativou v době dodání Předmětu koupě Kupujícímu.

1.6 Součástí závazku Prodávajícího je též doprava Předmětu koupě na místo plnění, předání dokladů a manuálů potřebných k převzetí a užívání Předmětu koupě Kupujícím a Implementace včetně zaškolení administrátorů a poskytování servisní podpory po dobu stanovenou touto smlouvou. Závazné požadavky na poskytování servisní a provozní podpory jsou uvedeny v Příloze č. 2 Smlouvy.

1.7 Součástí Předmětu koupě je i provedení prací výslovně neuvedených či činností, jejichž provedení je s ohledem na Předmět koupě nezbytné, potřebné, účelné či obvyklé, představuje standard či je spravedlivě ze strany Kupujícího očekávané s přihlédnutím k předpokládanému výsledku a znění Zadávací dokumentace výše uvedené veřejné zakázky.

1.8 Prodávající se zavazuje vykonávat veškerou činnost s náležitou odbornou péčí se zachováním práv a oprávněných zájmů Kupujícího v každém okamžiku při výkonu této činnosti.

1.9 Prodávající se zavazuje dodržovat při plnění Smlouvy pokyny Kupujícího ohledně termínů, pravidel chování a pohybu v prostorách Implementace, opatření bezpečnosti, požární ochrany a ochrany zdraví při práci.

1.10 Prodávající se zavazuje splnit své závazky z této Smlouvy vyplývající prostřednictvím osob s potřebnou kvalifikací a odborností uvedených v nabídce Prodávajícího.

1.11 Prodávající se zavazuje bez ohledu na další své povinnosti dle této Smlouvy, jejích příloh a Zadávací dokumentace veřejné zakázky dodat Předmět koupě za následujících podmínek:

a) hardware (tj. komponenty a zařízení) Předmětu koupě ponese označení CE v souladu s právními předpisy stanovujícími podmínky užití takového označení;

b) na hardware (tj. komponenty a zařízení) Předmětu koupě bude zajištěna ze strany výrobce hardware rozšířená záruka za jakost s garancí servisu dle podmínek stanovených v příloze č. 2 této Smlouvy, a to po dobu 60 měsíců ode dne předání Předmětu koupě;

c) na software Předmětu koupě bude příslušným výrobcem poskytnuta rozšířená servisní podpora, včetně možnosti stahovat nové verze firmware a přístupu k technickým zdrojům, v trvání 60 měsíců ode dne předání Předmětu koupě;

d) veškerý software Předmětu koupě a licence k užívání software budou zajištěny na dobu minimálně 60 měsíců ode dne předání Předmětu koupě, přičemž software a licence k němu musí být dodána v takovém rozsahu a nastavení, aby byla zajištěna funkčnost a rozsah funkcionalit dle Přílohy č. 2 této Smlouvy, aniž kupující musel vynaložit dodatečné náklady (např. náklady za rozšíření nebo dostupnost funkcionalit software specifikovaných v Příloze č. 1 této Smlouvy);

e) všechny funkce Předmětu koupě deklarované výrobcem budou bez omezení dostupné po dobu nejméně 60 měsíců ode dne předání Předmětu koupě;

f) Prodávající je povinen zajistit, aby implementaci uložiště pro nestrukturovaná data byl fyzicky přítomen a dohlížel technický specialista proškolený výrobcem software uložiště pro nestrukturovaná data, a to po celou dobu Implementace;

g) Spolu s předáním části Předmětu koupě zahrnující úložiště pro nestrukturovaná data je Prodávající povinen Kupujícímu předložit prohlášení výrobce uložiště, že Prodávající je oficiálním autorizovaným servisním partnerem výrobce úložišť pro nestrukturovaná data v České republice.

1.12 Prodávající prohlašuje, že je oprávněn Předmět koupě Kupujícímu prodat. Vlastnické právo k HW položkám Předmětu koupě a užívací práva (vlastnictví licencí) k SW položkám Předmětu koupě, jakož i nebezpečí škody na Předmětu koupě přechází z Prodávajícího na Kupujícího převzetím Předmětu koupě Kupujícím.

1.13 Pro Smlouvou předvídané účely slouží tyto kontaktní adresy Prodávajícího a Kupujícího:

Prodávající:

Email: pavel.rabeseifner@ixperta.comtel.: +420 603 200 159 (Head of Project Office)

Kupující:

Email: kk@hospital-pe.cz tel.: +420 731 691 345

jan.sobotka@nnm.cz, tel.: +420 566 801 613 (manažer kybernetické bezpečnosti)

II. Termín a místo plnění

2.1 Prodávající se zavazuje splnit požadavky Kupujícího v Kupujícím požadovaných a Prodávajícím odsouhlasených termínech dle Přílohy č. 2 této Smlouvy.

2.2 Prodávající se zavazuje dodat, provést montáž, instalovat a implementovat Předmět koupě Kupujícímu nejpozději do 15 měsíců od nabytí účinnosti Smlouvy podle ust. 11.9 této Smlouvy. Datum a čas zahájení plnění a Implementace Předmětu koupě navrhne písemně Prodávající Kupujícímu nejpozději 10 pracovních dnů předem. Tento návrh podléhá schválení ze strany Kupujícího.

2.3 Předmět koupě bude dodán a předán v místě sídla Kupujícího.

2.4 Předmět koupě včetně všech jeho součástí a s předáním Předmětu koupě spojených činností dle této Smlouvy bude předáván Kupujícímu postupně takto:

a) hardware (tj. komponenty a zařízení) dle jednotlivých položek Předmětu koupě v počtech kusů dle technického popisu nabízeného řešení, a to včetně provedení montáže, instalace a ověření funkčnosti. O předání a ověření funkčnosti takto dodaných položek Předmětu koupě bude Prodávajícím a Kupujícím vyhotoven a jejich zástupci podepsán písemný dílčí předávací protokol (dále jen „**dílčí protokol o předání položky hardware**“);

b) licence software a provedení Implementace položek Předmětu koupě (tj. předání software, jeho instalace a implementace) buď po jednotlivých opatřeních, nebo skupinách společně provázaných opatření dle kapitoly 5, přílohy č. 2 této Smlouvy, v rozsahu kapitoly 6, přílohy č. 2 této Smlouvy dále jen „Opatření“), pokud je toto jednotlivé Opatření, či skupina Opatření, plně funkční. O předání a ověření funkčnosti takto dodaných položek Předmětu koupě bude sepsán a Prodávajícím a Kupujícím podepsán protokol o předání software a implementace (dále jen „**dílčí akceptační protokol**“).

2.5 Předmět koupě je řádně předán Kupujícímu, jestliže Prodávající a Kupující sepsali a podepsali v souladu s touto Smlouvou dílčí protokoly o předání všech položek hardware a dílčí akceptační protokoly o předání všech položek software a jejich implementaci v rozsahu technického popisu nabízeného řešení. Všechny tyto dílčí protokoly o předání položek hardware, všechny dílčí akceptační protokoly, všechna dokumentace skutečného provedení (dle požadavků kapitoly 5, přílohy č. 2 této Smlouvy), doklady a manuály potřebné k převzetí a užívání Předmětu koupě jsou součástí závěrečného předávacího protokolu“ (dále jen **„Předávací protokol“)**. Náklady spojené s odevzdáním Předmětu koupě v místě plnění nese Prodávající.

Osobou oprávněnou k podpisu dílčích protokolů o předání položek hardware, dílčích akceptačních protokolů a Předávacího protokolu za Prodávajícího je: Pavel Rabenseifner.

Osobou oprávněnou k podpisu dílčích protokolů o předání položek hardware, dílčích akceptačních protokolů a Předávacího protokolu za Kupujícího je: Karel Kužel, vedoucí úseku informatiky.

Datum převzetí dílčích částí Předmětu koupě je datem podpisu jednotlivých dílčích protokolů dle bodu 2.4 písm. a) a b) Prodávajícím a Kupujícím. Datum převzetí Předmětu koupě jako celku je datum podpisu Předávacího protokolu Prodávajícím a Kupujícím.

2.6 Kupující je oprávněn odmítnout převzetí Předmětu koupě, pokud se na něm budou vyskytovat v okamžiku převzetí zjevné vady. Pro tento případ bude v Předávacím protokolu Kupujícím uvedeno, o jaké zjevné vady, které jsou překážkou převzetí Předmětu koupě Kupujícím, se jedná. Za vadu se považují i vady v Implementaci či dokladech nutných pro užívání Předmětu koupě. Věc se považuje za odevzdanou a závazek Prodávajícího odevzdat věc Kupujícímu bude splněn až okamžikem převzetí Předmětu koupě bez zjevných vad Kupujícím.

III. Způsob plnění

3.1 Správcem, zpracovatelem a vlastníkem dat použitých při plnění dle této Smlouvy nebo v souvislosti s ním, je vždy Kupující. Prodávajícímu na základě této Smlouvy nevzniká žádné právo na užití dat zpracovávaných prostřednictvím Předmětu koupě.

3.2 Kupující si vyhrazuje právo na provedení kontroly plnění dle této Smlouvy.

3.3 Prodávající je povinen kdykoli během průběhu plnění Smlouvy informovat Kupujícího o stavu plnění, vyžádá-li si Kupující tuto informaci. V případě, že bude Kupující mít za to, že plnění Smlouvy neodpovídá této Smlouvě a jejím podmínkám, je Prodávající povinen akceptovat toto sdělení Kupujícího a bezplatně upravit Předmět koupě tak, aby odpovídal Předmětu koupě dle této Smlouvy a jejím přílohám. Pro případ, že Prodávající poruší povinnost dle tohoto článku, sjednávají Smluvní strany, že se v takovém případě jedná o podstatné porušení smluvní povinnosti.

3.4 Prodávající se zavazuje plnit úkony definované v sestaveném a vzájemně odsouhlaseném disaster recovery plánu, který je součástí Prodávajícím zpracované a Kupujícímu předané Bezpečnostně provozní dokumentace dle přílohy č. 7 této Smlouvy.

3.5 Aspekty odpovědného zadávání

3.5.1 Prodávající se zavazuje, že při plnění Předmětu koupě bude dbát o dodržování důstojných pracovních podmínek osob, které se na jejím plnění budou podílet. Prodávající se proto zavazuje po celou dobu trvání smluvního vztahu založeného Smlouvou zajistit dodržování veškerých právních předpisů, zejména pak pracovněprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů a zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění zakázky podílejí (a bez ohledu na to, zda budou činnosti prováděny Prodávajícím či jeho poddodavateli). Prodávající se také zavazuje zajistit, že všechny osoby, které se na plnění Předmětu koupě podílejí (a bez ohledu na to, zda budou činnosti prováděny Prodávajícím či jeho poddodavateli), jsou vedeny v příslušných registrech, jako například v registru pojištěnců ČSSZ, a mají příslušná povolení k pobytu v ČR. Prodávající je dále povinen zajistit, že všechny osoby, které se na plnění zakázky podílejí (a bez ohledu na to, zda budou činnosti prováděny prodávajícím či jeho poddodavateli) budou proškoleny z problematiky BOZP, a že jsou vybaveny osobními ochrannými pracovními prostředky dle účinné legislativy.

3.5.2 Prodávající se zavazuje při své činnosti v maximální míře naplňovat požadavky, vyplývající z usnesení vlády České republiky ze dne 24. července 2017 č. 531, o Pravidlech uplatňování odpovědného přístupu při zadávání veřejných zakázek a nákupech státní správy a samosprávy, které zohledňuje sociální resp. širší společenské a zejména také environmentální aspekty směřující k prospěchu pro společnost a ekonomiku a minimalizaci negativních dopadů na životní prostředí.

3.5.3 V rámci plnění Předmětu koupě se Prodávající zavazuje dodržovat předpisy z oblasti ochrany životního prostředí, odpadového a vodního hospodářství zejména zákon č. 17/1992 Sb., o životním prostředí ve znění pozdějších předpisů, zákon č. 541/2020 Sb., o odpadech a zákon č. 477/2001 Sb., o obalech a o změně některých zákonů, ve znění pozdějších předpisů. Při realizaci Předmětu koupě se Prodávající tedy zavazuje zejména na vlastní účet a v souladu s platnými právními předpisy provést ekologickou likvidaci všech odpadů a obalů vzniklých při činnostech Prodávajícího u Kupujícího. Náklady na tyto činnosti jsou zahrnuty v ceně za Předmět koupě uvedené v čl. IV odst. 1 této Smlouvy.

3.5.4 Prodávající se zavazuje kdykoliv v průběhu plnění poskytnout Kupujícímu na základě jeho žádosti doklady a údaje týkající se jeho činnosti ve smyslu prokázání naplňování shora uvedených sociálních a environmentálních aspektů odpovědného zadávání, a to bez zbytečného odkladu.

3.6 Kybernetická bezpečnost:

3.6.1 Prodávající je povinen po celou dobu realizace Smlouvy dodržovat legislativu ČR i EU, která se týká bezpečnosti informací aktuálně platnou v době realizace plnění dle této Smlouvy.

3.6.2 Prodávající se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kupujícího uvedené v příloze č. 8 této Smlouvy. Prodávající se dále zavazuje vytvořit, a nejpozději ke dni předání a převzetí Předmětu koupě na základě podpisu Předávacího protokolu předat Bezpečnostně provozní dokumentaci v rozsahu přílohy č. 7 této Smlouvy a udržovat ji aktuální po dobu účinnosti této Smlouvy.

3.6.3 Prodávající je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto Smlouvou ve stejné míře u všech případných poddodavatelů či jiných osob, které mají přístup k informačním aktivům Kupujícího prostřednictvím Prodávajícího.

3.6.4 Prodávající je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti s touto Smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi Prodávající seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění Prodávajícího veřejně přístupnými stanou (dále jen „důvěrné informace“). Prodávající nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch Kupujícího. Povinnosti dle tohoto odstavce je Prodávající povinen zachovávat i po zániku této Smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění Prodávajícího. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je Prodávající povinen zveřejnit důvěrnou informaci na základě povinnosti uložené Prodávajícímu právním předpisem nebo rozhodnutím orgánu veřejné moci.

3.6.5 Průběžně během celé doby účinnosti této Smlouvy je Prodávající povinen identifikovat a řešit kybernetické bezpečnostní zranitelnosti související s Předmětem koupě.

3.6.6 Prodávající se zavazuje neprodleně reagovat na kybernetické bezpečnostní zranitelnosti, které mu budou oznámeny ze strany Kupujícího a zajistit nezbytnou součinnost.

3.6.7 Za nesplnění kterékoliv povinnosti obsažené v tomto odstavci 3.6, je Kupující oprávněn účtovat Prodávajícímu smluvní pokutu ve výši 10 000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto odstavci 3.6.

3.6.8 Kupující si vyhrazuje právo na informace o:

a) významné změně ovládání Prodávajícího podle zákona č. 90/2012 Sb., o obchodních korporacích v platném znění,

b) změně vlastnictví zásadních aktiv Prodávajícího, které souvisí s plněním této Smlouvy,

c) změně oprávnění nakládat s těmito aktivy,

d) způsobu řízení rizik informační bezpečnosti na straně Prodávajícího.

e) Prodávající je povinen informovat Kupujícího o výše popsaných změnách. Kupující je oprávněn v případě uskutečnění kterékoliv z těchto změn odstoupit od Smlouvy.

3.7 Prodávající se zavazuje v rámci plnění této Smlouvy nevyužívat v rozsahu vyšším než 10% ceny poddodavatele, který je:

a) fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku,

b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněn některým ze subjektů uvedených v písmeni a) tohoto odstavce, nebo

c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, který jedná jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b) tohoto odstavce.

3.8 Prodávající se zavazuje v rámci plnění této Smlouvy nerealizovat ani přímý ani nepřímý nákup či dovoz zboží uvedeného v Nařízení Rady (EU) č. 833/2014 ve znění poslední novely Nařízením Rady (EU) č. 2022/576.

3.9 Kupující si vyhrazuje právo na provedení kontroly či auditu plnění vybraných požadavků/ustanovení u Prodávajícího. Za vybrané požadavky/ustanovení jsou považovány Kontrola/audit plnění požadavků specifikovaných v článku III odst. 3.4 této Smlouvy a v příloze č. 8 této Smlouvy. V rámci kontroly či auditu u Prodávajícího se tento zavazuje poskytnout důkaz o plnění Kupujícím vybraného požadavku, a to buď fyzicky přímo v provozovně Prodávajícího, nebo vzdáleně pomocí elektronických prostředků.

3.10 Prodávající se zavazuje využít poddodavatele, jejichž prostřednictvím byla prokázána kvalifikace, na plnění předmětu této Smlouvy ve stejném rozsahu, v jakém poddodavatel za Prodávajícího prokazoval kvalifikaci.

IV. Kupní cena a platební podmínky

4.1 Sjednaná Kupní cena za Předmět koupě dle čl. 1 této Smlouvy **bez servisní podpory** činí 35 198 502,94Kč (slovy: třicet pět miliónů sto devadesát osm tisíc pět set dvě koruny a devadesát čtyři haléřů českých) bez DPH (dále jen „Kupní cena“), přičemž:

sazba DPH činí	21 %
výše DPH činí	7 391 685,62 Kč
cena vč. DPH činí	42 590 188,55 Kč

Sjednaná **cena za poskytování servisní podpory Předmětu** koupě na 60 měsíců činí 4 927 000 Kč (slovy: čtyři milióny devět set dvacet sedm tisíc korun českých) bez DPH (dále jen „Cena“), přičemž:

sazba DPH činí	21 %
výše DPH činí	1 034 670 Kč
cena vč. DPH činí	5 961 670 Kč

Sjednaná cena za poskytování servisní podpory Předmětu koupě v kategorii **vyžádané služby** za hodinové sazby je uvedena v Příloze č. 1 této Smlouvy.

Podrobný rozpis Kupní ceny je uveden v Příloze č. 1 této Smlouvy.

4.2 Kupní cena, cena za poskytování servisní podpory a hodinové sazby vyžádaných servisních služeb uvedené v odst. 4.1 představují souhrn cen všech prací a dodávek, uskutečněných Prodávajícím v rozsahu a obsahu stanoveném touto Smlouvou a jejími přílohami, zajišťující kompletní splnění veřejné zakázky v souladu se Zadávací dokumentací k veřejné zakázce. Kupní cena zahrnuje veškeré náklady Prodávajícího nezbytné k řádnému splnění jeho závazku dle této Smlouvy, tj. včetně dopravy, instalace, montáže, zaškolení, zisku, inflace a jiných nákladů, a je cenou konečnou a nepřekročitelnou. Cena za poskytování servisní podpory po dobu 60 měsíců u jednotlivých Opatření převzatých Kupujícím na základě dílčích protokolů o předání položek hardware a dílčích akceptačních protokolů bude Kupujícím hrazena měsíčně na základě Prodávajícím vystavené faktury. Servisní služby v kategorii vyžádané služby za hodinové sazby bude fakturována na základě prokázaného a vzájemně odsouhlaseného výkazu skutečně poskytnutých hodin služby, a to po odsouhlasení předmětného výkazu. Ceny za hodinové sazby jsou neměnné po celou dobu 60 měsíců u jednotlivých Opatření převzatých Kupujícím na základě dílčích protokolů o předání položek hardware a dílčích akceptačních protokolů.

4.3 Celkovou a pro účely fakturace rozhodnou cenou se rozumí cena včetně DPH. Kupující je plátcem DPH.

4.4 Smluvní strany se dohodly, že v případě změny zákonných sazeb DPH uvedených v Kupní ceně dle této Smlouvy nebudou uzavírat písemný dodatek na změnu Kupní ceny a DPH bude účtována podle předpisů platných v době uskutečnění zdanitelného plnění.

4.5 Prodávající vystaví a předá Kupujícímu dílčí daňový doklad (dále jen „faktura“) až po řádném předání každého dílčího Opatření Předmětu koupě bez zjevných vad Kupujícímu. Předání dílčího Opatření Předmětu koupě je doloženo dílčím protokolem o předání položky hardware nebo dílčím akceptačním protokolem.

4.6 Faktura musí obsahovat veškeré náležitosti daňového a účetního dokladu dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „ZDPH“) a bude mít náležitosti obchodní listiny dle § 435 Občanského zákoníku. Každá faktura musí být označena registračním číslem projektu CZ.06.01.01/00/22_004/0000177, názvem projektu a zkratkou IROP. V případě, že faktura nebude mít odpovídající náležitosti, je Kupující oprávněn zaslat ji ve lhůtě splatnosti Prodávajícímu zpět k opravě či doplnění. Lhůta splatnosti počíná běžet znovu od opětovného doručení opravené či doplněné faktury Kupujícímu.

4.7 Faktura bude splatná do 30 dnů ode dne jejího doručení Kupujícímu. Za den úhrady se považuje den, kdy byla fakturovaná částka odepsána z účtu Kupujícího ve prospěch účtu Prodávajícího. Úhrada bude prováděna převodem na účet Prodávajícího uvedený v záhlaví této Smlouvy.

4.8 Daňový doklad bude doručen v elektronické podobě na adresu Kupujícího na adresu epodatelna@nempe.cz a v kopii na faktury@nempe.cz

4.9 Přílohou vystavené a doručené faktury uvedené v článku 4.5. a 4.2 bude Kupujícím potvrzený dílčí protokol o předání položky hardware nebo dílčí akceptační protokol příp. výkaz poskytnuté servisní podpory. Bez těchto dokumentů není Prodávající oprávněn fakturu vystavit.

4.10 Úhrada za plnění z této Smlouvy bude realizována bezhotovostním převodem na účet Prodávajícího, který je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 98 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“).

4.11 Pokud se po dobu účinnosti této Smlouvy Prodávající stane nespolehlivým plátcem ve smyslu ustanovení § 106a zákona o DPH, smluvní strany se dohodly, že Prodávající uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Prodávající takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované Prodávajícím.

4.12 Kupující neposkytuje Prodávajícímu během realizace Předmětu koupě žádné zálohové platby.

V. Práva z vadného plnění a záruka za jakost

5.1 Prodávající odpovídá za to, že Kupující či jejich oprávněné osoby bude moci užívat Předmět koupě bez vad po dobu trvání záruky za jakost.

5.2 Prodávající poskytuje Kupujícím záruku za jakost Předmětu koupě spočívající v tom, že jím dodaný Předmět koupě bude mít po celou záruční dobu vlastnosti deklarované výrobcem a sjednané touto Smlouvou a jejími přílohami (včetně splnění a zajištění podmínek dodání Předmětu koupě dle čl. I. odst. 1.11 této Smlouvy), odpovídající příslušným obecně závazným právním předpisům, technickým předpisům a normám, platným v době realizace plnění dle této Smlouvy, bude prostý jakýchkoliv faktických či právních vad. Prodávající dále odpovídá za to, že Předmět koupě bude způsobilý pro sjednaný účel, nebyl-li účel sjednán, pak pro účel obvyklý a pro účel, k němuž je výrobcem určen. Prodávající se zaručuje, že si Předmět koupě po celou záruční dobu při obvyklém použití uchová své funkce a výkonnost.

5.3 Prodávající poskytuje Kupujícímu záruku za jakost Předmětu koupě v délce trvání 60 měsíců.

5.4 Záruka za jakost počíná plynout, není-li dále sjednáno jinak, ode dne řádného předání dílčích Opatření Předmětu koupě na základě jednotlivých dílčích protokolů o předání položek hardware a dílčích akceptačních protokolů.

5.5 Bude-li Předmět koupě v době předání vykazovat vady, je Kupující oprávněn Předmět koupě nepřevzít. Uvedené se vztahuje na předání hardware (tj. komponenty a zařízení) Předmětu koupě včetně provedení montáže, instalace a ověření funkčnosti (tj. dle dílčího protokolu o předání položky hardware) a na předání software a implementace Předmětu koupě (tj. dle dílčího akceptačního protokolu)

5.6 Předmět koupě má zejména vady, jestliže neodpovídá požadovaným vlastnostem pro sjednaný účel a jeho použití, popřípadě nemá vlastnosti výslovně stanovené touto Smlouvou, zejm. jak je uvedeno v odst. 5.2. této Smlouvy, a/nebo obecně závaznými předpisy a/nebo stanovené závaznými nebo doporučujícími technickými normami, podle nichž má být Předmět koupě proveden, a/nebo nemá vlastnosti deklarované výrobcem.

5.7 Při zjištění, že Předmět koupě vykazuje vady, má Kupující právo dle svého rozhodnutí uplatňovat tato práva z vad Předmětu koupě:

a) požadovat opravu vady v místě dodání Předmětu koupě, a to nejpozději do pěti pracovních dnů od nahlášení;

b) požadovat odstranění vady poskytnutím nového plnění v místě dodání Předmětu koupě, a to nejpozději do pěti pracovních dnů od nahlášení;

c) odstoupit od této Smlouvy.

5.8 Kupující je oprávněn oznámit Prodávajícímu záruční vadu i vadu, která existovala v době předání Předmětu koupě, a uplatnit práva z takové vady, kdykoliv v průběhu záruční doby, bez ohledu na to, kdy Kupující tuto vadu zjistil nebo kdy vada měla či mohla být Kupujícím zjištěna při vynaložení odborné péče. V případě, že Kupující oznámil Prodávajícímu vadu v průběhu záruční doby, je tato vada oznámena včas, přičemž aplikace dispozitivních norem stanovených právními předpisy, které se odchylují od shora uvedených podmínek, se vylučuje. Kupující oznámí vadu Prodávajícímu prostřednictvím služby HelpDesk postupem dle Přílohy č. 2 Smlouvy.

5.9 Kupující je oprávněn zvolit způsob řešení odstranění vad Předmětu koupě libovolně dle vlastního uvážení. Kupující je oprávněn svoji volbu práv z vad předmětu koupě libovolně měnit až do doby zahájení prací Prodávajícího na jejich odstranění.

5.10 V případě odstranění vady opravou věci se Prodávající zavazuje provádět tuto opravu věci u Kupujícího, bude-li to možné. Náklady spojené s dopravou, montáží a demontáží vadné věci nese Prodávající v plné výši.

5.11 Při dodání nové věci vrátí Kupující Prodávajícímu na jeho náklady věc původně dodanou. Na nově dodanou věc poskytuje Prodávající záruku v délce 24 měsíců ode dne převzetí nové věci Kupujícím, není-li v Příloze č. 2 této Smlouvy uvedeno jinak.

5.12 Prodávající je povinen zahájit odstraňování uplatněných vad vždy, tedy i v případě, že je sporné, zda Prodávající za vady odpovídá. Otázka případných nároků prodávajícího z odstranění vad bude řešena až po úplném odstranění uplatněných vad.

5.13 Doba od oznámení vady do jejího odstranění se do trvání záruční doby nezapočítává.

5.14 Jestliže Prodávající neodstraní vady ve stanovené lhůtě nebo oznámí-li před jejím uplynutím, že vady neodstraní, je Kupující oprávněn bez újmy ostatních práv Kupujícího ze záruky, nechat je odstranit třetí osobou na účet Prodávajícího. V takovém případě je Prodávající povinen zaplatit Kupujícímu skutečné náklady vynaložené na odstranění vad a současně platí, že takový postup Kupujícího nemá vliv na trvání záruky z této Smlouvy.

5.15 Odstranění vady nemá vliv na nárok Kupujícího na smluvní pokutu a náhradu škody.

5.16 Prodávající s přihlédnutím k ustanovení této Smlouvy o autorských právech prohlašuje, že veškeré jeho plnění dodané podle této Smlouvy bude prosté všech právních vad a zavazuje se odškodnit v

plné výši Kupujícího v případě, že třetí osoba úspěšně a oprávněně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění.

VI. Mlčenlivost

6.1 V průběhu plnění Předmětu Smlouvy může Prodávající přijít do styku s důvěrnými informacemi týkající se Kupujícího, jeho zaměstnanců či pacientů:

- mající povahu osobních údajů identifikovatelných fyzických osob, obchodních údajů, či údajů o jiných právních a faktických vztazích Kupujícího,
- které Prodávající obdržel či obdrží v souvislosti s touto Smlouvou nebo plněním dle této Smlouvy, a to ať již písemně, ústně, v elektronické či jiné formě, a to na jakémkoli nosiči, na němž takováto informace může být nahrána nebo uložena.

6.2 Za důvěrné informace se nepovažují informace, které jsou či se stanou veřejně přístupnými a mohou být kýmkoli získány bez nutnosti vyvinout větší úsilí za předpokladu, že nejsou získány jako důsledek protiprávního jednání.

6.3 V případě pochybností sdělí Kupující na žádost Prodávajícího, zda informaci považuje za důvěrnou. Nepožádal-li Prodávající o toto sdělení, má se v případě pochybností za to, že informace je důvěrná.

6.4 Prodávající zajistí zachování mlčenlivosti o veškerých důvěrných informacích a zajistí přenesení povinnosti mlčenlivosti v plném rozsahu této Smlouvy na své zaměstnance i jakékoli další osoby v právním či faktickém vztahu k Prodávajícímu, které se budou na realizaci předmětu Smlouvy podílet. To platí i pro ostatní povinnosti uložené touto Smlouvou. Zaměstnanci Prodávajícího, kterým bude umožněn přístup ke zpracovávaným osobním údajům, budou Prodávajícím doložitelně poučeni o povinnosti zachovávat mlčenlivost

6.5 Prodávající se dále zavazuje dodržovat pravidla a zásady zpracování a ochrany osobních údajů identifikovatelných fyzických osob podle zákona č. 110/2019 Sb., o zpracování osobních údajů a Obecného nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, zákona č. 372/2011 Sb., zákon o zdravotních službách, zákona č. 373/2011 Sb., o specifických zdravotních službách a vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci.

6.6 V případě, že je Předmětem koupě počítačové vybavení uchovávající jakékoliv osobní údaje a údaje zvláštní kategorie, je Prodávající povinen Kupujícího na tuto skutečnost upozornit a zajistit zabezpečení proti neoprávněnému přístupu vhodnými prostředky (PIN, přihlašovací údaje apod.). Tyto údaje současně předá Kupujícímu při převzetí Předmětu koupě.

6.7 Kupující prohlašuje, že v souvislosti se zajištěním servisní podpory, poskytované Prodávajícím, v záruční době nepožaduje zpracování dat (osobních údajů). V případě, že by v rámci zajištění servisní podpory muselo být zpracování dat (osobních údajů) provedeno, je Prodávající povinen na tuto skutečnost Kupujícího upozornit a uzavřít bez zbytečného odkladu zpracovatelskou smlouvu. V případě potřeby vzdáleného přístupu k informačním a komunikačním systémům a informacím Kupujícího, je Prodávající povinen dodržovat Pravidla pro zřízení a používání vzdáleného přístupu do počítačové sítě Nemocnice Pelhřimov, příspěvková organizace (viz Příloha č. 7 této Smlouvy).

6.8 Ustanovení tohoto článku se vztahují jak na období platnosti této Smlouvy, tak na období po jejím ukončení.

6.9 V případě, že Prodávající poruší ustanovení tohoto článku, je Kupující oprávněn požadovat po Prodávajícím smluvní pokutu ve výši 10.000,-- Kč (slovy: Desettisíc korun českých) za každé jednotlivé porušení tohoto článku ze strany Prodávajícího. Prodávající je povinen k úhradě takovéto pokuty. Smluvní pokuta je splatná do 14 dnů od doručení oznámení o uplatnění smluvní pokuty.

6.10 Zároveň se Prodávající zavazuje k úhradě škody (např. správní či jiné sankce, náhrady škody za neoprávněné nakládání s osobními údaji), která vznikla Kupujícímu v důsledku porušení povinností Prodávajícího stanovených právními předpisy či touto Smlouvou či v důsledku neposkytnutí příslušné součinnosti.

VII. Sankční ustanovení

7.1 Při nedodržení termínu splatnosti dle článku IV. odst. 4.7. může být Kupujícímu ze strany Prodávajícího účtován úrok z prodlení v zákonné výši z fakturované částky za každý den prodlení.

7.2 Za každý, i započatý, den prodlení s předáním Předmětu koupě dle čl. II. odst. 2.2 v rozsahu čl. I a čl. II, je Prodávající povinen zaplatit smluvní pokutu ve výši 0,05 % z Kupní ceny Předmětu koupě bez servisní podpory dle čl. IV. odst. 4.1.

7.3 Prodávající uhradí Kupujícímu smluvní pokutu ve výši 1 000,- Kč za každý kalendářní den prodlení a jednotlivý případ vady až do dne odstranění vad, maximálně ve výši 50% z ceny Předmětu koupě. V případě vad, které znemožňují užívání Předmětu koupě, vzniká Kupujícímu právo na smluvní pokutu až do výše 80% z ceny Předmětu koupě.

7.4 V případě prodlení Prodávajícího se zahájením řešení servisního požadavku Kupujícího předaného v rámci služby HelpDesk v reakční době dle Přílohy č. 2 Smlouvy se Prodávající zavazuje uhradit Kupujícímu smluvní pokutu ve výši

a) Pro incidenty se závažností chyb A, 500 korun českých bez DPH za každou hodinu porušení SLA,

b) Pro incidenty se závažností chyb B, 6000 korun českých bez DPH za každý den porušení SLA,

c) Pro incidenty se závažností chyb C, se sankce neaplikují.

Sankcí se rozumí smluvní pokuta za nedodržení SLA, která se počítá za každý incident zvlášť. Doba řešení se nepočítá pro situace, kdy Prodávající čeká na součinnost Kupujícího. Tímto Smluvní strany Smlouvy pro vztah touto Smlouvu založený výslovně sjednávají odchylnou úpravu od ustavení § 2050 OZ tak, že ujednání o smluvní pokutě se nedotýká nároku na náhradu škody v plné výši. Jakékoliv pohledávky vůči Prodávajícímu vzniklé v důsledku neodstraňování oznámených vad ve stanovených termínech je Kupující oprávněn jednostranně započíst na splatné či nesplatné pohledávky Prodávajícího.

7.5 Odstoupením od Smlouvy dle příslušných ustanovení této Smlouvy nejsou dotčena ustanovení týkající se smluvních pokut a ustanovení týkající se takových práv a povinností, z jejichž povahy vyplývá, že mají trvat i po odstoupení.

7.6 V případě ukončení Smlouvy před sjednanou dobou plnění, zejména z důvodu odstoupení od Smlouvy, sjednávají Smluvní strany přechodné období v délce trvání 6 měsíců, po které bude Prodávající nadále povinen plnit dle této Smlouvy tak, aby byl umožněn Kupujícímu řádný a plnohodnotný přechod na nové řešení, nedohodnou-li se Smluvní strany v konkrétním případě jinak. V rámci přechodného obdobní dle předchozí věty je Prodávající povinen Kupujícímu do jednoho týdne od začátku běhu přechodného období, předložit harmonogram přechodu jednotlivých činností a výkonu pro zachování kontinuity provozu řešení včetně plánu případné migrace a předání dat.

VIII. Ostatní ujednání

8.1 V případě, že pro splnění povinnosti Prodávajícího bude nezbytná součinnost Kupujícího, zavazuje se Kupující vyžádanou součinnost poskytnout. Prodávající je povinen Kupujícímu specifikovat tuto součinnost předem.

8.2 Kupující se zavazuje spolupracovat s Prodávajícím v rozsahu nutném k dosažení předmětu Smlouvy.

8.3 Prodávající je povinen spolupůsobit při výkonu finanční kontroly dle § 2 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění.

8.4 Kupující poskytne Prodávajícímu aktuální údaje, které má k dispozici v rozsahu a formátu potřebném k plnění Předmětu koupě. Prodávající takto získané údaje použije pouze pro plnění Smlouvy a neposkytne je třetí straně bez předchozího souhlasu Kupujícího.

8.5 Prostředky k placení Kupní ceny podle této Smlouvy získává Kupující, kromě vlastních zdrojů, ze zdrojů Evropské unie (dále v tomto článku jen „třetí osoba“). Vyplácení těchto prostředků za účelem placení Kupní ceny Prodávajícímu podléhá přezkumu plnění této Smlouvy třetí osobou. Vůči této třetí osobě obě Smluvní strany této Smlouvy prohlašují, že se nedovolávají ochrany obchodního tajemství. Jakékoliv neplnění závazků Prodávajícím může mít za následek znemožnění financování Předmětu koupě z prostředků shora uvedených.

8.6 Předmět koupě bude výlučným majetkem Kupujícího a ten je oprávněn jej postoupit či převést vlastnické a užívací právo k němu třetím osobám. Prodávající prohlašuje, že Kupujícímu postoupí veškerá práva (zejména užívací apod.), když cena za tato práva je již zahrnuta v kupní ceně.

8.7 Prodávající se zavazuje Kupujícího odškodnit a zprostit odpovědnosti za jakékoli ztráty, závazky z titulu odpovědnosti, náklady, nároky, škody, výdaje nebo požadavky (nebo úkony s nimi související), které Kupující utrpí nebo které mu vzniknou či které budou proti němu uplatněny a které jsou vzhledem k účelu Smlouvy a záměru Kupujícího účelně vynaložené, pokud takové ztráty, závazky z titulu odpovědnosti, náklady, nároky, škody, výdaje (včetně nákladů právního zastoupení) nebo požadavky vzniknou přímo nebo nepřímo z titulu nebo v souvislosti s:

a) jakýmkoli nesprávným, nepravdivým nebo zavádějícím prohlášením či ujištěním Prodávajícího uvedeným v této Smlouvě nebo

b) porušením jakéhokoli ujednání nebo závazku Prodávajícího stanoveného v této Smlouvě;

Prodávající nahradí Kupujícímu veškeré náklady, poplatky, platby a výdaje, které jsou vzhledem k účelu Smlouvy a záměru Kupujícího účelně vynaložené a které Kupující uhradí nebo které mu vzniknou v souvislosti s vedením jakéhokoli řízení nebo popírání jakéhokoli nároku nebo obhajobou či v souvislosti s vymáháním tohoto závazku Prodávajícího.

8.8 Prodávající je povinen archivovat veškeré dokumenty, které souvisí s touto veřejnou zakázkou včetně účetních dokladů minimálně do konce roku 2035. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji Prodávající použít.

8.9 Prodávající je povinen minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu (Předmětu koupě) a poskytnout jim při provádění kontroly součinnost. Prodávající je dále povinen poskytnout Kupujícímu veškeré doklady související s realizací veřejné zakázky a plněním monitorovacích ukazatelů, které si vyžádají kontrolní orgány IROP.

8.10 Veškeré povinnosti Prodávajícího jdou k jeho tíži.

8.11 Smluvní strany mohou smlouvu ukončit:

a) dohodou;

b) výpovědí ze zákonných důvodů,

c) odstoupením ze zákonných důvodů či důvodů uvedených v této Smlouvě.

Dohoda o zrušení práv a závazků musí být písemná, jinak je neplatná.

8.12 Kupující je oprávněn od Smlouvy odstoupit v případě, že Předmět koupě na základě této Smlouvy bude vykazovat vady ve formě špatné kvality či nedodržení rozsahu Předmětu koupě, ačkoliv na

výskyt vad s uvedením jejich specifikace byl Prodávající nejméně jednou písemně upozorněn a neprovedl příslušnou nápravu.

8.13 Prodávající je oprávněn od Smlouvy odstoupit v případě prodlení Kupujícího s placením faktur delším než 30 dní ode dne doručení.

8.14 Pokud se Prodávající stane subjektem ve smyslu ustanovení článku 5k Nařízení Rady (EU) č. 833/2014 v aktuálním znění, Kupující je oprávněn od Smlouvy odstoupit v okamžiku, kdy mu bude tato skutečnost známa. Odstoupení nabývá účinnosti dnem doručení Prodávajícímu.

8.15 Kupující si vyhrazuje právo na jednostranné odstoupení od Smlouvy bez jakýchkoliv sankcí, pokud:

a) dojde k významné změně ovládání Prodávajícího podle zákona č. 90/201 Sb., o obchodních korporacích,

b) dojde ke změně vlastnictví zásadních aktiv Prodávajícího, které souvisejí s plněním této Smlouvy,

c) nebo dojde ke změně oprávnění Prodávajícího nakládat s těmito aktivy.

8.16 Odstoupením od této Smlouvy nezanikají povinnosti nahradit vzniklou škodu a hradit smluvní pokuty sjednané pro případ porušení této Smlouvy a dále ty povinnosti smluvních stran, které vznikly před odstoupením od této Smlouvy, pokud z jejich povahy nevyplývá něco jiného.

8.17 Pokud se Prodávající dostane do úpadku, je Kupující oprávněn tuto Smlouvu vypovědět ve výpovědní lhůtě 14 ode dne doručení výpovědi, pokud ve výpovědi nestanoví lhůtu delší s ohledem na svoje potřeby.

8.18 Prodávající nesmí zastavit plnění vyplývající z této Smlouvy nebo její části, tj. ručit Smlouvou nebo právy z této Smlouvy, ani jinak omezit či modifikovat práva a povinnosti Kupujícího vyplývající z této Smlouvy. V případě, že takto Prodávající učiní a třetí strana tato práva uplatní, zaniká tato Smlouva bez dalšího.

8.19 Kupující si vyhrazuje změnu závazku podle §100 ods. 1 ZZVZ týkající se rozsahu a ceny dodávaného plnění dojde-li v době plnění ke změně legislativních požadavků ve vztahu k předmětu plnění.

IX. Prohlášení Prodávajícího

9.1 Prodávající prohlašuje, že je oprávněn udělit Kupujícímu případná oprávnění k výkonu práva Předmět koupě užít v souladu s podmínkami této Smlouvy.

9.2 Prodávající prohlašuje, že případná autorská práva, která touto Smlouvou uděluje, mu patří nebo je v rámci předání Předmětu koupě bez jakéhokoliv omezení zajistí, přičemž neomezeně ručí za škodu, která by Kupujícím vznikla v případě nepravdivosti tohoto prohlášení.

X. Informační doložka

10.1 Smluvní strany výslovně berou na vědomí a souhlasí s uveřejněním Smlouvy v souladu se ZZVZ či zákonem č. 340/2015 Sb., o registru smluv ve znění pozdějších předpisů a výslovně konstatují, že ve Smlouvě nejsou informace, které nemohou být poskytnuty podle zákona č. 340/2015 Sb., o registru smluv ve znění pozdějších předpisů a zákona č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů (např. obchodní tajemství). Povinnost zveřejnění Smlouvy v souladu s ZZVZ či zákonem o registru smluv nese Kupující.

10.2 Smluvní strany výslovně označují veškeré údaje této Smlouvy, jakož i informace poskytnuté vzájemně v průběhu trvání za důvěrné.

10.3 Je ujednáno, že Prodávající se zavazuje udržet v tajnosti a neprozradit nebo jinak zpřístupnit jakékoliv informace, které mají vztah k obchodům a obchodním transakcím, které budou uzavírány Smluvními stranami.

10.4 Povinnost dle tohoto článku se netýká informací určených písemnou dohodou Smluvních stran ke zveřejnění, či na informace, jež je Kupující povinen poskytovat či zveřejňovat dle platných právních předpisů, zejména dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů, zákona č. 340/2015 Sb., o registru smluv ve znění pozdějších předpisů a ZZVZ.

10.5 V případě, že Prodávající poruší povinnost uvedenou v tomto článku, je povinen nahradit Kupujícímu vedle škody i nemajetkovou újmu a Kupující je zároveň oprávněn odstoupit od této Smlouvy.

XI. Závěrečná ustanovení

11.1 Tuto Smlouvu lze měnit pouze oboustranně odsouhlasenými, písemnými a průběžně číslovanými dodatky, podepsanými oprávněnými zástupci obou Smluvních stran.

11.2 Smluvní strany se dohodly, že právní vztahy založené touto Smlouvou se budou řídit příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku.

11.3 Případné spory vzniklé z této Smlouvy budou řešeny podle platné právní úpravy věcně a místně příslušnými soudy České republiky.

11.4 Smluvní strany se zavazují, že budou jednat vždy ve prospěch této Smlouvy, a to jak vůči sobě navzájem, tak i třetím osobám. Smluvní strany se rovněž zavazují zdržet takového jednání, které by mohl být druhou stranou vykládáno jako jednání směřující proti smyslu a účelu této Smlouvy.

11.5 Pokud kterékoli ustanovení této Smlouvy nebo jeho část bude neplatné či nevynutitelné, nebo se stane neplatným či nevynutitelným, nebo bude shledáno neplatným či nevynutitelným soudem či jiným příslušným orgánem, pak tato neplatnost či nevynutitelnost nebude mít vliv na platnost či vynutitelnost ostatních ustanovení Smlouvy nebo jejich částí. Smluvní strany se zavazují takové ustanovení nahradit novým platným, které se bude co nejvíce blížit původnímu a bude v souladu s původní vůlí stran a účelem Smlouvy.

11.6 Smluvní strany se dohodly, že v případě zániku právního vztahu založeného touto Smlouvou zůstávají v platnosti a účinnosti i nadále ustanovení, z jejichž povahy vyplývá, že mají zůstat nedotčena zánikem právního vztahu založeného touto Smlouvou.

11.7 Všechny ujednání a podmínky v této Smlouvě se budou vztahovat na a budou závazné pro právní nástupce a postupníky příslušných Smluvních stran a budou je zavazovat, jako by byli v této Smlouvě jmenováni a vyjádřeni; a kdekoliv je v této Smlouvě zmínka o některé ze Smluvních stran, platí, že zahrnuje a vztahuje se na nástupce a postupníky takové Smluvní strany, stejně jako by byla v takovém případě uvedena.

11.8 V souladu s ust. § 630 odst. 1 OZ si smluvní strany sjednávají promlčecí dobu ve vztahu k veškerým právům přímo či odvozeně souvisejícím s touto smlouvou v délce pěti (5) let ode dne, kdy počala promlčecí doba plynout.

11.9 Tato Smlouva nabývá platnosti v den jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v informačním systému veřejné správy - Registru smluv.

11.10 Tato Smlouva je vyhotovená v elektronické nebo listinné podobě. Smlouva vyhotovená v elektronické podobě je opatřená kvalifikovanými elektronickými podpisy zástupců smluvních stran. Smlouva v listinné podobě je vyhotovená ve dvou provedeních, z nichž každé má platnost originálu, přičemž obě smluvní strany obdrží jedno vyhotovení.

11.11 Obě Smluvní strany potvrzují autentičnost této Smlouvy a prohlašují, že si Smlouvu přečetly, s jejím obsahem souhlasí, že Smlouva byla sepsána na základě pravdivých údajů, z jejich pravé a svobodné vůle a nejsou jim známy žádné skutečnosti bránící uzavření Smlouvy a plnění povinností z ní vyplývajících, což stvrzují svým podpisem, resp. podpisem svého oprávněného zástupce.

11.12 Nedílnou součástí Smlouvy jsou její níže uvedené přílohy:

Příloha č. 1: **Kalkulace ceny za předmět Smlouvy**

Příloha č. 2: **Technická specifikace předmětu plnění** k Zadávací dokumentaci ve veřejné zakázce Kybernetická bezpečnost nemocnice Pelhřimov

Příloha č. 3: **Technický popis nabízeného řešení**

Příloha č. 4: **Seznam osob realizačního týmu**

Příloha č. 5: **Seznam poddodavatelů**

Příloha č. 6**: Pravidla pro zřízení a používání vzdáleného přístupu do počítačové sítě Nemocnice Pelhřimov, příspěvková organizace**

Příloha č. 7: **Bezpečnostně provozní dokumentace – podmínky a požadavky**

Příloha č. 8: **Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kupujícího**

V Pelhřimově dne (dle elektronického podpisu)

Za Kupujícího

Radim Hošek

Digitálně podepsal Radim Hošek
Datum: 2024.11.18 11:10:01 +01'00'

Ing. Radim Hošek, ředitel

Nemocnice Pelhřimov, příspěvková organizace

V Praze dne (dle elektronického podpisu)

Za Prodávajícího

Pavel Šipr

Digitálně podepsal Pavel Šipr
Datum: 2024.11.14 10:28:48 +01'00'

Pavel Šipr, jednatel

IXPERTA s.r.o.

Kalkulace ceny za předmět Smlouvy *(vyplněná příloha 3c Zadávací dokumentace: Kalkulace nabídkové ceny pro Projekt Kybernetická bezpečnost Pelhřimov)*

Příloha č. 3.c. Kalkulace nabídkové ceny pro Projekt Kybernetická bezpečnost Nemocnice Pelhřimov

(1) Položky nabídkové ceny pro Fázi A – dodání, instalace a implementace technologií

Id	Dílčí plnění Dodavatele	Cena bez DPH [Kč]	DPH [%]	DPH [Kč]	Cena včetně DPH [Kč]	Limity nabídkové ceny v Kč bez DPH
1	Centrální firewally	4 789 656,84	21%	1 005 827,94	5 795 484,78	
2	Centrální sběr a management logů	451 350,00	21%	94 783,50	546 133,50	
3	Zavedení segmentace sítě	2 229 000,00	21%	468 090,00	2 697 090,00	
4	DLP	650 000,00	21%	136 500,00	786 500,00	
5	Úložiště pro PACS a NIS data formou NAS a S3	3 950 000,00	21%	829 500,00	4 779 500,00	
6	Infrastruktura pro zálohování a rychlou obnovu	5 292 201,00	21%	1 111 362,21	6 403 563,21	
7	Zvýšení dostupnosti záložního datového centra a lokální sítě	7 915 560,00	21%	1 662 267,60	9 577 827,60	
8	Ochrana operačních systémů a mobilních platforem	1 904 663,10	21%	399 979,25	2 304 642,35	
9	Přihlašování k počítačům a aplikacím v rámci klinických a THP provozů	8 016 072,00	21%	1 683 375,12	9 699 447,12	
10	**Dílčí nabídková cena Fáze A**	**35 198 502,94**	**21%**	**7 391 685,62**	**42 590 188,55**	35 500 000,00

(2) Položky nabídkové ceny pro Fázi B - provozní fáze - Servisní a provozní podpora po dobu 60 měsíců

		cena za 12 měs v Kč bez DPH	DPH [%]	DPH [Kč]	Cena včetně DPH [Kč]	Limity nabídkové ceny v Kč bez DPH
11	Centrální firewally	67 000,00	21%	14 070,00	81 070,00	
12	Centrální sběr a management logů	70 000,00	21%	14 700,00	84 700,00	
13	Zavedení segmentace sítě (včetně podpory síťových prvků)	128 400,00	21%	26 964,00	155 364,00	
14	DLP	70 000,00	21%	14 700,00	84 700,00	
15	Úložiště pro PACS a NIS data formou NAS a S3	50 000,00	21%	10 500,00	60 500,00	
16	Infrastruktura pro zálohování a rychlou obnovu (včetně podpory Veeam a VMware)	60 000,00	21%	12 600,00	72 600,00	
17	Zvýšení dostupnosti záložního datového centra a lokální sítě (včetně podpory síťových prvků)	160 000,00	21%	33 600,00	193 600,00	
18	Ochrana operačních systémů a mobilních platforem	130 000,00	21%	27 300,00	157 300,00	
20	Přihlašování k počítačům a aplikacím v rámci klinických a THP provozů	250 000,00	21%	52 500,00	302 500,00	
21	**Dílčí nabídková cena Fáze B - servisní a provozní podpora (po dobu 60 měsíců)**	**4 927 000,00**	**21%**	**1 034 670,00**	**5 961 670,00**	5 000 000,00

(3) Položky nabídkové ceny pro Fázi B - provozní fáze - Servisní (technická) podpora individuálně objednaných služeb - hodinová sazba

Id	Dílčí plnění Dodavatele	Počet hodin vyžádaných služeb (12 měsíců)*	Cena za 1 hodinu bez DPH [Kč]	Cena bez DPH [Kč]	DPH [%]	DPH [Kč]	Cena včetně DPH [Kč]	Limity nabídkové ceny v Kč bez DPH
22	Centrální firewally	150,00	2 250,00	337 500,00	21%	70 875,00	408 375,00	
23	Centrální sběr a management logů	25,00	2 250,00	56 250,00	21%	11 812,50	68 062,50	
24	Zavedení segmentace sítě	100,00	2 250,00	225 000,00	21%	47 250,00	272 250,00	
25	DLP	25,00	2 250,00	56 250,00	21%	11 812,50	68 062,50	
26	Úložiště pro PACS a NIS data formou NAS a S3	50,00	2 250,00	112 500,00	21%	23 625,00	136 125,00	
27	Infrastruktura pro zálohování a rychlou obnovu	50,00	2 250,00	112 500,00	21%	23 625,00	136 125,00	
28	Zvýšení dostupnosti záložního datového centra a lokální sítě	50,00	2 250,00	112 500,00	21%	23 625,00	136 125,00	
29	Ochrana operačních systémů a mobilních platforem	100,00	2 250,00	225 000,00	21%	47 250,00	272 250,00	
30	Přihlašování k počítačům a aplikacím v rámci klinických a THP provozů	100,00	2 250,00	225 000,00	21%	47 250,00	272 250,00	
31	**Dílčí nabídková cena Fáze B - Servisní (technická) podpora individuálně objednaných služeb (po dobu 60 měsíců)**			**7 312 500,00**	**21%**	**1 535 625,00**	**8 848 125,00**	9 000 000,00

**) modelový příklad pro výpočet hodnotícího kriteria*

(4) Celková nabídková cena

32	**Celková nabídková cena**	**47 438 002,94**	**21%**	**9 961 980,62**	**57 399 983,55 Kč**

Pokyny:
Dodavatel vyplní pouze žlutě označená pole.
Dodavatel je povinen respektovat limit výše dílčích částí nabídkové ceny tak, jak jsou uvedeny v tabulce

Technická specifikace předmětu plnění

k Zadávací dokumentaci ve veřejné zakázce

„Kybernetická bezpečnost Nemocnice Pelhřimov - 2“

(dále jen „Technická specifikace“)

Obsah

1. Zkratky a pojmy 19
2. Místo plnění 20
3. Doba plnění 20
4. Způsob prokázání splnění požadavků minimálního plnění 21
5. Požadavky na specifikaci jednotlivých bezpečnostních technologií 22
   - 5.1 Technická specifikace Centrálních Firewallů 22
   - 5.2 Technická specifikace centrálního sběru a managementu logů 25
     - 5.2.1 Technická specifikace řešení pro správu logů 25
     - 5.2.2. Požadavky na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX) 27
     - 5.2.3. Požadavky na řešení pro automatické vyhodnocování datových toků (NetFlow/IPFIX) 32
   - 5.3 Technická specifikace zavedení segmentace sítě 35
   - 5.4 Technická specifikace DLP 37
   - 5.5 Technická specifikace úložiště pro PACS a NIS data formou NAS a S3 39
   - 5.6 Technická specifikace infrastruktury pro zálohování a rychlou obnovu 40
   - 5.7 Technická specifikace pro zvýšení dostupnosti záložního datového centra a lokální sítě 41
   - 5.8 Technická specifikace ochrany operačních systémů a mobilních platforem 47
     - 5.8.1 Technická specifikace prostředí pro běh management a bezpečnostních prvků 51
   - 5.9 Technická specifikace pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů 54
6. Fáze A - Instalace a implementace 57
   - 6.1 Zpracování a akceptace Detailního realizačního projektu 61
   - 6.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb) 62
     - 6.6.1 Předání a převzetí dokumentů 62
     - 6.2.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb) 62
   - 6.3 Školení 63
   - 6.4 Dokumentace 64
7. Fáze B – provozní podpora dodaných technologií 64

1. Zkratky a pojmy

(1) Zkratky a pojmy užité v Zadávací dokumentaci jsou uvedeny v Příloze 3.a. Zadávací dokumentace, specifické zkratky a pojmy poplatné zejména této části VZ jsou v následující tabulce.

(2) Jedná se o podpůrnou informaci, kterou Zadavatel poskytuje pro zachování jednoznačného výkladu textu dokumentu.

Zkratka	Význam
NGFW	Next-Generation Firewall
IPS	Intrusion Prevention System
CPU	Central Processing Unit
RAM	Random Access Memory
RAID	Redundant Array of Inexpensive Disks
HW	Hardware
SW	Software
VLAN	Virtual Local Area Network
LACP	Link Aggregation Control Protocol
LDAP	Lightweight Directory Access Protocol
AD	Active Directory
SNMP	Simple network management protocol
FTP	File Transfer Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
DDoS	Distributed Denial of Service
VPN	Virtual private network
SSL	Secure Sockets Layer
SSH	Secure Shell
TCP	Transmission Control Protocol
SIEM	Security Information and Event Management
SOAR	Security orchestration, automation and response
NFS	Network File System
VM	Virtual Machine
VDI	Virtual Desktop Infrastructure
IPv4/v6	Internet Protocol version 4 / version 6
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol
EDR	Endpoint Detection and Response
XDR	Extended Detection and Response

OS	Operating System
IoC	Indicator of Compromise
OLE	Object linking and embedding
RAR	Roshal Archive
ZIP	Zig-zag Inline Package
GZ	G-Zip
ISO	International Standardization Organization
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
YARA	Yet Another Recursive Acronym
LM	Log Manager
EU	Evropská unie
REST	Representational State Transfer
API	Application Programming Interface
RBAC	Role-based access control
MDM	Mobile Device Management
BYOD	Bring Your Own Device
PC	Personal Computer
NB	Notebook
DLP	Data Loss Prevention
NBD	Next Business Day
2FA	Two Factor Authentication
MFA	Multi Factor Authentication
MGMT	Management

2. Místo plnění

Nemocnice Pelhřimov, příspěvková organizace, Slovanského bratrství 710, 393 01 Pelhřimov.

3. Doba plnění

(1) Dodávka bude zahájena po nabytí účinnosti smlouvy a bude řízena milníky uvedenými v tabulce Milníky.

(2) Milníky Fáze A instalace a implementace dle Smlouvy.

Id	Činnosti	Termín
01	Podpis Smlouvy	Bude přesněno podle ukončení zadávacího řízení
02	Zahájení realizace projektu	Bezprostředně po podpisu

Id	Činnosti	Termín
		smlouvy a nabytí její účinnosti
Dodávka technologií, instalace, implementace		
03	**Zpracování a akceptace Detailního realizačního projektu** Výstupem bude dokument Detailní realizační projekt Předání dílčího plnění a Akceptace dílčího plnění	do 3 měsíců od ID 02
04	**Dodávka a instalace technologií a implementace**	do 10 měsíců od ID 03
05	**Zkušební a testovací provoz** Akceptace Testovacího provozu	do 2 měsíců od ID 04
06	**Produkční provoz** Akceptace produkčního provozu, akceptace Fáze A Dodávka a aktivace licencí Ukončení Fáze A	Po ukončení ID 05

(3) Fáze B – HW a SW maintenance výrobce technologií a systémů dle Smlouvy bude zahájena ukončením Fáze A (ukončení projektu akceptací produktivního provozu).

(4) Termín ukončení se může změnit z objektivních příčin, způsobených třetími stranami nebo jinými okolnostmi, nezávislými na vůli smluvních stran.

(5) Dodavatel zpracuje jako součást Detailního realizačního projektu vyhotoveného dle odst. 6.1 této Technické specifikace vyhotoví detailní harmonogram realizace předmětu plnění v souladu s milníky, stanovenými zadavatelem výše.

4. Způsob prokázání splnění požadavků minimálního plnění

(1) Zadavatel požaduje, aby Dodavatelem nabízená dodávka splňovala veškeré dále uvedené požadavky (funkcionality a parametry) a tyto byly zahrnuty v nabídce Dodavatele a v celkové nabídkové ceně.

(2) Dodavatel ve své nabídce jednoznačně deklaruje splnění, popřípadě absenci každého z níže uvedených požadavků v tabulkách označených jako „Minimální požadavky …“, a to vyplněním příslušného pole „Splněno“ jedno ze dvou nabízených možností:

„**ANO**“ v případě že dodávka Dodavatele (Nabídka) minimální požadavek **splňuje**

nebo **„NE“** v případě že dodávka Dodavatele (Nabídka) minimální požadavek **nesplňuje**

(3) Zadavatel požaduje, aby Dodavatel zpracoval a v nabídce předložil podrobný technický popis nabízeného plnění reflektující všechny dále uvedené požadavky (funkcionality a parametry) (dále také „**Technický popis nabízeného řešení**“); materiál bude v rámci nabídky předložen jako příloha č. 3 kupní smlouvy.

Technický popis nabízeného řešení bude zadavateli sloužit ke kontrole splnění požadavků zadavatele na funkcionality a parametry nabízeného plnění – zejména ke kontrole splnění požadavků uvedených níže v tabulkách a označených jako „Minimální požadavky…“. Zadavatel proto

upozorňuje, že účastníci zadávacího řízení jsou v rámci nabídky povinni předložit Technický popis nabízeného řešení, jehož součástí musí být doklady, údaje a případně i informace, které budou jednoznačně prokazovat splnění deklarovaných parametrů a funkcionalit u požadavků uvedených níže v tabulkách označených jako „Minimální požadavky…".

Technický popis nabízeného řešení:

a) **musí být zpracován přehledně a zejména strukturovaně ve vztahu k minimálním požadavkům uvedeným dále v odst. 5, v odst. 6 a v odst. 7** včetně jejich pododstavců, tj. bude zpracován tak, aby se svým obsahem vždy vztahoval k příslušnému odstavci (odst. 5; 5.1; 5.2.; 5.2.1; 5.2.3; 5.3, 5.4 atd. ….až odst. 7).
b) musí obsahovat grafické schéma a podrobný popis nabízených technologií a systémů, datové listy, snímky obrazovek atd.
c) u požadavků na funkcionality musí obsahovat informace o skutečné funkcionalitě nabízených řešení, které bude možné ověřit nejpozději v testovacím provozu, např. v rámci školení administrátorů;
d) u parametrových požadavků musí být jeho součástí přílohy - produktové materiály a ostatní doklady (např. datové listy, snímky obrazovek atd.), které bez nejmenších pochyb budou prokazovat splnění takových požadavků;
e) **u veškerého nabízeného plnění musí být uvedeny „part number"** včetně vysvětlujícího popisu a počtu kusů (tato podmínka se nevztahuje na spotřební materiál); zadavatel připouští předložení „part number" k nabízenému plnění formou seznamu rozděleného dle jednotlivých odstavců definovaných výše u písm. a)

Zadavatel upozorňuje, že nepředložení Technického popisu nabízeného řešení obsahově plně odpovídajícího výše definovaným požadavkům zadavatele, může mít za následek vyloučení účastníka zadávacího řízení pro nesplnění podmínek účasti v zadávacím řízení.

(4) V případě pochybností o splnění minimální technické specifikace může Zadavatel vyžádat prokázání splnění technické specifikace formou vzorku. Za poskytnutí vzorku nebude Uchazeči vznikat nárok na úhradu nákladů s tím spojených. Podrobnosti k poskytnutí vzorku viz textová část Zadávací dokumentace.

(5) Nesplnění nebo neprokázání kteréhokoli ze stanovených minimálních požadavků, uvedených v této Technické specifikaci bude znamenat vyloučení účastníka ze zadávacího řízení.

5. Požadavky na specifikaci jednotlivých bezpečnostních technologií

(1) Předmětem VZ je dodávka bezpečnostních technologií, které jsou vyspecifikované v níže uvedených podkapitolách.

5.1 Technická specifikace Centrálních Firewallů

(1) Současný firewall nedokáže výkonem pokrýt datové požadavky uživatelů sítě, nelze ani dlouhodobě ukládat logy a celkově je technologicky nevyhovující, a to i z důvodu toho, že v případě výpadku není zajištěna vysoká dostupnost.

(2) Předmětem zadání je implementace 2ks NG segmentačních firewallů pro vytvoření clusteru s vysokou dostupností a dosavadního zajištění segmentace sítě (za použití standardů IEEE 802.1Q.a RFC 7348 pro řádově desítky segmentů). Dále pak 1ks SW licence pro analýzu logů firewallů a centrální správy celého systému firewallů. SW bude sloužit jako log proxy pro naplnění potřeby zjednodušení architektury toku logů. Log proxy bude nasazena mezi firewally a centrálním log management řešením. Funkce firewallu musí pokrýt okamžité potřeby správců firewallu a redukovat počet zdrojů logů na jeden. Řešení bude obsahovat firewall cluster v režimu vysoké dostupnosti active/active. Každý node clusteru pak bude umístěný v jednom DC.

(3) Kromě funkcionality síťového firewallu řešení bude také nabízet IPS, filtraci a kontrolu na úrovni aplikací a URL a dále pak ochranu před ransomware, malware a bude disponovat funkcí sandboxingu, antiviru a anti-bot. Musí být umožněna identifikace a definice politik na úrovni uživatelských identit a z toho plynoucí možnost integrace bezpečnostního řešení ke stávajícímu AD. Další rolí pak bude i

funkce VPN koncentrátoru, licenčně by mělo být umožněno připojit nejméně 50 vpn uživatelů na každý firewall současně.

(4) Součástí řešení bude i nezávislý centrální management server ve formě virtuálního stroje ve stávající virtualizační platformě VMware. Firewall infrastruktura bude nasazena v distribuované architektuře, kdy je pomocí tohoto serveru centrálně spravována, management centrálních firewallů dále bude sloužit také pro tvorbu a správu bezpečnostních politik a správu administrátorů celého systému.

Současně pak centrální server zajistí sběr a interpretaci logů a událostí z firewallů a auditní log firewall infrastruktury, umožní korelaci a analýzu bezpečnostních incidentů. Z těchto dat bude možné následně generovat bezpečnostní reporty.

(5) Minimální požadavky na technickou specifikaci centrálních firewallů jsou uvedeny v následující tabulce. Parametry jsou uvedeny pro jeden firewall.

ID	Požadované parametry	Splněno
01	Požadované funkcionality NG Firewall, IPS, aplikační a URL filtering, malware a botnet ochrana, zero-day ochrana, inspekce ssl provozu, sandboxu emulace provozu.	ANO
02	HW akcelerovaný IP provoz (například SR-IOV).	ANO
03	Nejméně 16 GB operační paměti DDR5 s podporou ECC.	ANO
04	Redundantní HA konfigurace řešení složená min ze dvou fyzických prvků.	ANO
05	Podpora HA redundance active-active i active-standby, stavová synchronizace TCP, UDP a NAT.	ANO
06	Podpora L2 a L3 HA konfigurace.	ANO
07	Podpora IPv4 a IPv6.	ANO
08	Podpora VLAN a VXLAN (min. 1024 VLAN, prvek musí mít v každé VLAN, VLAN interface).	ANO
09	Podpora protokolů pro dynamické směrování OSPFv3 a BGPv4.	ANO
10	Podpora LACP bonding.	ANO
11	Podpora redundance Internetového připojení (active-standby, loadbalancing).	ANO
12	DHCP server.	ANO
13	Podpora NAT (včetně IPv6 NAT – NAT46/NAT64/NAT66). Požadavek dle potřeb paragrafu 27 Vyhlášky o dlouhodobém řízení informačních systémů veřejné správy.	ANO
14	Podpora 802.1X a integrace s řešením nástroje pro segmentaci sítě, viz technická specifikace Nástroje pro zavedení segmentace sítě.	ANO
15	Integrace s AD a LDAP, podpora RADIUS.	ANO
16	Možnost rozdělení řešení na jednotlivé nezávislé virtuální instance, včetně aplikace kompletní funkcionality nezávisle na konfiguraci ostatních instancí. Tento požadavek zjišťuje možné úplné oddělení interní a návštěvnické komunikace.	ANO
17	Propustnost firewall (SPI) min 25Gbps (Enterprise mix).	ANO
18	N+1 redundance – zachování propustnosti i při výpadku jednoho prvku.	ANO
19	Propustnost firewall+IPS+antivirus/antibot+aplikační kontrola+NAT+VPN min 5Gbps (Enterprise mix).	ANO
20	Plná kontrola každého paketu bez vlivu na propustnost FW+IPS+AV/AB+NAT+VPN min 5Gbps (ID 18).	ANO
21	Min 8mil současných spojení v jeden čas.	ANO
22	Min 100 000 nových spojení/s.	ANO
23	Všechny funkcionality konfigurovatelné pomocí bezpečnostních politik.	ANO
24	Plná integrace IPS a firewall.	ANO
25	Předdefinované a ihned použitelné IPS politiky.	ANO
26	Možnost definice IPS pravidel pomoci kombinace src, dst, služba, IPS signatura.	ANO

ID	Požadované parametry	Splněno
27	Možnost nastavit IPS v režimu monitoring nebo prevent globálně i pro jednotlivé pravidlo.	ANO
28	Automatické vypnutí IPS v případě přetížení (CPU nebo paměť) nad definovaný práh.	ANO
29	Nové signatury označeny a možnost nastavit je v režimu monitoring.	ANO
30	Podpora SSL/TLS inspekce, podpora TLS1.2 a TLS1.3.	ANO
31	Blokování spojení na úrovni DNS dotazu. Cílem tohoto požadavku je zabránit překladu adres s nežádoucím obsahem.	ANO
32	Min 5000 předdefinovaných služeb/protokolů/aplikací.	ANO
33	Možnost vytvářet vlastní IoC indikátory.	ANO
34	Sandbox emulace (zero-day ochrana) podporuje protokoly HTTP, HTTPS, FTP, SMTP a SMB.	ANO
35	Emulace souboru o velikosti min 100 MB.	ANO
36	Možnost odstranění potencionálně škodlivého aktivního obsahu ze souborů, podpora MS Office, PDF, obrazových formátů a archivů (.zip, .tar, .7z, .rar).	ANO
37	Odstranění aktivního obsahu nebo konverze souboru do bezpečného PDF.	ANO
38	Dynamická analýza souborů se sledováním změn v souborovém systému, registrech, procesech a síťové komunikaci.	ANO
39	Logování a reporting změn detekovaných analýzou.	ANO
40	MITRE ATT@ACK reporting.	ANO
41	Ochrana proti botnet a Command & Control.	ANO
42	Detekce a filtrování malware URL.	ANO
43	Schopnost detekovat a zablokovat DDOS a bruteforce útoky.	ANO
44	Integrace řešení s AD bez nutnosti komponent třetích stran.	ANO
45	Definice bezpečnostních politik na základě AD skupin.	ANO
46	Možnost autentizace uživatele na základě portálu – podpora ověření za pomoci jméno/heslo a SSO Kerberos.	ANO
47	Podpora IPSec VPN.	ANO
48	Podpora SSL VPN v režimu tunel a v režimu web portal.	ANO
49	Podpora IP komprese S2S VPN.	ANO
50	VPN podporuje šifrování min AES-256.	ANO
51	VPN podporuje datovou integritu min SHA-256.	ANO
52	Min 50 SSL VPN konkurenčních spojení včetně licence, pokud je licenčně omezeno.	ANO
53	Podpora MFA pro SSL VPN jméno/heslo + 2FA (integrace s MS Authenticator, Email nebo SMS).	ANO
54	Management a konfigurace Firewall přes SSH.	ANO
55	Podpora 2FA/MFA administrátorského přístupu	ANO
56	Centrální management samostatný, fyzicky oddělený od firewall platformy.	ANO
57	Centrální management ve formě HW nebo virtuálního stroje.	ANO
58	Ukládání logů na oddělený centrální Log server.	ANO
59	Centrální správa politik a centrální konfigurace nastavení.	ANO
60	Centrální management podporuje režim HA.	ANO
61	Komunikace mezi firewallem a centrálním managementem je šifrovaná a autentizovaná.	ANO
62	Možnost vyhledat všechny logy na jednom místě pomoci definovaných filtrů (FW, IPS, malware logy).	ANO
63	Možnost exportu logů do souboru.	ANO
64	Možnost definice IPS politik přímo z logu.	ANO
65	Indexování logů umožňující rychlé prohledávaní.	ANO

ID	Požadované parametry	Splněno
66	Retence logů min 18měsíců.	ANO
67	Možnost přidat komentář ke každému pravidlu.	ANO
68	Možnost časově omezit platnost pravidel.	ANO
69	Možnost seskupování firewall pravidel do samostatných logických skupin a oddílů.	ANO
70	Možnost vyhledat využití objektů (výskyt v aktivních i neaktivních pravidlech, nebo v jiných objektech, např. ve skupinách).	ANO
71	Možnost práce a změn více administrátorů paralelně.	ANO
72	Detekce kolizí a duplicit v politikách.	ANO
73	Možnost definice skupin oprávnění ke změnám politik pro administrátory, možnost definovat práva na úrovní jednotlivých pravidel.	ANO
74	Konfigurace politik a nastavení prostřednictvím GUI.	ANO
75	Podpora autorizovaného a autentizovaného REST API.	ANO
76	Funkcionalita korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy a reporty.	ANO
77	Možnost vytváření uživatelsky definovatelných reportů (na základě log záznamů a bezpečnostních událostí), možnost periodických reportů.	ANO
78	Možnost integrace se SIEM, SOAR.	ANO
79	Dedikované MGMT rozhraní 1GbE.	ANO
80	Rozhraní pro lokální nezávislý management (out of band) - RJ45 + RS-232/USB.	ANO
81	Minimálně 4 x síťové rozhraní 1GbEx5	ANO
82	Minimálně 4 x síťové rozhraní 10/25GbE	ANO
83	Rozměry max 2U pro každý Firewall.	ANO
84	Rozměry standardní velikost 19“.	ANO
85	Redundantní napájení s podporou hot-swap.	ANO
86	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.2 Technická specifikace centrálního sběru a managementu logů

(1) V současné době není v Nemocnici Pelhřimov žádný centrální Log management.
(2) Předmětem této části VZ je dodávka a instalace SW. Bližší specifikace je uvedena v jednotlivých kapitolách níže (viz podkapitoly 5.2.1–5.2.3)

5.2.1 Technická specifikace řešení pro správu logů

(1) Níže jsou uvedené minimální požadavky na systém pro centralizovanou správu logů, událostí a strojových dat. **Minimální požadavky** jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Systém pracuje jako Virtuální appliance na stávající virtualizační platformě VMware vSphere 8.0 U1 nebo novější.	ANO
02	Systém umožňuje uživatelsky definované parsery. Dokumentace (v anglickém nebo českém jazyce) musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní. Vytváření a testování parserů nesmí mít vliv na provoz systému.	ANO

ID	Požadované parametry	Splněno
03	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: syslog (dle RFC3164, RFC5424, RFC5425). Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta.	ANO
04	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.	ANO
05	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a minimálně s identifikací IP adresy.	ANO
06	Systém zachovává původní informaci ze zdroje logu o časové značce události.	ANO
07	Systém musí umožňovat konfiguraci filtrace událostí v grafickém rozhraní vizuálního programovacího jazyka.	ANO
08	Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc).	ANO
09	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období.	ANO
10	Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění.	ANO
11	Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty.	ANO
12	Systém má možnost přehledného zobrazování příchozích logů.	ANO
13	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	ANO
14	Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů k jednotlivým ovládacím komponentům systému.	ANO
15	Systém obsahuje všechny softwarové komponenty architektury řešení a nevyžaduje žádné externí zdroje (například externí databázi, aplikační server atd.).	ANO
16	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300 GB uložených událostí za den.	ANO
17	Systém musí zpracovat nejméně 5000 EPS ve špičkovém provozu.	ANO
18	Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	ANO

ID	Požadované parametry	Splněno
19	Systém musí být vybaven základní množinou předpřipravených alertů s možností definice aletrů na základě vlastních podmínek.	ANO
Požadovaný seznam podporovaných zdrojů logů		
20	Apache httpd, Tomcat	ANO
21	CEF (generický/standardizovaný formát)	ANO
23	LEEF (generický/standardizovaný formát)	ANO
24	JSON (generický/standardizovaný formát)	ANO
25	MySQL	ANO
26	OpenSSH server	ANO
27	PostgreSQL	ANO
28	RFC5425 (generický/standardizovaný formát)	ANO
29	Vmware vCenter a ESXi (od verze 7.0.2 přes API)	ANO
30	Dodávané systémy požadované a popsané v této Technické specifikaci. Součástí řešení musí být vytvořený parser, nemusí se jednat o nativní funkcionalitu řešení.	ANO

5.2.2. Požadavky na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX)

(1) S ohledem na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX) je požadováno dodání 1 ks virtualizovaného kolektoru pro centralizaci sběru dat.

(2) **Minimální požadavky** na technickou specifikaci 1 ks kolektoru jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
01	Minimální nastavení 4 CPU cores	ANO
02	Minimální nastavení 8 GB RAM	ANO
03	Minimální nastavení 1000 IOPS	ANO
04	Minimální kapacita provozní paměti 6 TB	ANO
05	Virtualizační prostředí VMware ESXi 5.5 a vyšší	ANO
06	Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce.	ANO
07	Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků	ANO
08	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP.	ANO
09	Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.	ANO

Id	Požadované parametry	Splněno
10	Snadná instalace do stávající síťové infrastruktury – šablony pro nasazení virtuálního stroje.	ANO
11	Jednoduchá konfigurace pomocí dostupných konfiguračních šablon, které umožňují výběr z dostupných “Presets” a jejich aplikací vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace.	ANO
12	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.	ANO
13	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.	ANO
14	Podpora autentizace vůči LDAP (Active Directory).	ANO
15	Podpora autentizace vůči TACACS+.	ANO
16	Virtuální kolektor bude dodán na výše zmíněné virtualizační platformě. HW požadavky jsou dány požadavky na virtualizační platformu.	ANO
17	Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.	ANO
18	Časová synchronizace zařízení proti centrálnímu zdroji času na síti.	ANO
19	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.	ANO
20	Přístup na virtuální kontroler bude chráněn pomocí protokolu TLS 1.3 a vyšší.	ANO
21	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.	ANO
22	Podpora standardu Cisco AVC vč. položek HTTP hostname a URL.	ANO
23	Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2.	ANO
24	Podpora IPFIX položek proměnlivé délky.	ANO
25	Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions.	ANO
26	Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.	ANO
27	Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS).	ANO
28	Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů.	ANO
29	Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů.	ANO
30	Systém bude schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště musí umožnit uložit záznamy statistik po dobu minimálně šesti měsíců.	ANO
31	Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat.	ANO
32	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik.	ANO

Id	Požadované parametry	Splněno
33	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011.	ANO
34	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.	ANO
35	Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat.	ANO
36	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.	ANO
37	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele).	ANO
38	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).	ANO
39	Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů.	ANO
40	Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat).	ANO
41	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem.	ANO
42	Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami.	ANO
43	Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru.	ANO
44	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.	ANO
45	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.	ANO
46	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).	ANO

Id	Požadované parametry	Splněno
47	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.	ANO
48	Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).	ANO
49	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.	ANO
50	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.).	ANO
51	Možnost dohledat každý jednotlivý datový tok (flow záznam).	ANO
52	Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie.	ANO
53	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení.	ANO
54	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).	ANO
55	Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).	ANO
56	Monitorování dostupnosti zdroje flow dat pomocí SNMP.	ANO
57	Kolektory NetFlow dat jsou schopné zpracovat 40K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy.	ANO
58	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik.	ANO
59	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011.	ANO
60	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.	ANO
61	Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat.	ANO
62	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.	ANO
63	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco	ANO

Id	Požadované parametry	Splněno
	ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele).	
64	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).	ANO
65	Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů.	ANO
66	Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat).	ANO
67	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem.	ANO
68	Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami.	ANO
69	Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru.	ANO
70	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.	ANO
71	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.	ANO
72	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).	ANO
73	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.	ANO
74	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.	ANO
75	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.).	ANO
76	Možnost dohledat každý jednotlivý datový tok (flow záznam).	ANO
77	Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie.	ANO
78	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení.	ANO
79	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).	ANO
80	Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).	ANO

Id	Požadované parametry	Splněno
81	Monitorování dostupnosti zdroje flow dat pomocí SNMP.	ANO
82	Kolektory NetFlow dat jsou schopné 150K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy.	ANO
83	Dostupnost historie plných flow dat po dobu 12 měsíců	ANO
84	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.2.3. Požadavky na řešení pro automatické vyhodnocování datových toků (NetFlow/IPFIX)

(1) Předmětem této části VZ je dodávka a instalace SW pro detekci anomálií v síti. Systém pro automatické vyhodnocování IP toků umožňuje automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém je založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události je možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů výrazně zjednodušuje správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.

(2) **Minimální požadavky** na technickou specifikaci požadavků modulu na automatické vyhodnocování NetFlow dat.

Id	Požadované parametry	Splněno
01	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Podpora VPC flow logů z AWS, Azure a GCP.	ANO
02	Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií.	ANO
03	Systém detekce anomálií poskytuje veřejně dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod apod.).	ANO
04	Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí.	ANO
05	Systém pro automatické vyhodnocování NetFlow dat je schopné zpracovat 1K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy.	ANO
06	Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.	ANO
07	Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli.	ANO
08	Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním.	ANO
09	Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků.	ANO

Id	Požadované parametry	Splněno
10	Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události.	ANO
11	Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události.	ANO
12	Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií.	ANO
13	Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.	ANO
14	Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.	ANO
15	Detekce NATů v síti s využitím rozšířených informací z L3/L4.	ANO
16	Detekce P2P sítí a VPN komunikace.	ANO
17	Systém umožňuje detekovat závadnou komunikací na základě rozlišení legitimních domén (druhé úrovně) od náhodně generovaných domén.	ANO
18	Detekce použití TOR klientů v monitorované síti a detekce příchozí komunikace z TOR sítě na monitorované servery.	ANO
19	Systém umožňuje detekovat závadné komunikace monitorování JA3 otisků v síťovém provozu a jejich porovnáváním se seznamem známých závadných JA3 otisků.	ANO
20	Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci.	ANO
21	Systém lze napojit na MISP platformu a použít indikátory kompromitace (IoC) poskytované touto platformou k detekci závadných komunikací v monitorované síti.	ANO
22	Detekce nadměrné zátěže sítě, výpadků služeb, nových a cizích zařízení připojených k síti.	ANO
23	Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace.	ANO
24	Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování atd.).	ANO
25	Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí.	ANO
26	Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.).	ANO
27	Systém je schopen poskytnout přímý přístup k evidované události za pomoci ID události z externích systémů za pomoci unikátního URL, které je možné sestavit v externím systému při znalosti ID události.	ANO

Id	Požadované parametry	Splněno
28	Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána.	ANO
29	Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP/HTTPS.	ANO
30	Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP.	ANO
31	Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře.	ANO
32	Detekované události jsou mapovány na jednu nebo více MITRE ATT&CK taktik a technik pro poskytnutí širšího kontextu uživateli. Mapování je založeno na základě kontextové analýzy pro zajištění správného mapování taktiky a techniky na detekovanou událost. Stejný druh události tak může být mapován různě v závislosti na kontextu události nebo vývoji události v čase.	ANO
33	Systém poskytuje dashboard pro vizualizaci MITRE ATT&CK matice, která zobrazuje počet událostí detekovaných v jednotlivých taktikách a technikách čímž umožňuje poskytnout přehled nad stávající bezpečností situací a zobrazit útoky v jejich různých fázích dle MITRE ATT&CK frameworku.	ANO
34	Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen.	ANO
35	Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ).	ANO
36	Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit.	ANO
37	Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry.	ANO
38	Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí.	ANO
39	Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu.	ANO
40	Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní.	ANO
41	Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu.	ANO
42	Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu.	ANO
43	Pravidla pro falešné poplachy je možné definovat pomocí čísel autonomních systémů (ASN) nebo pomocí plně kvalifikovaného doménového jména (FQDN), čímž lze označit provoz, který nebude zpracováván detekčními metodami.	ANO
44	Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny	ANO

Id	Požadované parametry	Splněno
	konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management.	
45	Události je možné automaticky exportovat ve formátu CEF protokolem syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. Součástí exportu musí být event ID, které jednoznačně identifikuje danou událost.	ANO
46	Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap.	ANO
47	Události je možné exportovat do formátu CSV pro další zpracování.	ANO
48	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem.	ANO
49	Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k e-mailovému reportu.	ANO
50	Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. Tyto záchyty je možné uživatelsky spravovat.	ANO
51	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí NBD v místě instalace na 5 let.	ANO

5.3 Technická specifikace zavedení segmentace sítě

(1) Předmětem je implementace řešení, které ve spolupráci s LAN a WLAN infrastrukturou zajistí adaptivní řízení přístupu pro různé typy zařízení a různé uživatele. Bude možné rozlišit nastavení oprávnění a aplikování politik například pro zaměstnance, hosty nebo externí partnery, a to i z pohledu připojených zařízení.

(2) **Minimální požadavky** na technickou specifikaci pro zavedení segmentace sítě jsou uvedeny v následující tabulce.

(3) V Nemocnici Pelhřimov byly postupně nakoupeny a nasazeny tyto produkty technologie Aruba Networks:

JL558A Aruba 2930-48G	6 ks
Aruba 6200F 48G CL4 740W – JL728A	19 ks
Aruba AP-515	122 ks

Zbytek sítě je také postaven na prvcích Aruba Networks dříve nazývané HP Networking (Procurve s Provision OS, Colubris). V rámci Kraje Vysočina, jakožto zřizovatele nemocnice, byla vysoutěžena, mimo další, i rámcová smlouva na prvky Aruba Networks. Zřizované organizace jsou metodicky vedeny k nákupu technologií právě z těchto rámcových smluv. Požadavek na kompatibilitu s technologiemi Aruba Networks (a to i v dalších kapitolách) se váže právě na tyto prvky.

ID	Požadované parametry	Splněno
01	Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení	ANO
02	Forma dodání: virtuální appliance pro VMware	ANO
03	Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení - 2500 v redundantním clusteru	ANO

ID	Požadované parametry	Splněno
04	Řešení musí poskytovat vysokou dostupnost tak, aby v případě výpadku primárního serveru převzal jeho roli sekundární server.	ANO
05	Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru - 2.	ANO
06	Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance.	ANO
07	Podpora předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě).	ANO
08	Požadované metody autentizace uživatelů a zařízení: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace.	ANO
09	Podpora RADIUS CoA.	ANO
10	Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD.	ANO
11	Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období.	ANO
12	Možnost TACACS+ autentizace správců síťových zařízení.	ANO
13	Další požadované autentizační a autorizační zdroje a metody: LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).	ANO
14	Možnost integrace s MDM (Mobile Device Management) platformami třetích stran: minimálně AirWatch, Citrix, MobileIron, JAMF, InTune.	ANO
15	Podpora REST API pro většinu základních úkonů systému.	ANO
16	Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.)	ANO
17	Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení.	ANO
18	Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran.	ANO
19	Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.	ANO
20	LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – LinkedIn, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků.	ANO

ID	Požadované parametry	Splněno
21	Možnost licenčního rozšíření o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém).	ANO
22	Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí systému.	ANO
23	Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací.	ANO
24	Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení.	ANO
25	Možnost licenčního rozšíření o kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku.	ANO
26	Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux	ANO
27	Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem	ANO
28	Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je systém.	ANO
29	Zadavatel požaduje předložení návrhu implementace segmentace sítě (VLAN) a rozložení HW zdrojů do objektu Active Directory. Po schválení návrhu provede uchazeč implementaci dle schváleného návrhu.	ANO
30	Řešení musí být kompatibilní se stávajícími prvky Aruba Networks.	ANO
31	Technické řešení segmentace sítě musí být integrováno s firewally za účelem sdílení identity a předávání stavových informací o bezpečnosti přistupujícího klienta. Nástroj segmentace musí být schopen komunikovat s firewallem oboustranně. Nejmenší množina atributů integrace je IP adresa, uživatelské jméno, uživatelská role, doména, typ zařízení (PC, chytrý telefon apod.), doménové jméno zařízení, operační systém zařízení a finálně postoj platformy ke stavu ověření.	ANO
32	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.4 Technická specifikace DLP

(1) V současné době není implementována technologie DLP pro ochranu citlivých dat, a to jak na koncových stanicích, serverech nebo perimetru.

(2) Předmětem dodávky by měl být nástroj, který zajistí audit pohybu dat a detekci rizikových operací, pro klasifikaci citlivých a důvěrných dat a ochranu citlivých a důvěrných dat před únikem.

(3) **Minimální požadavky** na technickou specifikaci DLP pro 500 koncových stanic (PC, NB) jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Klasifikace dat na základě obsahu minimálně v běžných textových souborech (čisté txt, office dokumenty, pdf apod.). Platforma musí rozpoznat nejméně tyto typy souborů: výše zmíněné textové dokumenty, komprimované soubory, soubory tabulkových procesorů (například .xlsx), prezentace, bitmapová grafika, vektorová grafika a jiné multimediální soubory.	ANO
02	Vyhledávání vzorků pro obsahovou klasifikaci alespoň v textových formátech (viz bod 01).	ANO
03	Možnost zadání vzorků pro obsahovou klasifikaci alespoň pomocí regulárních výrazů a výčtem vyhledávaných řetězců.	ANO
04	Existence předpřipravených vzorků pro obsahovou klasifikaci alespoň pro část informací obecně považovaných za citlivé.	ANO
05	Klasifikace dat na základě zdroje, ze kterého byly získány (konkrétní aplikace/skupina aplikací, konkrétní webová stránka/skupina webů, síťová cesta/lokální cesta).	ANO
06	Klasifikace dat na základě typů souborů (záchytná varianta pro typy nepodporované přímo obsahovou klasifikací).	ANO
07	DLP politiky definovatelné jak obecně, pro všechna přenášená data, tak i pro jednotlivé datové typy, které vzešly z některého typu datové klasifikace.	ANO
08	Možnost tvorby DLP politik i za využití metadat klasifikace třetích stran (nejméně velikost a typ souboru). Zejména pak platí ve vztahu k platformám pro ochranu operačních systémů a mobilních platforem.	ANO
09	Možnost tvorby DLP politik s příslušnými atributy minimálně pro řízení e-mail komunikace (jak nativní aplikace, tak i webmaily), uploadu na síťová úložiště pomocí nativních aplikací, uploadu na web za použití browseru/webových aplikací obecně, uploadu souborů pomocí komunikačních aplikací (Teams, Zoom, instant messaging aplikace apod.).	ANO
10	Možnost řízení pohybu dat směrem na lokální výměnná datová úložiště (disky, optická média a USB zařízení, Bluetooth přenosy apod.).	ANO
11	Možnost řízení tiskových operací (lokální/síťové tiskárny, tisk do souborů).	ANO
12	Možnost definovat reakci politiky alespoň ve variantách povolit, zaznamenat (případně navíc upozornit uživatele), blokovat.	ANO
13	Možnost definice výjimek z jednotlivých DLP politik.	ANO
14	Možnost uchování dokumentů zachycených politikou pro pozdější analýzu.	ANO
15	GUI pro správu DLP systému (nativní aplikace pro Win OS platformu, nebo aplikace běžící v standardních webových prohlížečích).	ANO
16	Integrace s AD (načítání a párování informací o klientských stanicích a uživatelích, možnost definice výstupů z DLP politik s využitím informací na bázi AD objektů).	ANO
17	Centrální správa klientů (aktivace/deaktivace, upgrade).	ANO
18	Možnost deaktivace jednotlivých funkcionalit klienta pro případný troubleshooting.	ANO
19	Možnost zasílání upozornění o závažných provozních událostech a porušení DLP politik (např. e-mail, syslog nebo SNMP trap apod.).	ANO
20	Uchování auditních záznamů o konfiguračních úpravách DLP.	ANO
21	Možnost exportu auditních informací do jiných systémů (např. centrální logování, SIEM) minimálně pomocí syslog protokolu.	ANO
22	Generování reportů a grafů se záznamy o vyhodnocení/porušení DLP politik.	ANO
23	Komunikace mezi klientskými a serverovými komponentami, stejně jako mezi management rozhraním a serverem je zabezpečená kryptografickými prostředky aktuálně považovanými za bezpečné.	ANO
24	Administrátorům je možné přiřazovat role, které definují přístupová oprávnění k jednotlivým komponentám management rozhraní.	ANO

ID	Požadované parametry	Splněno
25	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.5 Technická specifikace úložiště pro PACS a NIS data formou NAS a S3

(1) Pro nestrukturovaná data bude k dispozici úložiště postavené na technologii scale-out. Cílem fungování tohoto úložiště je zajištění bezpečného místa pro uložení objemných soborů jako jsou například PACS data, a tím zajistit dostupnost informací. Úložiště bude přímo integrováno s Microsoft Active Directory.

(2) Řešení bude obsahovat scale out architekturu s nejméně 4 identickými uzly postavenou na principu redundance médií pomocí technologie erasure coding. Řešení musí být odolné na výpadek jednoho hardware uzlu a nejméně 2 médií-disků z každého uzlu. Jednotlivé aplikace k úložišti mohou přistupovat pomocí protokolů S3, NFS a případně SMB.

(3) **Minimální požadavky** na technickou specifikaci úložiště pro PACS a NIS data formou NAS a S3 jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Úložiště určené pro montáž do standardního racku 19“.	ANO
02	Nabízené úložiště je postavené na architektuře scale-out se škálovatelností min.na 30 nodů.	ANO
03	Požadujme minimálně 4 nody o celkové výšce max. 8 RU.	ANO
04	Úložiště má nativní podporu souborových protokolů SMB v3 a NFS v4.1 nebo vyšších verzí a objektového protokolu S3.	ANO
05	Data rozprostřená mezi nody jsou chráněna technologií erasure coding.	ANO
06	Úložiště pro získání identit či stromu přístupových oprávnění umí přistupovat do Microsoft Active Directory.	ANO
07	Podpora protokolu S3 pro přesouvání záloh z úložiště.	ANO
08	Požadujeme odolnost úložiště vůči výpadku jednoho nodu anebo nejméně dvou libovolných disků z libovolného nodu.	ANO
09	Datový prostor pro uživatele/aplikace musí být prezentován jako jeden prostor (name space). Požadujeme integrovaný load balancer pro rovnoměrné rozložení zátěže mezi nody.	ANO
10	Úložiště poskytuje funkce pro replikaci mezi dvěma úložišti na úrovni souborové vrstvy s kontinuálním průběhem (synchronní anebo asynchronní replikace).	ANO
11	Úložiště musí podporovat šifrování dat (data at rest encryption), minimálně na úrovni AES-256. Šifrování nesmí být závislé na hardware pro zajištění bezpečné přenositelnosti dat mezi různými hardwarovými platformami. Řešení musí zajistit ochranu dat proti krádeži médií i po vyřazení médií z provozu. Řešení podporuje externí PKI.	ANO
12	Požadujeme podporu vytváření uzamykatelných snapshotů, jako ochrana proti ransomware. Tato funkce ve spojení se zálohovacím softwarem by měla zaručit, že repositář záloh zůstane nezměnitelným úložištěm souborů.	ANO
13	Deduplikační a kompresní poměr nelze z důvodu ukládání již redukovaných dat započítat do celkové nabízené kapacity pole. Požadovaná čistá kapacita úložiště dostupná aplikacím/uživatelům je nejméně 180 TB při zachování všech požadovaných vlastností.	ANO
14	Úložiště bude osazeno minimálně 8 x 25GbE porty tj. min. dva porty na každý nod.	ANO
15	Požadovaný výkon nabízeného pole musí být minimálně 46 000 IOPS (NFSv4.1). Celkový požadovaný výkon úložiště pro operace čtení je min. 6 GB/s a pro operace zápisu min. 4 GB/s. Jeden klient musí být schopen zapisovat kontinuální	ANO

	rychlostí minimálně 1 GB/s a číst rychlostí 2GB/s. Takový výkon musí být pole schopné poskytnout na 100% požadované kapacity.	
16	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.6 Technická specifikace infrastruktury pro zálohování a rychlou obnovu

(1) V současné chvíli zálohování nemocnice neodpovídá požadavkům zákona o kybernetické bezpečnosti (ochrana proti ransomware a off line zálohování). Nové řešení by mělo zajistit lepší dostupnost informací.

(2) Předmětem dodávky je zálohovací server a také pásková knihovna.

(3) **Minimální požadavky na** technickou specifikaci infrastruktury pro zálohování a rychlou obnovu jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
	Zálohovací server	
01	Zálohovací server určený pro montáž do standardního racku 19“ o maximální výšce 2 RU.	ANO
02	Dvě CPU kompatibilní s virtualizační platformou VMware vSphere 8.0U2. Zadavatel předpokládá 2x8 jader. Pokud Uchazeč zvolí jinou kombinaci musí zajistit dostatečné licenční pokrytí počtu jader. CPU musí společně dosáhnout výkonu v testu SPEC CPU2017 nejméně 250 Floating point bodů pro metriku Base. Test by měl být vykonán nejméně na hardware stejného výrobce.	ANO
03	8x 16 GB DDR4 DIMM o frekvenci min.2400MHz s rozšiřitelností na min. dvojnásobek DIMMů.	ANO
04	Min.6x 480 GB SSD pro rychlou obnovu a OS na nezávislém řadiči.	ANO
05	Min.24x 20TB 7,2k NL disků pro zálohy na nezávislém řadiči.	ANO
06	Min. 4x 10/25GbE SFP28 porty na dvou nezávislých NIC kartách.	ANO
07	FC HBA s dvěma porty, každý o rychlosti min. 16 Gb pro připojení páskové knihovny.	ANO
08	OOB management serveru s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, RedFish API s časově neomezenou licencí.	ANO
09	OOB management podporuje: MFA, integraci s MS AD, Silicon Root Of Trust, Secure Boot a Chain Of Trust (kontrola celého výrobního řetězce), TPM 2.0.	ANO
10	Min.2x 800 W hot-plug napájecí zdroj s platinovou účinností.	ANO
11	Součástí serveru je licence Microsoft Windows Standard 2022 na všechna CPU jádra serveru.	ANO
12	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO
	Pásková knihovna	
13	Pásková knihovna určená pro montáž do standardního racku 19“ o maximální výšce 2 RU.	ANO
14	Nabízená pásková knihovna musí interně uložit data o kapacitě min. 288TB (nekomprimovaně) respektive 720 TB (2.5:1 komprimovaně) pomocí technologie LTO-8.	ANO
15	Knihovna má minimálně 24 interních pozic pro pásky a má zabudovanou čtečku čárových kódů.	ANO
16	Knihovna je osazena LTO-8 páskovou mechanikou s FC 8Gb rozhraním s možností osazení další mechaniky.	ANO

ID	Požadované parametry	Splněno
17	Pásková mechanika musí umět přizpůsobovat svoji rychlost rychlosti přicházejících dat tak, aby nedocházelo k zbytečnému opotřebení mechanik i pásek.	ANO
18	Mechanika LTO-8 v knihovně musí podporovat zápis na WORM média a mít vestavěnou podporu šifrování min.na úrovni AES 256.	ANO
19	Součástí nabídky bude příslušenství 20 ks LTO-8 pásek včetně barcode štítků a jeden ks pásky na čištění mechanik.	ANO
20	Přímý propojovací kabel QSFP28 25GbE 3 metry, Originální kabel výrobce síťových prvků kompatibilní s dodávanými technologiemi, 40 ks	ANO
21	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.7 Technická specifikace pro zvýšení dostupnosti záložního datového centra a lokální sítě

(1) Žadatel v současné době nedisponuje žádným systémem, který by vhodně zajistil zabezpečení infrastruktury nemocnice, jak z pohledu spolehlivosti a vysoké dostupnosti, tak z pohledu kybernetické bezpečnosti.
(2) Předmětem této části specifikace je popis technologie zajišťující přístup k informačním aktivům.
(3) Technické řešení bude integrováno do stávajícího síťového prostředí, které je postaveno na prvcích společnosti Aruba Networks.
(4) Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku.
(5) Páteřní přepínače slouží k agregaci přístupových přepínačů a také k připojení ostatních technologií v rámci datového centra. Páteřní přepínače musí utvářet dva logické stohy, které budou nakonfigurovány, tak že bude mezi serverovnami možné sdílet stejné adresní rozsahy. Tento požadavek vyplývá z potřeby zajištění migrace jednotlivých VM mezi dvěma výše zmíněnými stohy bez nutnosti re-adresace VM (vMotion).
(6) **Minimální požadavky** na technickou specifikaci zvýšení dostupnosti datového centra jsou uvedeny v následujících tabulkách této kapitoly.

ID	Požadované parametry	Splněno
	Páteřní přepínače 4ks	
1	Rackmount 19“	ANO
2	Plná podpora IPv4/IPv6	ANO
3	Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů	ANO
4	Provoz bez dostupnosti sítě internet	ANO
5	Jumbo frames větší než 9000 B	ANO
6	Management – serial konzole, SSH, https, SNMPv,3, REST API	ANO
7	SNMPv3 trap, syslog, RMON	ANO
8	NTP klient	ANO
9	IGMP, IGMP snooping	ANO
10	Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN	ANO
11	Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech	ANO
12	Implementace QoS – minimálně 8 HW fronty	ANO
13	RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator)	ANO

ID	Požadované parametry	Splněno
	Páteřní přepínače 4ks	
14	Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X	ANO
15	MSTP, RSTP, STP root guard, STP BPDU guard	ANO
16	Omezení počtu broadcastů na koncových portech – broadcast Storm control	ANO
17	Download/upload konfigurace v textovém tvaru	ANO
18	Archivování min. dvou verzí konfigurací a firmware přímo v zařízení	ANO
19	DHCP snooping, IPv6 MLD snooping	ANO
20	ARP inspection nebo obdobná funkcionalita dle výrobce	ANO
21	IP ACL na mgmt user interface	ANO
22	Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů	ANO
23	Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění	ANO
24	Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků	ANO
25	48 portů 10G/25G	ANO
26	6 portů QSFP28 100G+	ANO
27	Konfigurace jednotné rychlosti portů (1G/10G/25G) max. pro skupinu 4 portů	ANO
28	Dual stack IPv4 a IPv6 (včetně multicast komunikace pro obě rodiny protokolů)	ANO
29	Plná podpora L3 routingu IPv4, IPv6 (static, OSPFv3, BGPv4)	ANO
30	Stackování min. 2ks zařízení (jednotný management stacku jako jednoho zařízení včetně jednotné routovací tabulky), stohování přes QSFP28 moduly	ANO
31	MLAG – sdružení 8 linek přes 2 switche	ANO
32	LACP (802.3ad) při použití MLAG	ANO
33	Duální zdroje napájení hotswap	ANO
34	Data Center Bridging - DCBx Data Center Bridging Exchange Protocol, Priority Flow Control (PFC), Enhanced Transmission Selection (ETS)	ANO
35	Policy routing na základě ACL, IP prefix, as path	ANO
36	VRF s minimálně 16 instancemi při zapnutém dynamickém routingu	ANO
37	Směrování multicast provozu (včetně IPv6), IGMPv3	ANO
38	Protokol VRRP, použití v rámci VRF instancí	ANO
39	Protokol ECMP	ANO
40	DoS prevention nebo obdobná funkcionalita dle výrobce	ANO
41	Packet Port Buffer nejméně 32MB	ANO
42	Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) a objem dat se vzorkováním min. 20:1 – analýza přímo na zařízení s historií 180dní nebo export informací na 2 cílové destinace. Sběr na min. na 8 portech současně.	ANO
43	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

ID	Požadované parametry	Splněno
	Přístupové přepínače bez PoE 30ks	
1	Rackmount 19“	ANO
2	Plná podpora IPv4/IPv6	ANO
3	Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů	ANO

ID	Požadované parametry	Splněno
Přístupové přepínače bez PoE 30ks		
4	Provoz bez dostupnosti sítě internet	ANO
5	Jumbo frames větší než 9000 B	ANO
6	Management – serial konzole, SSH, https, SNMPv3, REST API	ANO
7	SNMPv3 trap, syslog, RMON	ANO
8	NTP klient	ANO
9	IGMP, IGMP snooping	ANO
10	Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN	ANO
11	Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech	ANO
12	Implementace QoS – minimálně 8 HW fronty	ANO
13	RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator)	ANO
14	Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X	ANO
15	MSTP, RSTP, STP root guard, STP BPDU guard	ANO
16	Omezení počtu broadcastů na koncových portech – broadcast Storm control	ANO
17	Download/upload konfigurace v textovém tvaru	ANO
18	Archivování min. dvou verzí konfigurací a firmware přímo v zařízení	ANO
19	DHCP snooping, IPv6 MLD snooping	ANO
20	ARP inspection nebo obdobná funkcionalita dle výrobce	ANO
21	IP ACL na mgmt user interface	ANO
22	Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů	ANO
23	Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění	ANO
24	Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků	ANO
25	Min. 48 portů RJ45 10/100/1000	ANO
26	Min. 4 porty 10G SFP/SFP+	ANO
27	Stackování min. 4ks zařízení do kruhu (jednotný management stacku jako jednoho zařízení včetně konfigurace LACP z více členů stacku), stackování přes SFP+ moduly se zařízeními v rámci komodit 3 až 6	ANO
28	Autentizace připojených zařízení dle 802.1x, MAC address - autorizace dvou zařízení (multi-user, multi-method authentication on each port), včetně splnění obou požadavků: a. každé v jiné VLAN na portu (telefon, PC), ověřování MAC adres na port, omezení počtu MAC na port b. v budoucnu doplnění funkcionality formou licence nebo appliance - každé zařízení v jiné vlan, nastavení bezpečnostních přístupových politik formou ACL (realizováno na koncovém portu switche nebo provoz směrován přes centrální appliance s nastavením filtrace)	ANO
29	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

ID	Požadované parametry	Splněno
Přístupové přepínače s PoE 30ks		
1	Rackmount 19“	ANO
2	Plná podpora IPv4/IPv6	ANO

ID	Požadované parametry	Splněno
	Přístupové přepínače s PoE 30ks	
3	Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů	ANO
4	Provoz bez dostupnosti sítě internet	ANO
5	Jumbo frames větší než 9000 B	ANO
6	Management – serial konzole, SSH, https, SNMPv3, REST API	ANO
7	SNMPv3 trap, syslog, RMON	ANO
8	NTP klient	ANO
9	IGMP, IGMP snooping	ANO
10	Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN	ANO
11	Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech	ANO
12	Implementace QoS – minimálně 8 HW fronty	ANO
13	RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator)	ANO
14	Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X	ANO
15	MSTP, RSTP, STP root guard, STP BPDU guard	ANO
16	Omezení počtu broadcastů na koncových portech – broadcast Storm control	ANO
17	Download/upload konfigurace v textovém tvaru	ANO
18	Archivování min. dvou verzí konfigurací a firmware přímo v zařízení	ANO
19	DHCP snooping, IPv6 MLD snooping	ANO
20	ARP inspection nebo obdobná funkcionalita dle výrobce	ANO
21	IP ACL na MGMT user interface	ANO
22	Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů	ANO
23	Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění	ANO
24	Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků	ANO
25	48 portů RJ45 10/100/1000	ANO
26	4 porty 10G SFP/SFP+	ANO
27	Stackování min. 4ks zařízení do kruhu (jednotný management stacku jako jednoho zařízení včetně konfigurace LACP z více členů stacku) stackování přes SFP+ moduly se zařízeními v rámci komodit 3 až 6	ANO
28	PoE class 4 (PoE+ - 802.3at max. 30W/port) s možností využití na všech portech switche při současném příkonu 15,4 W/port.	ANO
29	Autentizace připojených zařízení dle 802.1x, MAC address - autorizace dvou zařízení (multi-user, multi-method authentication on each port), včetně splnění obou požadavků: a. každé v jiné VLAN na portu (telefon, PC), ověřování MAC adres na port, omezení počtu MAC na port b. v budoucnu doplnění funkcionality formou licence nebo appliance - každé zařízení v jiné vlan, nastavení bezpečnostních přístupových politik formou ACL (realizováno na koncovém portu switche nebo provoz směrován přes centrální appliance s nastavením filtrace)	ANO
30	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

(7) Stávající přepínače využívají technologii Aruba Networks Virtual Switching Framework (VSF) pro stohování https://www.arubanetworks.com/techdocs/AOS-S/16.11/MCG/WC/content/wc/vir-swi-fra-vsf.htm . Zadavatel předpokládá využití technologie s nejméně stejnými vlastnostmi jako stávající VSF.

ID	Požadované parametry	Splněno
	Transceiver 8ks 100GBASE-SR4	
1	Transceiver QSFP28 100GBASE-SR4, MM, 100m, DDM	ANO
2	Kompatibilní s dodávanými aktivními prvky	ANO
3	Propojovací optický patchcord o délce 5m, konektorové osazení dle požadavků zadavatele	ANO
4	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

ID	Požadované parametry	Splněno
	Transceiver 4ks 100GBASE-LR4	
1	Transceiver QSFP28 100GBASE-SR4, MM, 100m, DDM	ANO
2	Kompatibilní s dodávanými aktivními prvky	ANO
3	Propojovací optický patchcord o délce 5m, konektorové osazení dle požadavků zadavatele	ANO
4	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

ID	Požadované parametry	Splněno
	Bezdrátové přístupové body 70ks	
1	konfigurace minimálně via SSH, seriový console port	ANO
2	minimálně 1x RJ45 lan port 10/100/1000Mbit/s	ANO
3	napájení přes PoE	ANO
4	certifikace Wi-Fi Alliance	ANO
5	802.11 g/n + 802.11a/n/ac/ax pracující v souběhu (dual radio)	ANO
6	WPA3	ANO
7	ruční i automatická volba kanálu (RF management)	ANO
8	AP v souladu s DFS a v souladu s podmínkami pro provoz systému v ČR	ANO
9	RF Management musí vybrat nové kanály na základě SNR (signal-to-noise ratio) a vytížení kanálu	ANO
10	virtuální SSID s podporou minimálně 10 vyzařovaných sítí/radio	ANO
11	802.1q, mapování VLAN–BSSID i při nedostupnosti kontroleru	ANO
12	ochrana rychlejších klientů na stejném rádiu	ANO
13	L2 izolace bezdrátových klientů	ANO
14	CAPWAP tunelování provozu na kontroler a zapouzdření dat z vysílaných sítí do CAPWAP tunelu nebo obdobné tunelovací řešení	ANO
15	vyústění provozu ze SSID sítí lokálně na AP (do VLAN) nebo až na kontroleru	ANO
16	802.11e protokol včetně WMM a U-APSD	ANO
17	“plug and play” instalace = (AP si vyhledá kontroler a nakonfiguruje se)	ANO
18	monitoring AP z kontroleru	ANO
19	při výpadku AP musí okolní AP zvýšit vlastní výkon - pokrytí. Optimální výběr kanálu musí být rekonfigurován dynamicky bez zásahu správce	ANO
20	802.1X – rodinu EAP protokolů s možností volby alespoň dvou AAA serverů Radius per SSID/WPAx/802.1X	ANO

ID	Požadované parametry	Splněno
Bezdrátové přístupové body 70ks		
21	podpora IP Quality of Service na bezdrátové i drátové straně. Rozlišování paketů musí být podporováno na vstupu i výstupu na DiffServ, IP ToS a IP Precedence.	ANO
22	filtrování multicast provozu	ANO
23	SNMPv3, SNMPv3 trap, syslog ve standalone mode	ANO
24	LED diody informující o stavu zařízení s možností vypnutí	ANO
25	úchyt AP na zeď/strop (montážní kit) v dodávce	ANO
26	přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků	ANO
27	Wi-Fi standard a/b/g/n/ac/ax	ANO
28	minimálně 2x RJ45 lan porty 100/1000Mbps	ANO
29	LACP	ANO
30	PoE standard 802.3 at	ANO
31	2x2 MIMO 2.4GHz pásmo	ANO
32	04x4 MIMO 5 GHz pásmo	ANO
33	integrovaná anténou	ANO
34	Fyzická instalace AP a připojení ke kontroleru (instalace strukturované kabeláže není součástí)	ANO
35	Záruka bez omezení doby (tzv. doživotní záruka) nebo nejméně na 7 let	ANO
36	Záruka výrobce na hardware v režimu 9x5 s dodáním náhradního dílu do 10 pracovních dní	ANO

ID	Požadované parametry	Splněno
Bezdrátové kontroléry 2ks		
1	licenční pokrytí pro min. 275 zařízení	ANO
2	režim HA s automatickým failoverem AP na záložní kontroler	ANO
3	RF management přístupových bodů výše	ANO
4	možnost rozšíření počtu spravovaných přístupových bodů	ANO
5	počet připojených WiFi zařízení, klientů: minimálně 5000 per kontroler	ANO
6	CAPWAP tunel pro správu přístupových bodů nebo obdobné řešení	ANO
7	konfigurace via SSH, jednoduché a rychlé začlenění (AUTO DISCOVERY – L2 autodiscovery, DHCP option) nově přidaných nenakonfigurovaných přístupových bodů do centrálního managementu kontroleru	ANO
8	WPA3/AES(CCMP) 802.11i	ANO
9	Nastavení 4x SSID s určením radius server (SSID1 jiný radius server než SSID2 ...)	ANO
10	alertování, logování, monitoring přístupových bodů	ANO
11	zjišťování Rogue AP	ANO
12	automatické řízení zátěže přístupových bodů a jejich balancování	ANO
13	guest access přístup, rozhraní pro netechnickou osobu (např. recepce) pro vytvoření dočasného účtu pro hosty	ANO
14	rychlý WiFi roaming dle standardu 802.11r a 802.11k, včetně roamingu zařízení v režimu AAA	ANO
15	podpora IP Quality of Service na bezdrátové i drátové straně. Rozlišování paketů musí být podporováno na vstupu i výstupu na DiffServ, IP ToS a IP Precedence.	ANO
16	rate limiting per client a BSSID	ANO
17	L2-L4 access control listy	ANO
18	SNMPv3, lokální a vzdálený syslog, SNMPv3 trap	ANO
19	API pro získávání informací do monitorovacího systému	ANO

ID	Požadované parametry	Splněno
	Bezdrátové kontroléry 2ks	
20	Ověřování MGMT na základě externích identit (např. RADIUS, Active directory,...)	ANO
21	centrální aktualizace firmware AP řízený kontrolerem	ANO
22	přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků	ANO
24	fyzický kontroler RACK mount provedení nebo jako součást AP	ANO
25	duální hotswap napájecí zdroje, redundantní úložiště dat a konfigurace (není požadováno při dodávce jako součást AP)	ANO
26	perpetual licence pro kontroler pro správu,mikrosegmentaci a dohled minimálně 275 přístupových bodů.	ANO
27	centralizování informací z jednotlivých AP	ANO
28	dohled stavu a výkonu AP, počtu klientů, bezdrátových sítí, aktuálně připojených uživatelů	ANO
29	statistiky, reporting o připojených klientech s retencí minimálně 180 dní, automatické odesílání definovaných reportů e-mailem	ANO
30	syslog, SNMP, REST API, alerting administrátora (zaslání informace o změně stavu systému)	ANO
31	architektura klient – server, šifrované připojení klienta	ANO
32	perpetual licence pro dohled 200 AP	ANO
33	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.8 Technická specifikace ochrany operačních systémů a mobilních platforem

(1) Řešení vykonává kompletní ochranu koncových stanic, včetně funkcí antimalware, webové a aplikační kontroly, detekce a prevence útoků, personálního firewallu, sandboxingu, a nástrojů detekce a odezvy na bezpečnostní události (EDR/XDR).

(2) Ochrana je docílena nasazením instalovaných agentů na servery, stanice a mobilní zařízení. Musí být zajištěna kompatibilita s OS Windows, MacOS, Linux platformami a také posledními verzemi OS Android a iOS/iPadOS.

(3) Je požadována centrální webová konzole k přehledu stavu zabezpečení organizace, celkové správě nasazených agentů, a získání nástrojů pro vyšetřování zaznamenaných bezpečnostních událostí.

(4) **Minimální požadavky** na technickou specifikaci bezpečnosti koncových zařízení jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	Flexibilní a konfigurovatelná ochrana koncových zařízení, která umožní správcům zapínání/vypínání jednotlivých ochran dle potřeb a postupného vynucování zabezpečení v organizaci. Minimálně ochrany typu skeny malware, kontrola webů a aplikací, řízení přístupu výměnných médií (např. USB), IDS/IPS a personální firewall.	ANO
02	Ochrana v koncových zařízení prostřednictvím instalovaných agentů členěná pro serverové OS (servery), desktopové OS (uživatelské počítače) a mobilní zařízení (mobily a tablety).	ANO
03	Zabezpečená webové konzole umístěné ve veřejném cloudu výrobce, obsahuje nástroje centrální správy instalovaných agentů, obsahuje nástroje pro pokročilé vyšetřování bezpečnostních událostí na základě sběru telemetrických dat (tzn. EDR/XDR funkce a detekce na základě ATT&CK MITRE).	ANO
04	K dosažení větší účinnosti ochrany („defence-in-depth“ přístup) agenti ochrany koncových zařízení musí využívat jiný antimalware engine (tzn. od jiného	ANO

ID	Požadované parametry	Splněno
	výrobce), než systém pro ochranu síťové bezpečnosti na perimetru organizace (NGFW).	
05	Spolehlivá funkce ochrany, musí zabraňovat útočníkům i uživatelům provádět neautorizované změny nastavení ochrany v agentech. Především musí být obsažena funkce proti odinstalaci agenta, zastavení agenta, jeho procesů a služeb, změnám zásad zabezpečení (politik) nastavených ochran.	ANO
06	Schopnost detekovat a zabránit pokusu o infekci známým i neznámým malwarem. Malware pak musí být označován do patřičné kategorie, např. trojan, worm, ransomware apod. Součástí zjištění musí být odkaz na webovou encyklopedii malware výrobce s vysvětlením nálezu.	ANO
07	Schopnost detekovat a odstranit malware na základě kombinace mechanismů signatur, vzorů chování a heuristické analýzy a sandboxingu. Možnost využití (předávání a získávání) indikátorů útoků (IoC) minimálně s atributy (doména, IP adresa, URL záznam a SHA1 řetězec). Požadována podpora standardizovaných rozhraní TAXII a MISP pro jejich výměnu s dalšími (bezpečnostními) technologiemi.	ANO
08	Schopnost detekovat a odstranit přítomnost malware v paměti OS (fileless hrozby), bootovacích sektorech disků, tabulkách diskových oddílů a na všech formách dat uložených na pevném disku systému a jiných vyměnitelných médiích.	ANO
09	Schopnost detekovat, blokovat a odstranit škodlivý software v reálném čase (realtime sken). Zajistit návrat záznamů ve Windows registrech do původního/výchozího stavu. Toto s minimálním dopadem na výkon koncových zařízení.	ANO
10	Umožnit nastavení způsobu notifikace uživatele o provedené akci agenta při porušení pravidel ochrany (možnost alarmy agenta potlačit, zobrazovat je jen jako agentské alarmy nebo umožňovat uživateli v agentu vypisování událostí za posledních pár dní/týden).	ANO
11	Instalovaný agent musí být v nástrojové liště OS Windows zobrazen ikonou, náhled na ikonu musí uživateli intuitivně přiblížit stav „zdraví“ agenta, včetně připojení ke cloudovým službám výrobce a aktuálních komponent ochran.	ANO
12	Možnost nastavit ukládání souborů s malwarem při jejich identifikaci do adresáře instalovaného agenta v zabezpečené formě (komprimovaný soubor s heslem) pro pozdější forenzní kontrolu nebo lokální akci obnovy.	ANO
13	Možnost selektivního povolení/zakázání a nastavení centrální karantény pro soubory s identifikovaným malware, obsažené nástroje k jejich centrální obnově.	ANO
14	Schopnost kontrolovat dokumenty z programů balíku Microsoft Office, včetně vložených souborů (OLE). Obdobně komprimovaných souborů (např. ZIP, RAR, 7z, ISO, GZ apod.). Možnost selektivního nastavení úrovně kontroly vnořených vložených/komprimovaných souborů (např. vnoření až do 5té úrovně). Různá nastavení pro sken v reálném čase a pro plánovaný sken.	ANO
15	Nástroje pro odezvu na zjištěné infikované koncové zařízení, vč. ad-hoc spuštěného skenu, odpojení koncového zařízení od sítě (izolace), spuštění remote shell přístupu (vč. podpory powershell a shell skriptů). Vypnutí uživatelského účtu a resetování uživatelského hesla v identitním systému (integrace s Active Directory, Entra).	ANO
16	Analytika k vizualizaci EDR/XDR vyšetřování k určení vstupního bodu průniku malware / útoku do organizace. Zobrazení interaktivního grafu s objekty (minimálně zařízení, uživatel, použitý proces a příkaz ve skriptu) včetně výpisu detailů údajů z telemetrických dat. Možnost zobrazit pohled vše najednou a sekvenčně dle průběh u události v čase. Možnost přímo z vizualizovaného grafu	ANO

ID	Požadované parametry	Splněno
	konstruovat strukturovaný vyhledávací dotaz (query) na hledaný údaj nebo jejich kombinaci.	
17	Schopnost blokovat útoky bez ohledu na to, zda jsou webové, e-mailové, nebo z vyměnitelného média. V případě webového provozu musí ochrana chránit proti webům, které jsou kategorizovány jako nebezpečné a podezřelé. V případě vyměnitelných médií musí být možné vydefinovat seznam výměnných médií, které jsou organizací považovány jako důvěryhodné (oproti zbytku povolené).	ANO
18	Ochrany proti technikám moderních útoků na základě aktuálního MITRE ATT&CK frameworku, ochrana musí identifikovat pokusy z pohledu útočných taktik a technik a poskytnout analytické nástroje pro jejich vyšetření.	ANO
19	Schopnost detekovat a zabránit neznámým (zero-day) útokům kombinací strojového učení, analýzy chování programového vybavení a vyhodnocením podezřelých souborů v cloudovém sandboxu. V případě sandboxu požadovány pro test detonace malware/sktiptů apod. alespoň dva různé OS, z toho minimálně to musí být alespoň OS Windows 10.	ANO
20	Podpora vyhodnocení (v sandboxu) spustitelných souborů, archivů, dokumentů (Office, PDF apod.), a Java souborů. Výsledek určí, zdali je testovaný soubor neškodný či nebezpečný, současně s výsledkem je automaticky generován podrobný report (webová forma a generovaný PDF soubor pro stažení). Nalezené nebezpečné artefakty jsou v reportu oproti zbytku zvýrazněny (jinak zbarveny či zvýrazněny).	ANO
21	Ochrana zabránění identifikovaných „command & control“ komunikací (identifikovaných botnet kanálů) na základě vzorků provozu z globální inteligence výrobce. Součástí je i vysvětlující detail, o co se jedná.	ANO
22	Ochrana proti ransomware útokům zabráněním spuštění šifrování (terminace procesu), včetně automatické obnovy postižených souborů, pakliže byly prvotní soubory již zašifrovány.	ANO
23	Ochrana proti nebezpečným nebo nepovoleným programům v organizaci. Výrobce musí do agentů automaticky distribuovat seznam široce rozšířených programů a jejich posledních verzí z jeho globální inteligence, na jejich základě nastavené politiky může agent uživatelům zakazovat/povolovat jejich použití (např. zakazovat nástroje na prolomení hesel nebo logování stisku tlačítek klávesnice).	ANO
24	Využití strojového učení k ochraně proti novým variantám malwaru s využitím globální informace výrobce (např. globálně byl identifikován/analyzován útok xy, který je svými symptomy podobný lokálně identifikovanému útoku).	ANO
25	Uživatel může prostřednictvím instalovaného agenta provádět (ad-hoc) vlastní skeny k nalezení malware ve svých zařízeních na úrovni jejich disků, adresářů nebo souborů.	ANO
26	Funkce personálního firewall u agentu, který může být nastaven do detekčního nebo prevenčního režimu, volba příslušné politiky může být automaticky volena podle toho, zdali je koncové zařízení zapojeno uvnitř organizace nebo je umístěno mimo ní (např. práce z domova, pracovní cesta / externí jednání).	ANO
27	Funkce detekce a prevence útoků (IDS/IPS), který může být nastaven do detekčního nebo prevenčního režimu. Seznam a aktualizace pravidel výrobce automaticky distribuuje do agentů na základě své globální inteligence, použití na základě nastavené politiky správcem.	ANO
28	Funkce forenzní analýzy k vyhodnocení napadeného koncového zařízení, správce v centrální konzoli získá nástroje centrálního vyšetřování, archiv k ukládání důkazů a prostředí spolupráce v incident response týmu. Může provést akce typu získání informací, vypsání stavu a údajů koncového zařízení (např. běžící služby a procesy,	ANO

ID	Požadované parametry	Splněno
	routovací tabulky), obraz RAM paměti, obsaženy dotazovací nástroje na základě standardizovaných prostředků Osquery a YARA rules.	
29	Zajištění bezpečného logování bezpečnostních událostí z cloudové platformy a jejích ochran do lokálních technologií zpracovávajících logy (LM/SIEM) nalézajících se uvnitř organizace a to bez rizikového neomezeného prostupu z cloudových služeb v internetu směrem do interních sítí organizace.	ANO
30	Interaktivní přehledný dashbord součástí centrální konzole správy, ve kterém bude zobrazen trend zabezpečení organizace v čase, včetně výkyvů z pohledu zjištěných bezpečnostních událostí (malware, EDR/XDR, webové, technické zranitelnosti a jiné).	ANO
31	Telemetrická data EDR/XDR obsahují minimálně informace o spuštěných procesech, síťových spojení a čtecích a zápisových operacích při práci se soubory. Dále jsou obohaceny o identity koncových zařízení a uživatelů. V případě detekcí bezpečnostních událostí a jejich analýzy jsou tyto údaje odlišeny (zvýrazněny či zbarveny) od ostatních běžných telemetrických dat.	ANO
32	Obsažena základní funkce threat inteligence výrobce, ochrana pak ověřuje, zdali pokrytá koncová zařízení nejsou zasažena globální kampaní útočníků na základě IoC poskytnutých výrobcem v rámci jeho globální inteligence (IoC Sweeping).	ANO
33	Možnost automaticky generovat předpřipravené reporty o stavu ochrany a výčtu bezpečnostních událostí za časové období. Ty pak posílat správcům emailem.	ANO
34	Obsažena ochrana mobilních zařízení (mobily a tablety), ochrana proti malwaru cílenému na mobilní platformy. Především OS Android.	ANO
35	Schopnost chránit mobilní zařízení před útoky na přenášený provoz. Především ochrana při použití neověřených WiFi sítí, možnost zajištění skrytí provozu prostřednictvím VPN brány výrobce v cloudu, podpora SSL inspekce ke kontrole obsahu webového provozu.	ANO
36	Možnost definice politiky pro mobilní aplikace, ty kategorizovat podle jejich reputace, např. zakazovat aplikace, které jsou rizikové.	ANO
37	Detekce konfiguračních nedostatků („rooting“ a „jailbraking“) mobilních zařízení.	ANO
38	Funkce webové kontroly pro mobilní zařízení opět s členěním kategorizací na nebezpečné, podezřelé stránky (jako u desktopů a serverů).	ANO
39	Schopnost detekovat a zabránit phishingu na základě globální inteligence výrobce.	ANO
40	Podpora blokování stahovaného souboru ve webovém prohlížeči, pakliže má daný soubor nebo URL špatnou reputaci, na základě globální inteligence výrobce.	ANO
41	Centrální správa bezpečnostních politik a nastavení agentů (servery, desktopy a mobily). A to prostřednictvím společné centrální konzole správy.	ANO
42	Výrobce umožňuje centrální ukládání vzniklých událostí (alertů apod.) v centrální cloudové konzoli, alespoň po dobu jednoho roku.	ANO
43	Komunikace agentů s centrální konzolí výrobce je bezpečná (autentizovaná a šifrovaná silnou kryptografií). Síla použitých krypto algoritmů je výrobcem dokumentovaná.	ANO
44	Integrace s identitními systémy lokální Active Directory a cloudová Entra k doplnění identit zařízení a uživatelů k obohacení výstupů. Je např. zřejmé, zdali jsou všechna koncová zařízení patřičně pokryta ochranou, pakliže některá nejsou, tak která. Obdobně integrace pro centrální ověřování správců prostřednictvím 2FA/MFA.	ANO
45	Možnost přejímat Active Directory skupiny pro konstrukci skupin koncových zařízení.	ANO
46	Schopnost vytvářet politiky na úrovni koncových zařízení, jejich skupin, či přiřazením specifických atributů prostřednictvím tagů či labelů.	ANO
47	Přehled stavu ochrany koncového zařízení (verze bezpečnostní politiky, verze OS, verze agenta, verze komponent ochran), viditelnost, jak z pohledu centrální	ANO

ID	Požadované parametry	Splněno
	cloudové konzole, tak z pohledu GUI agenta. Soulad a nesoulad graficky zobrazen a reportován.	
48	Výrobce a jeho cloudová služba je patřičně certifikována s doložením shody minimálně s ISO 27001 a SOC2 Type 2.	ANO
49	Sběr údajů do cloudu výrobce je v souladu s evropskou regulativou (GDPR), datové centrum je na území EU, výrobce jasně veřejně deklaruje, které údaje zpracovává a za jakým účelem.	ANO
50	Možnost využití zabezpečeného REST API, včetně dokumentovaného použití, kdy výrobce jasně vede uživatele k jeho požití pro automatizaci. Podpora pro snadné generování kódu pro API volání do knihoven v Python a Java.	ANO
51	Podpora řízení přístupu správců k funkcím správy a datům na základě RBAC.	ANO
52	Podpora integrace s globálně rozšířenými nástroji SIEM, SOAR. Cloudová konzole musí mít předpřipravené ke snadné integrace s nimi.	ANO
53	Možnost integrace s MDM systémy 3tích stran pro správu mobilních platforem (Intune, AirWatch).	ANO
54	Podpora zařízení typu BYOD a firemních zařízení.	ANO
55	Podpora aktuálních internetových prohlížečů Microsoft Edge, Google Chrome, Mozilla Firefox apod. pro bezchybný přístup k centrální cloudové konzoli.	ANO
56	Podpora OS serverů a koncových stanic k instalaci agentů ochran nejméně pro tyto systémy: Windows desktopy: - Windows 10 a 11 - Windows 7 SP1, 8 (minimálně funkce ochran, s omezenou telemetrií či bez telemetrie) Windows servery: - Windows Server 2012 R2, 2016, 2019 a 2022 MacOS: - 10.15 (Catalina) - 14.0 (Sonoma) Linux: - Centos 6, 7 a 8 - Debian 9, 10 a 11 - Ubuntu 16, 18, 20, 21, 22 - RHEL 7, 8 - OracleLinux 6, 7, 8, 9 - Rocky Linux 8, 9 - SLES 12, 15 Podpora Secure Boot v agentech.	ANO
57	Podpora aktuálních OS Android (8 a výše) a iOS/iPadOS (13 a výše) – v případě mobilních platforem.	ANO
58	Retence veškerých telemetrických dat alespoň po dobu 30 dní.	ANO
59	Požadovaná licence musí pokrýt nejméně 500 koncových zařízení (PC, NB) a 20 mobilních zařízení (chytrý telefon, tablet apod).	ANO
60	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.8.1 Technická specifikace prostředí pro běh management a bezpečnostních prvků

(1) S ohledem na požadovaný výkon a funkce bezpečnostních platforem je nezbytné vytvořit nezávislé prostředí pro běh management nástrojů. Je požadováno dodání 2ks virtualizačních serverů a blokové diskové úložiště pro zajištění jejich vysoké dostupnosti.

(2) Požadované licence pro technologii VMware a Veeam se vztahují výhradně k novým prvkům a musí zapadnout do stávajícího prostředí, které je postaveno na těchto produktech:

VMware vSphere, vSAN, vCenter server na několika platformách ve verzích Standard příp. Enterprise edition

Veeam Data Platform Foundation Standard Edition

(3) **Minimální požadavky** na technickou specifikaci 2 ks serverů jsou uvedeny v následující tabulce. (platí pro jeden server)

Id	Požadované parametry	Splněno
1	montáž do standardního 19“ racku o maximální výšce 1 RU, chassis pro min. 8x 2,5“ disků	ANO
2	minimálně jeden 16-jádrový procesor s hodnotou dle a SPECrate®2017 floating point speed base minimálně 180 pro 1 CPU konfiguraci (údaje musí být k dispozici pro daný server a CPU na www.spec.org)	ANO
3	min. 512 GB RAM	ANO
4	min. 2x 480GB NVMe RAID1 úložiště nevyužívající 2,5“ diskovou pozici	ANO
5	min. 4x 1GbE RJ-45 porty	ANO
6	min. 6x 10/25GbE SFP28 porty na třech nezávislých síťových kartách	ANO
7	management serveru nezávislý na operačním systému s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence	ANO
8	management musí podporovat dvoufaktorovou autentikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP, podpora Silicon Root Of Trust, Secure Boot a TPM 2.0	ANO
9	pro management požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, REDFISH	ANO
10	nejméně 2 redundantní, za chodu vyměnitelné napájecí zdroje s platinovou účinností min. 800W každý	ANO
11	rackové ližiny a rameno na kabeláž na zadní straně serveru	ANO
12	dodání včetně 4x SFP28 25Gb twinaxial kabelů o délce 3m pro každý server	ANO
13	certifikace pro VMware 6.7u3 a vyšší, Windows Server 2016 a vyšší, Red Hat Enterprise Linux a SUSE Linux Enterprise Server	ANO
14	pro oba servery dohromady dodání 1x licence VMware vSphere Essentials Plus na všechna CPU jádra s podporou na 5 let	ANO
15	Zálohovací SW Veeam Data Platform Foundation na všechna CPU socket s podporou na 5 let	ANO
16	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

(4) **Minimální požadavky** na technickou specifikaci 1 ks blokového diskového úložiště jsou uvedeny v následující tabulce.

Id	Požadované parametry	Splněno
1	montáž do standardního 19“ racku o maximální výšce 4 RU	ANO
2	diskové pole musí být typu All Flash - NVMe pole s disky podporujícími PCI Gen4 technologii.	ANO
3	podpora aktuální verze nejpoužívanějších OS min. VMware vSphere 8.0, Windows 2022, RedHat Linux 9, Ubuntu 22.04.	ANO
4	diskové pole musí poskytovat min.hrubou (RAW) kapacitu 45TB. Tato kapacita bude očištěna o systémovou a spare kapacitu a s využitím technik datové redukce bude dostupná kapacita pro ukládání dat alespoň 60TB. Tato kapacita diskového	ANO

Id	Požadované parametry	Splněno
	pole musí být v budoucnu rozšiřitelná alespoň na dvojnásobek. (v rámci základního šasi nebo přidáním diskových polic)	
5	diskové pole musí být flexibilně škálovatelné tj.podporovat škálování scale-up přidáváním NVMe diskových polic i scale-out pomocí zabudovaného klastrování.	ANO
6	Nabízené pole musí být škálovatelné alespoň na 24 NVMe disků v rámci základního šasi a musí být v budoucnu rozšiřitelné min. na dvojnásobek počtu disků v přídavných NVMe diskových policích (celkem tedy min. 48 NVMe disků).	ANO
7	V případě scale-out rozšiřování musí být možné rozprostřít LUNy přes všechy řadiče škálovatelného úložiště.	ANO
8	diskové pole musí být dodáváno s nejméně 64GB cache na jeden řadič pro operace čtení a zápisu.	ANO
9	operace zápisu musí být zcela chráněny a v případě výpadku napájení nesmí dojít ke ztrátě dat. Tento mechanismus se nesmí spoléhat na baterie.	ANO
10	diskové pole nesmí obsahovat Single Point Of Failure tj.musí být odolné min.proti výpadku jedné komponenty typu řadiče, zdroje, cache, ventilátoru, HBA apod.	ANO
11	výpadek žádné komponenty včetně řadiče diskového pole nesmí způsobit pokles požadovaného výkonu pole.	ANO
12	během kritických podpůrných činností, jako je aktualizace Firmwaru, aplikaci patche atd., musí být pole dostupné a nesmí dojít k degradaci výkonu.	ANO
13	diskové pole poskytuje na front-end portech diskového pole min. takovýto ustálený výkon: 55 tis.IOPS pro 100% random zátěž, velikost bloku 8kB a poměr čtení zápis 50/50. 2GB/s sekvenční čtení a 700MB/s sekvenční zápis při velikosti bloku 256kB.	ANO
14	diskové pole musí být odolné proti výpadku až tří disků současně. V případě, že to výrobce nepodporuje, pak RAID pole musí mít velikost maximálně 6D+2P	ANO
15	diskové pole musí být možné povýšit na novější generaci výměnou řadičů, aniž by bylo nutné měnit disky a případné diskové police.	ANO
16	Povýšení na novější generaci musí být možné provést bez odstávky diskového pole	ANO
17	diskové pole musí být dodáno min. s dvěma řadiči a 4x 25Gb IP porty. (každý front-end PCI slot musí mít nejméně 8 linek PCI Gen4)	ANO
18	diskové pole musí mít také podporu pro 100Gb ETH porty (pro případné rozšíření)	ANO
19	diskové pole musí podporovat nastavení Quality of Services (QoS) na úrovni LUN nebo VMware vVol s granularitou nastavení min. na úrovni IOPS a MB/sec.	ANO
20	diskové pole musí podporovat tyto funkce - inline de-duplikace, komprese a thin provisioning	ANO
21	diskové pole musí podporovat ne-deduplikované a duplikované LUNy současně	ANO
22	diskové pole musí podporovat synchronní i asynchronní replikaci dat mezi diskovými poli.	ANO
23	disková pole musí umět vytvořit jedno logické pole pro vytvoření storage geo-klastru s automatickým transparentním failoverem mezi lokalitami a funkcionalitou svědka na třetí lokalitě pro zabránění split-brain syndromu	ANO
24	diskové pole musí mít schopnost replikovat data z All Flash do Hybridního diskového pole, nebo naopak v rámci dané rodiny polí.	ANO
25	Prodejce poskytne licence pro všechny požadované funkce, jako je Snapshot, Clone, Replikace, QoS, management apod., pro celkovou kapacitu pole. Pro budoucí zvýšení kapacity nebude vyžadována žádná dodatečná softwarová licence. Jakákoli dodatečná licence vyžadovaná pro splnění technické specifikace musí být nabídnuta předem.	ANO
26	dodání včetně 4x SFP28 25Gb twinaxial kabelů o délce 3m	ANO

Id	Požadované parametry	Splněno
27	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO

5.9 Technická specifikace pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů

(1) Řešení nabídne univerzálně funkční SSO technologie pro jakékoli webové/desktopové/cloudové/virtualizované aplikace, která by pomohla výrazně snížit čas uživatelů potřebný k přihlašování do IT systémů a aplikací.

(2) **Minimální požadavk**y na technickou specifikaci pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
	Obecné požadavky	
01	Klientská část řešení musí podporovat Windows Desktop OS (Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy Windows a Android. Řešení musí licenčně pokrýt min. 1000 jmenovitých uživatelů.	ANO
02	Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry případně cloudy.	ANO
03	Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora minimálně VMware vSphere, Microsoft Hyper-V). Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora minimálně Microsoft Azure). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v datovém centru on premises a další virtuální stroj nebo stroje v cloudu, formou SaaS.	ANO
04	Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění.	ANO
05	Řešení musí být integrováno na adresářovou službu Microsoft Active Directory Directory Services (AD DS), identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Řešení nesmí modifikovat schéma Active Directory. Dodané řešení musí být možné integrovat na další adresářové (LDAP) služby. Řešení musí podporovat Security Assertion Markup Language 2.0 (SAML 2.0) a federaci s krajským řešením Vysočina ID.	ANO
06	Komunikace mezi jednotlivými komponentami řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data – zejména přihlašovací údaje uživatelů – musí být chráněna šifrováním AES 256.	ANO
	Více-faktorová autentizace	

ID	Požadované parametry	Splněno
07	Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty včetně karet Mifare DesFire a FIDO, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu).	ANO
08	Řešení musí pro vybrané uživatele poskytnout funkci tzv. „Push“ autentizace a/nebo autentizace pomocí OTP (One-Time Password) pro přihlášení ke koncovým zařízením s Windows OS a do VPN prostřednictvím mobilní aplikace (podporované mobilní OS: minimálně Android a iOS).	ANO
09	Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla např. v Active Directory). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111“ a jednoduchou číselnou řadu, jako např. „1234“).	ANO
10	Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. Tato technologie musí podporovat nejběžnější produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon).	ANO
11	Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci.	ANO
12	Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s rozlišením alespoň fyzická stanice/virtuální desktop/server vzdálené plochy.	ANO
13	Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních karet i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení.	ANO
14	Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu.	ANO

ID	Požadované parametry	Splněno
	Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény.	
15	Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.	ANO
	Autentizační předměty	
16	Je požadováno dodání 100 ks autentizačních předmětů v provedení: 100 ks karta (velikost ID-1 dle ČSN ISO/IEC 7810)	ANO
17	Dodaná klíčenka a karta bude obsahovat minimálně následující bezkontaktní čipy: nízkofrekvenční 125 kHz EM4200 a vysokofrekvenční 13,56 MHz NXP MIFARE S50, 1kb).	ANO
18	Dodaná karta musí být ve velikosti bankovní karty, formát: ID-1, v provedení umožňující potisk karty.	ANO
19	Dodaná klíčenka musí být v provedení přívěsku, z materiálu, který zaručuje odolnost vůči mechanickému poškození a voděodolnost.	ANO
20	Je požadováno dodání 100 ks autentizačních prostředků pro čisté operační sály nebo pro izolované zóny.	ANO
21	Autentizační prostředek pro čisté operační sály nebo pro izolované zóny (např. náramek pod ochranný oděv) bude obsahovat bezkontaktní vysokofrekvenční čip 13.56 MHz, minimálně NXP MIFARE S50, 1kb pro dvou-faktorové přihlašování ke koncovým (klientským) zařízením. Je požadováno voděodolné provedení, potisk náramku: Logo organizace a pořadové číslo prostředku.	ANO
	Čtečky karet	
22	Je požadováno dodání 600 ks stolních čteček s USB rozhraním pro připojení k PC	ANO
23	Požadované parametry stacionárních čteček bezkontaktní části karty, které v současnosti nemocnice používá: – Pracovní frekvence: 13,56 MHz – Podpora bezkontaktních karet/předmětů: rodina NXP Mifare® – Rozhraní: připojitelná přes USB – Typ: externí – Napájení: přes USB rozhraní – Formát: stolní – Přenos dat: zabezpečený, přes API (nesmí simulovat stisky kláves) Kompatibilita OS: Windows 10 a vyšší	ANO
	Single Sign-On (SSO)	
24	Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících aplikací: FONS Enterprise, FONS Openlims, FONS Akord Diet, FONS Medix, Anete Kredit, LEKIS. V případě webových aplikací musí být pro funkci SSO podporovány minimálně tyto prohlížeče: Microsoft Edge Chromium verze 110 a vyšší, Google Chrome verze 110 a vyšší. Dále musí být pro webové aplikace podporována autentizace pomocí protokolu SAML a pomocí OpenID Connect.	ANO
25	Řešení musí poskytovat funkci Single Sign-On do aplikací FONS Enterprise, FONS Openlims, FONS Akord Diet, FONS Medix, Anete Kredit, LEKIS) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli,	ANO

ID	Požadované parametry	Splněno
	a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény.	
26	Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, virtualizované aplikace, server vzdálené plochy. Řešení musí poskytnout plnou funkčnost SSO pro nejběžnější technologie virtualizace aplikací a desktopů na trhu (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon).	ANO
27	Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli Přihlašovací údaje do jednotlivých aplikací a systémů jsou šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické aplikace bylo přihlášení pomocí SSO vynucováno.	ANO
28	Řešení musí umožnit funkci SSO přihlašování do aplikací jak identitou (účtem) z Active Directory, tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP), kdy neuchovává přihlašovací údaje uživatelů.	ANO
29	Řešení bude obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.).	ANO
30	Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací.	ANO
31	Podpora celého řešení na 5 let. Záruka na dodaný HW /čtečky, autentizační předměty 2 roky.	ANO
Samoobslužný reset hesla		
32	Řešení musí poskytnout integraci na funkci samoobslužný reset hesla Active Directory účtu a musí umožnit vyvolání této funkce z přihlašovací obrazovky klientské stanice, bez nutnosti se předem přihlásit.	ANO

6. Fáze A - Instalace a implementace

(1) Instalace a implementace technologií popsaných v kapitolách 5.1 až 5.9 bude provedena v jednotlivých požadovaných krocích a termínech uvedených v kapitole **Chyba! Nenalezen zdroj odkazů.**.

(2) Požadavky na Instalaci a implementaci technologií jsou uvedeny v následující tabulce.

Id	Rozsah plnění členěný podle kapitol 5.1 až 5.9
5.1 Centrální Firewally	
01	Technický návrh
02	Fyzická instalace FW, instalace centrálního MGMT serveru do virtuálního prostředí, úvodní síťová konfigurace.
03	Segmentace interní LAN
04	Tvorba bezpečnostních politik a migrace stávajících pravidel. Počet bezpečnostních politik dosahuje řádově desítek. Každá bezpečnostní politika má řádově desítky pravidel.
05	Integrace se zdrojem identit (AD, LDAP, Radius…)
06	Rekonfigurace routingu a změna default GW na testovací skupině sítí
07	Kompletní rekonfigurace routingu a migrace klientů do nových subnetů
08	Implementace Threat prevention funkcionalit a politik
09	Fáze ladění
10	Dokumentace skutečného provedení.
5.2.1 Centrální správa logů	
01	Instalace systému jako virtuálního stroje do VMW infrastruktury zadavatele a nastavení management komunikace.
02	Konfigurace síťových rozhraní LM.
03	Vytvoření záznamů v DNS.
04	Napojení LM na AD a vytvoření skupin pro přístup.
05	Dle dokumentu „Detailní realizační projekt“.
06	Nastavení email komunikace.
07	Úprava nastavení Windows auditu na doménových serverech a řadičích.
08	Instalace agenta log manageru na servery. (pokud je potřeba)
09	Individuální nastavení serverů s extra logováním typu DHCP, IIS, Exchange.
10	Napojení LM na Vmware. Součinnost poskytuje zadavatel.
11	Napojení LM na O365. Technické řešení musí být realizováno pomocí API bez instalace dalších komponent. API musí umožnit třídění logů podle jednotlivých aplikací v rámci O365.
12	Nastavení syslog na síťových zařízeních typu Switch, firewall, AP. Úpravy úrovně logování jsou v kompetenci zadavatele.
13	Nastavení klasifikace logů dle zařízení a zařazení do prefixlistů.
14	Doplnění LM do další dashboardy pro snažíš správu Windows serverů.
15	Nastavení základních alertů.
5.2.2 Monitorování sítí na bázi datových toků (NetFlow/IPFIX)	
01	Technický návrh zapojení.
02	Konfigurace a nastavení síťových rozhraní.
03	Instalace a konfigurace virtuálního kolektoru.

Id	Rozsah plnění členěný podle kapitol 5.1 až 5.9
04	Nastavení uživatelských účtů.
05	Konfigurace kvót datových uložišť pro jednotlivé moduly.
06	Nastavení monitoring centra a profilů, vestavěného kolektoru a pole databáze toků.
07	Konfigurace dashbordů a reportů.
5.2.3 Automatické vyhodnocování datových toků (NetFlow/IPFIX)	
08	Nastavení modulu ADS, konfigurace zdrojů dat, základní filtry IP rozsahů a nastaví implicitní parametry detekčních metod, IP rozsahy a veřejné adresy
09	Dokumentace skutečného provedení
5.3 Zavedení segmentace sítě	
01	Instalace a konfigurace dvou VM boxů do clusteru.
02	Instalace posledního stabilního firmware.
03	LDAP připojení do domény.
04	Instalace/konfigurace certifikační autority.
05	Vytvoření templates na certifikační autoritě pro klienty a nastavení automatické instalace pro zařízení v doméně.
06	Vydání certifikátu pro RADIUS.
07	Revize zapojených zařízení v síti LAN a WLAN.
08	Vytvoření ověřovací matice – definice ověřování uživatelů, zařízení, jejich kombinace, druh autentikační metody a přiřazení definovaných rolí na základě splnění autorizačního procesu.
09	Konfigurace podmínek ověřovacích služeb.
10	Konfigurace a ověřování přístupu hostů do izolované sítě.
11	Distribuce nastavení suplikanta pro zařízení ověřovaná metodou 802.1x.
12	Ruční nastavení suplikanta a nahrání certifikátu pro zařízení, u kterých nelze toto zajistit pomocí hromadné distribuce.
13	Konfigurace přístupových switchů a AP – definice ověřovacích serverů a služeb, konfigurace DHCP relay a konfigurace portů či ESSID.
14	Ověření funkčnosti na vybraném vzorku zařízení a uživatelů.
15	Po ověření funkčnosti kompletní nasazení pro celou síť.
16	Dokumentace skutečného provedení.
5.4 DLP	
01	Určení vhodných typů dat (údajů) organizace k ochraně prostřednictvím DLP.
02	Aktivace licencí a aktivace funkcí ochrany DLP ve webové konzoli nástroje.
03	Úprava výchozích politik a pohledů a reportů.
04	Nasazení DLP ochrany na vybranou testovací skupinu uživatelů.
05	Vyhodnocení událostí, analýza provozu.
06	Ladění DLP politik vč. ladění klasifikace dat.
07	Ověření laděných politik na testovací skupině uživatelů.

Id	Rozsah plnění členěný podle kapitol 5.1 až 5.9
08	Postupné rozšiřování DLP ochrany a politik na zbytek uživatelů.
09	Dokumentace skutečného provedení.
5.5 Úložiště pro PACS a NIS data formou NAS a S3	
01	Technický návrh řešení, design nasazení
02	HW instalace 4ks storage nodů
03	Fyzické zapojení úložiště do síťového prostředí
04	Konfigurace OOB managementu
05	Instalace OS/SW/firmware v dohodnuté verzi
06	Konfigurace storage clusteru, IP adresace
07	Konfigurace vzdáleného dohledu
08	Připojení k LDAP
09	Konfigurace práv uživatelských/administrátorských účtů
10	Konfigurace sdílených adresářů/namespace a práv k nim
11	Připojení úložiště k systémům, které budou toto úložiště využívat
12	Testovací nasazení
13	Výkonnostní testy (zálohy, souborové servery atp.)
14	Produkční nasazení
15	Dokumentace skutečného provedení.
5.6 Infrastruktura pro zálohování a rychlou obnovu	
01	Technický návrh řešení, design nasazení
02	HW instalace 1ks zálohovacího serveru a 1ks páskové knihovny
03	Fyzické zapojení zálohovacího serveru a páskové knihovny do síťového/SAN prostředí
04	Instalace OS/SW/firmware v dohodnuté verzi
05	Konfigurace operačního systému, systémová nastavení
06	Konfigurace OOB managementu
07	Instalace zálohovacího software
08	Konfigurace práv uživatelských/administrátorských účtů
09	Konfigurace komponent zálohovacího software (backup server, proxy, dohled)
10	Integrace s úložišti záloh
11	Integrace zálohovacího software s primárním prostředím (virtualizace, úložiště)
12	Definice zálohovacích / archivačních úloh
13	Testovací nasazení
14	Výkonnostní a funkční testy (zálohy, archivace, obnovy)
15	Produkční nasazení
16	Dokumentace skutečného provedení.

Id	Rozsah plnění členěný podle kapitol 5.1 až 5.9
5.7 Zvýšení dostupnosti záložního datového centra a lokální sítě	
01	Fyzická instalace a konfigurace dvou HW controllerů do clusteru v režimu active-active, který zajistí předávání session a patřičných licencí
02	Instalace posledního stabilního firmware
03	Návrh a konfigurace mikrosegmentace mezi gateway a koncovým prvkem (switch/AP). Integrace s RADIUS serverem
04	Ověření funkčnosti na vybraném vzorku zařízení a uživatelů
05	Po ověření funkčnosti kompletní nasazení pro celou síť
06	Dokumentace skutečného provedení
5.8 Ochrana operačních systémů a mobilních platforem	
01	Tvorba bezpečnostních politik v centrální webové konzoli
02	Integrace se zdrojem identit (AD)
03	Distribuce a instalace SW klientů na testovací skupinu stanic a testování
04	Kompletní nasazení agentů včetně systému EDR/XDR
05	Ladění politik a nastavení
06	Dokumentace skutečného provedení
5.9 Přihlašování k počítačům a aplikacím v rámci klinických a THP provozů	
01	Technický návrh
02	Instalace a konfigurace infrastrukturních části
03	Integrace požadovaných aplikací
04	Napojení adresářových služeb, synchronizace uživatelů
05	Vytvoření profilů uživatelů, koncových stanic, aplikací
06	Konfigurace pro mobilní zařízení
07	Migrace koncových stanic do Active Directory
08	Ladění, ověřování
09	Deployment, rollout
10	Dokumentace skutečného provedení

I. 6.1 Zpracování a akceptace Detailního realizačního projektu

(1) Dokument Detailní realizační projekt bude obsahovat minimálně:

a) definici cílového stavu, která bude vycházet z požadavků na budoucí stav, viz tento dokument,

b) akceptační kritéria cílového stavu;

pro ověření plnění Dodavatele v rámci Smlouvy jsou uvedena v tomto dokumentu, a to v tabulkách označených „Minimální požadavky …“, kde Dodavatel bude deklarovat svoji připravenost poskytovat bezvadné plnění již v rámci Zkušebního (testovacího) provozu.

c) detailní harmonogram realizace zakázky, který vychází z milníků uvedených v kapitole 3

(2) **Předání a převzetí Detailního realizačního plánu bude provedeno** vzájemně odsouhlaseným Předávacím protokolem realizačního plánu (Dodavatel předává dokument Detailní realizační **„Kybernetická bezpečnost Nemocnice Pelhřimov“** reg. č. CZ.06.01.01/00/22_004/0000177

projekt) a Akceptačním protokolem realizačního plánu, kterým Zadavatel akceptuje splnění podmínek.

II. 6.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)

6.6.1 Předání a převzetí dokumentů

(1) Dokumenty, které mají být vypracovány Dodavatelem a které se poskytují Zadavateli jako součást poskytování díla (zejména Detailní realizační koncept), budou nejdříve předloženy Zadavateli ve formě návrhu k posouzení.

(2) Dodavatel se zavazuje předat první verzi dokumentu Zadavateli k akceptaci ve lhůtě domluvené mezi Dodavatelem a Zadavatelem na základě Smlouvy, nebo jinak stanovené v souladu se Smlouvou.

(3) Zadavatel je oprávněn ve lhůtě deseti (10) pracovních dnů od doručení příslušného dokumentu písemně předložit Dodavateli své připomínky k návrhu.

a) Po diskusi o těchto připomínkách upraví Dodavatel příslušný návrh v souladu s dohodnutými změnami a se zapracováním těchto dohodnutých změn jej předá ve stejné lhůtě deseti (10) pracovních dnů Zadavateli.

b) V případě, že Zadavatel nemá k předaným dokumentům výhrady, považují se za převzaté k okamžiku doručení jejich konečné verze Zadavateli.

c) V případě, že Zadavatel připomínky ve lhůtě deseti (10) dnů nepředloží, má se za to, že s předloženým dokumentem souhlasí a dokument se považuje za řádně převzatý.

6.2.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)

(1) V případě, že součástí poskytování plnění Dodavatelem dle Smlouvy je plnění, které podléhá akceptaci Zadavatelem, musí dojít k podpisu Předávacích protokolů ohledně tohoto plnění v termínech uvedených v harmonogramu, není-li výslovně uvedeno jinak.

Zadavatel vybere klíčové funkce z výše popsaných technických parametrů a ty stanoví jako akceptační kritéria. Akceptace je možná pouze za předpokladu, že akceptační kritéria budou splněna bez dalších výhrad.

Jestliže plnění nebo jeho jednotlivé části splní kritéria akceptačního řízení, považují se za řádně ukončené a Zadavatel je povinen jej převzít.

(2) Akceptační procedury zahrnují porovnání skutečných vlastností plnění se závaznou specifikací předmětu plnění dle Smlouvy.

a) Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů obsahující popis testů, testovací data, příslušné prostředí, pořadí provádění testů a akceptační kritéria.

Nedohodnou-li se smluvní strany jinak, vypracuje specifikaci akceptačních testů Dodavatel a předá Zadavateli k odsouhlasení v termínu deseti (10) pracovních dnů před zahájením akceptační procedury dle harmonogramu.

Odsouhlasení bude provedeno písemnou formou v termínu deseti (10) pracovních dnů před zahájením akceptační procedury. Jestliže se Zadavatel v této lhůtě ke specifikaci akceptačních testů písemně nevyjádří, má se za to, že specifikaci akceptačních testů odsouhlasil.

Jestliže Zadavatel specifikaci akceptačních testů v uvedené lhůtě neodsouhlasil, je povinen Zadavatel v této lhůtě sdělit připomínky k Dodavatelem předložené specifikaci akceptačních testů a poskytnout Dodavateli veškerou potřebnou součinnost k dokončení a odsouhlasení specifikace akceptačních testů.

Lhůta pro provedení akceptačních testů a lhůta pro předání plnění nebo jeho části se prodlužuje o dobu, o kterou se prodloužilo písemné odsouhlasení specifikace akceptačních testů z důvodu připomínek na straně Zadavatele oproti lhůtě stanovené.

b) Dodavatel bude písemně informovat Zadavatele, resp. jeho oprávněné osoby nejméně deseti (10) dní předem o termínu zahájení akceptačních testů.

Zadavatel je oprávněn se těchto testů zúčastnit a osvědčit jejich konání, a to formou předávacího protokolu (nebo dílčích předávacích protokolů), podepsaného (podepsaných) oprávněnými osobami obou smluvních stran. Pokud se Zadavatel nedostaví v termínu určeném pro provedení akceptačních testů, ačkoli byl s tímto termínem řádně seznámen, je Dodavatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti.

Takto provedené akceptační testy se považují za provedené v přítomnosti Zadavatele. Kopie veškerých dokumentů vypracovaných v souvislosti s provedením těchto akceptačních testů budou Zadavateli poskytnuty do deseti (10) dnů.

c) Základním předpokladem pro řádné předání plnění (nebo jeho části) Dodavatelem a převzetí tohoto plnění (nebo jeho části) Zadavatelem, a to formou předávacího protokolu podepsaného oprávněnými osobami obou smluvních stran je skutečnost, že plnění splní kritéria akceptačních testů uvedená v dohodnutých kontrolních specifikacích a bude provedeno v souladu se závaznou specifikací předmětu plnění dle Smlouvy.

d) Jestliže plnění nebo jeho část splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje v den následující po ukončení akceptačních testů umožnit Zadavateli plnění nebo jeho část převzít a Zadavatel se zavazuje v tomto termínu plnění nebo jeho část převzít.

Pokud Zadavatel plnění nebo jeho část v tomto termínu nepřevezme, ačkoli převzetí plnění nebo jeho části bylo Dodavatelem řádně umožněno, má se za to, že plnění nebo jeho část bylo řádně předáno a Zadavatelem převzato právě v den následující po ukončení akceptačních testů.

e) Jestliže plnění nesplňuje stanovená akceptační kritéria kteréhokoliv akceptačního testu, budou výsledky akceptačního testu (splněno/nesplněno/s výhradami) spolu s uvedením termínů pro nápravu uvedeny ve vyhodnocení Akceptačního protokolu.

Dodavatel napraví tyto nedostatky a příslušné akceptační testy budou provedeny znovu.

Tento proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně.

Proces testování a následných oprav lze opakovat, dokud Dodavatel nesplní veškerá akceptační kritéria pro příslušný akceptační test, nejvýše však natřikrát (3x).

V situaci, kdy by bylo nutné opakovat akceptační testy více jak třikrát (3x) pro konkrétní fázi projektu, je v takovém případě nutný souhlas nadřízeného orgánu projektu – tzn. řídícího výboru nebo ředitelů projektu dle použité metodiky řízení projektu.

f) Žádný akceptační test se však nebude považovat za nesplněný, jestliže daný nedostatek nebyl způsoben Dodavatelem, nebo byl zjištěn nebo měl být zjištěn Zadavatelem před nebo při předcházejícím akceptačním testu, ale nebyl v té době oznámen Dodavateli, nebo byl nepodstatný, tzn., neměl vliv na řádné poskytování funkčnost díla nebo jeho části tak, jak jsou vymezeny ve Smlouvě.

g) Při převzetí plnění nebo kterékoliv jeho části v souladu s tímto článkem je Zadavatel povinen podepsat potvrzení o přijetí plnění nebo dané části a Zadavatel i Dodavatel se zavazují podepsat příslušný předávací případně akceptační protokol (dílčí předávací případně akceptační protokoly), tj. potvrzení o předání a přijetí (převzetí) plnění nebo jeho určité části.

III. 6.3 Školení

(1) Dodavatel poskytne školení pro administrátory IS tak, aby byli schopni řádně užívat, respektive administrovat, instalované technologické části specifikované v kapitole 5. Rozsah školení bude 5 pracovních dnů pro nejvýše 5 technických specialistů Zadavatele. Zadavatel počet školených technických specialistů upřesní před provedením samotného školení. Zadavatel může rozhodnout o

dělení školení na 5 nespojitých setkání. Součástí školení bude vždy ukázka na dodávané technologii a teoretická část vysvětlující principy fungování technologie.

IV. 6.4 Dokumentace

(1) Dodaná dokumentace slouží k zachycení a vyhodnocování plánovaných činností a též k dokumentaci skutečného stavu.

7. Fáze B – servisní a provozní podpora dodaných technologií

(1) Požadavky, které musí dodavatel minimálně naplnit na servisní a provozní podporu dodaných technologií, jsou v níže uvedené tabulce.

Id	Plnění požadavku	Splněno
01	Dodavatel zajistí Helpdesk v režimu 24x7 bez přerušení. HelpDesk musí být možné kontaktovat pomocí telefonu, e-mailem a webového rozhraní s přehledem řešených požadavků. Helpdesk musí hovořit českým jazykem. Lhůty pro plnění ze strany Uchazeče jsou pozastaveny za předpokladu: a) Čekání na součinnost zákazníka b) Čekání na součinnost třetí strany (například výrobce HW nebo SW, či bug výrobce)	ANO
02	Veškeré požadavky budou evidovány v systému servisní podpory Dodavatele nebo výrobce zařízení (HelpDesk).	ANO
03	Kontaktní místo umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím služby HelpDesk, popř. služby Hot-line.	ANO
04	Služba HelpDesk umožní Zadavateli upřesnit nebo doplnit požadavek.	ANO
05	Služba HelpDesk bude Zadavateli poskytovat přehled o aktuálně nahlášených požadavcích, jejich stavu a aktuálním způsobu jejich řešení. Služba HelpDesk bude Zadavateli zasílat notifikace o změně stavu jeho požadavku (např. zadaný, v řešení, uzavřený atd.) a musí Zadavateli umožnit schvalování uzavření nahlášeného požadavku.	ANO
06	Služba HelpDesk bude poskytovat Zadavateli přístup i k uzavřeným požadavkům a způsobu jejich řešení, bude poskytovat podrobné údaje o historii požadavků od jejich nahlášení, po jejich vyřešení.	ANO
07	Dodavatel zajistí podporu certifikovaných expertů v režimu 24x7. Technické specialisty musí být možné kontaktovat pomocí oddělení Helpdesk. Podpora bude obsahovat tyto technologické pohotovosti: a) Kybernetická bezpečnost b) Síťové prvky c) Technologie Datových center d) Nástroj zajišťující přihlašování k počítačům v rámci klinických a THP provozů e) Technologie společnosti Microsoft (na které spoléhají jednotlivé produkty) každá pohotovost v každé oblasti musí být držena nejméně čtyřmi certifikovanými technickými specialisty na dodávané technologie. Jeden technický specialista může být členem nejvýše dvou pohotovostí. Technická certifikace musí odpovídat požadavkům na technickou kvalifikaci dle Zadávací Dokumentace.	ANO
08	Technická podpora je poskytována s rozpočtem dvou člověkodní měsíčně. V případě nevyužití služby jsou nevyužité dny převáděny do dalších měsíců v rámci kalendářního roku.	ANO

Id	Plnění požadavku	Splněno
09	Bude prováděna průběžná aktualizace dokumentace k programovému vybavení tak, aby u Zadavatele byla vždy aktuální dokumentace k provozované technologii.	ANO
10	Bude poskytována součinnost při zásadním upgrade softwarových částí instalované infrastruktury na vyšší verze.	ANO
11	Bude zajištěna udržitelnost SW třetích stran, dodaných Dodavatelem v rámci veřejné zakázky.	ANO
12	HW a SW maintenance výrobce budou poskytovány po celou dobu smluvního vztahu.	ANO
13	Technická podpora a servis zařízení HW a SW budou zabezpečeny Dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.	ANO
14	Technická podpora a servis budou realizovány v místě Zadavatele. Výjimku tvoří činnosti realizované vzdáleným připojením Dodavatele, výrobce zařízení do prostředí Zadavatele. Uchazeč musí disponovat vlastní provozní dokumentací, kolaborativním správcem hesel v souladu s Vyhláškou Zákona o Kybernetické Bezpečnosti. Provozní dokumentace Uchazeče musí být na vyžádání k dispozici Zadavateli online.	ANO
15	Dodavatel zajistí provozní monitoring všech dodávaných komponent po dobu poskytování služby. Monitorována budou následující: - U každé technologie alespoň jedna služba (nebo typ služby), která nejvíce odpovídá charakteru zařízení. (například u diskového pole pro nestrukturovaná data dostupnost single namespace apod.) - Alespoň jeden fyzický interface prokazující dostupnost zařízení. Monitorovací intervaly by měly být nastaveny podle charakteru služby v intervalu 5 vteřin a 5 minut. Monitorovací metoda nesmí zbytečně přetěžovat monitorovanou komponentu.	ANO

(2) V rámci zajištění podpory a servisu po dobu udržitelnosti projektu platí následující parametry SLA.

Definice stupňů závažnosti incidentů:

Závažnost Závady nebo Chyby		Definice závažnosti Závad a Chyb
A	**Kritická chyba**	Chyba způsobí, že poskytované řešení nelze zcela provozovat nebo má kritický vliv na provozované aplikace či stav podporovaného systému – vyžaduje okamžité řešení. Typická situace je výpadek všech i redundantních prvků poskytujících řešení. Za kritickou chybu se dále považuje situace, kdy poskytované řešení obsahuje ***bezpečnostní zranitelnost*** s **kritickou** mírou závažnosti.
B	**Provozní chyba**	Chyba, která ovlivňuje provozní vlastnosti, ale nebrání v užití poskytovaného řešení. Provozní chybou se rozumí výpadek pouze dílčí části poskytovaného řešení. Typická situace je výpadek jednoho z redundantních prvků, kdy jiný prvek je stále dostupný. Za provozní chybu se dále považuje situace, kdy poskytované řešení obsahuje ***bezpečnostní zranitelnost*** se **střední** mírou závažnosti.
C	**Změnový požadavek nebo incident s nízkou mírou bezpečností zranitelnosti**	Požadavek na změnu konfigurace řešení, či konzultace. Za změnový požadavek se dále považuje situace, kdy poskytované řešení obsahuje ***bezpečnostní zranitelnost*** s **nízkou** mírou závažnosti.

Kategorie bezpečnostních zranitelností:

Kategorie	**Popis**
Kritická	Zranitelnost dosáhne základního skóre 7.0 – 10.0 bodů dle obecného systému hodnocení zranitelností (otevřený standard CVSSv3.1 base score).
Střední	Zranitelnost dosáhne základního skóre 4.0-6.9 bodů dle obecného systému hodnocení zranitelností (CVSSv3.1 base score).
Nízká	Zranitelnost dosáhne základního skóre 0.0-3.9 bodů dle obecného systému hodnocení zranitelností (CVSSv3.1 base score) .

Definice maximální doby nástupů k řešení incidentů podle závažnosti:

Závažnost Chyby	**Doba zahájení činnosti (od nahlášení)**	**Doba odstranění chyby**	**Řešení**
A	4 pracovní hodiny	Nejpozději do 24 hodin	**a)**
B	8 pracovní hodiny	Nejpozději do tří pracovních dní (7:00-17:00)	**a), b)**
C	1 pracovní den	Nejpozději do šesti pracovních dní (7:00-17:00)	**b)**

Struktura dohody o úrovni poskytování služeb (dále jen SLA).

(3) Řešením se rozumí:

a) Odstranění chyby řešení. Opravy Chyb bude provádět Dodavatel do Aktualizované verze (kritické chyby ihned). Na odstranění chyby pracuje Dodavatel neodkladně,

b) Poskytnutí přijatelného náhradního řešení problému ze strany Dodavatele.

(4) Technické požadavky se závažností chyby A a B lze čerpat na následující technologické oblasti dle kapitol:

5.1 Centrální firewall (kybernetická bezpečnost)

5.3 Segmentace sítě

5.5 Úložiště pro PACS a NIS data formou NAS a S3 (datová centra)

5.6 Infrastruktura pro zálohování a rychlou obnovu (datová centra)

5.7 Zvýšení dostupnosti záložního datového centra a lokální sítě (síťové prvky)

5.8 Ochrana operačních systémů a mobilních platforem (kybernetická bezpečnost)

5.9 Přihlašování k počítačům a aplikací v rámci klinických a THP provozů

(5) Na ostatní části lze čerpat pouze podporu se závažností chyby C. Tyto části jsou:

5.2 Řešení pro správu logů

5.4 DLP

Příloha č. 3 Kupní smlouvy

Technický popis nabízeného řešení
(z nabídky dodavatele v souladu s požadavky a podmínkami uvedenými v Zadávací dokumentaci v čl. 4 a také v čl. 4 v Příloze č. 3.b Zadávací dokumentace)

---

5. Vyplněná příloha č. 3b – Technická specifikace

Vyplněná příloha č. 3b je nedílnou součástí této nabídky jako **Příloha č. 5** – Technická specifikace Pelhřimov.

5.1. Technická specifikace Centrálních Firewallů

5.1.1. Popis stávajícího řešení

V současnosti je páteřní síťová infrastruktura tvořena L2 prvky společnosti HPe. Základní segmentaci sítě a také výchozí bránu do veřejné sítě Internet zajišťuje firewall Kerio Control, který také plní funkci perimetrového firewallu.

5.1.2. Záměr projektu

Návrh počítá s dodávkou a nasazením bezpečnostního řešení síťového perimetru a segmentace interní sítě. Cílem řešení je zajistit redundanci a spolehlivost a také zvýšit kybernetickou bezpečnost sítě. Řešení bude obsahovat firewall cluster v režimu vysoké dostupnosti active/standby. Oba prvky pak budou propojeny s centrálním management serverem zajišťujícím sběr a analýzu logů a centralizovanou správou bezpečnostních politik.

5.1.2.1. Specifikace HW a SW

Host HW pro VMware zajistí servery HPE ProLiant DL320 Gen11 osazené 12jádrovými procesory Intel Xeon, 32GB paměti DDR5 a 1 + 10/25GbE portovou výbavou.

Software Check Point R81.20 jako nosná bezpečnostní platforma pro Check Point Firewall cluster i mgmt server. Použité licence Checkpoint (Part Number):

- CloudGuard Network virtual core for VMware ESXi, Hyper-V, KVM Gateway *(CPSG-VSEC-VEN-BUN-NGTX-3Y + CPSG-VSEC-VEN-BUN-NGTX-2Y)*
- Mobile Access Blade for 50 concurrent connections *(CPSB-MOB-50)*
- Next Generation Security Management Software for 5 gateways *(CPSM-NGSM5 + CPSB-EVS-5-3Y + CPSB-EVS-5-1Y)*
- vše pokryto licencí na 5let + 5let podpory od výrobce *Collaborative Standard Support (CPCES-CO-STANDARD)*

5.1.2.2. Firewall

Ochrana perimetru sítě a také segmentace interní LAN bude zajištěna next-generation firewally Check Point v režimu vysoké dostupnosti (High Availability). Vše bude postavené na platformě Check Point appliance v konfiguraci active/standby cluster. Vysokou dostupnost firewall bran samotných zajišťuje ClusterXL technologie na úrovni software CheckPoint.

Firewall cluster bude připojen ke stávající Internetové lince a do LAN. Produkční VLAN budou terminovány na firewallu, který bude výchozí bránou. Tím je zajištěna segmentace sítě a zvýšena bezpečnost. Připojení bude provedeno přes síťová rozhraní 10/25Gb (resp. 1Gb pro Internet).

Nabízená licence NGTX nabízí formou zásuvných modulů kromě firewall funkcionality také ochranu proti ransomware, malware a 0-day hrozbám emulací škodlivého kódu v sandboxu, antivirus, ochranu Anti-Bot, IPS, detekci a filtraci na úrovní aplikační kontroly, URL filtering nebo i službu Identity Awareness, pracující s daty propojených databází uživatelů (např. AD). Bude tedy řešena bezpečnost v rámci infrastruktury, ale také zabezpečení uživatelského provozu – pomocí Application Control a IPS. Síťový provoz bude filtrován dle pravidel bezpečnostní politiky. Úroveň ochrany bude tedy až na 7. síťovou vrstvu. Další rolí firewallu pak bude Remote Access Gateway (VPN koncentrátor) pro vzdálené připojení klientů.

TECHNOLOGY	NEXT GENERATION THREAT PREVENTION (NGTP PACKAGE)	SANDBLAST NETWORK (NGTX PACKAGE)
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
Application Control	✓	✓
Content Awareness	✓	✓
URL Filtering	✓	✓
Anti-bot	✓	✓
Anti-Virus		✓
Anti-Spam		✓
SandBlast Threat Emulation		✓
SandBlast Threat Extraction		✓

https://www.checkpoint.com/downloads/products/sandblast-network-solution-brief.pdf

Licence NGTX v nabídce byla zvolena na 5 let + 5 let podpory od výrobce. Během této doby má zákazník přístup k nejnovějším signaturám Threat Prevention modulů, opravným balíčkům pravidelně vydávaných výrobcem a také nejnovější verzi operačního systému GAIA. Licenčně

je dále umožněn přístup až 50 uživatelů prostřednictvím klientské VPN, počet S2S není limitován.

5.1.2.3. Centrální management

Firewall infrastruktura bude nasazena v distribuované architektuře, jejíž součástí bude i nezávislý Security Management server. Pomocí tohoto serveru jsou firewally centrálně spravovány, management současně také slouží pro tvorbu a správu bezpečnostních politik a správu administrátorů systému. Management licence obsahuje i SmartEvent modul, který zajišťuje sběr a interpretaci logů a událostí ze síťových prvků nebo auditní log firewall infrastruktury. Z těchto dat lze následně generovat uživatelské reporty. Server bude implementován ve formě samostatného virtuálního stroje ve stávající virutalizační platformě zákazníka. Pro potřeby serveru je vyžadována platforma VMware ESXi, Hyper-V nebo KVM.

Rulebase konfigurovaná v centrálním management serveru

Centrální logserver + analýza událostí

Part number:

Počet	Part Number	Popis
12	CPSG-VSEC-VEN-BUN-NGTX-3Y	1 CloudGuard Network virtual core for VMware ESXi, Hyper-V, Gateway. Annual subscription for 3 years
12	CPSG-VSEC-VEN-BUN-NGTX-REN-2Y	1 CloudGuard Network virtual core for VMware ESXi, Hyper-V, Gateway. Annual subscription for 2 years
2	CPSB-MOB-50	Mobile Access Blade for 50 concurrent connections
1	CPSM-NGSM5	Next Generation Security Management Software for 5 gate (SmartEvent & Compliance 1 year)
1	CPSB-EVS-5-3Y	SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & server) 3 year subscription
1	CPSB-EVS-5-1Y	SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & server) 1 year subscription
32	VCF-VSP-STD-8	VMware vSphere Standard 8
5	Letá podpora výrobce	

Součástí technické specifikace na Centrální firewally, jsou produktové listy nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.6** – Produktové listy_materiály_5.1 a-c.

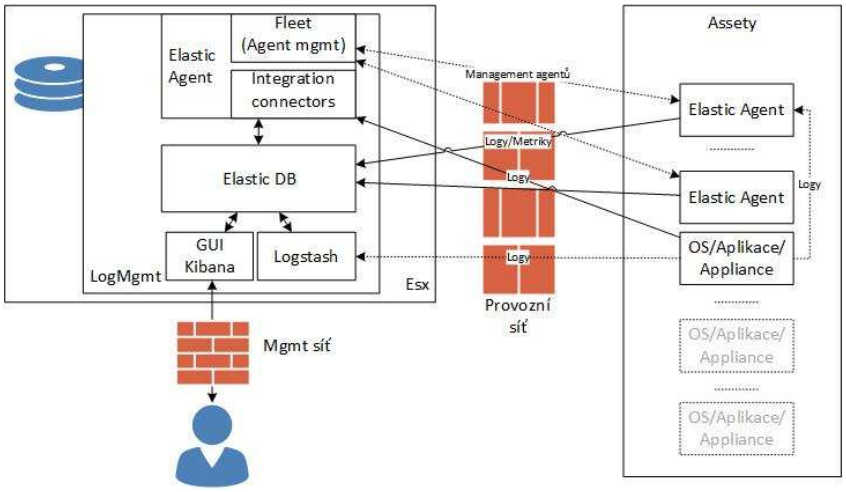
5.2. Technická specifikace centrálního sběru a managementu logů

5.2.1. Technická specifikace řešení pro správu logů

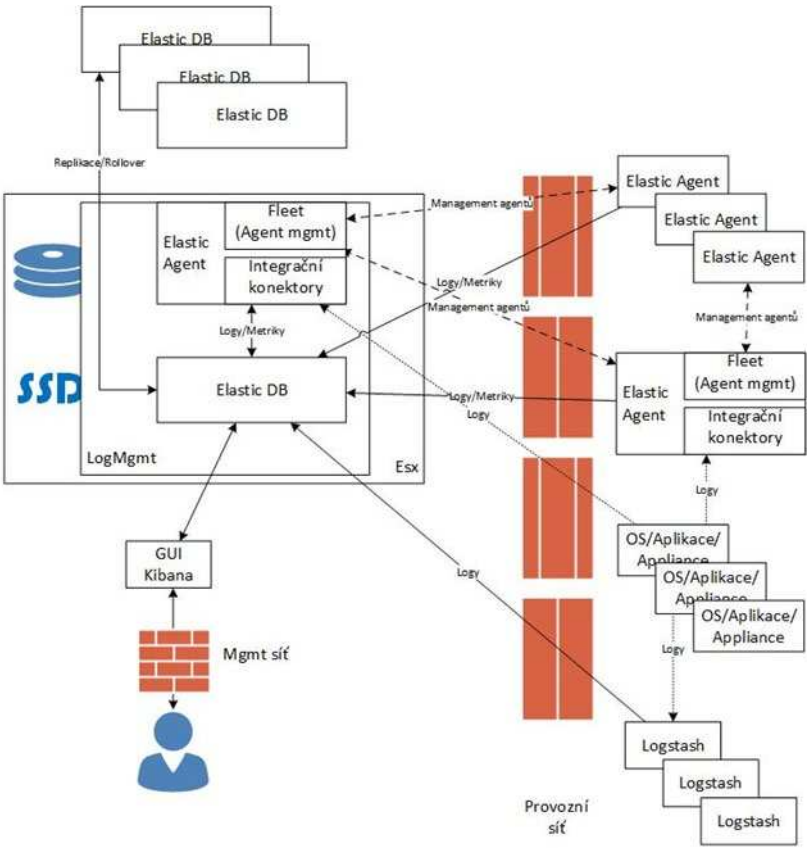
Jako centrální prvek pro sběr a správu logů bude implementován Elastic Stack. Tento produkt nabízí, kromě samotného ukládání logů a jejich správy z hlediska retence, také množství užitečných funkcí pro dohledávání a vizualizaci ukládaných dat, které mohou sloužit jak pro řešení provozních, tak i pro řešení bezpečnostních úkonů a problémů.

Jedná se o platformu složenou z většího množství do velké míry samostatných modulů, které se starají o práci s daty. Hlavními součástmi jsou Elasticsearch, který poskytuje výkonnou databázi pro ukládání logů, Kibana, která slouží jako GUI pro administraci a také jako silná vizualizační základna pro dohledávání a zobrazování dat, a množství komponent souhrnně označovaných jako Integrace, které umožňují příjem a zpracování dat jak různými protokoly, tak i ze široké škály produktů.

Velkou výhodou Elastic stacku je snadná škálovatelnost. Všechny komponenty mohou běžet na jednom serveru (node),



ale mohou být také rozmístěny na různých serverech. Hlavní komponenty je možné nasadit také v HA režimu a rozkládat mezi nimi zátěž. Toto škálování přidáváním prvků je možné provádět průběžně, bez zásahů do existujících komponent a potřeb složitější rekonfigurace systému. Je tak možné účelněji využít zdroje a kapacity během času rozšiřovat v závislosti na dlouhodobých provozních požadavcích.



Navrhované řešení počítá s jedním nodem, obsahujícím všechny potřebné komponenty, instalovaným jako virtuální server, s potenciální možností implementace některého z transportních prvků do uzavřených sítí, z důvodů zpřehlednění a zjednodušení správy sítě.

Řešení by mělo být instalováno v segmentu sítě co nejvíce separovaném od uživatelského provozu, předpokládá se provoz na dvou IP adresách, jedna pro management systému, dostupná z management segmentů sítě, druhá provozní pro příjem logů (ať už přímý, nebo zprostředkovaný), dostupná ze segmentů sítě, které budou do centrálního úložiště logy posílat.

Příjem dat bude probíhat dvěma základními cestami. Jednou je přímá komunikace jedné z komponent, tzv. Elastic Agenta, s centrální databází. Elastic agent je utilita, kterou je možné instalovat přímo na servery, a která zprostředkovává vlastním protokolem lokální logy (ať už z eventlogu/syslogu, nebo i přímo z konkrétních souborů) centrální databázi a obchází tak potřebu úpravy nastavení každého jednotlivého systému (především pro Windows OS, kde je jinak pro odesílání event logů nutná aplikace třetích stran). Po prvotní instalaci, kterou je nutné iniciovat ze serveru, který je zdrojem logů, už další správa probíhá přes centrální GUI.

Druhý způsob je přímý příjem logů ze zdrojových zařízení (servery, síťové prvky, různé appliance a aplikace), které umí logovat po síti. Tento příjem bude povětšinou probíhat za pomoci Syslog protokolu a může se pro jednotlivé zdroje logů v některých detailech lišit.

Nemalá část integrací (včetně elastic agentů) umožňuje kromě samotných logů také sběr provozních metrik systémů, které mohou být užitečné jak při investigaci bezpečnostního problému, tak i jako samostatná položka sloužící například jako doplněk dohledu. Tato data budou ale považována za sekundární, předpokládá se, že budou mít nastavena výrazně nižší retenci než samotné logové záznamy a budou sbírána pouze v případě, že nebudou mít zásadnější dopad na zdroje celého systému.

Vzhledem k tomu, že v síti zadavatele podobné řešení prozatím není implementováno, bude potřeba je vybudovat od základů. Primárně to znamená potřebu identifikovat ze strany zadavatele potenciální zdroje logů (tj. servery, aplikace, appliance apod.), roztřídit je do skupin podle formátu logů, možností jejich přenosu do centrálního úložiště, potenciální důležitosti z hlediska bezpečnosti apod. Implementace řešení pak počítá, kromě samozřejmé instalace a základní konfigurace systému, také s asistencí při spuštění a konfiguraci příjmu pro vzorová zařízení z jednotlivých takto definovaných skupin.

Vzorová implementace bude probíhat v několika navazujících krocích a pořadí jednotlivých typů zdrojů bude určeno s ohledem na poměr počtu instancí vůči složitosti implementace s přihlédnutím k bezpečnostním hlediskům tak, aby se pokryla co největší šíře provozního prostředí v co nejkratším čase, atypické a málo zastoupené zdroje bez bezpečnostního významu se mohou řešit v pozdějších fázích. Jednotlivé kroky se mohou pro jednotlivé typy zdrojů logů částečně překrývat a je možné v implementaci postupovat do jisté míry paralelně.

Fáze 1

Vzhledem k tomu, že primárním záměrem projektu je získat centrální úložiště dat zahrnující co možná největší rozsah logů z provozovaných assetů a technologií, bude první krok a hlavní implementační činnost spočívat právě v připojování nových zdrojů tak, aby byla data odesílána na log management server a zde uchovávána pro případnou forenzní analýzu.

Z hlediska součinnosti zadavatele se v této fázi předpokládá dodání výše popsaného seznamu, tj. především spolupráce na identifikaci jednotlivých zdrojů logů z hlediska typu, množství instancí a popsání variant transportu logů do log management systému. Následně pak spolupráce při konfiguraci testovacích instancí, úpravě nastavení provozní sítě z hlediska povolení a směrování logů a ověření kompletnosti přenesených informací (zda jsou přeneseny všechny odeslané logy a nedochází k jejich poškození). Po ověření funkčnosti na testovacích instancích se z praktických důvodů předpokládá replikace nastavení na zbylé instance stejného typu samostatně pracovníky zadavatele, dodavatel bude vystupovat především v konzultační roli a při řešení případných problémů.

První fáze bude ukončena ve chvíli kdy bude takový jednotlivý dostatečně popsaný typ zdroje logů zapojen do log management systému, nebo bude z nějakého důvodu rozhodnuto, že se tento zdroj nebude do centrálního úložiště ukládat. Je potřeba do systému zapojit dostatečné množství instancí jednotlivých systémů, aby se dalo říct, že připojení dalších nebude zásadně měnit výkonové, či jiné parametry systému. Počítá se s tím, že zbývající zdroje se poté mohou k centrálnímu úložišti připojovat v dalších fázích projektu, případně i v rámci rutinního provozu.

2. fáze

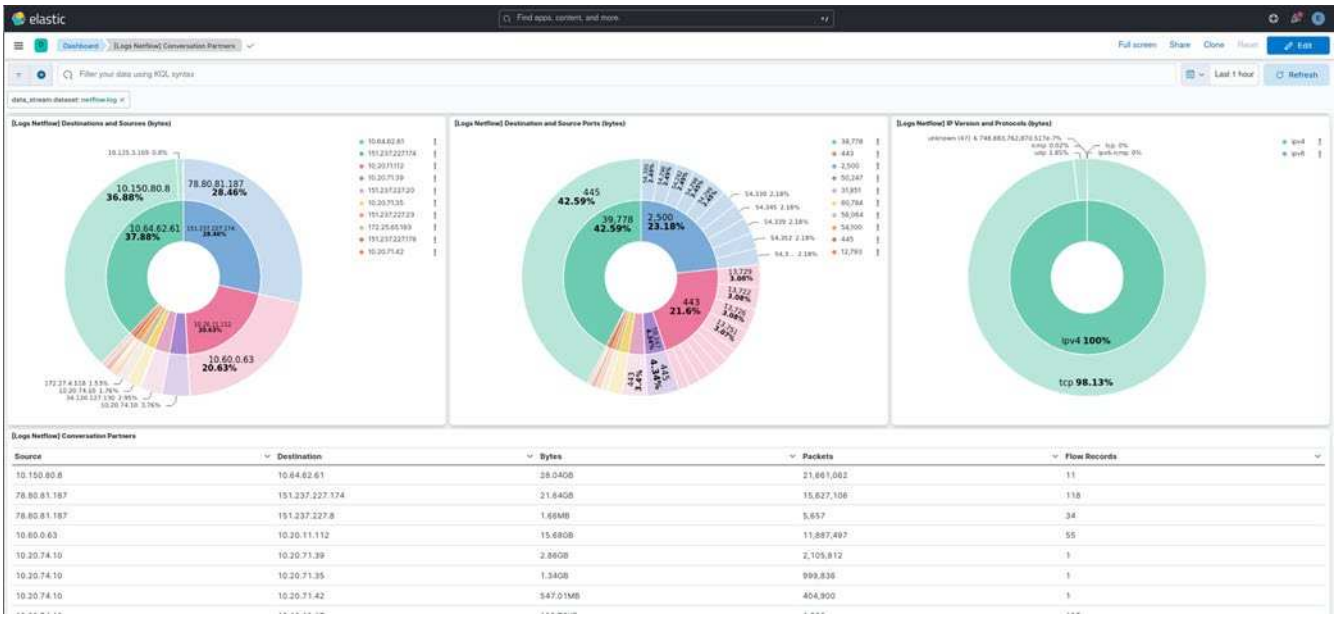
Jednotlivé logové záznamy jsou ukládány do databáze ve své zdrojové formě, jak je systém přijal. Nad takovými nestrukturovanými daty je však možné provádět z větší části pouze operace typu fulltext search, které nejsou praktické pro dohledávání specifických atributů záznamu, anomálií, agregace apod. Proto je vhodné provést normalizaci dat rozdělením komplexního logového záznamu do co nejpopisnějšího setu konkrétních atributů. Tento krok umožní rychlé dohledávání a přehledné vizualizace jak bezpečnostních, tak i provozních událostí. Aby to ale bylo možné, je potřeba rozklíčovat strukturu a význam jednotlivých segmentů logových záznamů.

V tomto kroku se pro jednotlivé začleněné zdroje logů identifikuje jejich obsah a struktura tak, aby bylo možné normalizovat vstupní data pro indexaci do granulárního setu atributů. U prvků, kde je struktura obecně známá a ideálně je již v log managementu definovaná a podporovaná při importu, bude nastavení provedeno zároveň s nastavením transportu dat v 1. fázi, u zbylých bude potřeba popsat (a případně po domluvě vybrat, pokud je zde více možností, a na zdroji nakonfigurovat) strukturu logových záznamů z hlediska formátu (zda může být nastaven některý ze standardizovaných strukturovaných formátů identifikující atributy, jako je CEF, LEEF, JSON apod., pokud ne, tak jestli je možné identifikovat v záznamu některé atributy a popsat je například regulárním výrazem apod.).

Validním stavem v této fázi může být také rozhodnutí, že daný log bude uložen pouze ve zdrojové formě bez jakéhokoliv dalšího zpracování, protože jeho struktura nemá pevné prvky, které by bylo možné rozebrat, nebo jeho význam pro případné další vytěžení informací je zanedbatelný a v zřídkavých využitích jeho obsahu bude postačovat fulltext search a není tak potřeba investovat čas do implementace a údržby příslušných importních procedur.

3.fáze

Nadstavbovým krokem implementace bude prozkoumání možností využití konkrétních dat pro provozní a bezpečnostní účely. Tato fáze bude zaměřena na přípravu GUI tak, aby co nejlépe vyhovovala provozním nárokům zadavatele.



Zde nejsou stanovené žádné konkrétní cíle, v best effort režimu budou připravovány jednotlivé uložené dotazy, vytvářeny a nastavovány vizualizační prvky a dashboardy pro jednotlivé přehledy, které budou reflektovat potřeby provozu. Množství takových přehledů je v Elastic stacku dostupné v rámci Integrací, takže budou primárně využívány a případně obohacovány tyto, hlavním iniciátorem zde ale budou pracovníci zadavatele, kteří budou popisovat činnosti a identifikovat informace v log záznamech a jejich vztahy, které jim v plnění těchto činností mohou pomoci., dodavatel pak dodá podporu při definici uložených vyhledávání, vizualizačních komponent a dashboardů.

Z hlediska součinnosti zadavatele se zde předpokládá těsná spolupráce na identifikaci zajímavých událostí a jejich projevů (vycházející ze znalosti prostředí, obsahu specializovaných logů a provozních požadavků a rizik), návrhy a ověřování vyhledávacích kritérií z hlediska výsledků.

Poznatky z 3. fáze se mohou zpětně promítnout do úprav nastavení logování pro jednotlivé assety (změna severity zasíkaných logů, přidání logování pro další komponentu systému apod.), případně i úpravami zpracování logů vytvořenými v předchozích fázích.

Part number: u HW sdílený s HW u části 5.8.1.

Součástí technické specifikace řešení pro správu logů, jsou odkazy nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.7** – Odkazy_na_produktovou_dokumentaci_5.2.1.

5.2.2. Požadavky na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlox/IPFIX)

POPIS ŘEŠENÍ PRO ČÁSTI 5.2.2 a 5.2.3

Záměr projektu

Návrh počítá s dodávkou a nasazením bezpečnostního řešení behaviorální analýzy síťového provozu. Cílem řešení je zajistit zpracování a vyhodnocení flow dat a také zvýšit kybernetickou bezpečnost sítě. Řešení bude obsahovat virtualizovaný kolektor Flowmon kolektor 6000 VA s modulem ADS standart pro monitorování a vyhodnocení datových toků pro monitorování sítě na bázi datových toků. Obě sondy pak budou propojeny s kolektorem zajišťujícím sběr a analýzu logů a centralizovanou správou bezpečnostních pravidel.

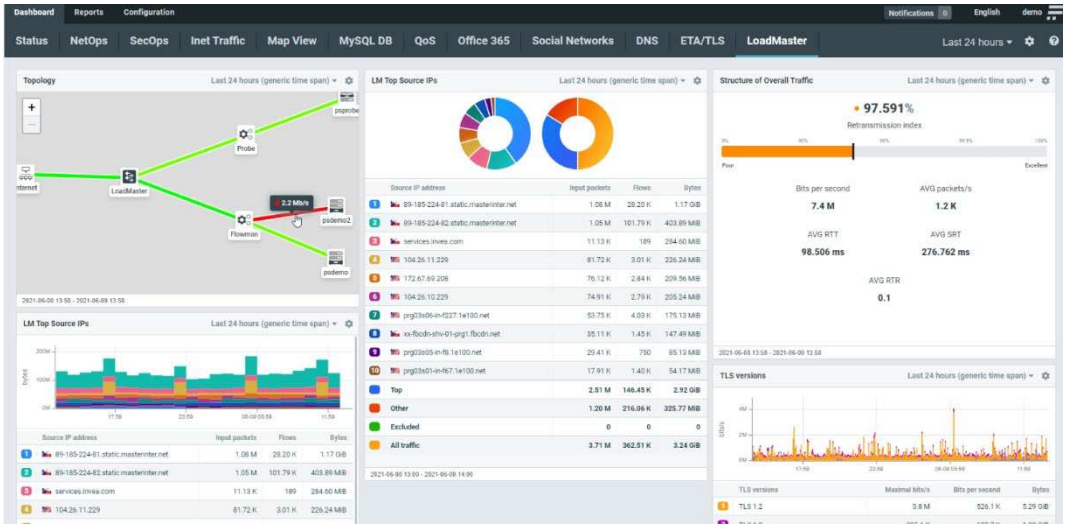
5.2.2.1. Flowmon kolektor

Monitoruje síť, sbírá, ukládá i zpracovává data o síťovém provozu. A to včetně jejich normalizace, vizualizace a analýzy. To všechno umí Flowmon kolektor. Navíc vám dá výborný přehled o síťové a aplikační telemetrii prostřednictvím plně přizpůsobitelného dashboardu. Najdete v něm potřebné statistiky, vizualizace dat i možnost podrobného rozpadu údajů, která vám zefektivní řešení problémů i plánování kapacit. Analýza metadat síťového provozu (ve formátech NetFlow/IPFIX) umožňuje řešit odstávky, dlouhé odezvy a další výkonnostní problémy pomocí. Informace jsou sbírány přímo z monitorované infrastruktury, ať už fyzické, virtuální nebo cloudové. Informace o struktuře síťového provozu, uživatelích a službách vytěžujících kapacitu sítě nebo o zpoždění jsou prezentovány srozumitelně ve formě tabulek, grafů a statistik. K dispozici jsou předdefinované dahsboardy, možnost vytvořit si svoje vlastní i sdílené.

V řešení síťového monitoringu bude použit virtuální kolektor IFC-6000-VA Flowmon Collector 6000 VA s výkonem až 150,000 flows za sekundu. Kapacita 6 TB, VMware ESXi je min 5.5, Microsoft Hyper-V 2012 R2 a novější, KVM - KVM 3.10.0 a vyšší QEMU 1.5.3 a vyšší libvirt 4.5.0 a vyšší. Minimální požadavky konfigurace virtualizačního prostředí jsou 4 CPU jader, 8 GB RAM, 1000 IOPS.

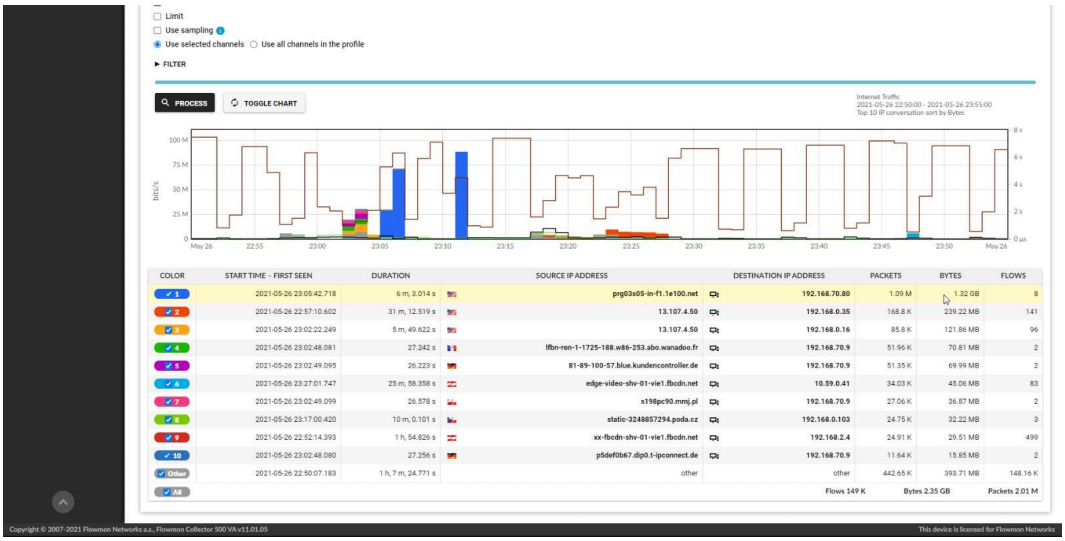
5.2.2.1.1. Dashboardy a vizualizace

Plně nastavitelné rozhraní navržené pro srozumitelnou vizualizaci struktury síťového provozu, výkonnostních metrik a topologie infrastruktury. Jednoduše přizpůsobitelné díky tzv. widgetům. K dispozici je řada předdefinovaných šablon reflektujících nejběžnější potřeby uživatelů (Office 365, G Suite, sociální sítě, protokoly DNS, DHCP a další). Ať už jste uživatel nebo poskytovatel služeb, můžete svůj dashboard sdílet s ostatními.



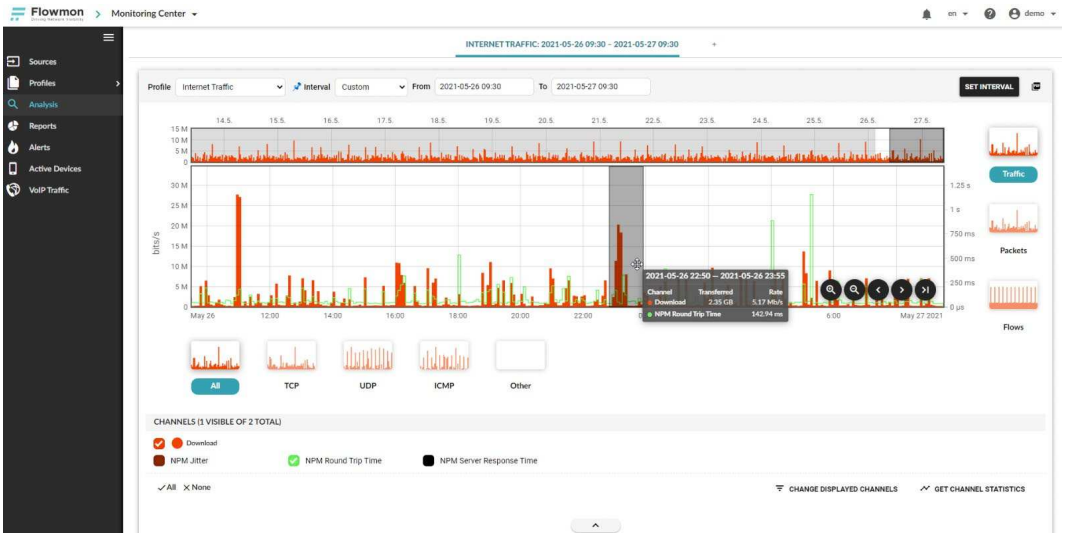
5.2.2.1.2. Podrobná analytika

Drill-down, tedy rozpad události na větší detail, je dostupný z kteréhokoliv místa dashboardu. Každý widget může být zobrazen z analytického pohledu. Událost tak v případě potřeby prozkoumat hlouběji, až na level jednotlivých datových toků a paketů. Můžete přitom zobrazit i velmi konkrétní detaily jako jsou informace o aktivních zařízeních, výrobcích nebo zdrojích datových toků. K dispozici máte funkci filtrování dle protokolů, časových úseků, zdrojových/cílových IP adres a další. Statistiky lze exportovat na každé úrovni drill-downu.



5.2.2.1.3. Troubleshooting a forenzní analýza

Kolektor nesleduje jen aktuální stav zelená/červená, zaznamenává interakce uživatelů s aplikacemi, abyste získali ucelený přehled o celém digitálním prostředí. Tento holistický přístup umožňuje okamžitě identifikovat příčinu problémů ovlivňujících uživatele a služby, a přijmout nápravná opatření.



Part number:

1	IFC-6000-VA	Flowmon kolektor 6000 VA
5	Letá podpora výrobce	

Součástí technické specifikace řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX), jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.8** – Produktové listy_materiály_5.2.2.

5.2.3. Požadavky na řešení pro automatické vyhodnocování datových toků (NetFlox/IPFIX)

POPIS ŘEŠENÍ PRO ČÁSTI 5.2.2 a 5.2.3

Záměr projektu

Návrh počítá s dodávkou a nasazením bezpečnostního řešení behaviorální analýzy síťového provozu. Cílem řešení je zajistit zpracování a vyhodnocení flow dat a také zvýšit kybernetickou bezpečnost sítě. Řešení bude obsahovat virtualizovaný kolektor Flowmon kolektor 6000 VA s modulem ADS standart pro monitorování a vyhodnocení datových toků pro monitorování sítě na bázi datových toků. Obě sondy pak budou propojeny s kolektorem zajišťujícím sběr a analýzu logů a centralizovanou správou bezpečnostních pravidel.

5.2.3.1. Flowmon ADS

Zaregistrujte včas škodlivé chování, útoky na důležité podnikové aplikace, narušení dat i signály, které ukazují na možné napadení sítě. To všechno dokáže Flowmon ADS (Anomaly Detection System). Toto řešení pro síťovou bezpečnost funguje jako doplněk tradičních bezpečnostních nástrojů. Jeho základem je inteligentní detekční engine, který využívá behaviorální analýzu. Právě díky ní dokáže odhalit anomálie skryté v síťovém provozu a ochránit takzvanou bílou zónu mezi zabezpečením perimetru a koncovými stanicemi.

Flowmon nabízí jak vynikající detekční schopnosti, tak podrobné analýzy. Díky tomu se na něj můžete spolehnout po celou dobu od začátku bezpečnostního incidentu až po jeho vyřešení.

Flowmon ADS přidává do vaší bezpečnostní matice síťově orientovanou obrannou vrstvu (viz SOC Visibility Triad), která odhalí i nepatrné síťové anomálie indikující aktivitu neznámých a vnitřních hrozeb, které nelze odhalit pomocí zabezpečení perimetru a koncových bodů. Přehledná vizualizace v rámci MITRE ATT&CK® frameworku následně informuje o rozsahu, závažnosti a dalším vývoji narušení.

Díky více než 40 detekčním metodám využívajícím umělou inteligenci a více než 200 sofistikovaným algoritmům jsou všechny hrozby odhaleny okamžitě a zcela automaticky. Odhalte neznámé hrozby, malware, ransomware, zneužití zranitelnosti Windows DNS serveru SIGRed, útok trojany nebo hrozby skryté v šifrovaném provozu. ADS lze integrovat s NAC, autentizační službou, firewallem nebo jinými nástroji pro okamžitou reakci na incident.

Zaměřte se pouze na relevantní problémy. ADS rozlišuje mezi anomáliemi a běžným provozem a upozorní vás pouze v případě, že se jedná o skutečné nebezpečí. Detekované

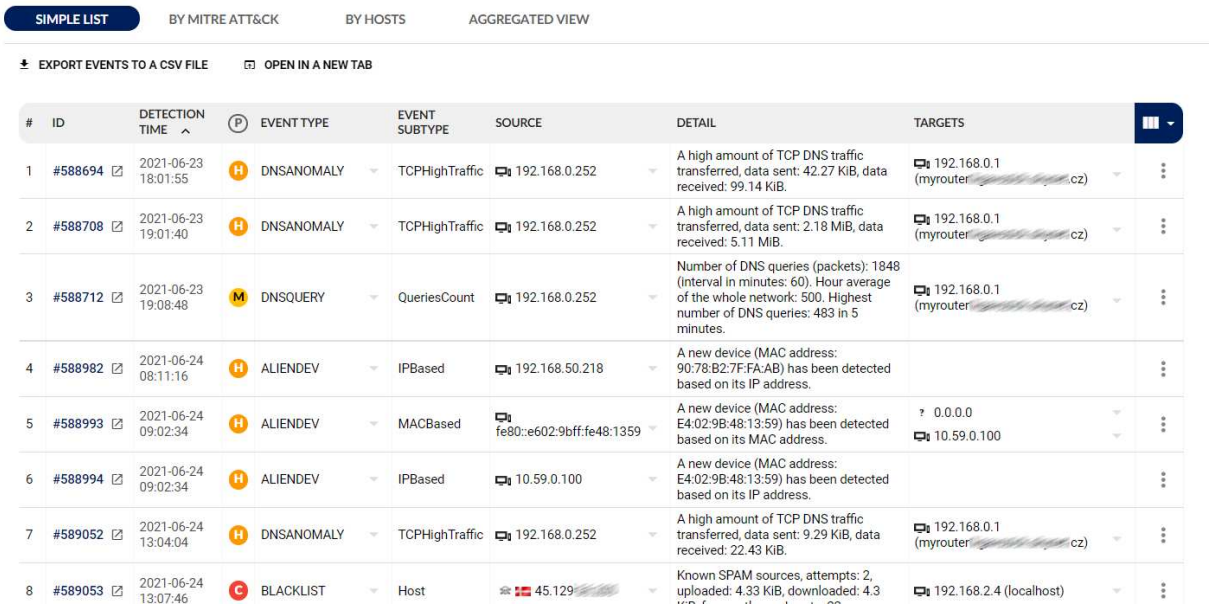
bezpečnostní události jsou řazeny dle závažnosti. Vestavěná expertní databáze dokáže poskytnout požadovaný kontext, čímž pomáhá zvýšit povědomí o situaci a urychlit vaši reakci.

V řešení síťového monitoringu bude použit modul ADS ve verzi standart.

		Lite FP-ADS-L	Standard FP-ADS-S	Business FP-ADS-B	Coporate FP-ADS-C	Enterprise FP-ADS-E	Ultimate FP-ADS-U
Data processing	**Flow data**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	External information	Flowmon Threat Intelligence (reputation databases, indicators of compromise), whois, IP tools, weblinks					
	Behavioral detections	machine learning, adaptive baselining, behavior analysis, heuristics					
	IDS detections	built-in integration with Suricata IDS running on Flowmon Probes					
Event reporting	**Reporting and alerting**	e-mail, PDF/CSV, syslog, SNMP, packet capture trigger, script trigger					
	SIEM support	Using CEF (over syslog), SNMP trap					
Performance indicators[1]	**Stream data processing (flows/s)**	100	1,000	5,000	20,000	50,000	100,000
	Behavior patterns processing (flows/s)	100	1,000	5,000	20,000	25,000	25,000
	Data feeds	1	3	5	20	50	100
	Required memory (GB)	4	8	16	32	64	128
	Required CPU cores	1	2	4	8	16	24
User interface	**Event visualizations**	Event analysis tree, Timeline, Details, Evidence, Interactive					
	3rd Party integration	IBM QRadar App, LDAP/AD, McAfee ePO					

5.2.3.1.1. Detekce

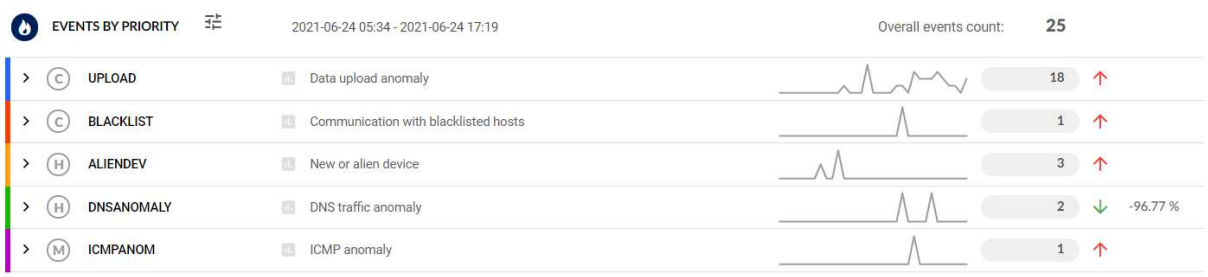
Strojové učení, adaptivní baselining, heuristika, vzorce chování, reputační databáze, detekce založená na signaturách – využívá řady detekčních mechanismů analyzujících síťový provoz z různých pohledů a pokrývá tak širší spektrum scénářů. Zjistěte, který uživatel nebo hostname byl zapojen do útoku pomocí sbírání logů z autentifikačních systémů a jejich korelováním ve Flowmonu. Každá autentifikační služba nebo výrobce umožňující propojení přes syslog je podporován, včetně Cisco ISE a AD/LDAP.



#	ID	DETECTION TIME	EVENT TYPE	EVENT SUBTYPE	SOURCE	DETAIL	TARGETS
1	#588694	2021-06-23 18:01:55	DNSANOMALY	TCPHighTraffic	192.168.0.252	A high amount of TCP DNS traffic transferred, data sent: 42.27 KiB, data received: 99.14 KiB.	192.168.0.1 (myrouter[redacted].cz)
2	#588708	2021-06-23 19:01:40	DNSANOMALY	TCPHighTraffic	192.168.0.252	A high amount of TCP DNS traffic transferred, data sent: 2.18 MiB, data received: 5.11 MiB.	192.168.0.1 (myrouter[redacted].cz)
3	#588712	2021-06-23 19:08:48	DNSQUERY	QueriesCount	192.168.0.252	Number of DNS queries (packets): 1848 (interval in minutes: 60). Hour average of the whole network: 500. Highest number of DNS queries: 483 in 5 minutes.	192.168.0.1 (myrouter[redacted].cz)
4	#588982	2021-06-24 08:11:16	ALIENDEV	IPBased	192.168.50.218	A new device (MAC address: 90:78:B2:7F:FA:AB) has been detected based on its IP address.	
5	#588993	2021-06-24 09:02:34	ALIENDEV	MACBased	fe80::e602:9bff:fe48:1359	A new device (MAC address: E4:02:9B:48:13:59) has been detected based on its MAC address.	0.0.0.0 10.59.0.100
6	#588994	2021-06-24 09:02:34	ALIENDEV	IPBased	10.59.0.100	A new device (MAC address: E4:02:9B:48:13:59) has been detected based on its IP address.	
7	#589052	2021-06-24 13:04:04	DNSANOMALY	TCPHighTraffic	192.168.0.252	A high amount of TCP DNS traffic transferred, data sent: 9.29 KiB, data received: 22.43 KiB.	192.168.0.1 (myrouter[redacted].cz)
8	#589053	2021-06-24 13:07:46	BLACKLIST	Host	45.129[redacted]	Known SPAM sources, attempts: 2, uploaded: 4.33 KiB, downloaded: 4.3	192.168.2.4 (localhost)

5.2.3.1.2. Reportování

Analytický pohled poskytuje vizualizaci útoku, včetně jeho kontextu a mapování na MITRE ATT&CK® framework. Možnost rozpadu události na větší detail (drill-down) dovoluje plně porozumět, co se ve vaší síti děje.

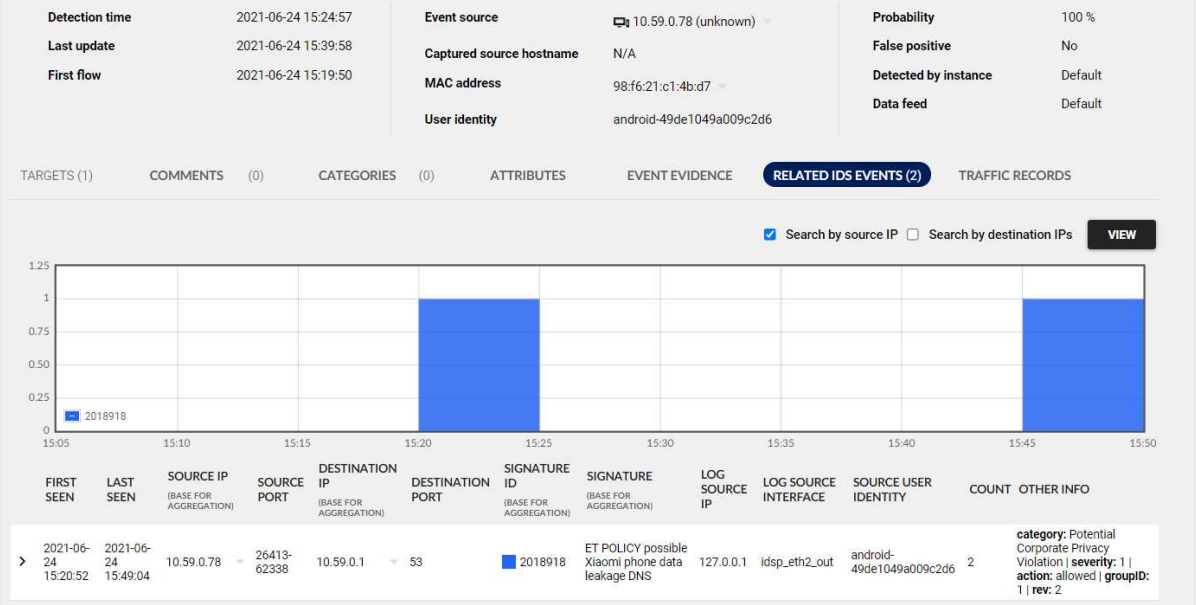


5.2.3.1.3. Třídění

Incidenty jsou hodnoceny přesně podle vašich priorit a konfigurace nastavení a přizpůsobením systému vašim potřebám.

5.2.3.1.4. Reakce

Flowmon ADS lze integrovat s celou řadou nástrojů, jako jsou systémy řízení přístupu k síti (Network Access Control), autentifikační systémy, firewally a ostatní systémy pro okamžitou reakci na incident.



Part number:

1	FPC-ADS-S	Flowmon ADS Standard
5	Letá podpora výrobce	

Součástí technické specifikace řešení pro automatické vyhodnocování datových toků (NetFlow/IPFIX), jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.9** – Produktové listy_materiály_5.2.3.

5.3. Technická specifikace zavedení segmentace sítě

Zadání:

Předmětem je implementace řešení, které ve spolupráci s LAN a WLAN infrastrukturou zajistí adaptivní řízení přístupu pro různé typy zařízení a různé uživatele. Bude možné rozlišit nastavení oprávnění a aplikování politik například pro zaměstnance, hosty nebo externí partnery, a to i z pohledu připojených zařízení.

Řešení:

Nabízíme řešení postavené na výrobcích od HPE Aruba, které splňuje minimální požadavky poptávané zadavatelem. Konkrétně jde HPE ARUBA Clearpass a potřebné licence v poptávaném počtu.

Popis nabízených produktů je v souboru s partnumbery, kde jsou rozepsány všechny nabízené SW produkty.

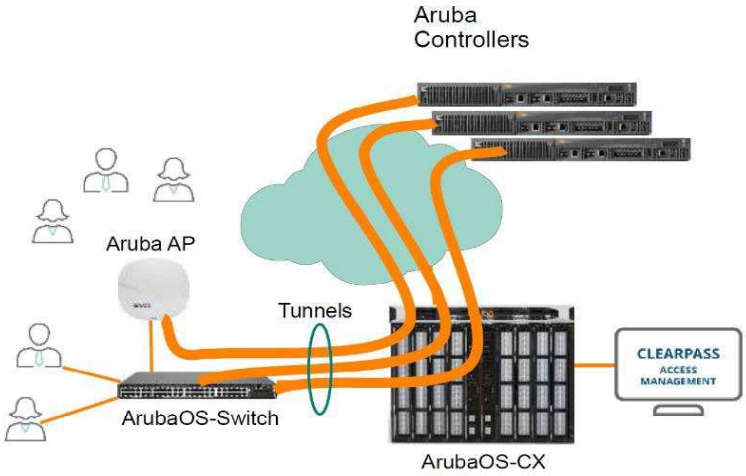
Všechny HW komponenty, které nyní Zadavatel vlastní a vypsal v technické specifikaci v příloze č.3:

JL558A Aruba 2930-48G	6 ks
Aruba 6200F 48G CL4 740W – JL728A	19 ks
Aruba AP-515	122 ks

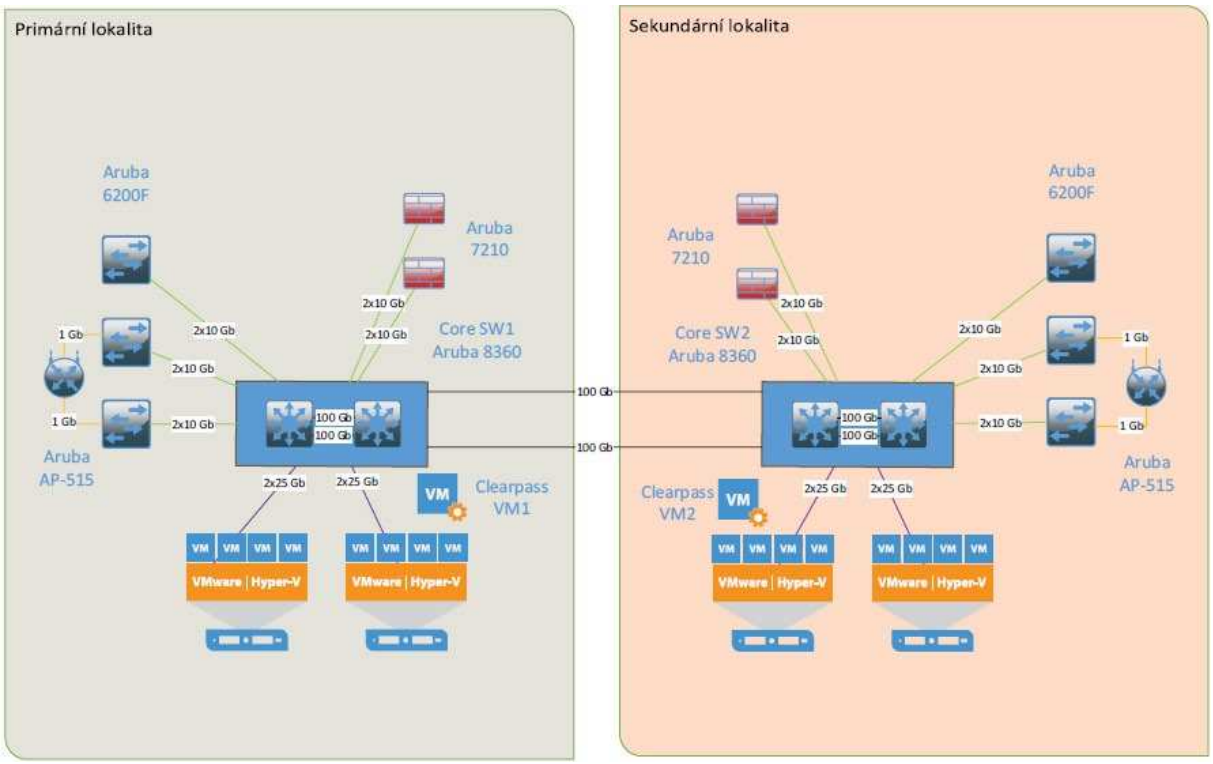
Umí nabízený produkt HP ARUBA Clearpass začlenit do svého ekosystému.

Nabízené řešení, které ve spolupráci s LAN a WLAN infrastrukturou zajistí adaptivní řízení přístupu pro různé typy zařízení a různé uživatele. Bude možné rozlišit nastavení oprávnění a aplikování politik například pro zaměstnance, hosty nebo externí partnery, a to i z pohledu připojených zařízení. Řešení funguje ve vysoce dostupném aplikačním clusteru a má vazbu na další aplikace – např. AD, CA.

Základ je popsán v konceptuálním schématu:



Detailnější popis implementace je jasně znázorněný na tomto již detailnějším obrázku:



Part number:

P/N	SW licence	ks
JZ403AAE	Aruba ClearPass NL AC 2500 CE E-LTU s 5 letou podporou	1
JZ399AAE	Aruba ClearPass Cx000V VM Appl E-LTU s 5 letou podporou	2

Součástí technické specifikace řešení zavedení segmentace sítě, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.10** – Produktové listy_materiály_5.3.

5.4. Technická specifikace DLP

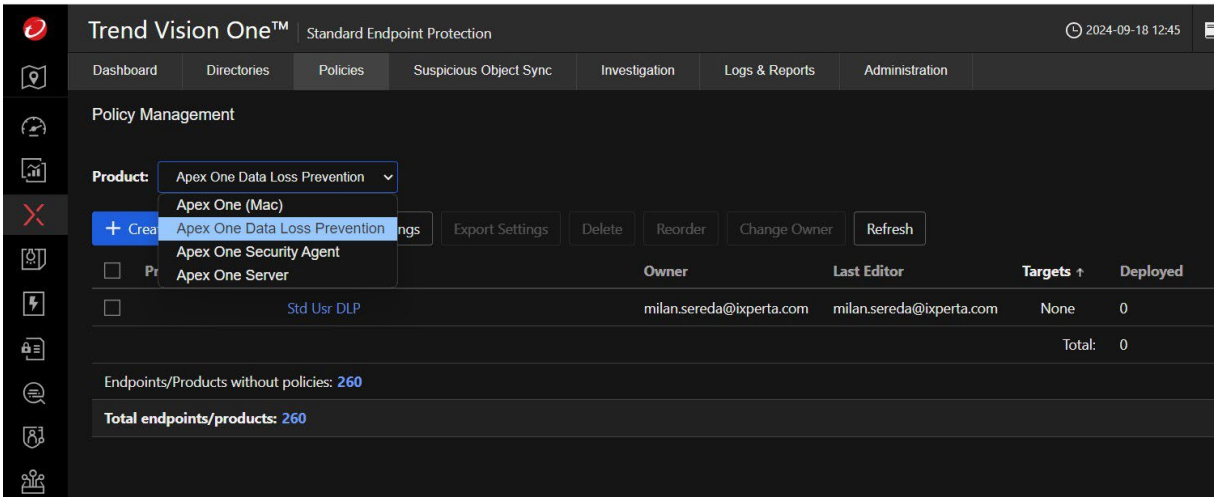
Popis nabízeného řešení

5.4.1. Ochrana DLP – souhrnný technický popis

DLP se rozumí jedna ochrana ze sady ochran endpointů popisovaných v samostatné části/kapitoly „ochrany koncových zařízení“ včetně a nástrojů vyšetřování EDR/XDR.

Základem je centrální XDR platforma Trend Vision One v cloudu výrobce, která slouží jako agregační, konfigurační, integrační, automatizační, správní a monitorovací bod sady pořizovaných ochran (popisována podrobněji v části „ochrany koncových zařízení“).

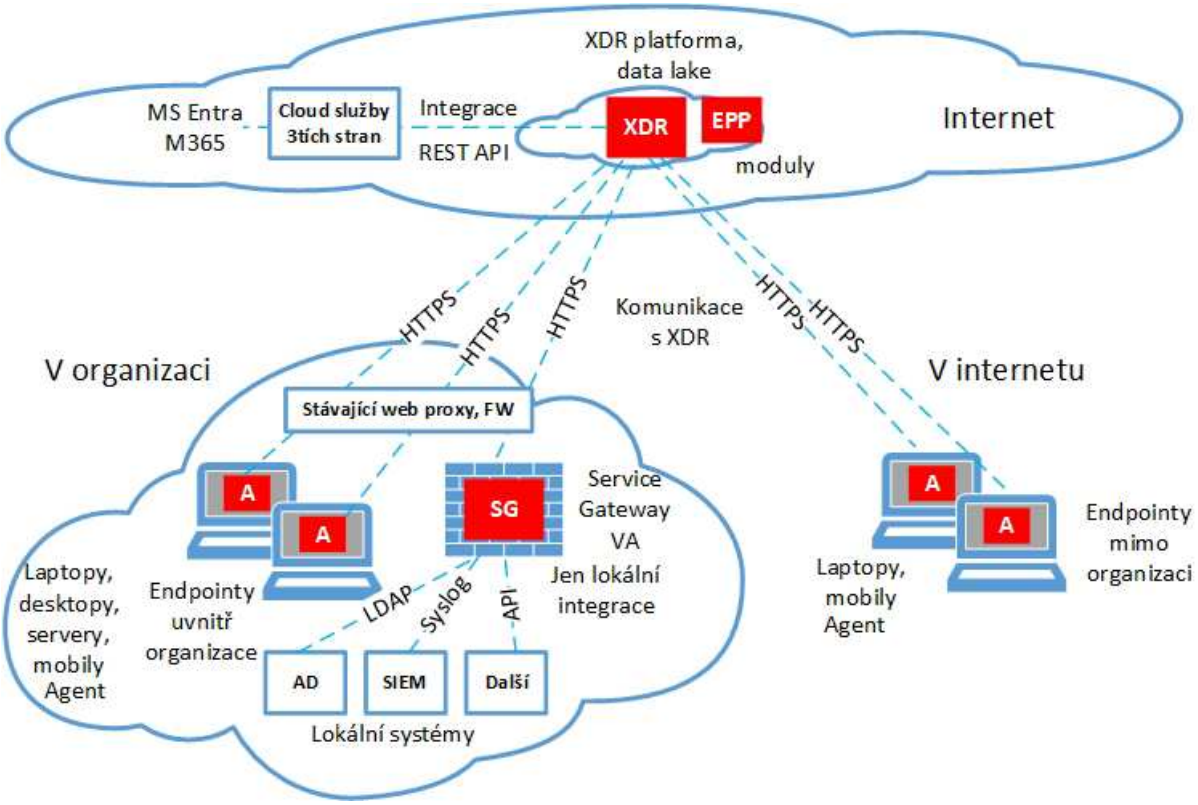
Její součástí je balík ochran koncových zařízení pod názvem Standard Endpoint Protection (rovněž Apex One), jeho součástí je i DLP. Ochrana DLP je zavedena a vynucována do endpointů prostřednictvím samostatné DLP politiky. Agent instalovaný do endpointů je stejný s ochranou endpointů, v agentu je DLP modul, který je pro ochranu aktivován.



Obrázek 1 – DLP v rámci XDR platformy

Obrázek 2 – DLP v jednotném agentu

5.4.1.1. Ochrana DLP – blokové schéma



Obrázek 3 – Blokové schéma – ochrana DLP

Legenda: Červeně jsou zvýrazněny komponenty předmětu nasazení. Symbol „A“ identifikuje instalovaného agenta do endpointů. Symbol „SG“ je komponenta Service Gateway ve formě virtuální appliance, která zajišťuje potřebné lokální integrace. Symbol „XDR“ ukazuje XDR platformu v cloudu výrobce včetně modulu ochrany endpointů symbol „EPP“. Toto je shodné i pro DLP ochranu.

5.4.2. Technická specifikace DLP

(1) V současné době není implementována technologie DLP pro ochranu citlivých dat, a to jak na koncových stanicích, serverech nebo perimetru.

Ano, navržené řešení doplní DLP ochranu v rámci ochrany koncových zařízení od výrobce Trend Micro, kdy DLP funkcionalita je jednou z dalších ochran. Níže je popsáno, jak potřebu ochrany DLP shrnuje výrobce:

https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-digital-asset-contro

Lze primárně vyhledat v datovém listu „Trend Vision One™ - Endpoint Security“, včetně DLP.

Konfigurace ochrany prostřednictvím politik je popsáno zde:

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-apex-one-dlp-policies

Předmětem dodávky by měl být nástroj, který zajistí audit pohybu dat a detekci rizikových operací, pro klasifikaci citlivých a důvěrných dat a ochranu citlivých a důvěrných dat před únikem.

Ano, předmětem dodávky je DLP ochrana, která cílí na kontrolu přenosu souborů a jejich dat, čímž chrání před prozrazením či únikem. Ochrany DLP a Device Control jsou součástí TM Vision One XDR platformy jakožto ochrana endpointů pod názvem Standard Endpoint Protection (Apex One), celek má rozcestník dokumentace zde https://docs.trendmicro.com/en-us/documentation/trend-vision-one/

DLP část je zde: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-loss-prevention-email-security

DLP funkce jsou podrobněji popsány zde:

https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-officescan-data-loss_001

Minimální požadavky na technickou specifikaci DLP pro 800 koncových stanic (PC, NB) jsou uvedeny v následující tabulce.

Ano, DLP ochrana bude zajištěna v rámci ochrany koncových zařízení (endpointů) vč. XDR, kde požadavek na pokrytí endpointů je shodný. DLP nečerpá žádnou samostatnou či specifickou licenci. Je to vidět i z datového listu výrobce.

ID	Požadované parametry	Splněno
01	***Klasifikace dat na základě obsahu minimálně v běžných textových souborech (čisté txt, office dokumenty, pdf apod.). Platforma musí rozpoznat nejméně tyto typy souborů: výše zmíněné textové dokumenty, komprimované soubory, soubory tabulkových procesorů (například .xlsx), prezentace, bitmapová grafika, vektorová grafika a jiné multimediální soubory.*** Ano, DLP umí vytvářet politika a pravidla na základě obsahu v rozšířených typech souborů. V rámci XDR konzole v sekci SEP, DLP, Data Identitiers, File Attributes, členěno na skupiny: „Documents, Graphycs, Multimedia Files, Compressed Files, Database, Spreadsheets, Presentations, Linked	ANO

ID	Požadované parametry	Splněno
	and Embedded Files a Encrypted Files“. Jelikož podrobnost dokumentace výrobce nesahá do takové hloubky, rozpad na jednotlivé typy souborů v printscreenech. Typy identifikátorů dat: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-dlp-data-identifier-types Atributy souborů: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-file-attri Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm printscreeny	
02	***Vyhledávání vzorků pro obsahovou klasifikaci alespoň v textových formátech (viz bod 01).*** Ano, DLP provádí kontrolu na základě definovaných klíčových slov, které pak hledá v textových formátech. V rámci XDR konzole v sekci SEP, DLP, Data Identitiers, Key Lists. Jelikož podrobnost dokumentace výrobce nesahá do takové hloubky, rozpad na jednotlivé typy souborů v printscreenech. Klíčová slova: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-keywords Konfigurace pravidel prevence ztráty dat:	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm printscreeny	
03	***Možnost zadání vzorků pro obsahovou klasifikaci alespoň pomocí regulárních výrazů a výčtem vyhledávaných řetězců***. Ano, DLP provádí kontrolu s využitím vlastních či připravených regex výrazů. V rámci XDR konzole v sekci SEP, DLP, Data Identitiers, Expressions. Regex výrazy: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-expressions-ems-dlp Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm printscreeny	ANO
04	***Existence předpřipravených vzorků pro obsahovou klasifikaci alespoň pro část informací obecně považovaných za citlivé.*** Ano, předpřipravené výrazy jsou cílené i pro prostředí Evropy a ČR. Například předpřipraveny vzory k identifikaci rodného čísla občanů ČR. Regex vzory: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-loss-prevention-templates	ANO

ID	Požadované parametry	Splněno
	Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm printscreen	
05	***Klasifikace dat na základě zdroje, ze kterého byly získány (konkrétní aplikace/skupina aplikací, konkrétní webová stránka/skupina webů, síťová cesta/lokální cesta).*** Ano, DLP podporuje tvorbu politik a pravidel na základě různých komunikačních kanálů. V rámci XDR konzole v sekci SEP, DLP Policy, Channels, včetně Network Channels, Systém a Application Channels, Printers a Windows clipboard. Síťové kanály: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-network-channels Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm Printscreens	ANO
06	***Klasifikace dat na základě typů souborů (záchytná varianta pro typy nepodporované přímo obsahovou klasifikací).*** Ano, DLP podporuje tvorbu politik a pravidel na základě různých typů předdefinovaných i vlastních souborů (extensions.). Jejich kompletní výčet výrobce v dokumentaci nemá, ale jsme schopni je vypsat v printscreenech. Konfigurace pravidel prevence ztráty dat:	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm Printscreens extensions	
07	***DLP politiky definovatelné jak obecně, pro všechna přenášená data, tak i pro jednotlivé datové typy, které vzešly z některého typu datové klasifikace***. Ano, DLP politiky podporují kombinaci různých pravidel popisovaných výše. Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm	
08	***Možnost tvorby DLP politik i za využití metadat klasifikace třetích stran (nejméně velikost a typ souboru). Zejména pak platí ve vztahu k platformám pro ochranu operačních systémů a mobilních platforem.*** Ano, v rámci politik lze definovat typ souborů na základě předpřipraveného seznamu nebo zadáním vlastních. Obdobně lze nastavovat velikost souboru. Lze pracovat s informacemi o zařízení importem. Device list: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-running-the-device-list-tool Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm	ANO
09	***Možnost tvorby DLP politik s příslušnými atributy minimálně pro řízení e-mail komunikace (jak nativní aplikace, tak i webmaily), uploadu na síťová úložiště pomocí nativních aplikací, uploadu na web za použití browseru/webových aplikací obecně, uploadu souborů pomocí***	ANO

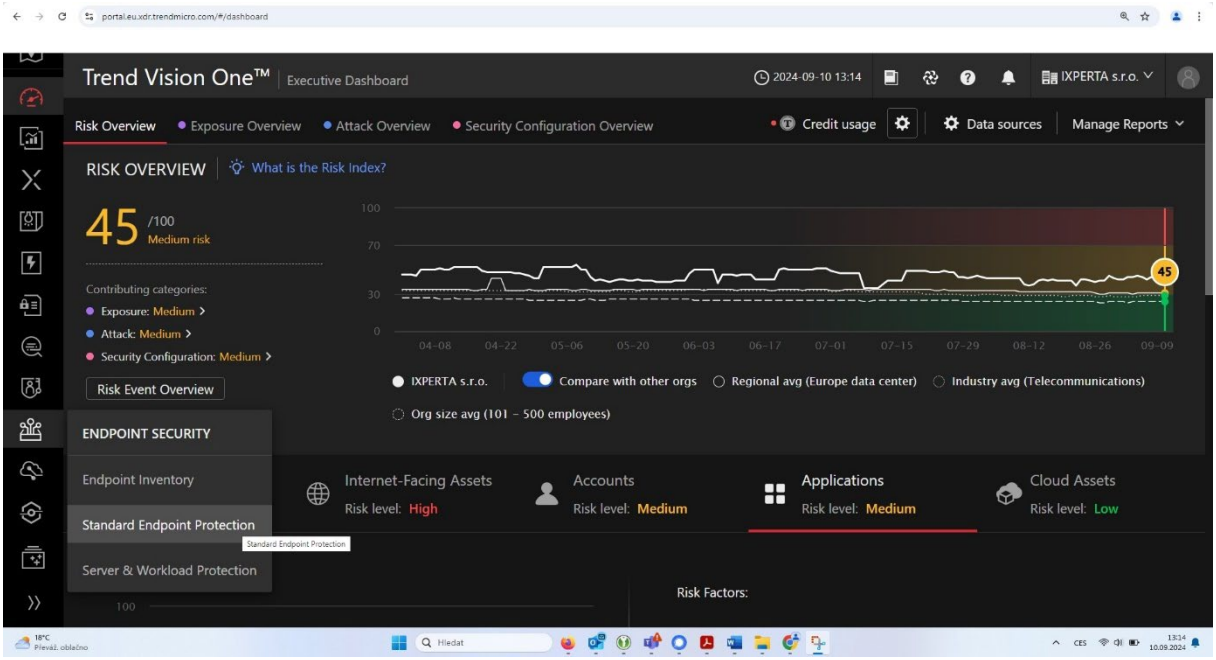
ID	Požadované parametry	Splněno
	komunikačních aplikací (Teams, Zoom, instant messaging aplikace apod.). Ano, toto nastavení politik a pravidel využívá definované komunikační kanály. Jejich kompletní výčet výrobce v dokumentaci nemá, ale jsme schopni je vypsat v printscreenech. Síťové kanály: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-network-channels Konfigurace pravidel prevence ztráty dat: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-dlp-rule-create-tmcm	
10	***Možnost řízení pohybu dat směrem na lokální výměnná datová úložiště (disky, optická média a USB zařízení, Bluetooth přenosy apod.).*** Ano, řízení pohybu dat je pak řešen ve spolupráci s další ochranou s názvem Device Control, kde politiky a pravidla určují, jak se řídí přenosy s externími zařízení a přenosy. Nastavení rámci XDR konzole v sekci SEP, Device Control. Systémové a aplikační kanály: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-system-application-channels Device Control: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-device-control-overview	ANO

ID	Požadované parametry	Splněno
	Nastavení Device Control: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configure-device-control-settings	
11	***Možnost řízení tiskových operací (lokální/síťové tiskárny, tisk do souborů).*** Ano, v rámci XDR konzole v sekci SEP, DLP Policy, Channels, Printers Printscreen	ANO
12	***Možnost definovat reakci politiky alespoň ve variantách povolit, zaznamenat (případně navíc upozornit uživatele), blokovat.*** Ano, DLP politika podporuje akce: blokace, povolení, notifikace, záznam (record data) a zašifrování (encrypt). Printscreen	ANO
13	***Možnost definice výjimek z jednotlivých DLP politik***. Ano, v DLP politiky je rovněž nastavení výjimek https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-loss-prevention-exceptions	ANO
14	***Možnost uchování dokumentů zachycených politikou pro pozdější analýzu.*** Ano, DLP politika podporuje akce: blokace, povolení, notifikace, záznam (record data) a zašifrování (encrypt). Toto v rámci record data. Printscreen	ANO
15	***GUI pro správu DLP systému (nativní aplikace pro Win OS platformu, nebo aplikace běžící v standardních webových prohlížečích).***	ANO

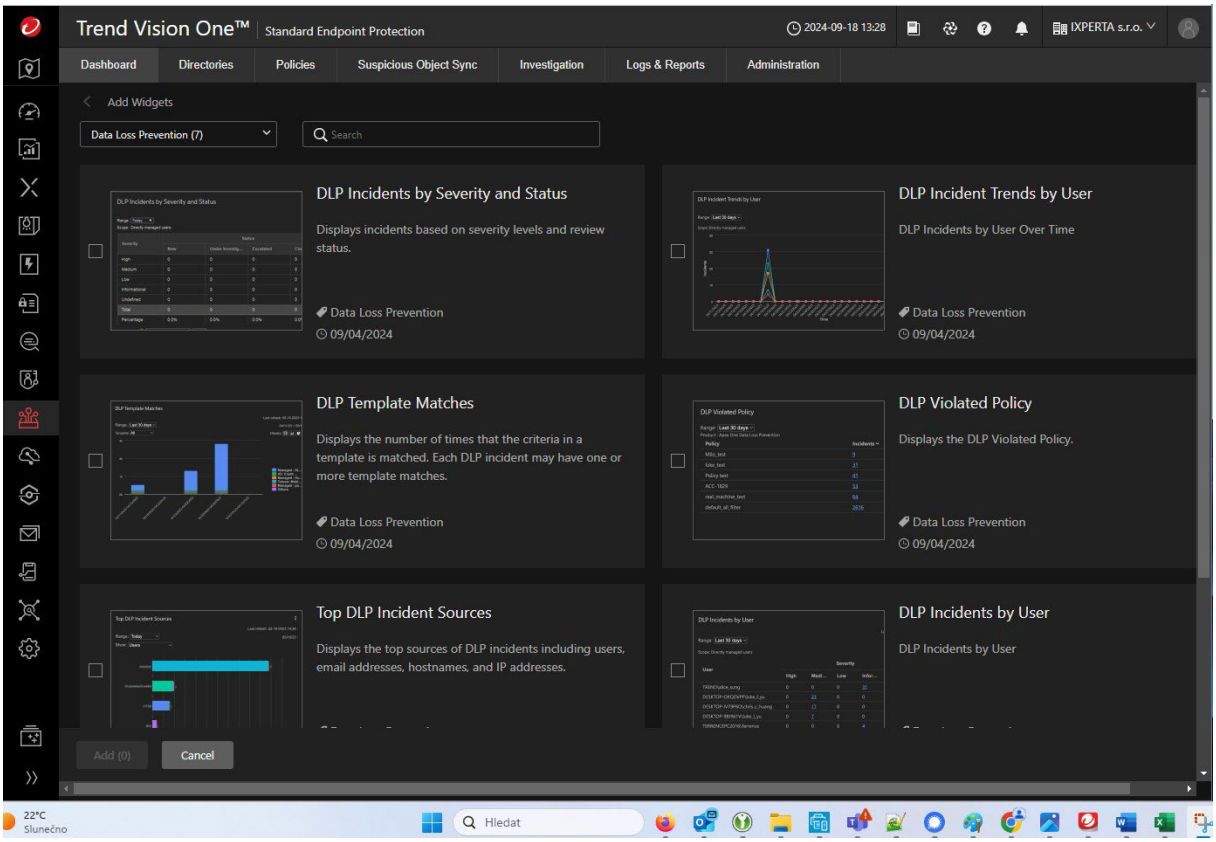
ID	Požadované parametry	Splněno
	Ano, GUI pro správu a kontrolu výstupů DLP je jednou z ochran zajištěných pod centrální XDR konzolí na základě webové služby. https://portal.eu.xdr.trendmicro.com/	
16	***Integrace s AD (načítání a párování informací o klientských stanicích a uživatelích, možnost definice výstupů z DLP politik s využitím informací na bázi AD objektů).*** Ano, aplikaci politik na endpointy lze provést i s vyžitím labelů a tagů, které lze mapovat i na skupiny definované v AD. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-custom-tags-filters	ANO
17	***Centrální správa klientů (aktivace/deaktivace, upgrade).*** Ano, centrální správa klientů (agentů) včetně aktivace/deaktivace a upgrade. Agent je shodný s ochranou koncových zařízení (endpointů).	ANO
18	***Možnost deaktivace jednotlivých funkcionalit klienta pro případný troubleshooting.*** Ano, změnou v politice lze aktivovat/deaktivovat funkcionality ochran vč. DLP. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-understanding-policy-list	ANO
19	***Možnost zasílání upozornění o závažných provozních událostech a porušení DLP politik (např. e-mail, syslog nebo SNMP trap apod.).*** Ano, ochrany včetně DLP umí poslat alerty komunikačními kanály e-mail a syslog. Nastavení prostřednictvím Event Notifications. Logy lze rovněž posílat z Centrální XDR konzole a lokální instance Service Gateway, která umí forwardovat syslog do lokálního LM/SIEM nástroje. SNMP trap/inform prostřednictvím monitorovacích nástrojů 3tích stran.	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-event-notifications-apex https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-logs-chapter-apex	
20	***Uchování auditních záznamů o konfiguračních úpravách DLP.*** https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-audit-logs https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-log-names-data-views	ANO
21	***Možnost exportu auditních informací do jiných systémů (např. centrální logování, SIEM) minimálně pomocí syslog protokolu.*** Ano, DLP ochrana podporuje syslog pro logování auditních informací. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-audit-logs https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-event-notifications-apex	ANO
22	***Generování reportů a grafů se záznamy o vyhodnocení/porušení DLP politik.*** Ano, DLP ochrana podporuje generování reportů a grafů se známy o vyhodnocení/porušení DLP politik. Je to konkrétně v rámci XDR konzole v sekci SEP v Dashboard / Data Loss Prevention. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-reports-section-apex	ANO

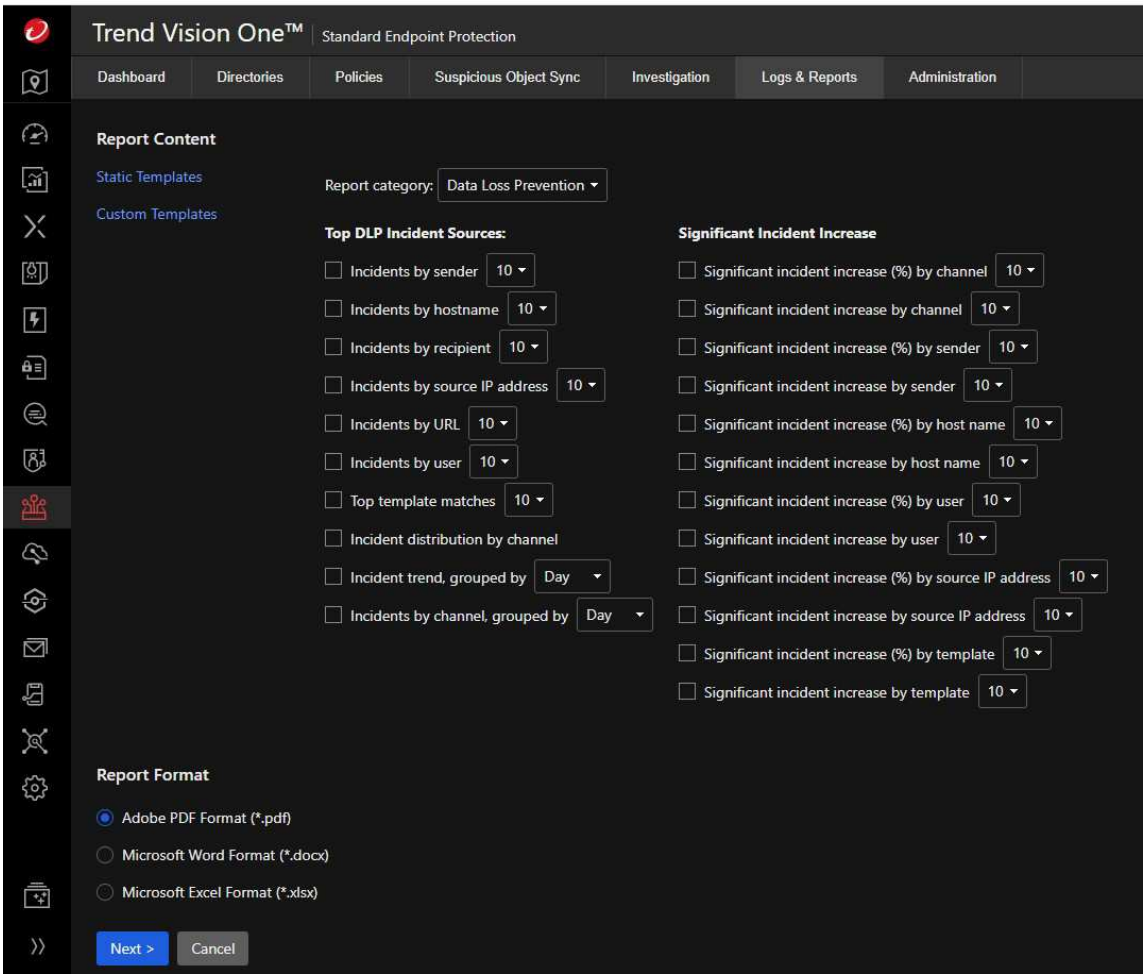
ID	Požadované parametry	Splněno
	printscreen	
23	***Komunikace mezi klientskými a serverovými komponentami, stejně jako mezi management rozhraním a serverem je zabezpečená kryptografickými prostředky aktuálně považovanými za bezpečné.*** Ano, obdobně, jak je popisováno u ochrany koncových zařízení (endpointů) přístupem k centrální XDR konzoli. Výrobce definuje použité algoritmy k ochraně dat při přenosu v „Supported Cyphers“ k použitému mechanizmu TLS 1.2. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-privacy-security-compliance	ANO
24	***Administrátorům je možné přiřazovat role, které definují přístupová oprávnění k jednotlivým komponentám management rozhraní.*** Ano, správa rolí a účtů (RBAC) je prováděna na úrovni XDR konzole. Lze zřídit roli dedikovanou pouze k obsluze ochrany DLP. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configuring-user-roles-accounts Printscreen.	ANO
25	***Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.*** Ano, SLA bude zajištěno v požadovaném rozsahu.	ANO



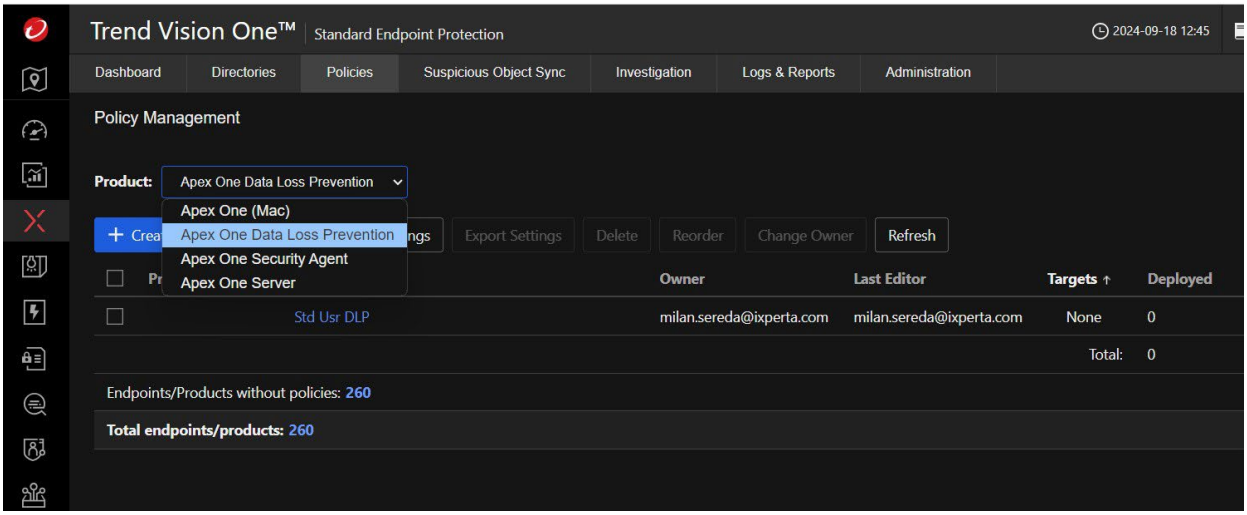
Obrázek 4 – XDR konzole cesta do části SEP, kde jsou DLP nastavení a výstupy



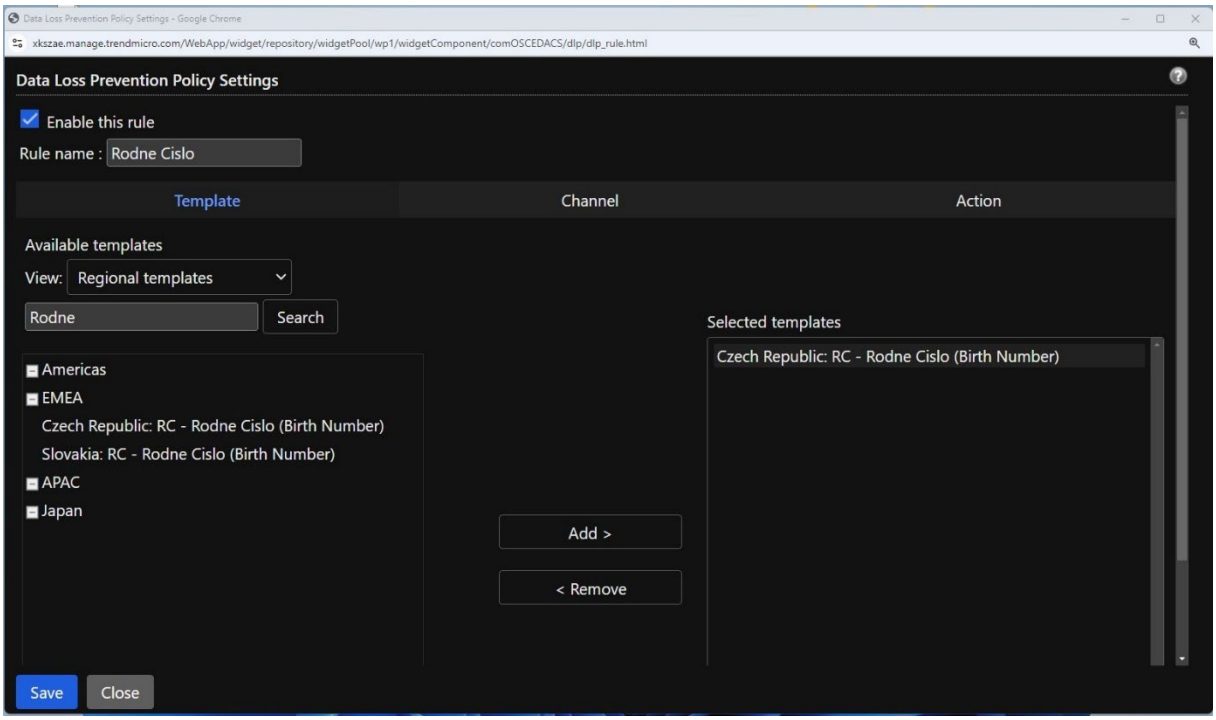
Obrázek 5 – Před připravené DLP dashboardy výrobcem



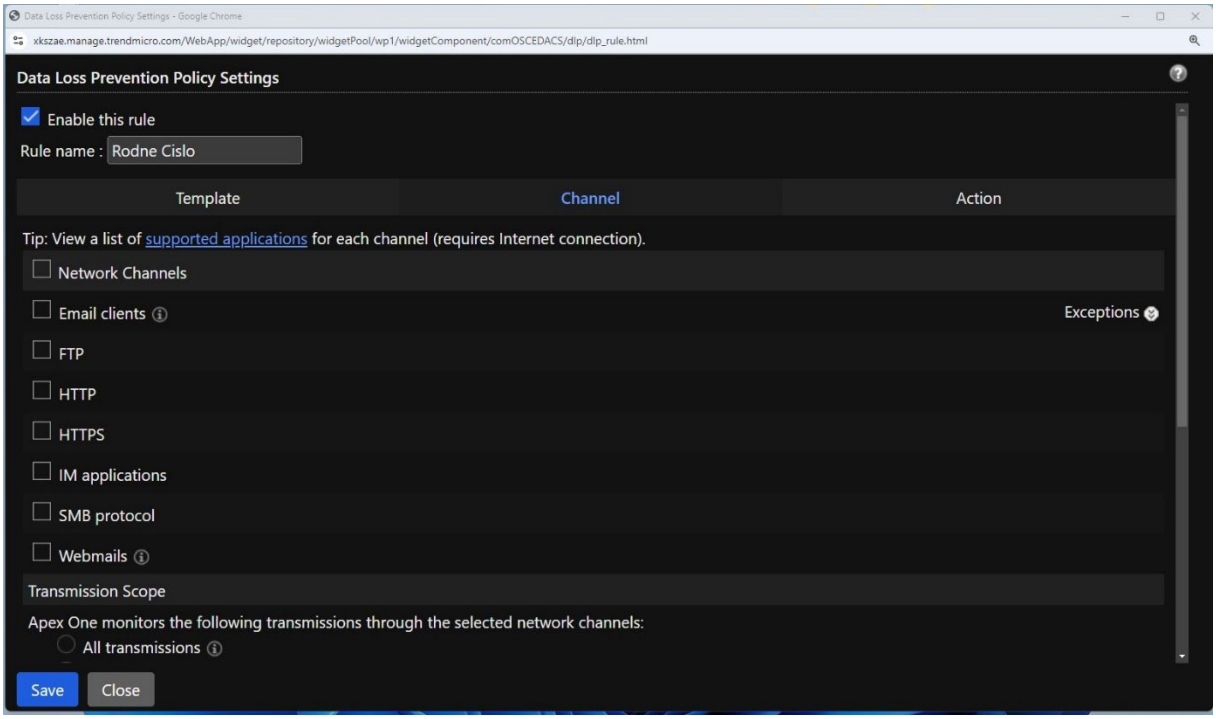
Obrázek 6 – Nastavení DLP reportingu



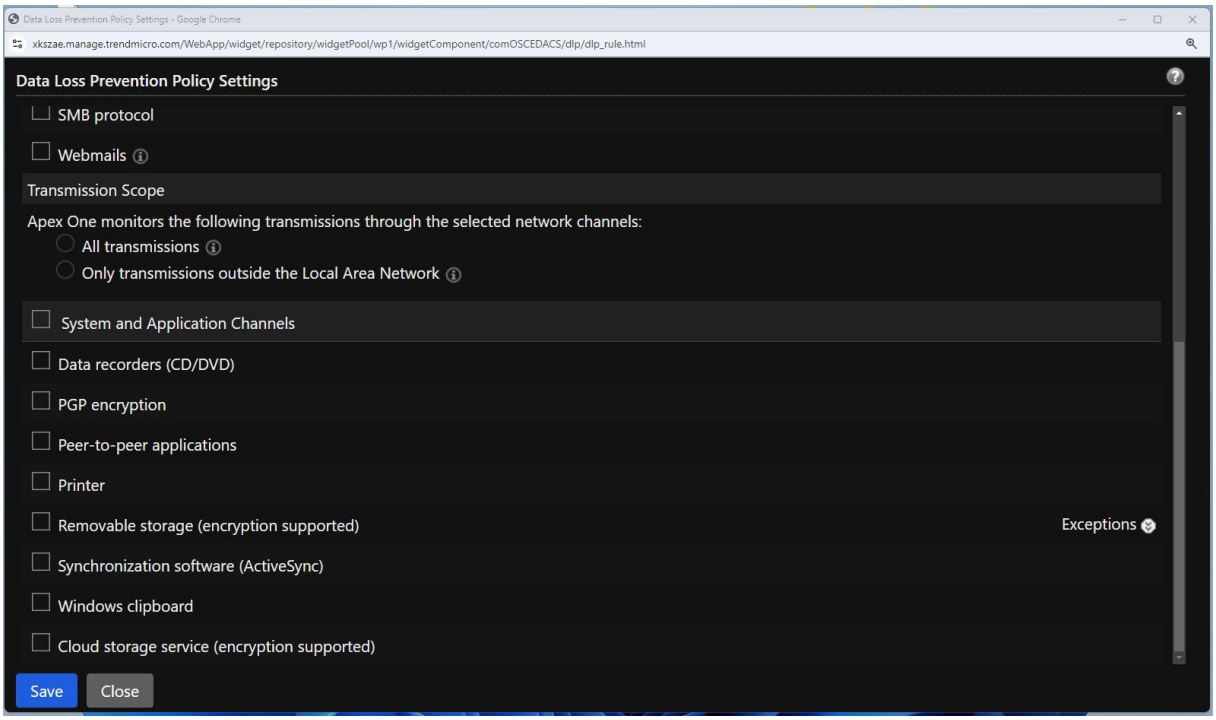
Obrázek 7 – Výběr DLP politiky



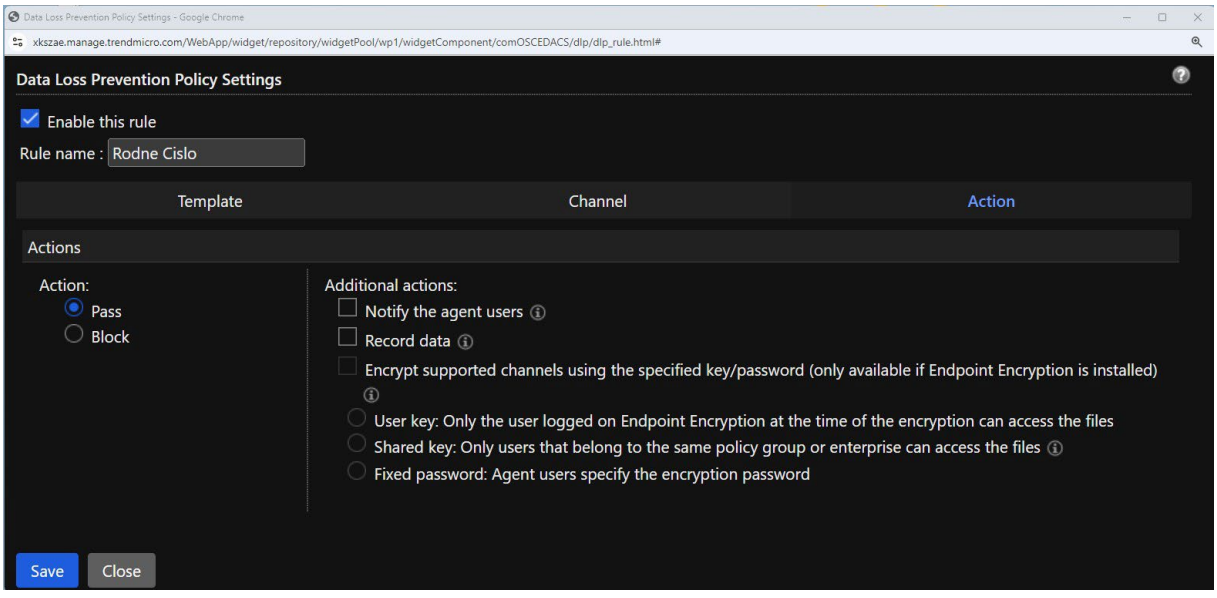
Obrázek 8 – Filtr na národní vzory a rodné číslo



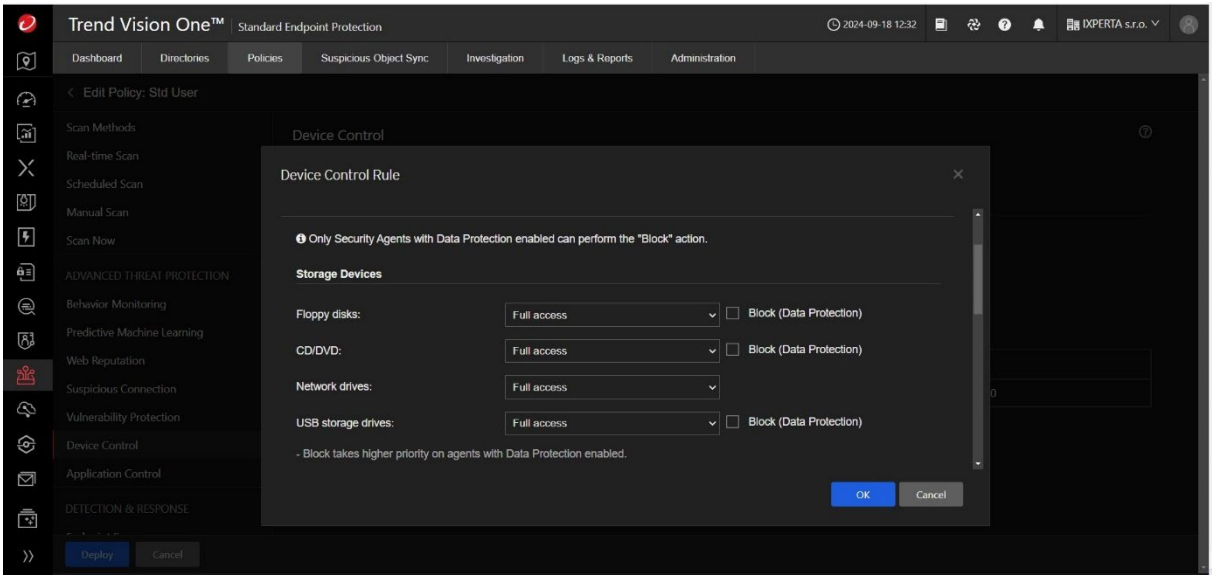
Obrázek 9 – síťové kanály v DLP politice



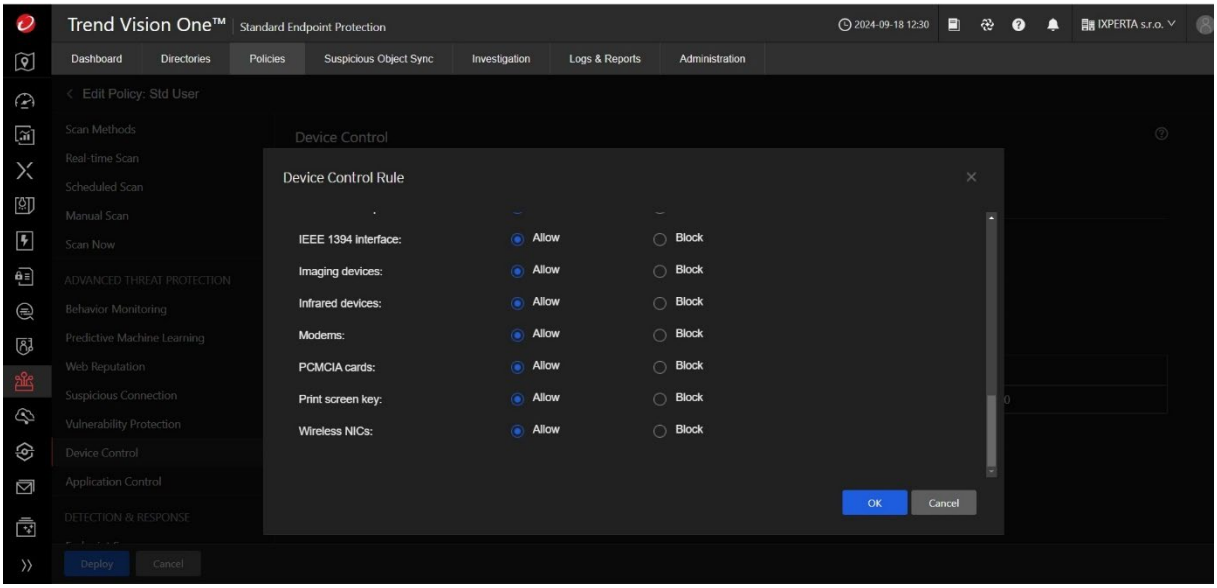
Obrázek 10 – Systémové a aplikační kanály v DLP politice



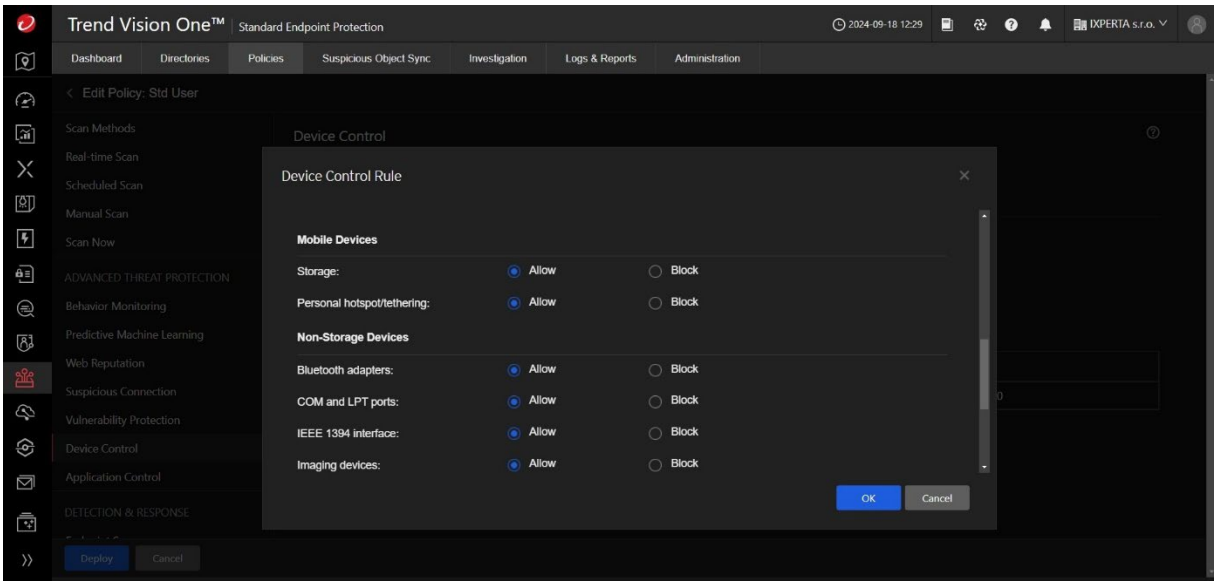
Obrázek 11 – Akce v DLP politice



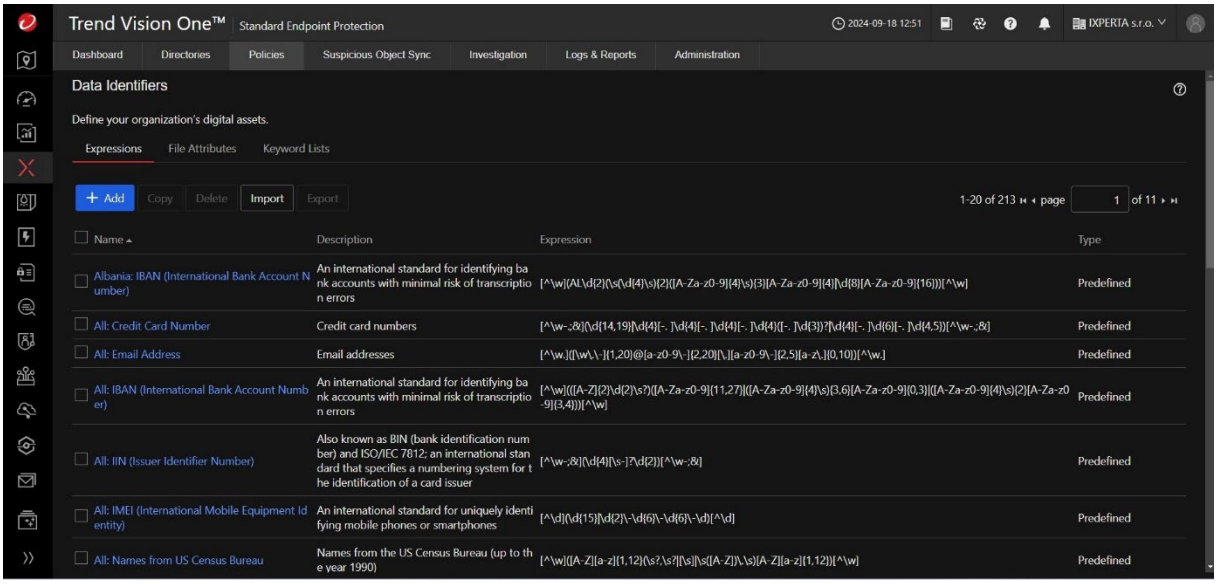
Obrázek 12 – kontrola výměnných zařízení



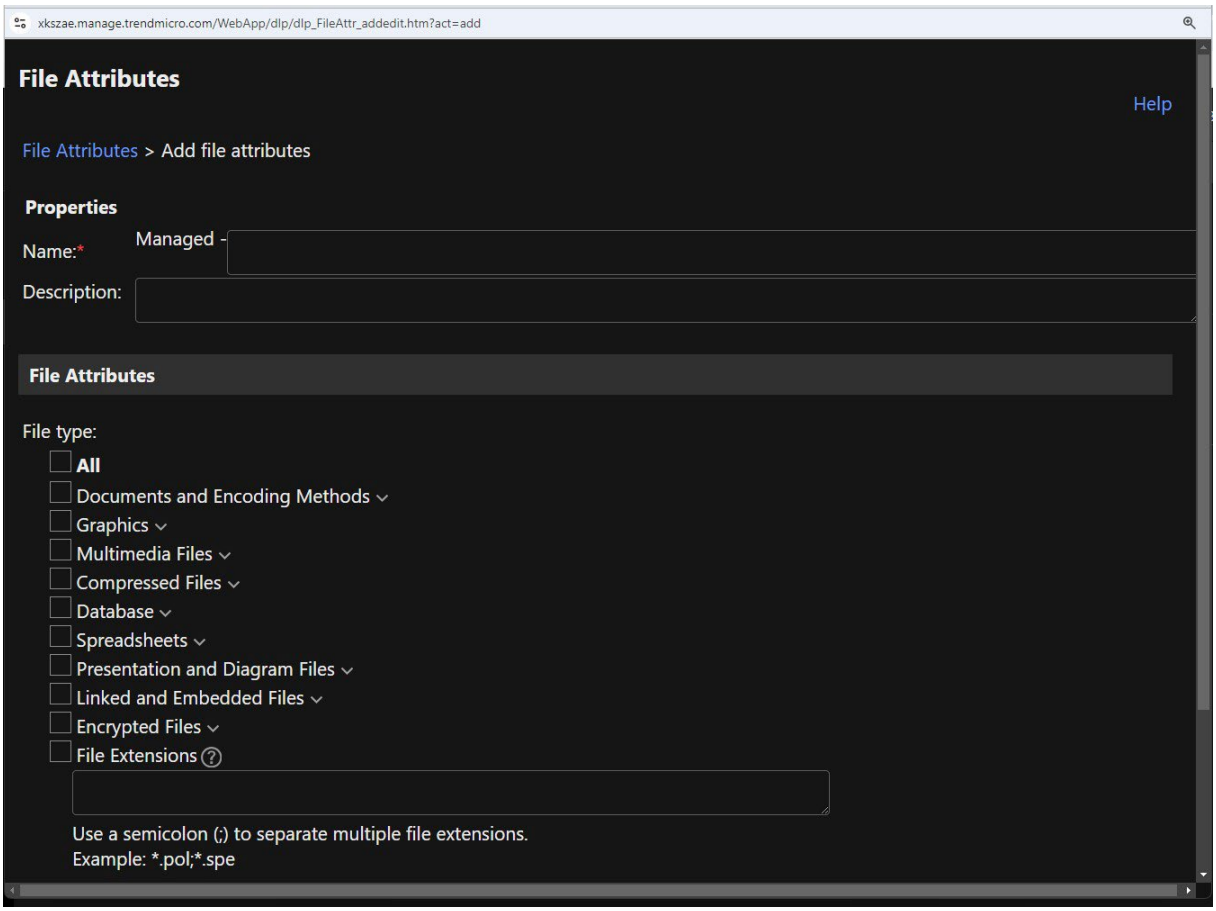
Obrázek 13 – kontrola výměnných zařízení



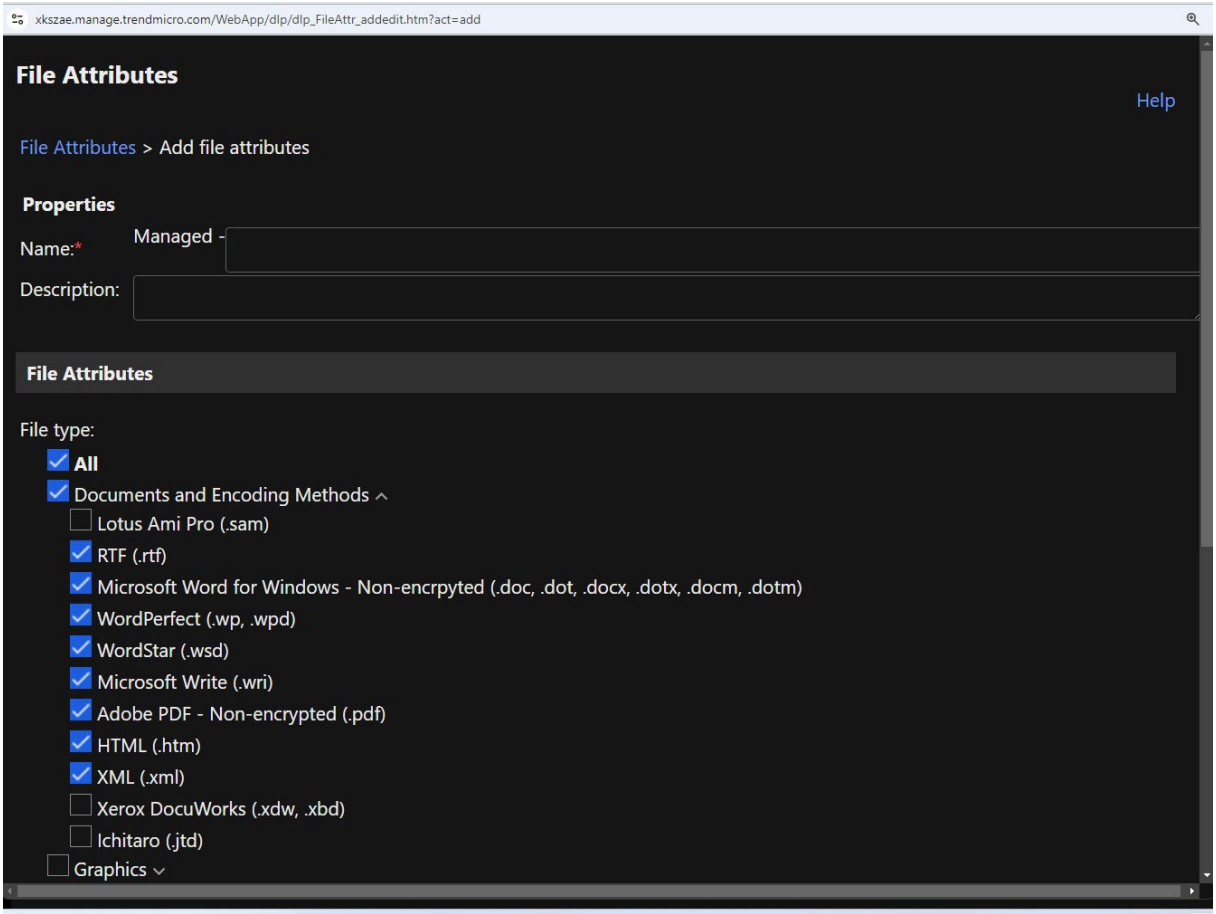
Obrázek 14 – kontrola výměnných zařízení



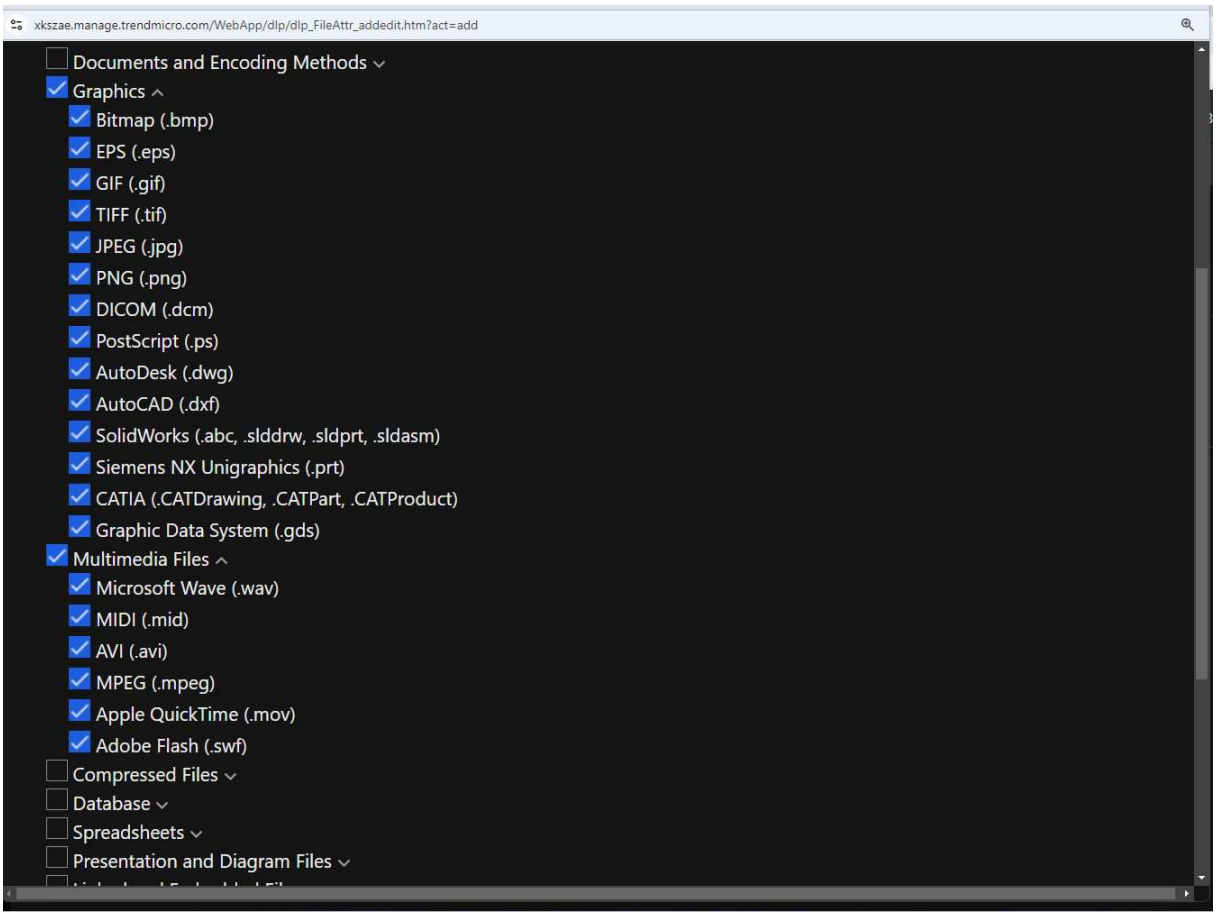
Obrázek 15 – Připravené regex výrazy



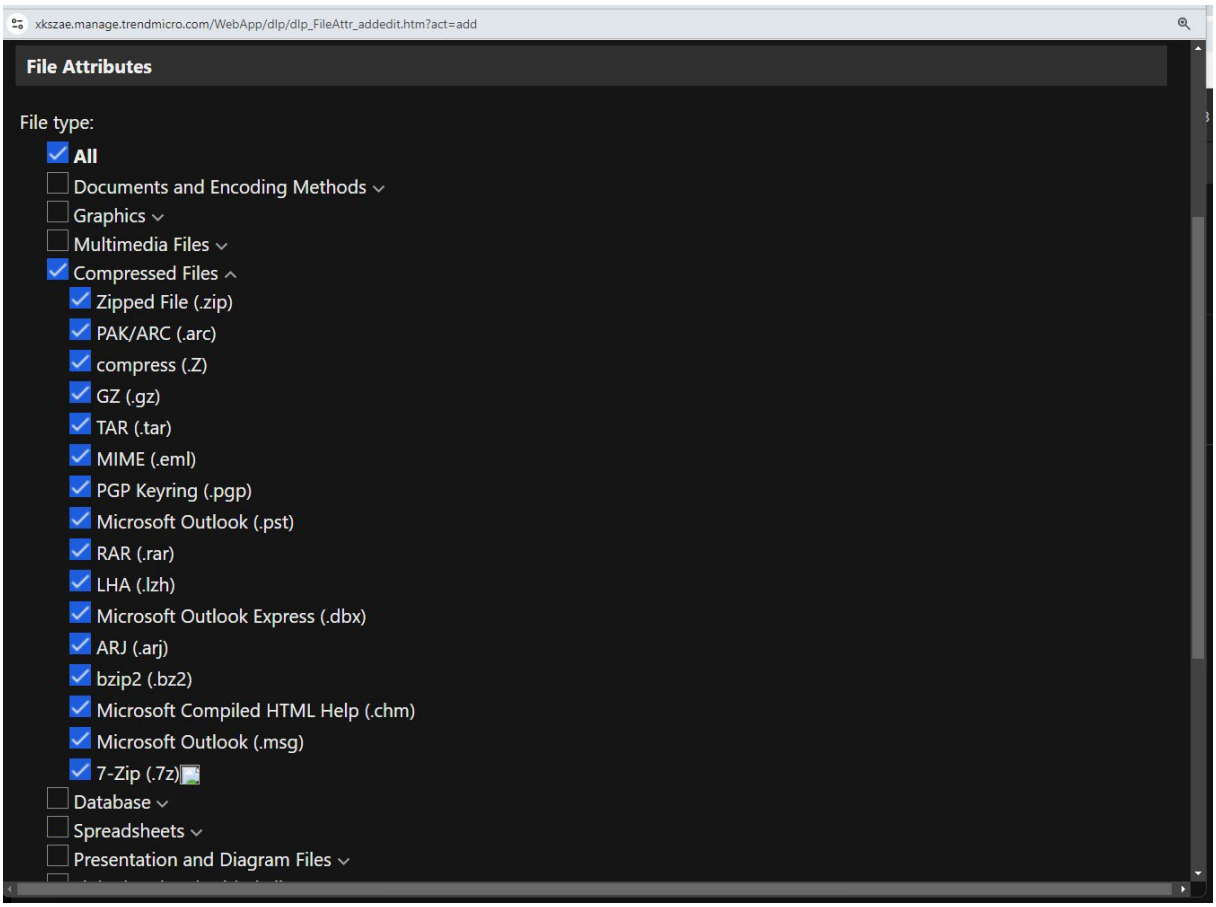
Obrázek 16 – připravené typy souborů



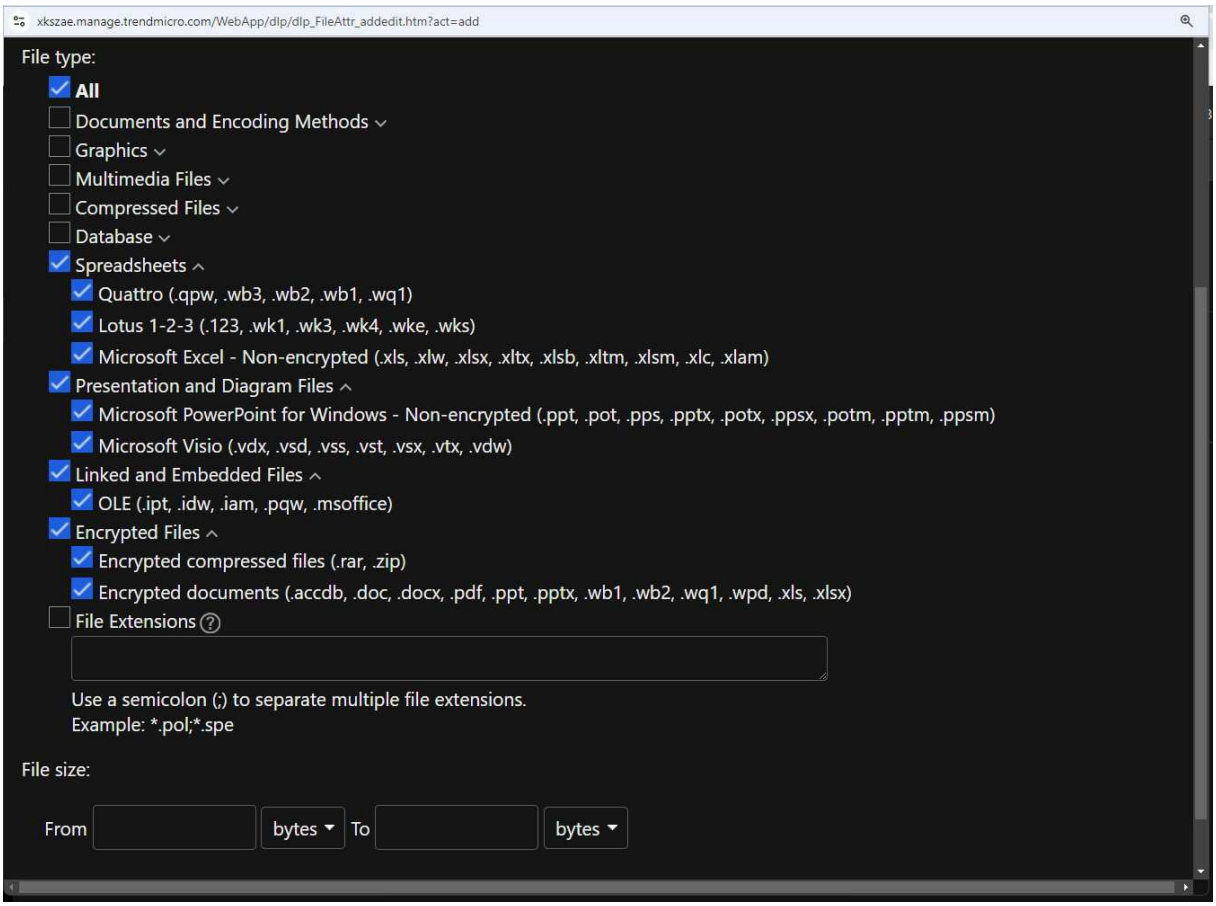
Obrázek 17 – připravené typy souborů – dokumenty



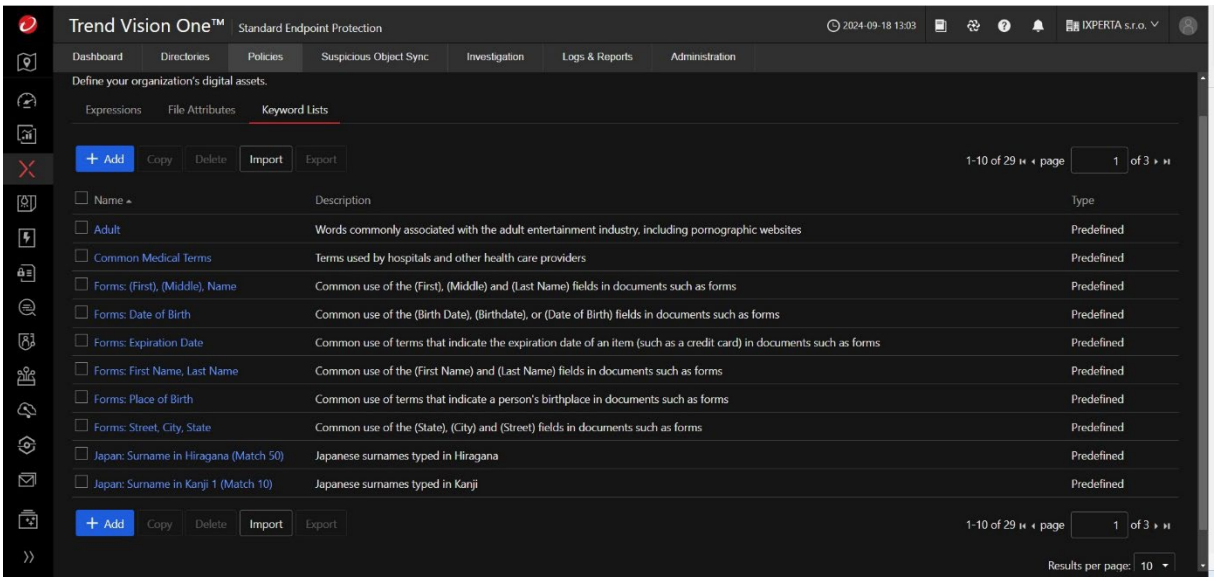
Obrázek 18 – připravené typy souborů - grafika a multimédia



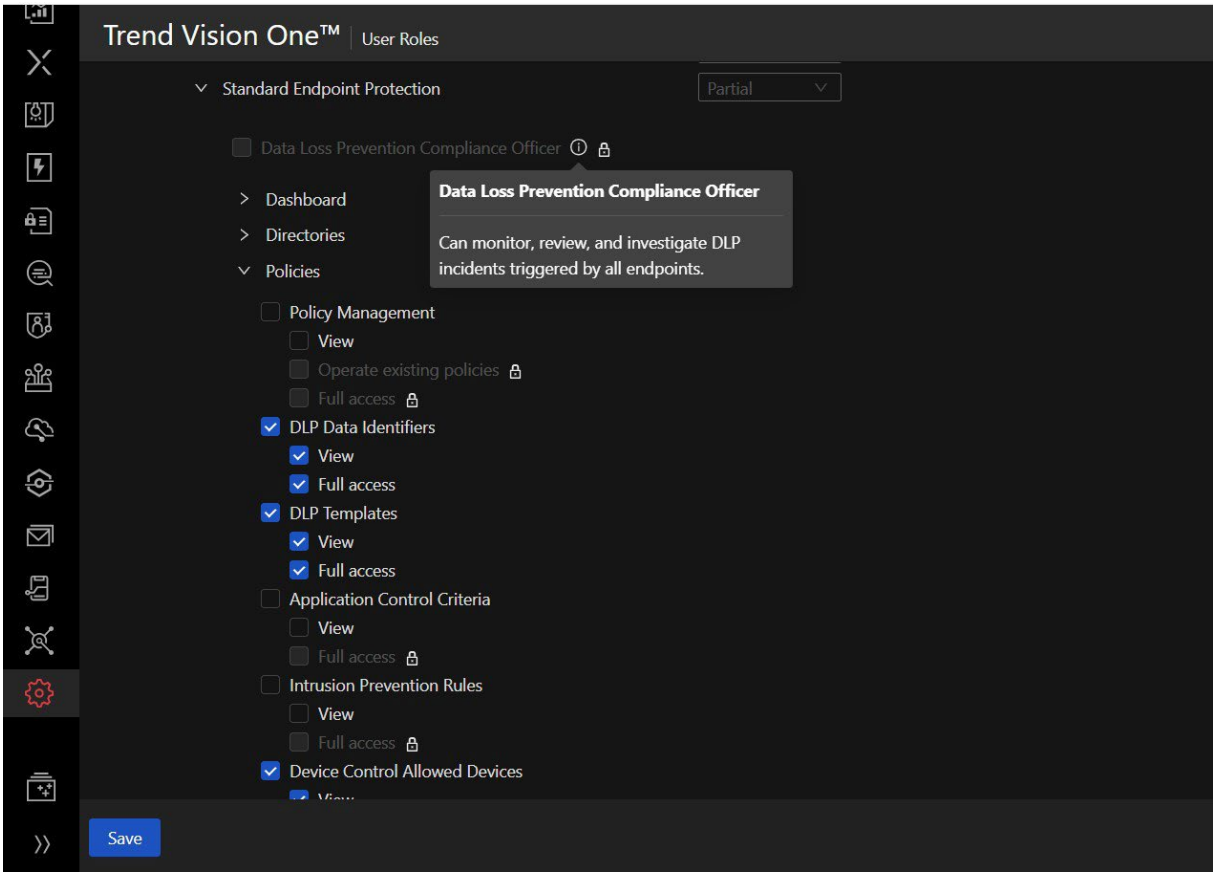
Obrázek 19 – připravené typy souborů - archivy



Obrázek 20 – připravené typy souborů – ostatní a volitelé přípony



Obrázek 21 – připravená klíčová slova v politice



Obrázek 22 – řízení přístupu k DLP

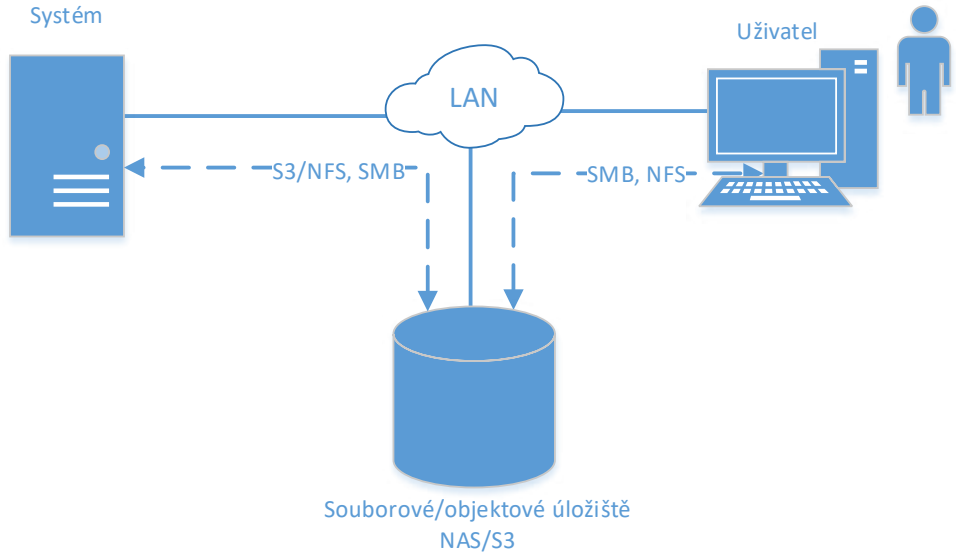
Part number: jsou sdílené společně s částí 5.8, kde jsou uvedeny.

Součástí technické specifikace DLP, jsou produktové listy nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.11** – Produktové listy_materiály_5.4.

5.5. Technická specifikace úložiště pro PACS a NIS data formou NAS a S3

Jako diskové pole pro PACS a NIS data nabízíme scale-out řešení od společnosti Qumulo (tzv. Qumulo cluster) založené na HW řešení od společnosti Hewlett-Packard Enterprise.

Systémy a uživatelé budou moci využívat protokoly NFS, SMB, S3 pro přístup k tomuto úložišti a toto úložiště bude integrováno se službou Active Directory pro možnost řízení klientských oprávnění.



Řešení nasazení úložiště pro nestrukturovaná data

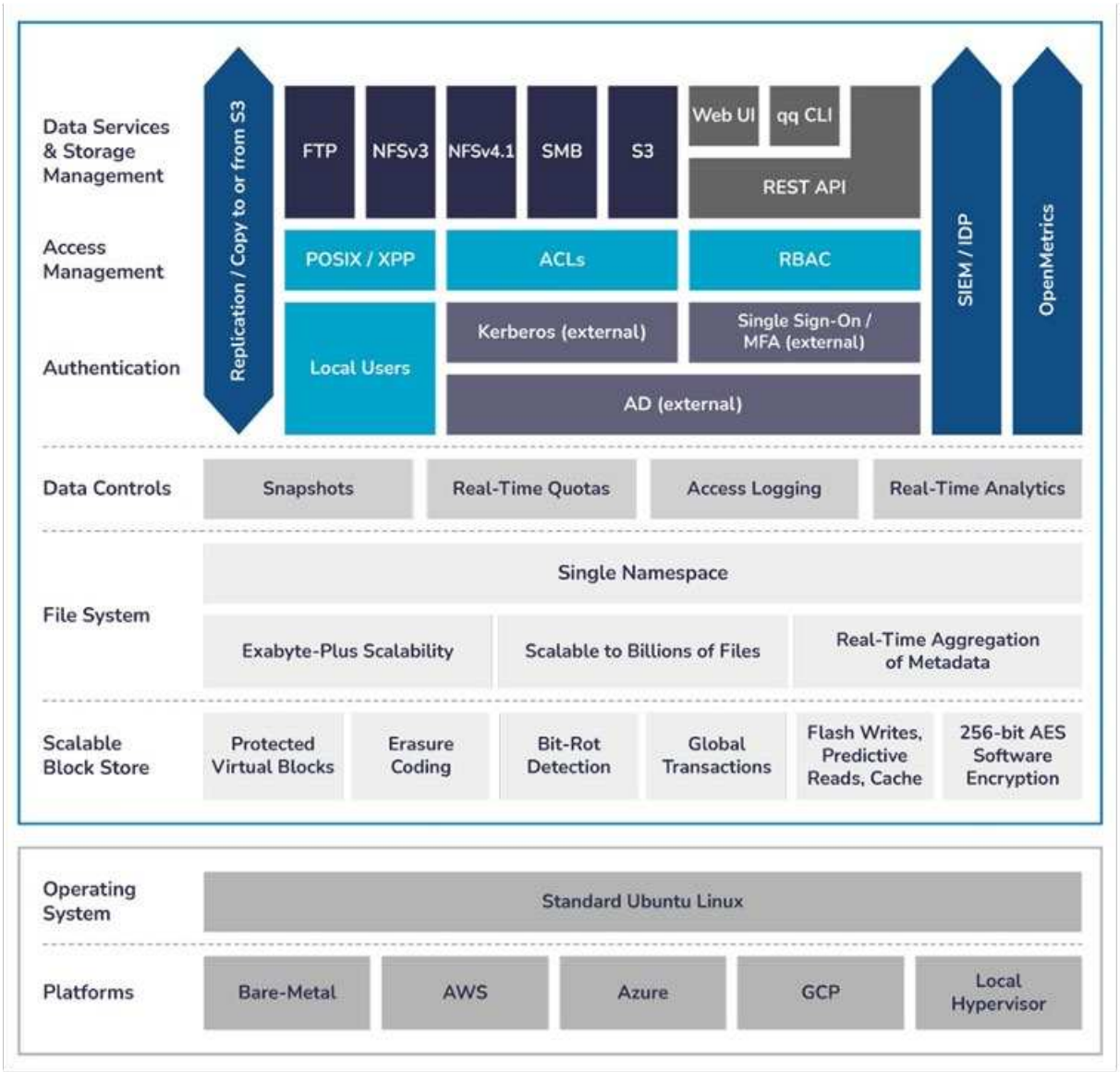
5.5.1. Platforma Qumulo

Qumulo poskytuje distribuovaný systém pro data, které prezentuje jako tzv. „Single namespace“ (jeden velký prostor pro data). Qumulo jako souborová datová platforma se skládá z shared-nothing clusterů nezávislých nodů. Každý z nodů poskytuje kapacitu a výkon. Jednotlivé nody se stále koordinují navzájem. Každý klient se může připojit k jakémukoliv nodu a provádět čtení a zápis z namespace.

Qumulo je vysoce dostupné a okamžitě konzistentní. Tato datová platforma pro nestrukturovaná data je vybudována pro zotavení se z chyb jednotlivých komponentů infrastruktury a stále poskytuje spolehlivé služby pro své klienty. Toto je dosaženo díky softwarové abstrakci, kódování erasure coding, vyspělých sítových technologií a také díky pečlivému testování. Když data jsou zapsáno do Qumulo software, potvrzení ke službě, uživateli nebo výpočetnímu nodu dorazí až ve chvíli kdy jsou data bezpečně uložena na persistentní části úložiště.

Qumulo platforma je API-first. Každá nová funkcionalita je API endpoint. Tato množina endpointů je následně prezentována v Qumulo command line interface (CLI) a v grafickém rozhraní.

Qumulo customer success team je vysoce responzivní, znalý a agilní. Každá souborová datová platforma má možnost se připojit pomocí vzdáleného monitoringu díky Qumulo Mission Control cloud-based monitoring služby. Qumulo supportní team používá tato data k pomoci se zákaznickými incidenty, poskytuje “insight” ohledně používání produktu a taktéž upozorňuje zákazníka v případě jakýchkoliv problémů. Kombinace inteligentního supportu a velice rychlé produktové inovace vede k v IT průmyslu ojedinělém NPS skóre 80+.



Qumulo Data Platform

Datový přístup je možný přes síťové souborové protokoly NFS, SMB a FTP a objektový přístup přes S3 rozhraní. Tyto protokoly existují jako nezávislé a škálovatelné zdroje na každém nodu Qumulo clusteru. Koncový uživatelé vidí jednotný namespace, který může růst jak kapacitně, tak výkonově. Tento namespace může být přístupný z jakéhokoliv Windows, Mac nebo Linux výpočetního zařízení a také pomocí API z jakékoliv aplikace.

Naše autentifikační vrstva podporuje dvě standardní identity služby: Active Directory (AD) a Lightweight Directory Access Protocol (LDAP). Připojení Qumulo datové platformy vyžaduje velice jednoduchou konfiguraci a pracuje velice dobře v komplexním a distribuovaném prostředí z hlediska identity služeb (toto bývá velký problém v enterprise, private a public cloud prostředích).

Každý datový přístupový protokol používá společnou autentifikační vrstvu ke komunikaci s daty uloženým na naší souborové datové platformě. To umožňuje uživatelům se pohybovat mezi aplikacemi, operačními systém a prostředími a přistupovat na stejná data. Protože se data přesouvají v průběhu jejich životního cyklu, toto oddělení vrstev nabízí kritickou flexibilitu a redukuje počet systémů, které musí zákazník administrovat.

Management a vrstva programovatelnosti je vybudována díky třem vlastnostem – REST API, command line interface (CLI) a grafickému rozhraní.

Mezi základní výhody našeho řešení patří:

Lineární škálovatelnost jak výkonu, tak kapacity, tak i síťové propustnosti

Přidáním nebo ubíráním nodů dosahujeme vždy téměř lineárního zvýšení výkonu celého clusteru a to jak z hlediska výkonu, tak z hlediska kapacity a síťové propustnosti.

Konstantní výkon v jakékoliv situaci

Deklarovaný výkon je k dispozici v každém okamžiku bez ohledu, zda úložiště provádí nějaké automatické interní operace, případně dochází například k situaci, kdy klientská operace vyžaduje údržbu tzv. proces tree-walk.

Stejné nody z hlediska procesorů, disků, atd.

Naše řešení není kombinací například rychlejší a pomalejší části, což už z principu vyžaduje další overhead z hlediska nutnosti monitorování, přesunu souborů mezi jednotlivými tiers atd. Garantovat lze homogenní pole, které pro celou deklarovanou diskovou kapacitu dokáže garantovat výkon: latenci, prostupnost i IOPs. Nikoliv jen za předpokladu cache hit apod.

Rychlejší inovace

Qumulo souborová platforma je softwarové řešení a díky tomu, nabízí výrazně rychlejší inovace a to jak z hlediska softwarových funkcionalit, kdy nové release s novými funkcionalitami jsou vydávány v průměru každé dva týdny, tak i hardwaru. Naše řešení umožňuje oproti konkurenci výrazně rychlejší inovaci z hlediska použití nejnovějších

výpočetních, storage a síťových technologiích oproti řešení tzv. „black boxů“, kde už z podstaty je inovační cyklus výrazně pomalejší.

100% kapacity

Naše řešení umožňuje opravdu naplnit pole daty na 100% na plnou nabízenou kapacitu. U konkurenčních řešeních (Netapp, EMC Isilon) již například při 80% zaplněnosti dochází k citelnému zpomalení. Tento problém s námi řešit nebudete muset.

Možnost převodu licencí cloud on-prem a zpět

Qumulo souborová platforma používá tzv. transferable capacity licencing. Tedy pokud v budoucnu například přemýšlíte o přechodu k některému z velkých cloud providerů, tak je možno licenci převést a Qumulo software používat v úplně stejném režimu jak znáte. Jsme si vědomi strategie go to cloud a rádi bychom podotkli, že řešení Qumulo je nezávislé na umístění a stejné licence můžete provozovat jak ve veřejném coudu, tak on premise.

No vendor lock-in

Qumulo datová platforma je softwarové řešení. Pokud v budoucnosti z jakéhokoliv důvodu budete potřebovat změnit HW platformu, tak je toto bez problémů možné.

Qumulo jako společnost

Qumulo je agilní softwarová společnost, která je plně fokusovaná na poskytování co nejlepšího řešení pro zákazníky v oblasti souborové datové platformy. To co nabízíme není tedy jenom jedna malá část celkového portfolia daného vendora, kde už z principu není jistota, že tato technologii bude v budoucnu daným vendorem podporována a vylepšována. Tato skutečnost se odráží jak v kvalitě supportu tohoto produktu, který je rychlý, znalý a vysoce responzivní, tak například ve velice rychlé inovaci.

NFS a SMB přístup pro stejná data

Vzhledem k unikátnímu řešení Cross-Protocol Permission (XPP) uživatelé mohou opravdu bez problému pracovat nad stejnými daty a to jak pomocí SMB, tak NFS protokolu.

Real Time analytics

Naše řešení jako jedno z mála na trhu umožňuje opravdu v reálném čase monitorovat, co se se systémem v dané chvíli děje a díky tomu i případně okamžitě reagovat.

GUI, CLI, API

Většina funkcí řešení Qumulo je dostupná pomocí všech možných kanálů. Integrace je jednoduchá a hlavně pro většinu běžně dostupných aplikací už hotová. Stačí si jen vybrat: https://qumulo.github.io/.

Velké či malé soubory?

Některá řešení jsou závislá na velikosti ukládaných dat. Pole mohou být optimalizována pro broadcasting, media archive či obecnou NAS. Qumulo zvládne vše. Malé soubory Vaše nové Qumulo pole nijak nezpomalí.

5.5.2. Technické řešení

Navrhované řešení Qumulo je postaveno na hardware platformě HPE Apollo 4200 Gen10+, což je vysoce kapacitní serverové řešení, které zabezpečuje běh SW Qumulo a zároveň mu poskytuje diskovou kapacitu.

HPE Apollo 4200 Gen 10+

Každý jeden uzel tohoto řešení je koncipován jako hybridní systém s těmito vlastnostmi:

- HDD (7k2) kapacitní diskový prostor (9x10TB)

- SSD kapacita pro cache (3x800GB)
- 64GB RAM
- Intel Xeon 4310 (2.1Ghz, 12 core)
- 2 x PSU
- 2 x 25 GbE NIC + 1x1GbE OOB Management
- 2 RU

Celková použitelná kapacita jednoho Qumulo clusteru je 199 TB a výkonnostní a provozní charakteristiky jsou uvedeny v přiložených konfiguracích z oficiálního konfigurátoru výrobce Qumulo a jsou platné pro jednu instanci diskového pole pro nestrukturovaná data (clusteru).

Qumulo

Report generated Wed, 12 Jun 2024 21:15:16 GMT - Version 34e981c

New Qumulo Cluster
4 nodes, 199.93 TB Usable

Capacity

Capacity (Usable)	199.93 TB
Config Can Scale to	18,881.43 TB
Encoding	6,4
Capacity (Raw)	360 TB
Efficiency	56 %

Performance

Performance Class	Active
Cached Read	6,436 MB/s
Sustained Write	2,552 MB/s
Uncached Read	4,256 MB/s
SS Uncached Read	1,536 MB/s
Burst Write	4,852 MB/s
IOPS	46,764
Single Stream Write	1,095 MB/s
SS Cached Read	2,786 MB/s

Nodes

Nodes in Cluster	4 nodes

Data Protection

Drive Outage Tolerance	2
Node Outage Tolerance	1

Endurance

Write Volume (Max)	16 TB/day
Cluster Overwrite Cadence (Max)	12 days

Networking

Front-end Ports	8 ports
Back-end Ports	0 ports
Front-end Networking	25 GbE
Back-end Networking	25 GbE

Environmentals

Rack Space Required	8 U
Height (Node)	3.5 in
Width (Node)	17.2 in
Depth (Node)	33 in
Weight (Total)	393.6 lbs
Typical Watts (Total)	1,200 W
Typical Amps @110/115V (Total)	10.91 A
Typical Amps @240V (Total)	5 A
Typical Thermal BTU/hr (Total)	4,092 BTU/hr

Seznam HW a SW

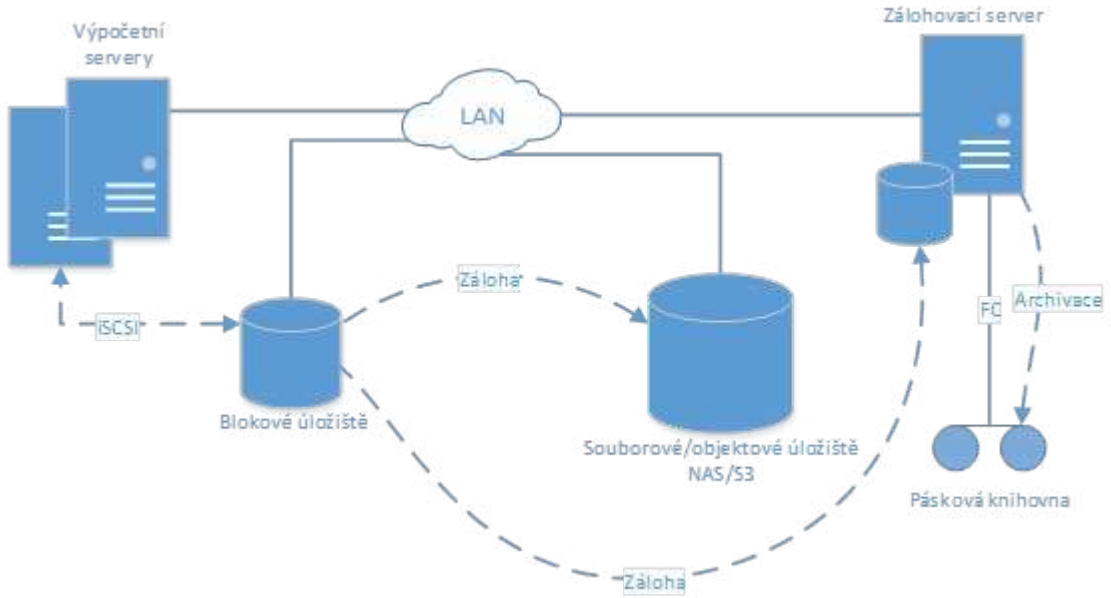
Počet	Part Number	Popis
4	S0D91A	HPE A4200 G10+ 90TB 25G Hyb TAA Qumulo
360	R0G85AAE	Qum A-Tier1TB 5Y Sub QSvc/Sup E-LTU
4	HU4B2A5#ZX3	HPE Apollo 4200 Gen10+ Support
8	844477-B21	HPE 25Gb SFP28 to SFP28 3m DAC

Součástí technické specifikace úložiště pro PACS a NIS data formou NAS a S3, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.12** – Produktové listy_materiály_5.5.

5.6. Technická specifikace infrastruktury pro zálohování a rychlou obnovu

V nabízeném řešení počítáme s využitím samostatného zálohovacího serveru a jeho diskového subsystému jako primárního úložiště záloh v kombinaci s páskovou knihovnou jako archivního úložiště. Zálohovací řešení se dá dále integrovat s úložištěm pro nestrukturovaná data a využít tak výhod tohoto úložiště jako velmi výkonného repozitáře části nebo všech záloh včetně funkce instantní obnovy zálohovaných systémů.

Navržená HW platforma je založena na řešení high-dense serveru HPE Apollo, SW platforma na řešení Veeam Data Platform a archivační pásková knihovna HPE MSL 2024.



Řešení nasazení zálohování

5.6.1. HW pro zálohování

Pro splnění požadavku na zálohovací server navrhujeme vysoce kapacitní serverové řešení na hardware platformě HPE Apollo 4200 Gen10+, která v nabízené konfiguraci splňuje požadované parametry uvedené v technické specifikaci.

HPE Apollo 4200 Gen 10+

Konfigurace nabízeného zálohovacího serveru má mimo jiné tyto vlastnosti:

- 24x LFF disková pozice osazená kapacitními disky (24x20TB 7k2)
- 8x SFF disková pozice osazená SSD disky pro OS (6x480GB)
- 128GB RAM
- Intel Xeon 5315 (16-core)
- 2 x 800W PSU
- 4 x 25 GbE NIC port + 1x1GbE OOB Management
- 2 RU
- Fibre Channel HBA (2x16Gbps FC port)
- podpora na 5 let (NBD)

Licence operačního systému (Windows Server OS) jsou součástí nabídky.

5.6.2. HW pro archivaci

Navrhujeme snadno spravovatelnou a kyberneticky odolnou páskovou knihovnu HPE MSL2024 vybavenou jednou páskovou mechanikou LTO-8, kterou je možno rozšířit pomocí další mechaniky a páskových médií LTO (8/7).

Tato pásková knihovna sestává z jednoho šasi o výšce 3RU osazeného jednou páskovou mechanikou LTO-8 s FC rozhraním. Šasi má 24 slotů pro pásky a dva sloty pro páskové mechaniky.

Jako média jsou používány LTO-8 pásky (20ks). Kapacita pásek při kompresi je až 600TB. Nekomprimovaná kapacita jedné LTO-8 pásky je 12TB, tj. celkem 240TB.

Nativní rychlost LTO-8 mechaniky je 300 MB/s, jak pro zápis, tak pro čtení.

5.6.3. Zálohovací software

Stávající zálohovací řešení založené na platformě Veeam bude doplněno o komponenty potřebné k zajištění bezpečnosti dat záloh, případně bude systém optimalizovaný dle best practice popsaných výrobcem Veeam SW. Jako bezpečné úložiště záloh bude sloužit Veeam hardened repository chránící data záloh proti pozměnění (ochrana proti ransomware) a následně budou data archivována na pásková média do přímo připojené páskové knihovny. Je také možno samotnou roli Veeam zálohovacího serveru přesunout na nově instalovanou instanci virtuálního serveru (Windows OS).

Data záloh mohou být také ukládána na výkonnější úložiště pro nestrukturovaná data.

Bude využita funkcionalita Direct SAN Access, kdy zálohovací server bude připojen do iSCSI SAN sítě a data během zálohovací úlohy budou přenášena přímo z primárního úložišťě pro strukturovaná data. Případně mohou být na primární virtualizaci nasazeny backup proxy a využívat funkcionalitu HotAdd.

5.6.4. Sizing Veeam komponent

Konfigurace všech novývh komponent systému Veeam (repository, proxy atp.) budou odpovídat oficiálnímu designu od společnosti Veeam pro dodržení výkonnostních a funkčních předpokladů.

5.6.5. Licence

Stávající licence pro SW Veeam budou doplněny o licence typu Veeam Data Platform Foundation ve formě Subscription pro pokrytí všech workloadů prostředí pro běh management a bezpečnostních prvků.

Seznam HW a SW

Počet	Part Number	Popis
1	P28700-B21	HPE A4200 Gen10+ 24LFF TAA CTO System
1	P28700-B21#B19	HPE A4200 Gen10+ 24LFF TAA CTO System
2	P42910-B21	INTXeon-S4314KitApollo4200Gen10+
8	P06031-K21	HPE 16GB 2Rx8 PC4-3200AA-R Smart Kit
1	P28703-B21	HPE A4200 G10+ 8SFF x4 TM BC Cage3 Kit
6	P40497-K21	HPE 480GB SATA RI SFF BC MV SSD
24	P53554-K21	HPE 20TB SATA 7.2K LFF LP ISE MV HDD
1	P28711-B21	HPE Apollo 4200 G10+ PCIe Prim Riser Kit
1	P04220-B21	Microchip SR932i-p Cntrl for HPE Gen10+
1	P26262-B21	BCM 57414 10/25GbE 2p SFP28 Adptr
1	P28717-B21	HPE A4200 G10+ PCIe Sec/Tert Riser Kit
1	P9D94A	HPE SN1100Q 16Gb 2p FC HBA
1	P01366-B21	HPE 96W Smart Stg Li-ion Batt 145mm Kit
1	804331-B21	HPE Smart Array P408i-a SR Gen10 Ctrlr
1	P10115-B21	BCM 57414 10/25GbE 2p SFP28 OCP3 Adptr
2	P38995-B21	HPE 800W FS Plat Ht Plg LH Pwr Sply Kit
1	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
1	P28705-B21	HPE A4200 G10+ 8SFF Cage3 CPU1 TM Kit
1	P07818-B21	HPE DDR-4 DIMM Blanks Kit
1	P28725-B21	HPE Apollo 4200 Gen10+ Rail Kit
1	P28726-B21	HPE Apollo 4200 Gen10+ CMA
1	P41662-B21	HPE Apollo 4200 G10+ Stnd Air Baffle Kit
2	P41666-B21	HPE Apollo 4200 G10+ Stnd Heat Sink Kit
1	P43601-B21	HPEA4200Cage1-AROCP1FIOCtrlMode
1	P43607-B21	HPEA4200Cage2-AROCP2FIOCtrlMode
1	P46171-021	MS WS22 16C Std ROK en/cs/pl/ru/sv SW
1	P46195-B21	MS WS22 16C Std Add Lic WW SW
1	AK379A	HPE MSL2024 0-Drive Tape Library
1	Q6Q67A	HPE MSL LTO-8 FC Drive Upgrade Kit
1	AF568A	HPE 1.83m 10A C13 EU Pwr Cord
1	C7978A	HPE Ultrium Universal Cleaning Cartridge

1	Q2078AN	HPE LTO-8 30TB RW Non Cust Lbl 20 Crtg
2	S1W64AAE	Veeam Pub DPF Socket 5yr Sub E-LTU
1	HU4B2A5#ZX3	HPE Apollo 4200 Gen10+ Support
1	HU4B2A5#R2M	HPE iLO Advanced Non Blade Support
1	HU4B2A5#80N	HPE MSL2024 Library Support

Součástí technické specifikace infrastruktury pro zálohování a rychlou obnovu, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.13** – Produktové listy_materiály_5.6.

5.7. Technická specifikace pro zvýšení dostupnosti záložního datového centra a lokální sítě

Zadání:

Žadatel v současné době nedisponuje žádným systémem, který by vhodně zajistil zabezpečení infrastruktury nemocnice, jak z pohledu spolehlivosti a vysoké dostupnosti, tak z pohledu kybernetické bezpečnosti.

Předmětem této části specifikace je popis technologie zajišťující přístup k informačním aktivům.

Technické řešení bude integrováno do stávajícího síťového prostředí, které je postaveno na prvcích společnosti Aruba Networks.

Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku.

Páteřní přepínače slouží k agregaci přístupových přepínačů a také k připojení ostatních technologií v rámci datového centra. Páteřní přepínače musí utvářet dva logické stohy, které budou nakonfigurovány, tak že bude mezi serverovnami možné sdílet stejné adresní rozsahy. Tento požadavek vyplývá z potřeby zajištění migrace jednotlivých VM mezi dvěma výše zmíněnými stohy bez nutnosti re-adresace VM (vMotion).

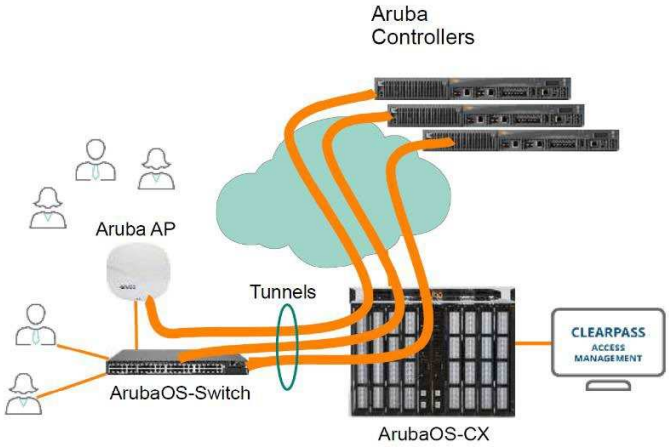
Řešení:

Nabízíme řešení postavené na výrobcích od HPE Aruba včetně propojovacího materiálu, které splňuje minimální požadavky poptávané zadavatelem. Konkrétně jde o páteřní switche, přístupové switche více typů, bezdrátové přístupové body, bezdrátové přístupové kontroléry a potřebné licence v poptávaném počtu.

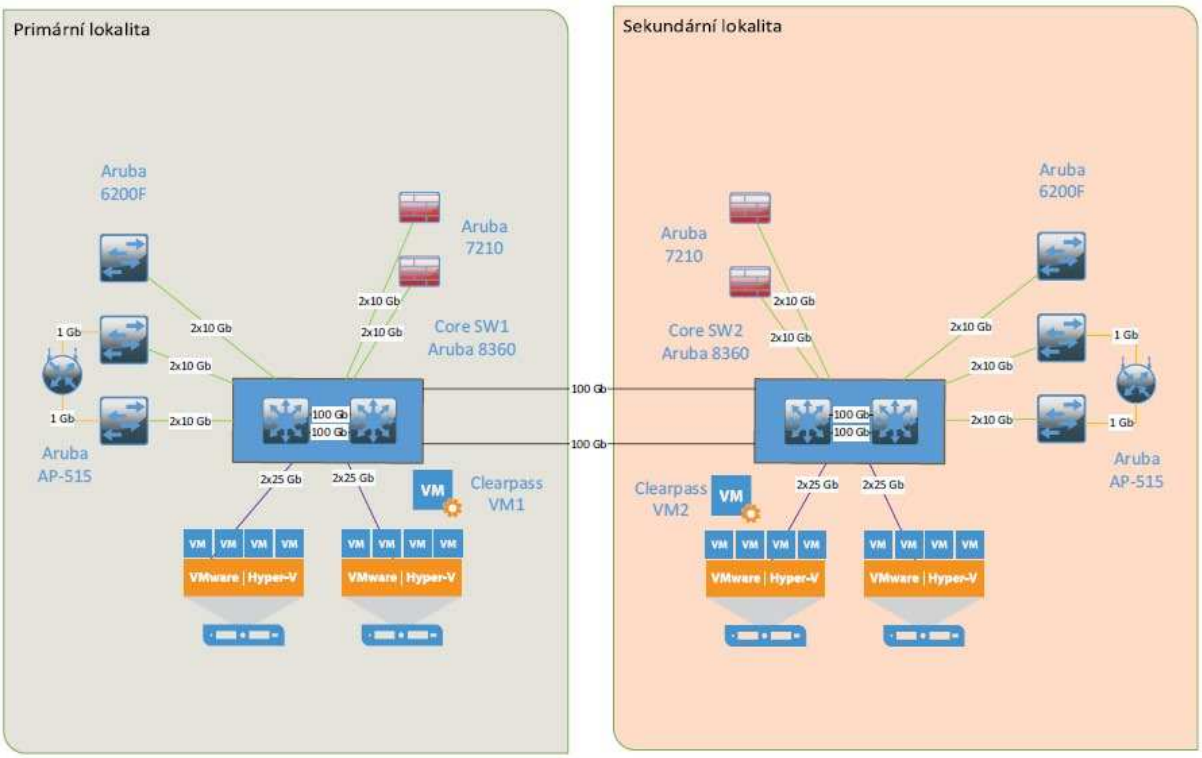
Popis nabízených produktů je v souboru s partnumbery, kde jsou rozepsány všechny nabízené HW produkty.

Řešení tedy zajišťuje v prvé řadě robustnost a vysokou dostupnost síťové komunikace. A to díky možnostem propojení a nastavením směřování provozu. Páteřní přepínače tvoří logické stohy, které budou nakonfigurovány, tak že bude mezi serverovnami možné sdílet stejné adresní rozsahy. Ve druhé řadě nabízí vysokou bezpečnost díky mikrosegmentaci provozu pro vybrané sítě vyvedením provozu až na bezdrátové kontrolery.

Toto fungování znázorňuje obrázek níže.



Detailnější popis implementace je jasně znázorněný na tomto obrázku:



Part number:

P/N	*Hardware*	ks
JL728A/B	Aruba 6200F 48G Class4 PoE 4SFP+ 740W Switch	30
JL726A/B	Aruba 6200F 48G 4SFP+ Switch	30
JL704C	Aruba 8360-48Y6C v2 FB 5F 2AC Bdl	4
OEM	QSFP28 100GBase-L4 Optics for up to 10km transmission	8
OEM	QSFP28 100GBase-SR4 Optics for up to 100m transmission	4
Spotřební materiál	Všechny nutné nové minigibic + optické kabely na propojení všech dodaných switchů a serverů, počet vyjde z prováděcího projektu	
Q9H62A	Aruba AP-515 (RW) Unified AP + držák	70
JW743A	Aruba 7210 (RW) Controller	2
P/N	**SW licence**	**ks**
JW472AAE	Aruba Cntrlr Per AP Capacity Lic E-LTU	275
JW473AAE	Aruba Cntrlr Per AP PEF Lic E-LTU	275
JW546AAE	Aruba AirWave 1 Device Lic E-LTU	200

Součástí technické specifikace infrastruktury pro zvýšení dostupnosti záložního datového centra a lokální sítě, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.14** – Produktové listy_materiály_5.7.

5.8. Technická specifikace ochrany operačních systémů a mobilních platforem

Souhrnný technický popis

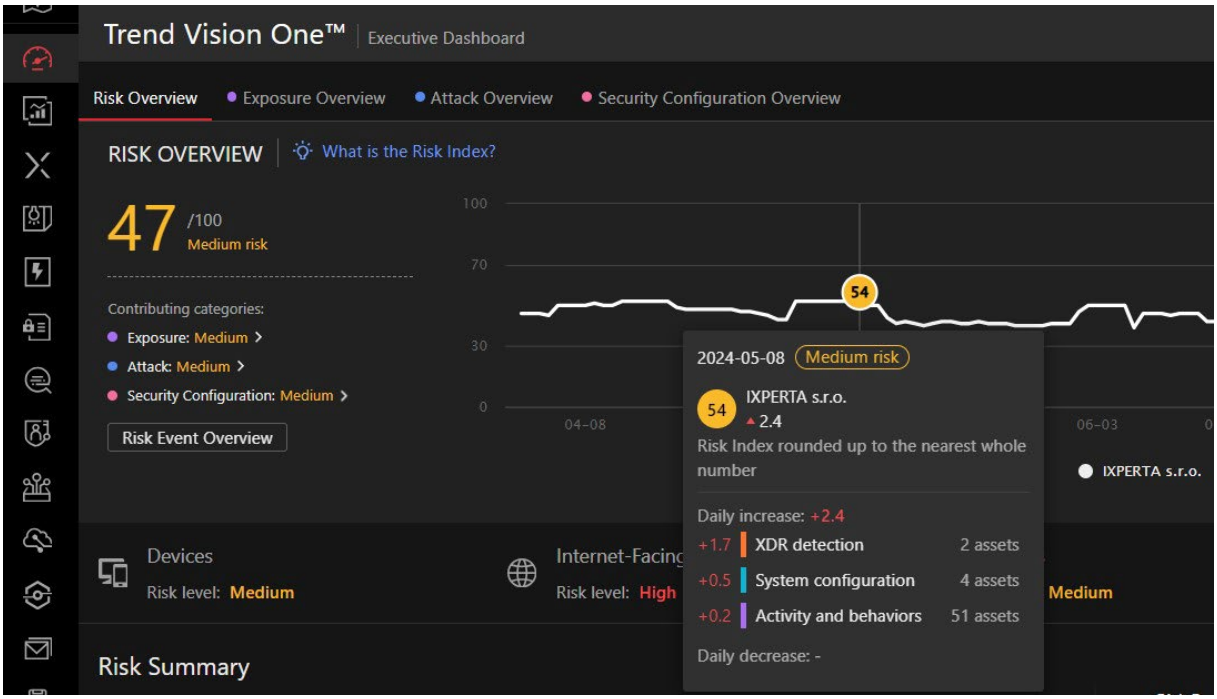
Ochranou koncových zařízení (endpointů) se rozumí ochrana desktopů, serverů i mobilů. Funkce ochrany obsahují antimalware, webovou a aplikační kontrolu, detekci a prevenci útoků (IDS/IPS), firewallu, sandboxingu, device control a DLP (samostatný požadavek zadavatele) a nástrojů vyšetřování EDR/XDR.

Základem je centrální XDR platforma v cloudu výrobce, která slouží jako agregační, konfigurační, integrační, automatizační, správní a monitorovací bod sady pořízených ochran.

XDR platforma a k čemu je určena

XDR platforma je cloudové prostředí výrobce provozované v geograficky rozmístěných datových centrech po světě, kde jsou pro XDR platformu a přiděleného tenanta dedikovaného pro zákazníka ve vybraném geografickém datovém centru přiřazeny patřičné výkonové a úložné zdroje (nebližší Německo). K práci s ní slouží XDR konzole.

XDR platforma od výrobce TM se nazývá „Trend Vision One



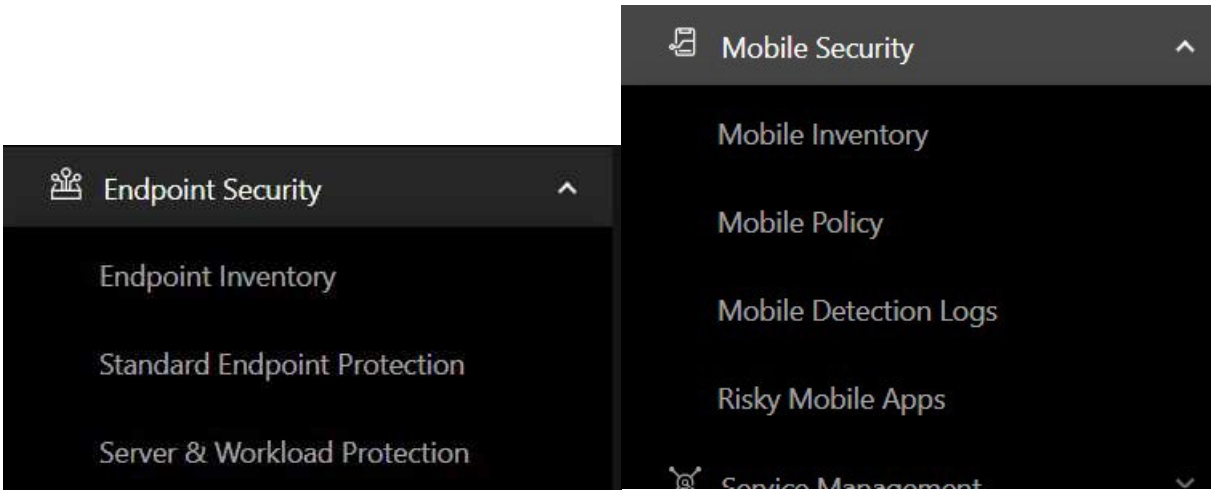
Obrázek 1 – Náhled na Trend Vision One

XDR konzole v rámci XDR platformy

Zákazník komunikuje s XDR platformou prostřednictvím XDR konzole, což je forma zabezpečeného webového portálu s grafickým rozhraním, kdy potřebným nástrojem na straně zákazníka je podporovaný webový prohlížeč. Zde pak zákazník přistupuje k jednotlivým funkčním modulům a provádí patřičnou konfiguraci, správu, monitoring a vyhodnocování. XDR konzole je vysoce intuitivní a vede správce při výkonu jeho činnosti (konfigurační průvodci, navigace v menu a konfiguraci, informační popisy a online help), umožňuje správci provádět aktivity v souvislosti s přidělenými oprávněními (RBAC). Určité činnosti a postupy vyžadují zaškolení, aby nově určený správce správně chápal souvislosti a dopady svých akcí.

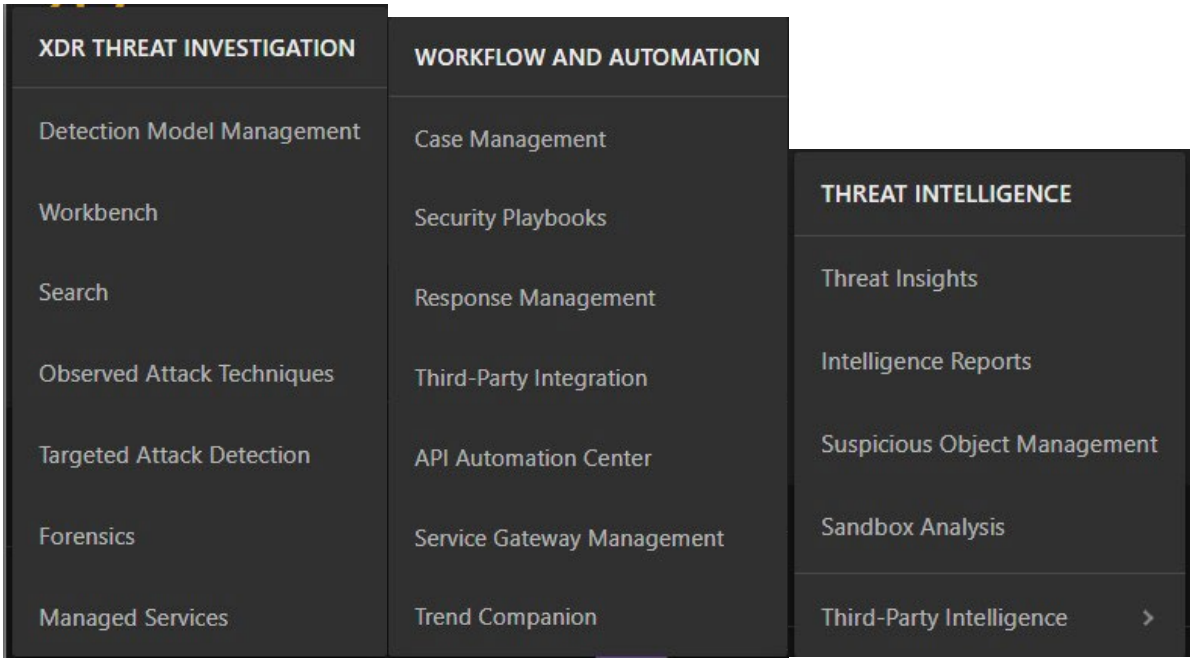
Funkce ochrany endpointů v XDR platformě

Z pohledu ochrany endpointů (EPP) jde primárně o nastavení bezpečnostních funkcí a definice politik přiřazených patřičné skupině endpontů. Funkcionalita je dostupná v rozcestníku v menu XDR konzole pod názvem „Endpoint Security“, který se rozpadá na další dva velké funkční bloky (moduly) podle typu ochrany na „Standard Endpoint Protection“ a na „Server & Workload Protection“. V případě mobilů se rozcestník jmenuje „Mobile Security“.



Obrázek 2 – Rozcestník funkcí ochrana endpointů

Z pohledu EDR (Endpoint Detection & Responce) jde o vyhodnocení telemetrických dat získaných z endpointů, která zachycují stavy endpointů s ohledem na jejich spuštěné procesy, vytvořená spojení a práci se soubory.

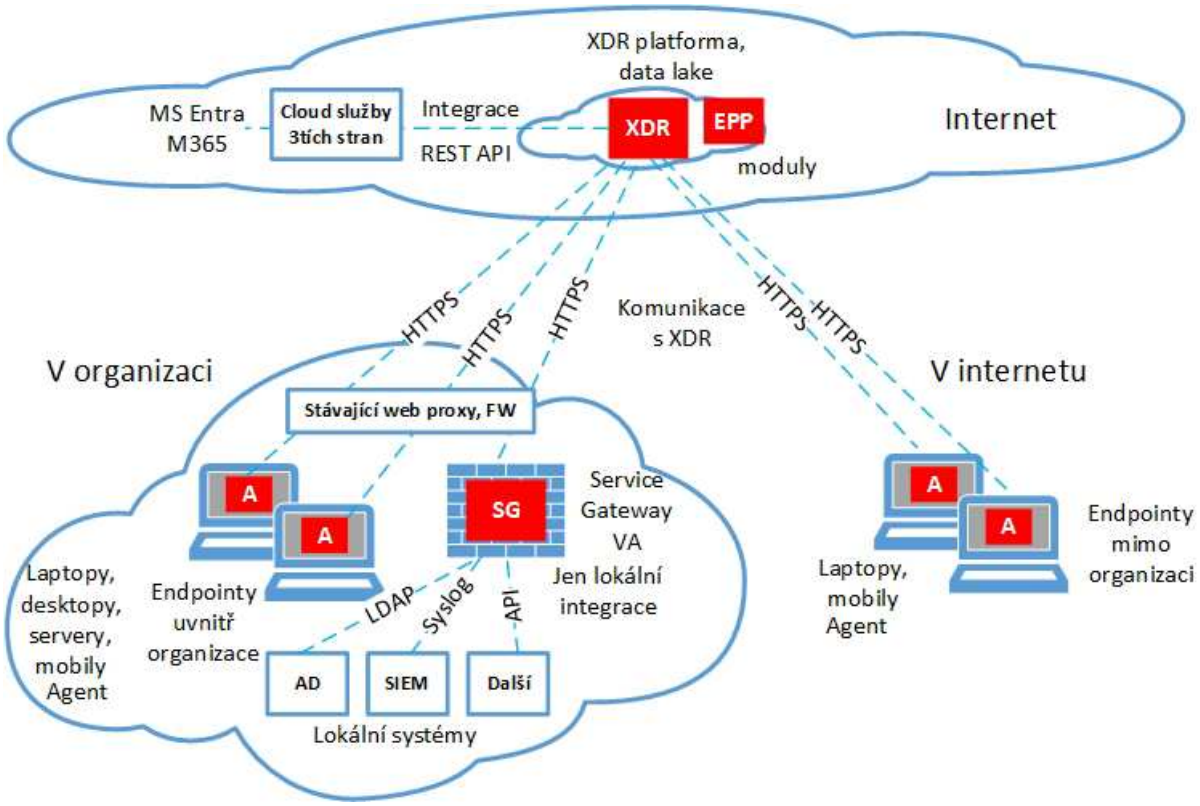


Obrázek 3 – Rozcestník XR funkcí, automatizace a threat inteligence

Vynucení ochrany v endpointech agentem

Ochrana endpointů a vynucení ochrany je pak prováděna prostřednictvím instalovaného agenta, který pověřený správce stahuje z XDR platformy a vhodným způsobem ho instaluje do endpointů. Installer agenta je předpřipravený a nakonfigurovaný. Ke startu ochrany stačí installer spustit, sám se bez interakce nainstaluje, stáhne potřebné nastavení a politiku. Ochrana endpointů má svá specifika s ohledem na platformu OS Windows, linux/Unix, MacOS, Android, iOS. Agenti se proto liší i v množině funkcí (typicky servery vs. desktopy vs. mobily). Obecně se předpokládá aktuální build a instalované bezpečnostní opravy.

Ochrana endpointů – blokové schéma



Obrázek 4 – Blokové schéma – ochrana endpointů

Legenda: Červeně jsou zvýrazněny komponenty předmětu nasazení. Symbol „A“ identifikuje instalovaného agenta do endpointů. Symbol „SG“ je komponenta Service Gateway ve form2 virtuální appliance, která zajišťuje potřebné lokální integrace. Symbol „XDR“ ukazuje XDR platformu v cloudu výrobce včetně modulu ochrany endpointů symbol „EPP“. Toto je shodné i pro DLP ochranu.

Pokrytí mobilní platformy

Ochrana mobilních zařízení[2] je jednou z funkcí XDR platformy

Aktivace vyžaduje pořízení počtu patřičných licencí (XDR kreditů) odpovídajících počtu mobilních zařízení.

Množství funkcí se liší dle mobilní platformy.

Konfigurace úvodním průvodcem, výběr, co se od ochrany mobilů očekává, zdali je ochrana cílena na ochrany (malware, web apod.) nebo požadovány i MDM funkce pro vynucování správy a zabezpečení mobilních zařízení.

Stažení a instalace agenta pro mobilní platformy do mobilů je přímo z obchodů výrobců OS mobilních zařízení, tzn. Google Play, Apple Store apod.

Poznámka: výrobce TM má více produktů k ochraně mobilů, a tedy i různé agent pro home nebo enterprise nasazení, správný agent v případě XDR platformy je Mobile Security for Business[3].

V případě použití MDM funkcí, pak je třeba vybrat vhodnou integraci s používaným 3rd party MDM, které zákazník provozuje nebo použít obsažený Mobile Device Director[4], který zajišťuje MDM funkcionalitu přímo v XDR platformě.

V každém případě je nutné určit, jak silný enforcement ke správě mobilů má být použit (pro mobily ve správě uživatele, v kombinované správě, či kompletně ve správě jen organizace).

Ukládání dat a jejich retence

Telemetrická data (atomické statistiky) z agentů (EDR) a případně dalších integrovaných zdrojů, která se zpracovávají v XDR platformě, jsou uložena v asociovaném úložišti (datalake) po dobu stanovené retence. Retence telemetrických dat je dána pořízenou licencí, v základu je to 30 dní. Oproti tomu vzniklé alarmy, reporty a další konsolidované výstupy z telemetrických dat pak mají delší retenci s ohledem na konkrétní vzniklý typ výstupu, maximálně nastavitelná retence je až 1 rok, více publikované informace o retencích od výrobce.

API rozhraní XDR platformy

Komunikačním kanálem s XDR platformou je rovněž i rozhraní API, kterým služby a produkty 3tích stran uskutečňují svojí integraci na základě předpřipravených konfigurací a prvků důvěry (API tokenů). API výrobce TM je jasně dokumentováno, strukturováno, s funkcemi vyhledávání, umožňuje rovnou generovat kód pro vložení do knihoven integračních nástrojů (např. skripty v Python a Java. Typickým příkladem jejich použití jsou automatizační a

[3] https://play.google.com/store/apps/details?id=com.trendmicro.entsecurity&hl=en_US
[4] https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mdd-mobile-device-di

orchestrační platformy SOAR, které přistupují k XDR na základě vytvořených konektorů pro různé scénáře výměny dat či iniciace akcí (např. spustit sken).

XDR platforma a komunikace s dalšími platformami

Obdobně hybatelem integrace může být i XDR platforma, kdy XDR platforma obsahuje v sobě připravené konektory pro přístup na API 3tích stran, např. zde relevantní příklady[5]:

- API MS Entra pro ověřování, 2FA/MFA, obohacení o identitní informace.
- API M365 pro kontrolu e-mailů a dalších (cloudových) služeb.

Výrobci XDR produktů rádi marketingově označují XDR jako „Lite-SOAR“.

Service Gateway

Komponenta Service Gateway má zde na tomto odkazu uvedeny požadavky k nasazení: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-deployment-guides

Dokumentace

Popsáno v datovém listu výrobce: Trend Vision One™ - Endpoint Security

Základní rozcestník online helpu je zde, zde lze vyhledávat libovolné hledané výrazy:

https://docs.trendmicro.com/en-us/documentation/productgroup/?groupname=xdr-and-management-platforms

Poznámky: XDR platforma umí integrovat řadu dalších ochran a funkcí. Ochrana cloudových mailových služeb (M365) a/nebo ochrana perimetrovou mailovou branou nejsou součástí řešení, protože tyto ochrany nebyly v zadání požadovány. Nebude rovněž licencován síťový XDR senzor k monitorování malwaru na síti, monitoring sítě bude řešen jinou ne-Trend Micro technologií. Obdobně zjištění bezpečného vzdáleného přístupu Zero Trust Secure Access nebo ochrana internetového provozu webovou branou na perimetru nejsou součástí XDR. Součástí také není extenzivní extra placená služba Threat Insight, které poskytuje celosvětový přehled zpracované globální threat-intell informace od analytiků. V řešení bude na místo ní využita nelicencovaná funkce Intelligence Reports viz dále. Záměrem je využití Trend Micro ochran na pokrytí koncových zařízení (endpointů) včetně XDR. To platí i o ochraně DLP.

[5] https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-third-party-integrat

Plnění technické specifikace ochrany operačních systémů a mobilních platforem

(1) Řešení vykonává kompletní ochranu koncových stanic, včetně funkcí antimalware, webové a aplikační kontroly, detekce a prevence útoků, personálního firewallu, sandboxingu, a nástrojů detekce a odezvy na bezpečnostní události (EDR/XDR).

Ano, řešení obsahuje tyto ochrany, lze primárně vyhledat v datovém listu „Trend Vision One™ - Endpoint Security“, konkrétně:

- Antimalware skeny, vč. funkce Demage Cleanup
- Advanced Threat Protection, shrnující ochrany:
    - Behavior Monitoring – kontrola chování procesů
    - Predictive Machine Learning – vyhodnocení souborů strojovým učením
    - Web Reputation – kontrola webového provozu, vč. funkce Browser Exploit Prevention
    - Suspicious Connection – detekce C&C provozu na botnety
    - Vulnerability Protection – IDS/IPS
    - Device Control – kontrola připojitelných zařízení (vč. USB)
    - Applicaton Control – kontrola (škodlivých) programů/aplikací
- Firewall
- DLP (extra požadavek na řešení)

Konfigurace některých ochran prostřednictvím politik je popsáno zde:

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-apex-one-security-agent-policies

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-apex-one-dlp-policies

(2) Ochrana je docílena nasazením instalovaných agentů na servery, stanice a mobilní zařízení. Musí být zajištěna kompatibilita s OS Windows, MacOS, Linux platformami a také posledními verzemi OS Android a iOS/iPadOS.

Ano, ochrana je dosažena instalací agentů, agenti pro desktopy a servery se stahují přímo z XDR konzole, agenti pro mobily se stahují z portálů jejich výrobců (Apple, Google).

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-agent-platform-compatibility

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-system-requirements-mobile

(3) Je požadována centrální webová konzole k přehledu stavu zabezpečení organizace, celkové správě nasazených agentů, a získání nástrojů pro vyšetřování zaznamenaných bezpečnostních událostí.

Ano, vše je postaveno na XDR platformě, která zastřešuje ochrany a integruje produkty a služby 3tích stran. Správa se pak kompletně prování prostřednictvím centrální XDR konzole. URL XDR konzole v případě evropských datových center je: https://portal.eu.xdr.trendmicro.com/

(4) Minimální požadavky na technickou specifikaci bezpečnosti koncových zařízení jsou uvedeny v následující tabulce.

ID	Požadované parametry	Splněno
01	***Flexibilní a konfigurovatelná ochrana koncových zařízení, která umožní správcům zapínání/vypínání jednotlivých ochran dle potřeb a postupného vynucování zabezpečení v organizaci. Minimálně ochrany typu skeny malware, kontrola webů a aplikací, řízení přístupu výměnných médií (např. USB), IDS/IPS a personální firewall.*** Ano, konfigurace ochran je postavena na politikách, které jsou přiřazovány požadovaným endpointům. Politika je v podstatě profil aplikovaný na libovolnou skupinu endpointů. V rámci politiky se pak nastavují jednotlivé ochrany. Zde lze i jednotlivé ochrany na základě politik zapínat či vypínat. Ochrany lze přizpůsobit i OS platformě a členit (zapínat/vypínat) je podle serverového a desktopového OS. V případě DLP je pro DLP funkce konfigurovatelná další nezávislá politika. Výrobce ve své online dokumentaci popisuje použití politik zde: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-policy-management-apex-overview https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-apex-one-security-agent-policies Printscreen zapnutí a vypnutí politik dole	ANO
02	***Ochrana v koncových zařízení prostřednictvím instalovaných agentů členěná pro serverové OS (servery), desktopové OS (uživatelské počítače) a mobilní zařízení (mobily a tablety).*** Ano, ochrana je přizpůsobena rozdílným potřebám desktopů a serverů. Proto je toto rozdělení respektováno v nastavení politik (výběr server nebo desktop) a rovněž z pohledu funkcí na „Standard Endpoint Protection“ (rovněž Apex One) a „Server and Workload Protection“ (rovněž Cloud One). Pro mobily je zase určena sekce „Mobile Security“. Předpoklad je použití funkcí „Standard Endpoint Protection“, použití „Server and Workload Protection“ jen pro příklady, kde je to opodstatněné. Licence je pro obě shodně nastavené ochrany stejná.	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-endpoint-security-for-sep-swp https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security	
03	***Zabezpečená webové konzole umístěné ve veřejném cloudu výrobce, obsahuje nástroje centrální správy instalovaných agentů, obsahuje nástroje pro pokročilé vyšetřování bezpečnostních událostí na základě sběru telemetrických dat (tzn. EDR/XDR funkce a detekce na základě ATT&CK MITRE).*** Ano, obsahuje nástroje správy agentů (Endpoint Inventory): https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-endpoint-inventory-intro-part Ano, dokumentace popisuje XDR vyšetřovací funkce zde: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-xdr-threat-investigation Dále MITRE hodnotilo výrobce Trend Micro z pohledu efektivity použití MITRE ATT&CK framework, podrobné hodnocení zde: https://resources.trendmicro.com/MITRE-Attack-Evaluations.html a pak „read full report“ včetně printscreenů funkcí.	ANO
04	***K dosažení větší účinnosti ochrany („defence-in-depth“ přístup) agenti ochrany koncových zařízení musí využívat jiný antimalware engine (tzn. od jiného výrobce), než systém pro ochranu síťové bezpečnosti na perimetru organizace (NGFW).*** Ano, v dodávaném řešení jsou ochrana koncových zařízení a ochrana perimetru řešeny jinými výrobci, každý výrobce má svojí vlastní ochranu včetně komponent typu scan engine. Lze porovnat názvy výrobců.	ANO
05	***Spolehlivá funkce ochrany, musí zabraňovat útočníkům i uživatelům provádět neautorizované změny nastavení ochrany v agentech. Především musí být obsažena funkce proti odinstalaci agenta, zastavení agenta, jeho procesů a služeb, změnám zásad zabezpečení (politik) nastavených ochran.*** Ano, agenti jsou chráněni proti neautorizovaném zásahu včetně zastavení, změně i odinstalování. Odinstalace je chráněna heslem zadaném v natavené politice. Rovněž vypnutí a odemčení (Unload a Unlock) agenta jsou chráněny heslem. Obdobně odinstalace (Uninstall) agenta je chráněna heslem. Dále lze granulárně nastavit, co z agenta uživatel může použít nebo vidět, to platí i o notifikacích. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-privilege-and-other-setting	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-one-service-pack-1-patch-2-online-help-prmt-self-prot-unloa https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-one-service-pack-1-patch-2-online-help-restricting-access-t	
06	***Schopnost detekovat a zabránit pokusu o infekci známým i neznámým malwarem. Malware pak musí být označován do patřičné kategorie, např. trojan, worm, ransomware apod. Součástí zjištění musí být odkaz na webovou encyklopedii malware výrobce s vysvětlením nálezu.*** Ano, pro ochranu proti známým a neznámým je použita kombinace ochran, které se navzájem doplňují. Známý malware je identifikován ochranou dle jeho typu a dalšího označení a je takto kategorizovaný v Trend Micro Threat Encyclopedia. https://www.trendmicro.com/vinfo/us/threat-encyclopedia Zde lze vyhledat např. klíče WORM, RANSOM nebo TROJ. Neznámý malware může nalézt heuristika nebo jsou odvozeny od generického základu a jsou označeny jako generické. Neznámý malware je pak identifikován ochranou Predictive Machine Learning, který hledá podobnost se vzory jiných malware dříve zjištěných někde jinde na světě. Neznámý malware umí i identifikovat sandboxing. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-unknown-threat-protection	ANO
07	***Schopnost detekovat a odstranit malware na základě kombinace mechanismů signatur, vzorů chování a heuristické analýzy a sandboxingu. Možnost využití (předávání a získávání) indikátorů útoků (IoC) minimálně s atributy (doména, IP adresa, URL záznam a SHA1 řetězec). Požadována podpora standardizovaných rozhraní TAXII a MISP pro jejich výměnu s dalšími (bezpečnostními) technologiemi.*** Ano, sandboxing doplňuje sadu ochrany a může být zdroje IOC. Rovněž XDR konzole umí získávat IOC od výrobce Trend Micro a 3tích stran prostřednictvím funkce Intellegence Reports, pak prostřednictvím Auto Sweeping hledá, zdali nenajde v prostředí shodu. Dále podporuje rozhraní TAXII, STIX a MISP pro výměnu IOC. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-misp-integration	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-taxii-feed-integration https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sandbox-analysis https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-intelligence-reports	
08	***Schopnost detekovat a odstranit přítomnost malware v paměti OS (fileless hrozby), bootovacích sektorech disků, tabulkách diskových oddílů a na všech formách dat uložených na pevném disku systému a jiných vyměnitelných médiích.*** Ano, ochrana proti fileless hrozbám (malware v paměti) je prostřednictvím Real-time skenu a jeho nastavení („Quarantine malware variants detected in memory“). Ano, ochrana diskových/USB (připojovaných) médií rovněž, např. „Scan the boot sector of the USB storage device after plugging in“. Příklady malware identifikovaného v Threat Encyclopedia cíleného na disky (MBR apod.) v odkazu. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-realtime-scan-target-tab-apex https://www.trendmicro.com/vinfo/us/threat-encyclopedia/search/boot	ANO
09	***Schopnost detekovat, blokovat a odstranit škodlivý software v reálném čase (realtime sken). Zajistit návrat záznamů ve Windows registrech do původního/výchozího stavu. Toto s minimálním dopadem na výkon koncových zařízení.*** Ano, již zmiňovaný Real-time Sken. K obnově registrů po malware slouží funkce Demage Cleanup. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configuring-real-time-scan-settings https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-files-infected-trojans https://www.trendmicro.com/vinfo/us/security/definition/damage-cleanup-services https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_agent_olh/osce-osce-feat-ben-a.html	ANO

ID	Požadované parametry	Splněno
10	***Umožnit nastavení způsobu notifikace uživatele o provedené akci agenta při porušení pravidel ochrany (možnost alarmy agenta potlačit, zobrazovat je jen jako agentské alarmy nebo umožňovat uživateli v agentu vypisování událostí za posledních pár dní/týden).*** Ano, notifikaci může provádět přímo agent, pokud bylo takové nastavení zadáno v politice v Priviledges and Other Setting. Uživatel má možnost vidět seznamy alarmů (logy) za určitou dobu, pokud je mu to povoleno. Konfigurace povolení dle ochrany, příklad Behavior Monitoring. https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-one-service-pack-1-online-help-enabling-the-sending	ANO
11	***Instalovaný agent musí být v nástrojové liště OS Windows zobrazen ikonou, náhled na ikonu musí uživateli intuitivně přiblížit stav „zdraví“ agenta, včetně připojení ke cloudovým službám výrobce a aktuálních komponent ochran.*** Ano, agent ochrany už na úrovni ikony zobrazuje stav (zdraví) ochrany a to symboly A zabarvením. To znamená, že již náhledem na ikonu uživatel okamžitě pozná, zdali je vše v pořádku nebo něco nefunguje/liší se od normálu. https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_agent_olh/c-s-connect-icons-ag.html	ANO
12	***Možnost nastavit ukládání souborů s malwarem při jejich identifikaci do adresáře instalovaného agenta v zabezpečené formě (komprimovaný soubor s heslem) pro pozdější forenzní kontrolu nebo lokální akci obnovy.*** Ano, funkce „Back up files before cleaning“, lze jí zapnout či vypnout. Slouží vytvoření zašifrované kopie infikovaného souboru v endpointu ve složce <instalační složka agenta>\Backup. Vytvoření záložní kopie souboru umožňuje v případě potřeby obnovit původní verzi souboru. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-realtime-scan-action-apex	ANO
13	***Možnost selektivního povolení/zakázání a nastavení centrální karantény pro soubory s identifikovaným malware, obsažené nástroje k jejich centrální obnově.*** Ano, použití karantény lze aktivovat a modifikovat ve smyslu výběru úložiště karantény, ve výchozím stavu je to centrální cloudová instance ochrany, alternativně lze úložiště změnit. Agent odešle zašifrovanou kopii souboru v karanténě na cloudovou instanci nebo jinou zadanou lokaci. Aktivita karantény je logována.	ANO

ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-realtime-scan-action-apex https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-quarantine-directory https://docs.trendmicro.com/en-us/documentation/article/apex-one-as-a-service-online-help-viewing-central-quar_001	
14	***Schopnost kontrolovat dokumenty z programů balíku Microsoft Office, včetně vložených souborů (OLE). Obdobně komprimovaných souborů (např. ZIP, RAR, 7z, ISO, GZ apod.). Možnost selektivního nastavení úrovně kontroly vnořených vložených/komprimovaných souborů (např. vnoření až do 5té úrovně). Různá nastavení pro sken v reálném čase a pro plánovaný sken.*** Ano, ochrana podporuje kontrolu vložených objektů prostřednictvím OLE („Scan OLE objects“) včetně výběru úrovně kontroly v sobě obsažených vrstev (OLE v OLE) do 10té úrovně. Úplně stejné nastavení je použito i pro komprimované soubory („Scan compressed files“) a to opět vrstev až do 10té úrovně. Ano, výrobce zveřejnil seznam typů balíčků: https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-one-(mac)-patch-12-server-online-help-supported-compressed Ochrana cílí i na ISO soubory, viz Threat Encyclopedia: příklad Generic ISO. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/search/geniso	ANO
15	***Nástroje pro odezvu na zjištěné infikované koncové zařízení, vč. ad-hoc spuštěného skenu, odpojení koncového zařízení od sítě (izolace), spuštění remote shell přístupu (vč. podpory powershell a shell skriptů). Vypnutí uživatelského účtu a resetování uživatelského hesla v identitním systému (integrace s Active Directory, Entra).*** Ano, jedná se o nástroje reakce v rámci XDR konzole („Response Actions“), v případě reakce využívající identitní systém, je prerekvizitou integrace s ním a zavedení patřičných účtů a oprávnění. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-response-actions-section	ANO
16	***Analytika k vizualizaci EDR/XDR vyšetřování k určení vstupního bodu průniku malware / útoku do organizace. Zobrazení interaktivního grafu s objekty (minimálně zařízení, uživatel, použitý proces a příkaz ve skriptu) včetně výpisu detailů údajů z telemetrických dat. Možnost zobrazit pohled vše najednou a sekvenčně dle průběh u události v čase. Možnost přímo z vizualizovaného grafu konstruovat strukturovaný vyhledávací dotaz (query) na hledaný údaj nebo jejich kombinaci.***	ANO

ID	Požadované parametry	Splněno
	Ano, toto odpovídá funkcím sekce „XDR Investigation/Search“. Zde lze provádět dolování výstupů z telemetrických dat. Z těchto telemetrických dat pak nástroj hledá shodu na základě MITRE AT&CK technik a taktik a kategorizuje je do výstupů v sekci „XDR Investigation /Observed Attack Techniques“. Ze zjištěných technik a taktik pak nástroj konstruuje „XDR Investigation/Workbench“ aletry, které reprezentují bezpečností události k vyšetření, kde jsou použity vizualizační a analytické funkce. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-search-app https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-observed-attack-techniques https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-workbench printscreen vizualizace události v grafu	
17	***Schopnost blokovat útoky bez ohledu na to, zda jsou webové, e-mailové, nebo z vyměnitelného média. V případě webového provozu musí ochrana chránit proti webům, které jsou kategorizovány jako nebezpečné a podezřelé. V případě vyměnitelných médií musí být možné vydefinovat seznam výměnných médií, které jsou organizací považovány jako důvěryhodné (oproti zbytku povolené).*** Ano, XDR platforma je připravena chránit proti útokům všemi kanály, kterými se mohou šířit, a to včetně vizualizace výstupů ochran v XDR dashboardech, kdy těmito kanály je např. endpoint, mailová služba/produkt výrobce, síťové prostředí a cloud. V případě webu je součástí ochrany endpoinů i ochrana proti nebezpečným webům. Ochrana se jmenuje Web Reputation. Lze vybrat sílu ochrany High, Medium a Low, což odpovídá kategoriím Dangerous, Highly Suspicious a Suspicious. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-web-reputation-apex https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configuring-web-reputation-policy Výrobce má i web kde lze webovou reputaci stránek testovat, například zadáním testovací URL http(s)://wrs21.winshipway.com/ do: https://global.sitesafety.trendmicro.com/	ANO
18	***Ochrany proti technikám moderních útoků na základě aktuálního MITRE ATT&CK frameworku, ochrana musí identifikovat pokusy z pohledu útočných taktik a technik a poskytnout analytické nástroje pro jejich vyšetření.*** Ano, XDR je postaveno na MITRE ATT&CK frameworku, „Observed Attack Techniques“ a „Workbench“ používají jejich ID, popis a odkazují i na definici MITRE.	ANO

ID	Požadované parametry	Splněno
	Dále nástroj má přímo dashboardy zobrazující události v MITRE ATT&CK struktuře („MITRE ATT&CK® Mapping“). https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-observed-attack-techniques https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-security-dashboard printscreen dashboardu	
19	***Schopnost detekovat a zabránit neznámým (zero-day) útokům kombinací strojového učení, analýzy chování programového vybavení a vyhodnocením podezřelých souborů v cloudovém sandboxu. V případě sandboxu požadovány pro test detonace malware/sktiptů apod. alespoň dva různé OS, z toho minimálně to musí být alespoň OS Windows 10.*** Ano, ochrana proti neznámým hrozbám („Unknown Threat Protection“) je postavena na ochranách Behavior Monitoring, Predictive Machine Learning, Suspicious Connection a Sandboxing. Sandboxing v sobě obsahuje dvě instance OS s OS Windows 7 a Windows 10. Výčet ochran v datovém listu a níže odkazy na dokumentaci. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-unknown-threat-protection https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-predictive-machine-learning https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-behavior-monitoring-policy-settings https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-suspicious-connection-config https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sandbox-analysis report sandbox dva OS	ANO
20	***Podpora vyhodnocení (v sandboxu) spustitelných souborů, archivů, dokumentů (Office, PDF apod.), a Java souborů. Výsledek určí, zdali je testovaný soubor neškodný či nebezpečný, současně s výsledkem je automaticky generován podrobný report (webová forma a generovaný PDF soubor pro stažení). Nalezené nebezpečné artefakty jsou v reportu oproti zbytku zvýrazněny (jinak zbarveny či zvýrazněny).***	ANO

ID	Požadované parametry	Splněno
	Ano, seznam souborů k vyhodnocení v sandboxu v příloze. Jinak v reportu ze sandboxu je neškodný výstup zelený, podezřelý je oranžový a nebezpečný červený. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-supported-file-types report sandbox a barevné zvýraznění	
21	***Ochrana zabránění identifikovaných „command & control" komunikací (identifikovaných botnet kanálů) na základě vzorků provozu z globální inteligence výrobce. Součástí je i vysvětlující detail, o co se jedná.*** Ano, tato ochrana je postavena na ochraně Suspicious Connection, která obdobně jako u ostatních ochran využívá vzory z globálních zdrojů výrobce. Popis o ochraně v datovém listu, rovněž dokumentace. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-suspicious-connection-config Rovněž funkce IntelliTrap v rámci Real-time Scan, "Detects malicious code, such as bots, in compressed files". https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-realtime-scan-target-tab-apex	ANO
22	***Ochrana proti ransomware útokům zabráněním spuštění šifrování (terminace procesu), včetně automatické obnovy postižených souborů, pakliže byly prvotní soubory již zašifrovány.*** Ano, toto v rámci ochrany Behavior Monitoring, více datový list výrobce, jinak nastavení v dokumentaci výrobce. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ransomware-protection https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configuring-bm-rules-exceptions	ANO
23	***Ochrana proti nebezpečným nebo nepovoleným programům v organizaci. Výrobce musí do agentů automaticky distribuovat seznam široce rozšířených programů a jejich posledních verzí z jeho globální inteligence, na jejich základě nastavené politiky může agent uživatelům zakazovat/povolovat jejich použití (např. zakazovat nástroje na prolomení hesel nebo logování stisku tlačítek klávesnice).***	ANO

ID	Požadované parametry	Splněno
	Ano, toto v rámci ochrany Application Control, více v datovém listu a dokumentaci. List ověřeného software ke konfiguraci pravidel se nazývá Certified Software List. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-application-control-overview	
24	***Využití strojového učení k ochraně proti novým variantám malwaru s využitím globální informace výrobce (např. globálně byl identifikován/analyzován útok xy, který je svými symptomy podobný lokálně identifikovanému útoku).*** Ano, takto funguje ochrana Predictive Machine Learning, která může k ochraně využívat lokální či globální list. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-predictive-machine-learning	ANO
25	***Uživatel může prostřednictvím instalovaného agenta provádět (ad-hoc) vlastní skeny k nalezení malware ve svých zařízeních na úrovni jejich disků, adresářů nebo souborů.*** Ano, toto se jmenuje v agentu „Manual Sken“, nastavení skenu je nezávislé na ostatních typech skenů, v nastavení GUI agenta si uživatel vybírá, co potřebuje oskenovat, vidí průběh skenu v procentech až na skenované soubory. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-manual-scan https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_agent_olh/osce-scn-adv-sttng-m.html	ANO
26	***Funkce personálního firewall u agentu, který může být nastaven do detekčního nebo prevenčního režimu, volba příslušné politiky může být automaticky volena podle toho, zdali je koncové zařízení zapojeno uvnitř organizace nebo je umístěno mimo ní (např. práce z domova, pracovní cesta / externí jednání).*** Ano, agent obsahuje funkci personálního firewallu, rozlišuje automaticky zdali je endpoint uvnitř organizace či mimo ní na základě dostupnosti referenčního serveru a podle toho může vynucovat jiná FW pravidla pro venek či vnitřek. Toto mohou využívat i jiné ochrany. https://docs.trendmicro.com/en-us/documentation/article/apex-one-as-a-service-online-help-using-the-officescan https://docs.trendmicro.com/en-us/documentation/article/apex-one-as-a-service-online-help-reference-servers	ANO

ID	Požadované parametry	Splněno
27	***Funkce detekce a prevence útoků (IDS/IPS), který může být nastaven do detekčního nebo prevenčního režimu. Seznam a aktualizace pravidel výrobce automaticky distribuuje do agentů na základě své globální inteligence, použití na základě nastavené politiky správcem.*** Ano, jedna z ochran je i IPS neboli Vulnerability Protection, IPS může být nastavena do režimu „inline“ nebo „tap“, podle toho pak funguje v režimu prevence nebo detekce. Aktualizace pravidel se automaticky stahuje od výrobce, typicky nová pravidla k ochraně proti posledním hrozbám, správce je pak může otestovat a aplikovat do provozu. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-vulner-prot-policy-settings https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-intrusion-prevention-rules	ANO
28	***Funkce forenzní analýzy k vyhodnocení napadeného koncového zařízení, správce v centrální konzoli získá nástroje centrálního vyšetřování, archiv k ukládání důkazů a prostředí spolupráce v incident response týmu. Může provést akce typu získání informací, vypsání stavu a údajů koncového zařízení (např. běžící služby a procesy, routovací tabulky), obraz RAM paměti, obsaženy dotazovací nástroje na základě standardizovaných prostředků Osquery a YARA rules.*** Ano, XDR konzole obsahuje v sekci „XDR Investigation“ funkce „Forensics“. Funkci lze zdarma využít k vyšetřování a dotazování aktiv prostřednictvím YARA Rules a Osquery či prostředky remote shell. Forensics má i další nadstavbové funkce, při kterých při kterých může trvale čerpat cloudový prostor pro ukládání důkazních dat. Trvalé čerpání cloudového prostoru pak čerpá placené kredity nad rámec zadání. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-triage-endpoints https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-run-osquery-task https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-run-yara-rules-task https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-start-remote-shell-session-task	ANO
29	***Zajištění bezpečného logování bezpečnostních událostí z cloudové platformy a jejích ochran do lokálních technologií zpracovávajících logy (LM/SIEM)***	ANO

ID	Požadované parametry	Splněno
	nalézajících se uvnitř organizace, a to bez rizikového neomezeného prostupu z cloudových služeb v internetu směrem do interních sítí organizace. Ano, výstupy XDR konzole (XDR aletry z detekcí/ochran) mohou být přenášeny bezpečně z cloudu do lokálního LM/SIEM prostřednictvím připravené hardenované appliance výrobce instalované lokálně, která se nazývá „Service Gateway“. Service Gateway slouží pro různé lokální integrace, kdy se v ní prostřednictvím XDR konzole aktivují připravené konektory. Jedním z nich je i předání logů do lokálního LM/SIEM, kdy Service Gateway čte logy z cloudu prostřednictvím zabezpečené web service na základě REST API a pak je forwarduje lokálně syslogem ve formátu CEF. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-service-gateway-management https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-__configure-syslog-forwarding-2	
30	***Interaktivní přehledný dashbord součástí centrální konzole správy, ve kterém bude zobrazen trend zabezpečení organizace v čase, včetně výkyvů z pohledu zjištěných bezpečnostních událostí (malware, EDR/XDR, webové, technické zranitelnosti a jiné).*** Ano, toto je zobrazeno v „Executive Dashboard“, kde je vidět celkový trend organizace, následně se trend rozpadá na jednotlivé kategorie odpovídající pořizovaným ochranám. Dále lze si vytvářet z připravených widgetů vlastní dashboardy, podle toho, co potřebuje zákazník řešit. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-executive-dashboard https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-dashboards-reports	ANO
31	***Telemetrická data EDR/XDR obsahují minimálně informace o spuštěných procesech, síťových spojení a čtecích a zápisových operacích při práci se soubory. Dále jsou obohaceny o identity koncových zařízení a uživatelů. V případě detekcí bezpečnostních událostí a jejich analýzy jsou tyto údaje odlišeny (zvýrazněny či zbarveny) od ostatních běžných telemetrických dat.*** Ano, telemetrická data obsahují informace o změnách vzniklých z procesů (např. jméno procesu), souborů (jméno souboru) a spojení (URL, IP adresa apod.). Přístup ke strukturovaně rozděleným telemetrickým datům je zajištěno prostřednictvím sekce „Search“, kdy lze přepínat pohledy na telemetrická data, jedno z možných přepnutí zobrazí jen detekce („Detection“), kdy z telemetrických dat je na základě	ANO

ID	Požadované parametry	Splněno
	pravidel výrobce či vlastních vytvořen alert („Workbench“). Pak tyto detekce jsou zobrazeny červenou barvou, běžná telemetrická data jsou pak modrá. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-search-method-data-sources printscreen detekce zvýraznění	
32	***Obsažena základní funkce threat inteligence výrobce, ochrana pak ověřuje, zdali pokrytá koncová zařízení nejsou zasažena globální kampaní útočníků na základě IoC poskytnutých výrobcem v rámci jeho globální inteligence (IoC Sweeping).*** Ano, XDR platforma obsahuje tzv. Intelligence Reports, které automaticky přijímají od výrobce a 3tích stran popisy (IOC) zaznamenaných kampaní, tyto IOC pak hledají v prostředí organizace („Auto Sweeping“) https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-intelligence-reports https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-sweeping-types	ANO
33	***Možnost automaticky generovat předpřipravené reporty o stavu ochrany a výčtu bezpečnostních událostí za časové období. Ty pak posílat správcům emailem.*** Ano, toto je v sekci „Dashboards and Reports“, lze nastavovat jednorázové či opakované reporty a ty pak posílat na vybrané správce (uživatele XDR konzole) emailem.) https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-reports	ANO
34	***Obsažena ochrana mobilních zařízení (mobily a tablety), ochrana proti malwaru cílenému na mobilní platformy. Především OS Android.*** Ano, ochrana mobilních platforem včetně Android je součástí XDR platformy v sekci „Mobile Security“. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-system-requirements-mobile https://play.google.com/store/apps/details?id=com.trendmicro.entsecurity&hl=en https://apps.apple.com/us/app/mobile-security-for-business/id1533217333	ANO

ID	Požadované parametry	Splněno
35	***Schopnost chránit mobilní zařízení před útoky na přenášený provoz. Především ochrana při použití neověřených WiFi sítí, možnost zajištění skrytí provozu prostřednictvím VPN brány výrobce v cloudu, podpora SSL inspekce ke kontrole obsahu webového provozu.*** Ano, ochrana mobilních zařízení chrání před nebezpečnými WiFi sítěmi funkcí „Wi-Fi Protection“ v kombinaci se „SSL Stripping“ a VPN odchodem do internetu u výrobce. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security	ANO
36	***Možnost definice politiky pro mobilní aplikace, ty kategorizovat podle jejich reputace, např. zakazovat aplikace, které jsou rizikové.*** Ano, ochrana podporuje definici politiky pro aplikace na základě jejich reputace (rizikovosti) v kategorii „Malware Detection“. Nalezené rizikové aplikace jsou základem pro XDR detekce (alerty). https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security-platform-features	ANO
37	***Detekce konfiguračních nedostatků („rooting“ a „jailbraking“) mobilních zařízení.*** Ano, obdobně tyto funkce jsou obsaženy v kategorii „Configuration Manager“. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security-platform-features	ANO
38	***Funkce webové kontroly pro mobilní zařízení opět s členěním kategorizací na nebezpečné, podezřelé stránky (jako u desktopů a serverů).*** Ano, obdobně tyto funkce jsou obsaženy v kategorii „Web Reputation“. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security-platform-features	ANO
39	***Schopnost detekovat a zabránit phishingu na základě globální inteligence výrobce.*** Ano, obdobně tyto funkce jsou obsaženy v kategorii „Web Reputation“ ve funkci „WTP: Web Guard & Phishing Detect“. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-mobile-security-platform-features	ANO
40	***Podpora blokování stahovaného souboru ve webovém prohlížeči, pakliže má daný soubor nebo URL špatnou reputaci, na základě globální inteligence výrobce.***	ANO

ID	Požadované parametry	Splněno
	Ano, „Web Reputation“ zablokuje URL závadného souboru okamžitě a „File Reputation“ zablokuje závadný soubor okamžitě při zahájení stahování, kdy prohlížeč pracuje s dočasným souborem, stažení se neuskuteční. V logu je pak název odpovídající, jak prohlížeč, např. Chrome, pracuje s dočasnými soubory. Pokud je nebezpečný soubor neznámý v reputačních službách výrobce, pak ochranu proti skrytým exploitům může vykonat „Browser Exploit Prevention“ funkce v rámci Web „Reputation“. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configuring-web-reputation-policy	
41	***Centrální správa bezpečnostních politik a nastavení agentů (servery, desktopy a mobily). A to prostřednictvím společné centrální konzole správy.*** Ano, to vše prostřednictvím centrální XDR konzole a jeho menu, viz souhrnný popis či dokumentace výrobce.	ANO
42	***Výrobce umožňuje centrální ukládání vzniklých událostí (alertů apod.) v centrální cloudové konzoli, alespoň po dobu jednoho roku.*** Ano, maximální možná doba retence zaznamenaných událostí je jeden rok (365 dní) což je dáno globálním nastavením cloudové XDR platformy. Rozšíření retence není možné. Výchozí nastavení retence telemetrických dat je 30 dnů. Zvýšení retence nad rámec jednoho roku je řešena integrací s LM/SIEM s využitím integračního konektoru, kde pak záznamy jsou dány nastavením retenčními pravidly LM/SIEM. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-privacy-security-compliance	ANO
43	***Komunikace agentů s centrální konzolí výrobce je bezpečná (autentizovaná a šifrovaná silnou kryptografií). Síla použitých krypto algoritmů je výrobcem dokumentovaná.*** Ano, výrobce definuje použité algoritmy k ochraně dat při přenosu v „Supported Cyphers“ k použitému mechanizmu TLS 1.2. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-privacy-security-compliance	ANO
44	***Integrace s identitními systémy lokální Active Directory a cloudová Entra k doplnění identit zařízení a uživatelů k obohacení výstupů. Je např. zřejmé, zdali jsou všechna koncová zařízení patřičně pokryta ochranou, pakliže některá nejsou, tak která. Obdobně integrace pro centrální ověřování správců prostřednictvím 2FA/MFA.*** Ano, XDR platforma předpokládá integraci s identitními systémy organizace, integrace s AD je možná prostřednictvím komponenty Service Gateway nebo AD agenta, integrace s cloudovou Entra prostřednictvím IdP SAML.	ANO

ID	Požadované parametry	Splněno
	Pokud je integrace provedena, umí XDR platforma porovnat záznamy a určit, zdali ochrana pokrývá všechny endpointy. Obdobně integrace s Entra přes SAML IdP. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-integration-aad-third-party https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-ad-premises-integration https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-enable-confige-mfa https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-connecting-your-idp-solutions https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-online-help-configuring-the-anti	
45	***Možnost přejímat Active Directory skupiny pro konstrukci skupin koncových zařízení.*** Ano, část ochrany endpointů Standard Endpoint Protection umí konstruovat labely a tagy na základě AD skupin, ty pak používat v politikách nebo hledání. https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-online-help-endpoint-and-user-gr	ANO
46	***Schopnost vytvářet politiky na úrovni koncových zařízení, jejich skupin, či přiřazením specifických atributů prostřednictvím tagů či labelů.*** Ano, část ochrany endpointů Standard Endpoint Protection umí konstruovat labely a tagy na základě AD skupin, ty pak používat v politikách nebo hledání. https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-online-help-endpoint-and-user-gr	ANO
47	***Přehled stavu ochrany koncového zařízení (verze bezpečnostní politiky, verze OS, verze agenta, verze komponent ochran), viditelnost, jak z pohledu centrální cloudové konzole, tak z pohledu GUI agenta. Soulad a nesoulad graficky zobrazen a reportován.*** Ano, sumární grafické zobrazení v XDR konzoli v „Executive Dashboard“, obdobě je stav vidět z pohledu agenta konkrétního endpointu. XDR konzole rovněž poskytuje reporting, který reportuje i stav pokrytí ochranou. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-executive-dashboard	ANO

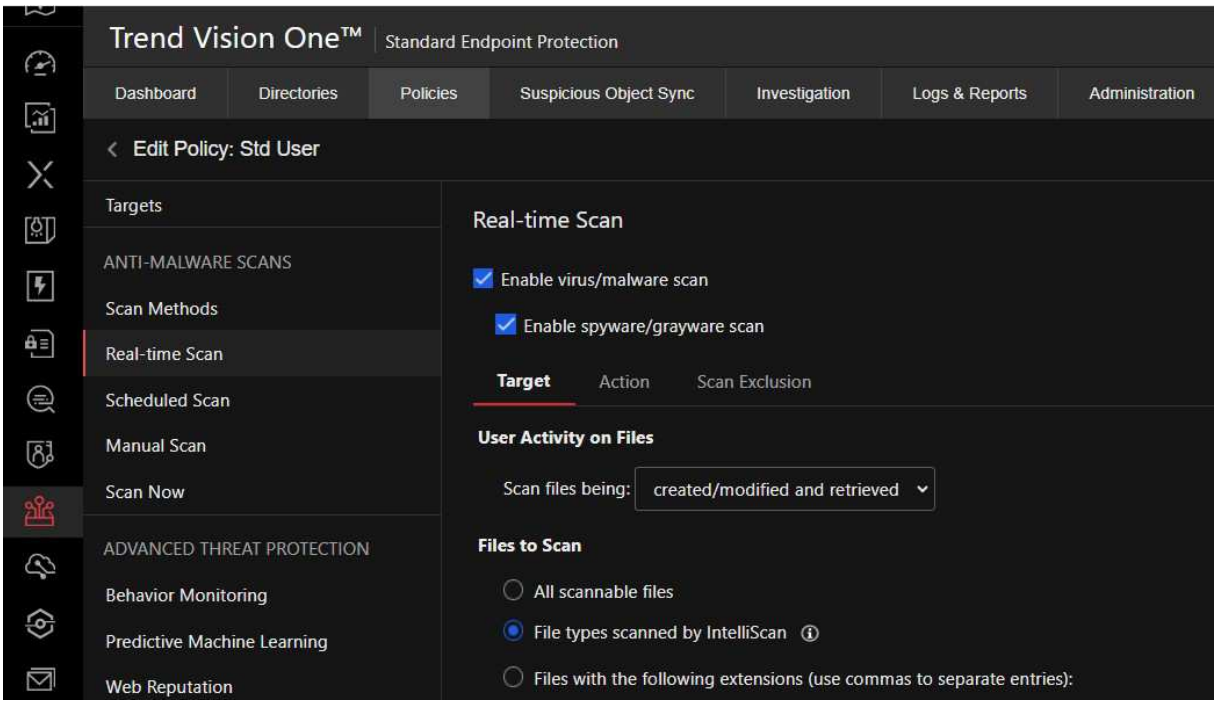
ID	Požadované parametry	Splněno
	https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_agent_olh/osce-agent-status-os.html https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_agent_olh/c-s-connect-icons-ag.html https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-reports	
48	***Výrobce a jeho cloudová služba je patřičně certifikována s doložením shody minimálně s ISO 27001 a SOC2 Type 2.*** Ano, výrobce publikoval tyto dokumenty (k ISO 27001, ISO 27017 a dalším ISO a SOC 2/3) ve své dokumentaci na následujícím odkazu: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-privacy-security-compliance	ANO
49	***Sběr údajů do cloudu výrobce je v souladu s evropskou regulativou (GDPR), datové centrum je na území EU, výrobce jasně veřejně deklaruje, které údaje zpracovává a za jakým účelem.*** Ano, výrobce publikoval tyto informace ve své dokumentaci na následujícím odkazu: https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-privacy-security-compliance https://success.trendmicro.com/en-us/solution/ka-0010805	ANO
50	***Možnost využití zabezpečeného REST API, včetně dokumentovaného použití, kdy výrobce jasně vede uživatele k jeho požití pro automatizaci. Podpora pro snadné generování kódu pro API volání do knihoven v Python a Java.*** Ano, viz API dokumentace výrobce včetně exportu kódu do Java a Python. https://automation.trendmicro.com/ https://automation.trendmicro.com/xdr/api-v3	ANO
51	***Podpora řízení přístupu správců k funkcím správy a datům na základě RBAC.*** Ano, XDR platforma řídí přístup uživatelů (správců) prostřednictvím RBAC. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-configuring-user-roles-accounts	ANO

ID	Požadované parametry	Splněno
52	***Podpora integrace s globálně rozšířenými nástroji SIEM, SOAR. Cloudová konzole musí mít předpřipravené ke snadné integrace s nimi.*** Ano, XDR platforma podporuje integraci s předními výrobci SIEM a SOAR. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-third-party-integration	ANO
53	***Možnost integrace s MDM systémy 3tích stran pro správu mobilních platforem (Intune, AirWatch).*** Ano, podpora integrace s MDM MS Intune a VMware Workspace ONE (AirWatch) a Google Workspace. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-getting-started-mobile-security	ANO
54	***Podpora zařízení typu BYOD a firemních zařízení.*** Ano, MDM/Trend Micro mobile Traffic Director (MTD) podporují rozsahem správy jak BYOD, tak firemních zařízení. Pro firemní zařízení je k dispozici „Whole Device“ profile, který ovládne celé zařízení, pro BYOD zařízení vznikne „Work“ profil, který vytvoří podnikový prostor v mobilu, alternativně jen zajistí ochranu proti malware instalovanou aplikací (bez MDM). https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-enrolling-android-devices	ANO
55	***Podpora aktuálních internetových prohlížečů Microsoft Edge, Google Chrome, Mozilla Firefox apod. pro bezchybný přístup k centrální cloudové konzoli.*** Ano, XDR platforma se neomezuje jen na uvedené prohlížeče, prohlížeče musí být aktuální (podporované jejich výrobcem, většina používá Chromium = stejný engine). Publikovaná definice webového prohlížeče má napojená ochrana Cloud One, která je propojená s XDR platformou. https://cloudone.trendmicro.com/docs/browser-requirements/	ANO
56	***Podpora OS serverů a koncových stanic k instalaci agentů ochran nejméně pro tyto systémy:*** ***Windows desktopy:*** ***Windows 10 a 11*** ***Windows 7 SP1, 8 (minimálně funkce ochran, s omezenou telemetrií či bez telemetrie)*** ***Windows servery:*** ***Windows Server 2012 R2, 2016, 2019 a 2022*** ***MacOS:*** ***10.15 (Catalina) - 14.0 (Sonoma)*** ***Linux:***	ANO

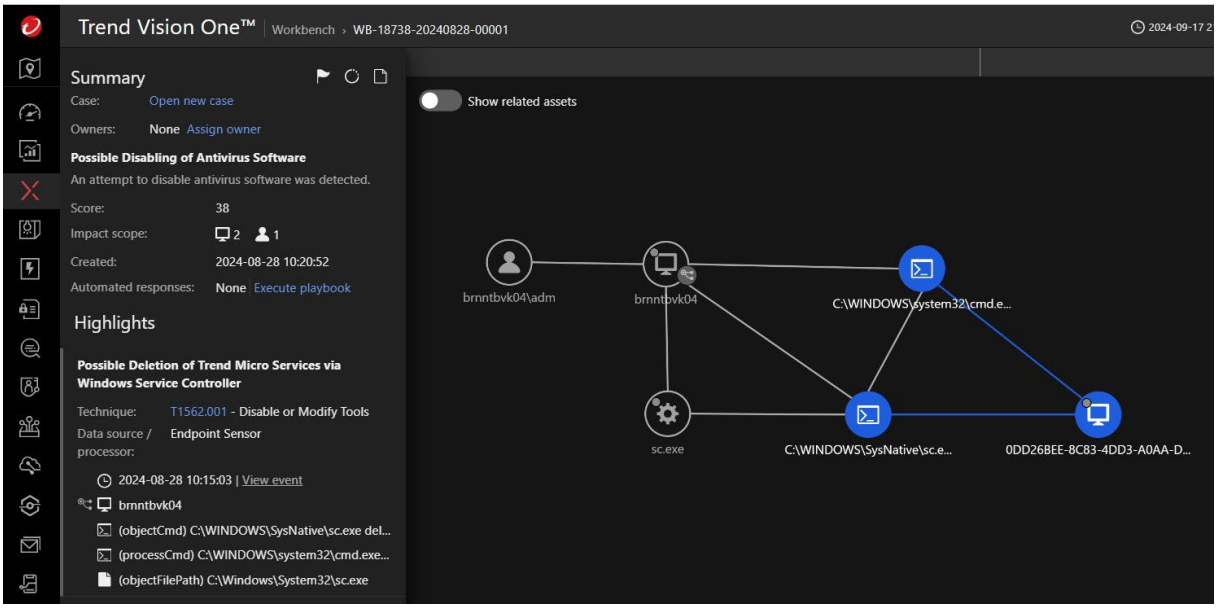
ID	Požadované parametry	Splněno
	Centos 6, 7 a 8 ***Debian 9, 10 a 11*** ***Ubuntu 16, 18, 20, 21, 22*** ***RHEL 7, 8*** ***OracleLinux 6, 7, 8, 9*** ***Rocky Linux 8, 9*** ***SLES 12, 15*** ***Podpora Secure Boot v agentech.*** Ano, výrobce podporuje pro ochranu uvedené OS. Výrobce rozděluje OS, na podporované jejich výrobci (nejsou EoL), v nich je dostupná plná XDR funkcionalita (XDR sensor). Pak výrobce pro OS, které jsou nepodporované jejich výrobcem nebo specifických linux/Unix distribucí poskytuje ochranu s omezeným sběrem / bez sběru telemetrických dat. U EoL OS jsou na druhou stranu rozšířeny funkce ochrany (IPS), které jsou připraveny chránit tyto OS proti vytěžení jejich nepatchovaných zranitelností (např. Windows 7,8). https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-getting-started-xdr-for-endpoints https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-agent-system-requirements https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-linux-secure-boot-support https://cloudone.trendmicro.com/docs/workload-security/agent-compatibility/ https://cloudone.trendmicro.com/docs/workload-security/agent-linux-secure-boot-support/	
57	***Podpora aktuálních OS Android (8 a výše) a iOS/iPadOS (13 a výše) – v případě mobilních platforem.*** Ano, platformy jsou podporovány. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-system-requirements-mobile	ANO
58	***Retence veškerých telemetrických dat alespoň po dobu 30 dní.*** Ano, telemetrická data mají výchozí retenci na 30 dní, rozšiřitelnost na 365 dní. Již popisováno dříve. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-data-privacy-security-compliance	ANO

ID	Požadované parametry	Splněno
59	***Požadovaná licence musí pokrýt nejméně 500 koncových zařízení (PC, NB) a 20 mobilních zařízení (chytrý telefon, tablet apod).*** Ano, požadovaná licence ochrany endpointů vč. XDR pokrývá 800 desktopových/serverových endpointů, licence je počítána per endpoint, automaticky se přepočítává (konvertuje) na kredity. Licence dále pokrývá 100 mobilních endpointů, licence je počítána kredity, kdy jeden mobil konzumuje 5 kreditů, tedy konzumuje 500 kreditů. Výrobce toto jasně definuje v „License Entitlement“, které organizace obdrží. Přehled pořízených licencí lze vidět i přímo v XDR konzoli. To odpovídá objednacím položkám. Později lze uvolněné/nevyužité kredity používat k alokaci na funkce, které zadání nepožadovalo. https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-license-information https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-license-calculated-credits	ANO
60	***Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let.*** Ano, SLA bude zajištěno v požadovaném rozsahu.	ANO

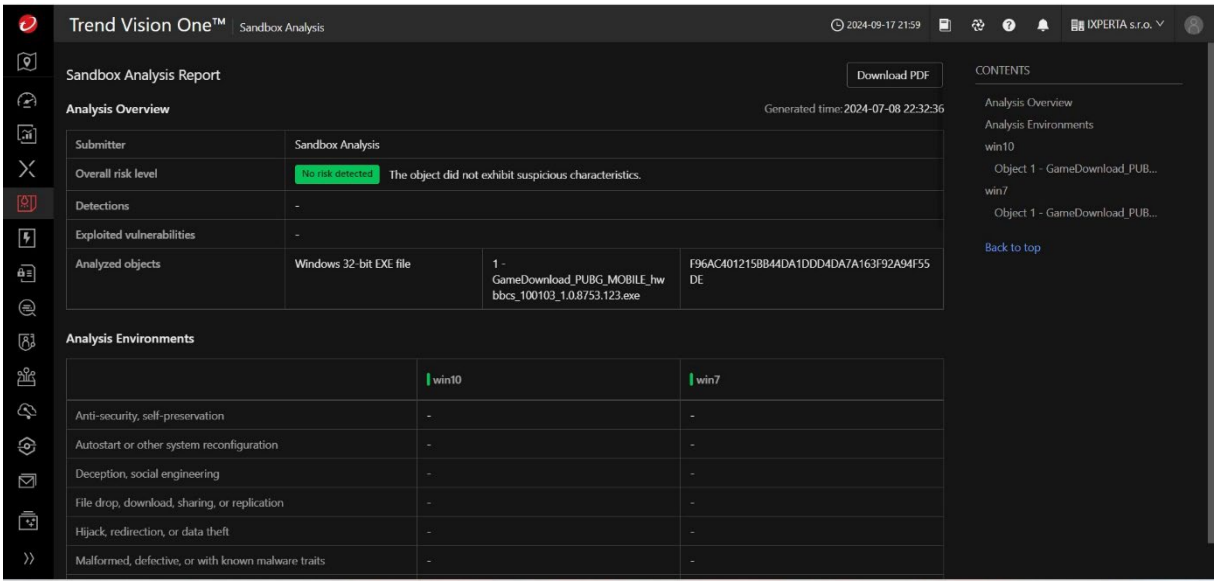
Printscreen, jak lze vypnout / zapnout jednu z ochran, v tomto případě Real-time Sken, ale obdobně je to pro všechny ochrany.



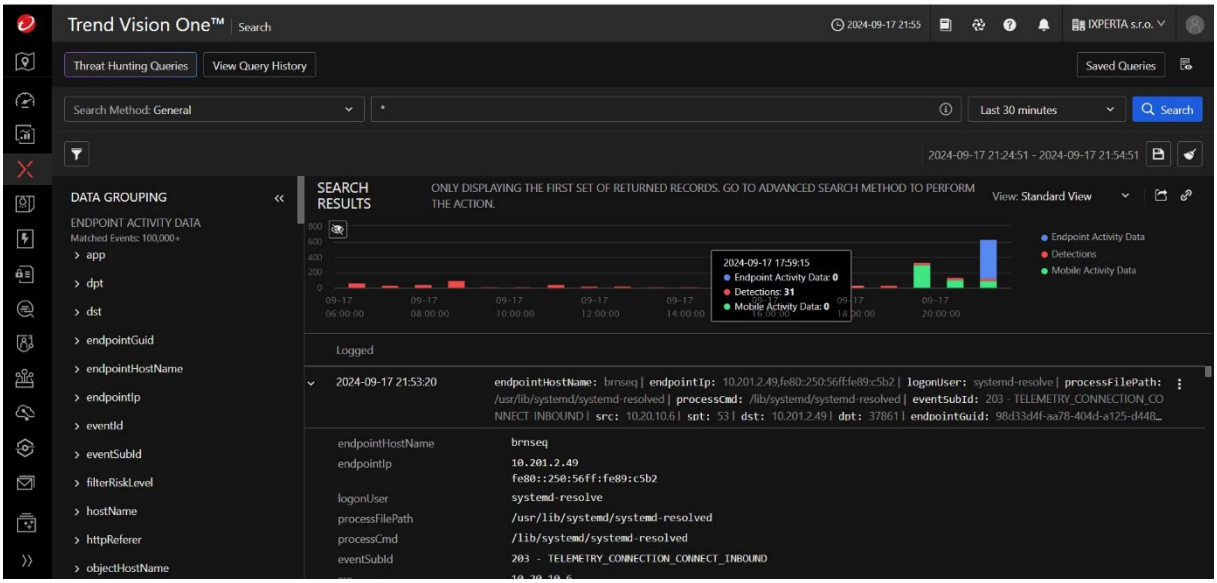
Obrázek 5 – zapnutí / vypnutí ochran příklad



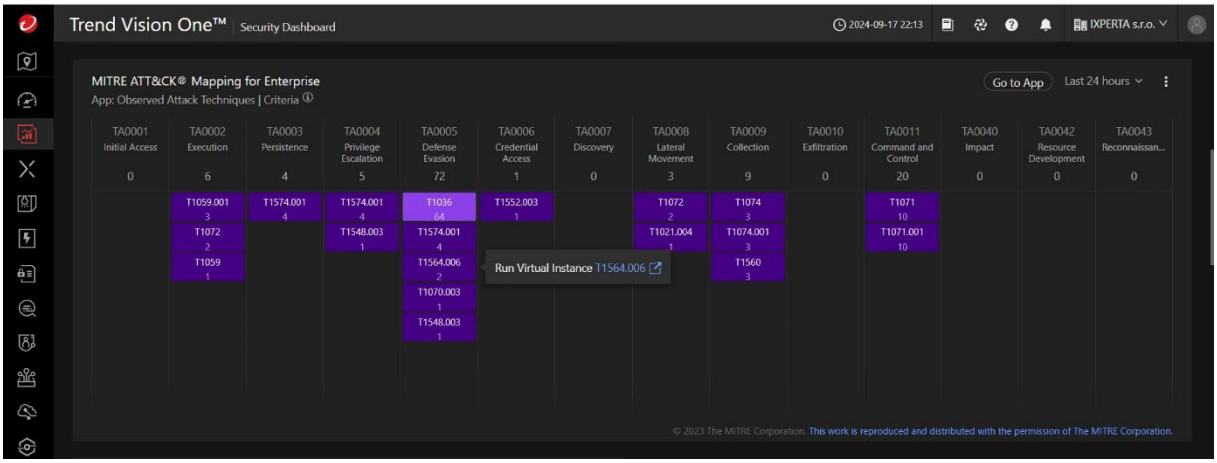
Obrázek 23 – vyzualizace XDR vyšetřování



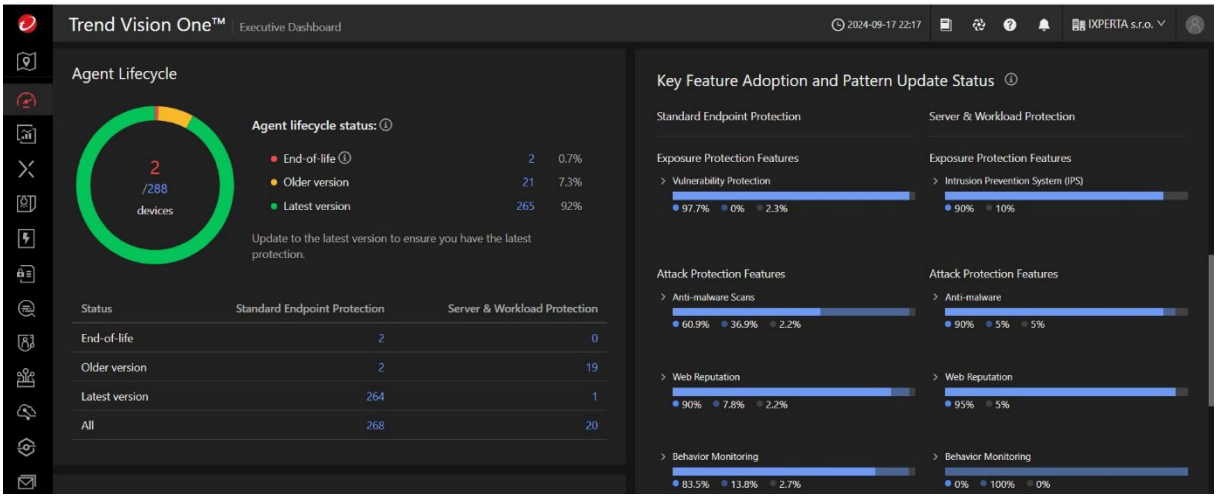
Obrázek 7– report ze sandboxu (zelená = neškodný soubor)



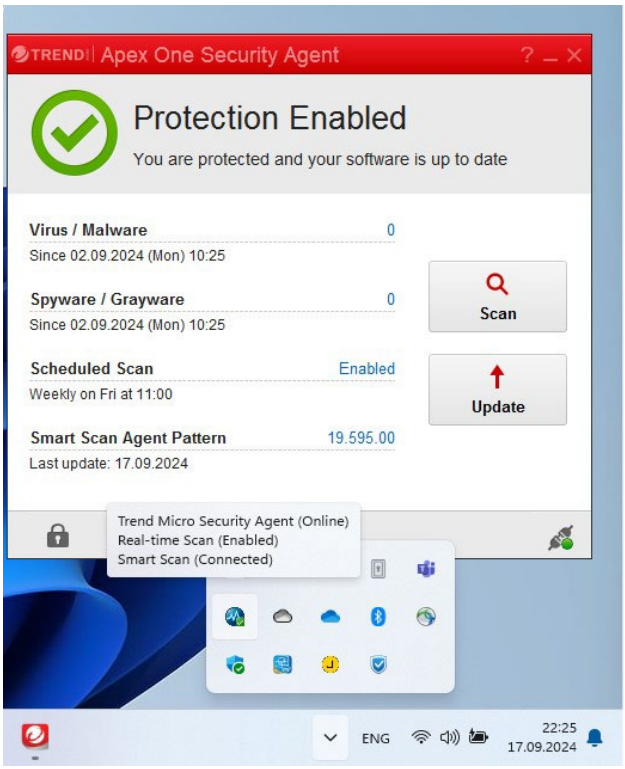
Obrázek 24 – telemetrická data, detekce jsou červené



Obrázek 9 – přehled dle MITRE matice



Obrázek 10 – stav a zdrví ochran



Obrázek 11 – stav a zdraví agenta

Part number: pro část 5.4 a 5.8

501	VO01191190	Trend Vision One - Endpoint Security (Essentials), Government, 501-1000 Licens
400 (250 mobily + 150 Sandbox	VO01158935	Trend Micro Vision One Credits, Government, License

Součástí technické specifikace ochrany operačních systémů a mobilních platforem, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.15** – Produktové listy_materiály_5.8.

5.8.1. Technická specifikace prostředí pro běh management a bezpečnostních prvků

Virtualizační servery

HPE ProLiant DL360 Gen11

HPE ProLiant DL360 Gen 11

V nabízeném řešení jsou využity servery HPE ProLiant DL360 Gen11 (2ks), což je nejnovější generace serverů výrobce Hewlett Packard Enterprise poskytující nejmodernější funkcionality a nejvíce bezpečnostních prvků v historii produktové řady.

Tyto dvousocketové servery o velikosti 1U podporují nejnovější generaci procesorů Intel Xeon (5th generation Intel Scalable Series Processors) a až 32 DIMM modulů per server (až 8TB DDR5 RAM). Pro SAN iSCSI konektivitu jsou navrženy 10/25GbE síťové adaptéry.

Součástí nabídky jsou licence VMware vSphere Essentials pokrývající všechny fyzická CPU jádra a instance VMware vCenter Essentials s podporou na 5 let.

Management serveru (OOB) je vyřešen pomocí dedikovaného ASIC čipu v podobě vestavěného ARM procesoru Integrated Lights Out 6 (iLO 6) s Advanced licencí zahrnující mimo jiné funkcionality:

- Active Health System Log
- Agentless Management
- Deployment and provisioning
- Embedded remote support
- Firmware management
- Firmware verification and recovery
- iLO backup and restore
- iLO Federation management
- iLO RESTful API (DMTF Redfish compliant) and RESTful Interface Tool (iLOREST)
- iLO Service Port
- iLO Web Interface
- Integrated Management Log
- IPMI
- One-button secure erase

- Power consumption and power settings
- Power management
- Secure recovery
- Security log
- Security dashboard
- Security Protocol and Data Model (DMTF SPDM) support
- Security states
- Server health monitoring
- System diagnostics
- Two-factor authentication
- Local or Directory-based user accounts with Role based access control
- Virtual NIC
- Virtual media
- Workload advisor
- One-button secure erase

HW konfigurace a podporované funkcionality serverů vyhovují požadovaným parametrům uvedeným v technické specifikaci.

Blokové diskové uložiště

Diskové pole pro strukturovaná data bude nasazeno jako úložiště připojené k virtualizačním serverům. Konektivita směrem k virtualizačním hostům je řešena pomocí iSCSI protokolu přes 25Gb ethernetovou síť.

Z tohoto důvodu jsou virtualizační servery taktéž vybaveny dostatečným počtem 25Gb ethernet portů.

HPE Alletra 6010

Nabízené blokové úložiště HPE Alletra 6010 je dvoukontrolérové diskové pole s 24 NVMe pozicemi pro diskové moduly v základním šasi. Tyto NVMe pozice je možno rozšířit také pomocí expanzní police. V navrhovaném řešení jsou osazeny diskové NVMe moduly o velikosti 1.92TB v počtu 24ks (celkem 46TB RAW / efektivní kapacita 97TB při deduplikačním poměru 1:3) a je možno tuto kapacitu zdvojnásobit využitím expanzní police.

HPE Alletra řady 6000

Diskové pole typu Alletra 6000 má až 3x vyšší výkon než předešlá generace polí HPE Nimble, převážně díky využití procesorů výrobce AMD a sběrnici PCIe gen4 se zvýšeným počtem PCIe linek.

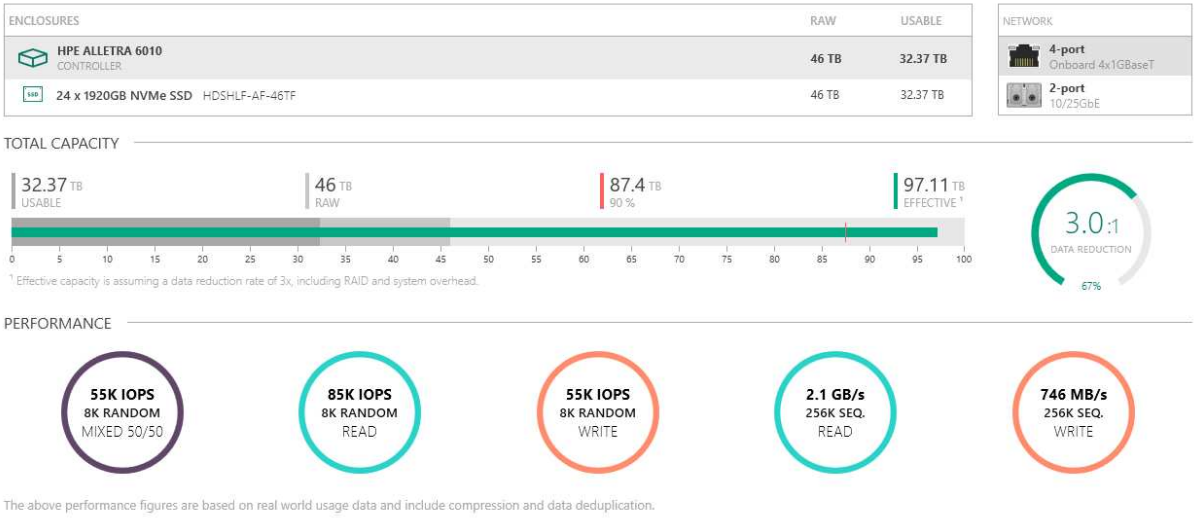
Toto diskové pole podporuje trojí RAID paritu a 1/10/25/100 Gbit Ethernet porty a také 32Gbit Fibre Channel konektivitu. V nabízené konfiguraci je navržena konektivita iSCSI pomocí 25Gbit Ethernet rozhraní.

Vlastnosti pole HPE Alletra 6000:

- umožňuje správu pole prostřednictvím cloudové služby dostupné odkudkoliv
- navrženo pro prostředí s potřebou vysoké dostupnosti = garantovaná dostupnost 99.9999%
- Triple+ Parity RAID toleruje současný výpadek tří diskových modulů + další ochranu na úrovni intra-drive parity
- podporuje šifrování s certifikací FIPS
- podpora aplikačně-konzistentních snapshotů a replikací
- integrace se zálohovacími řešeními
- hot-swap komponenty včetně napájecích zdrojů, kontrolérů, diskových modulů i IO karet
- predikce a prevence výpadků skrze celou server-storage infrastrukturu
- prediktivní podpora a doporučení na základě dat z instalované báze diskových polí
- vizualizace možných problémů mezi diskovým polem a virtuálními servery
- upgrade kontrolérů bez nutné odstávky diskového pole (non-dsiruptive)
- všechna funkcionalita je obsažena v rámci základní dodávky

Nabízená disková pole splňují všechny požadované parametry popsané v technické specifikaci.

Výkonnostní parametry nabízeného úložiště v nabízené konfiguraci jsou znázorněny ve výstupu z oficiálního konfigurátoru výrobce (hodnoty jsou platné pro jedno úložiště).



Seznam HW a SW

Počet	Part Number	Popis
2	P52499-B21	HPE DL360 Gen11 8SFF CTO Server
2	P52499-B21#B19	HPE DL360 Gen11 8SFF CTO Server
2	P49598-B21	INT Xeon-G 6426Y CPU for HPE
16	P43331-B21	HPE 64GB 2Rx4 PC5-4800B-R Smart Kit
4	P26262-B21	BCM 57414 10/25GbE 2p SFP28 Adptr
2	P10115-B21	BCM 57414 10/25GbE 2p SFP28 OCP3 Adptr
2	P51181-B21	BCM 5719 1Gb 4p BASE-T OCP Adptr
2	P48908-B21	HPE DL3X0 Gen11 1U High Perf Fan Kit
4	865438-B21	HPE 800W FS Ti Ht Plg LH Pwr Sply Kit
2	BD505A	HPE iLO Adv 1-svr Lic 3yr Support
2	S1A05A	HPE Cmp Cloud Mgmt Srv FIO Enablement
2	P51911-B21	HPE DL360 Gen11 CPU1/OCP2 x8 Enable Kit
2	P26489-B21	HPE DL300 Gen10+ 1U CMA for Rail Kit
2	P48183-B21	HPE NS204i-u Gen11 Ht Plg Boot Opt Dev
2	P48905-B21	HPE DL360 Gen11 High Perf Heat Sink Kit
2	P48920-B21	HPE DL360 Gen11 NS204i-u Front Cbl Kit
2	P52341-B21	HPE DL3XX Gen11 Easy Install Rail 3 Kit
1	F6M50AAE	VMw vSph EssPlus Kit 6P 5yr E-LTU
2	S1W64AAE	Veeam Pub DPF Socket 5yr Sub E-LTU
2	R7A12AAE	HPE GreenLake COM En 5y Up ProLiant aaS
1	R4U28A	HPE Alletra 6010 CTO Base Array
1	R0R12A	HPE Alletra 6000 2x10/25GbE 2p FIO Adpr
1	R7S82A	HPE Alletra 6000 46TB 24x1.92TB FIO Bdl
4	R9D23A	HPE C13 - C14 2m WW PDU FIO Pwr Cord
1	R9X15A	HPE Alletra Tier 1 Storage Array Std Trk
1	S0R22A	HPE Alletra 6000 4x 800W Ti FIO PS Kit
1	Q8G27B	HPE Tier 1 Storage OS Default FIO SW
4	R7D17A	HPE Alletra 6000 2x25Gb SFP28 3m DAC
46	S0R29AAE	HPE Alletra STG 6000 /TB 5yr SW/Sup SaaS
1	HU4B2A5	HPE 5Y Tech Care Basic SVC
1	HU4B2A5#ZUN	HPE Alletra 6000 2x10/25GbE 2p Kit Supp
1	HU4B2A5#ZUE	HPE Alletra 6010 Base Array Supp
1	HU4B2A5#ZV4	HPE Alletra 6000 AF 46TB 1.92 Flash Supp
2	HU4B2A5#R2M	HPE iLO Advanced Non Blade Support
2	HU4B2A500DJ	HPE DL360 Gen11 Support
16	JL295A	HPE X240 25G SFP28 to SFP28 3m DAC

Součástí technické specifikace prostředí pro běh management a bezpečnostních prvků, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.16** – Produktové listy_materiály_5.8.1.

5.9. Technická specifikace pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů

Zadání:

Řešení nabídne univerzálně funkční SSO technologie pro jakékoli webové/desktopové/cloudové/virtualizované aplikace, která by pomohla výrazně snížit čas uživatelů potřebný k přihlašování do IT systémů a aplikací.

Řešení:

Nabízíme produkt IMPRIVATA, který splňuje minimální požadavky poptávané zadavatelem. Popis nabízených produktů je v souboru s partnumbery, kde jsou rozepsány všechny nabízené HW a SW produkty.

Jedná se o HW řešení na stanicích:

- Čtečky karet MIfare na koncové stanice zákazníka pro čtení identifikačních prostředků

Jedná se o HW řešení na identifikaci uživatele pro přístup k datům:

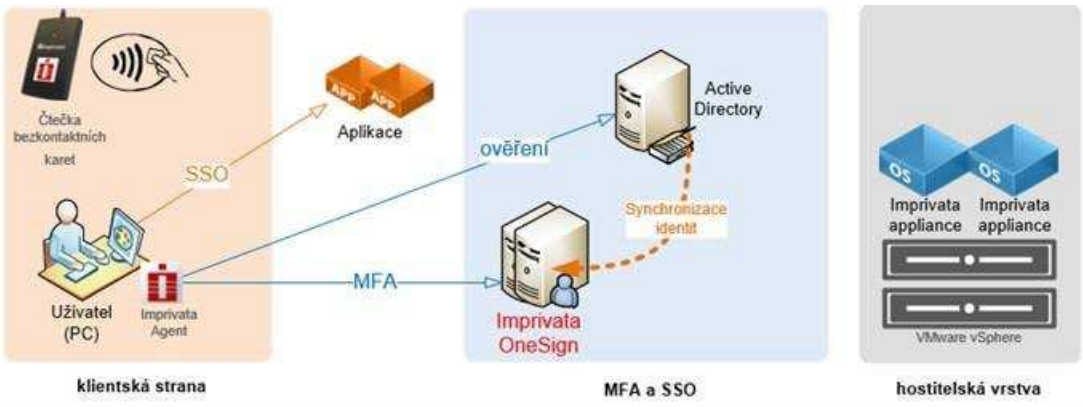
- Čipový náramek
- Čipovou kartu
- Čipovou klíčenka

Jedná se o SW řešení, které zprostředkovává jednotné přihlášení uživatele k vybraným aplikacím.

- MFA a SSO licence Imprivata OneSign (SSO/AM)

K tomuto SW jsou ještě dodatečné SW licence, které zákazník poptával v minimálních technických parametrech.

Základ je popsán v konceptuálním schématu:



Hostitelská vrstva s Imprivata applience je základní stavební prvek řešení. V rámci redundance jsou dvě.

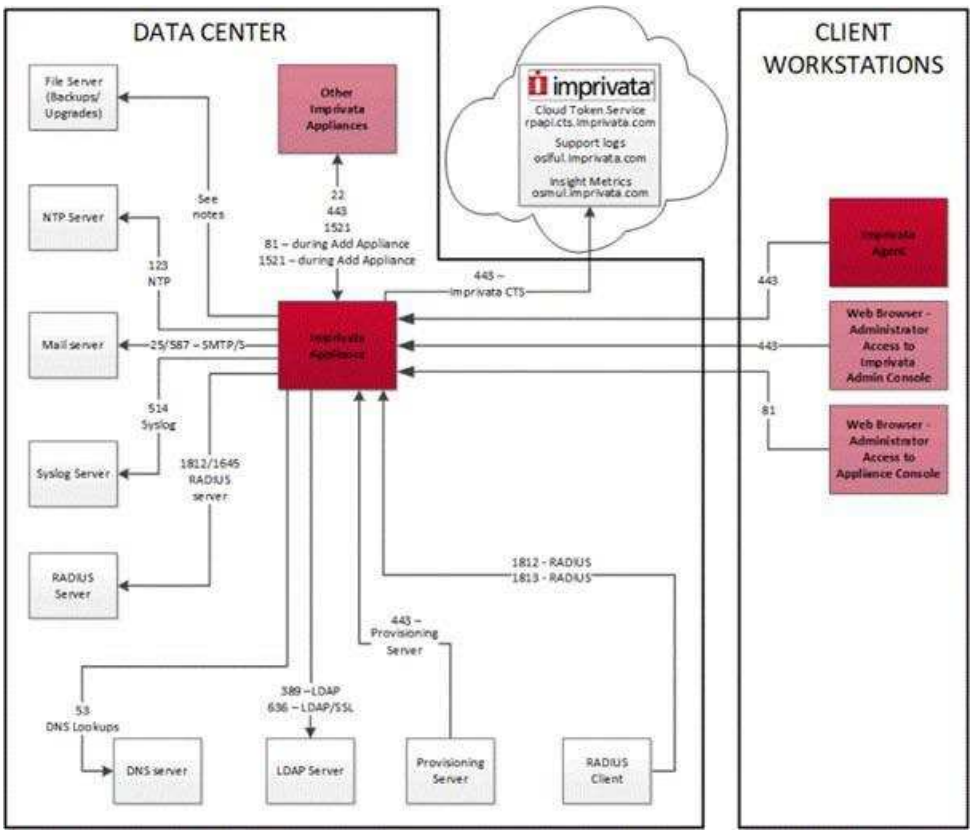
Celá technologie pak funguje následovně:

- Uživatel má svůj účet v AD ze kterého čerpá a synchronizuje se s ním Imprivata OneSign
- Na klientské vrstvě je nainstalován Imprivata Agent, který aktivně komunikuje s Imprivata OneSign
- Klient má svůj HW prostředek /karta, náramek, klíčenka s čipem/, který přečte čtečka Imprivata a přes Imprivata Agenta a Imprivata OneSign rychle přihlásí uživatele do aplikací na které má právo
- Admin zákazníka má díky zakoupeným licencím velké množství variant jak si vyžádat credential uživatele a tím prokázat jeho identitu

IMPRIVATA technologie tedy řeší:

- Bezpečné přihlášení uživatele k jeho aplikacím
- Rychlé přihlášení uživatele k jeho aplikacím
- Univerzální SSO pro webové/desktopové/cloudové/virtualizované aplikace dle minimálních technických požadavků.

Síťová komunikace IMPRIVATA je na následujícím obrázku z hlediska hostitelské vrstvy.



Part number:

P/N	*Hardware*	ks
HDW-IMP-MFR75A	Čtečka karet Imprivata Mifare	600
Spotřební materiál	Čipový náramek Mifare	100
Spotřební materiál	Čipová karta DUAL	100

P/N	SW licence	ks
SUB-SSO/AM-S	MFA a SSO licence Imprivata OneSign (SSO/AM)	1000
SUB-SSPW-S	Samoobslužný reset hesla Imprivata OneSign (SSPW)	25
SUB-CID-RA-S	Mobilní aplikace MFA Imprivata OneSign (CID-RA)	25
SUB-MobileDeviceAccess-S	Tablety Android Imprivata OneSign (MDA)	20
SUB-VIR-APP-G4	MFA a SSO serverová strana - Imprivata Appliance	2

Součástí technické specifikace pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů, jsou produktové listy a snímky nabízeného řešení, které jsou nedílnou součástí této nabídky jako **Příloha č.17** – Produktové listy_materiály_5.9.

6. Fáze A – Instalace a implementace

6.1. Zpracování a akceptace Detailního realizačního projektu

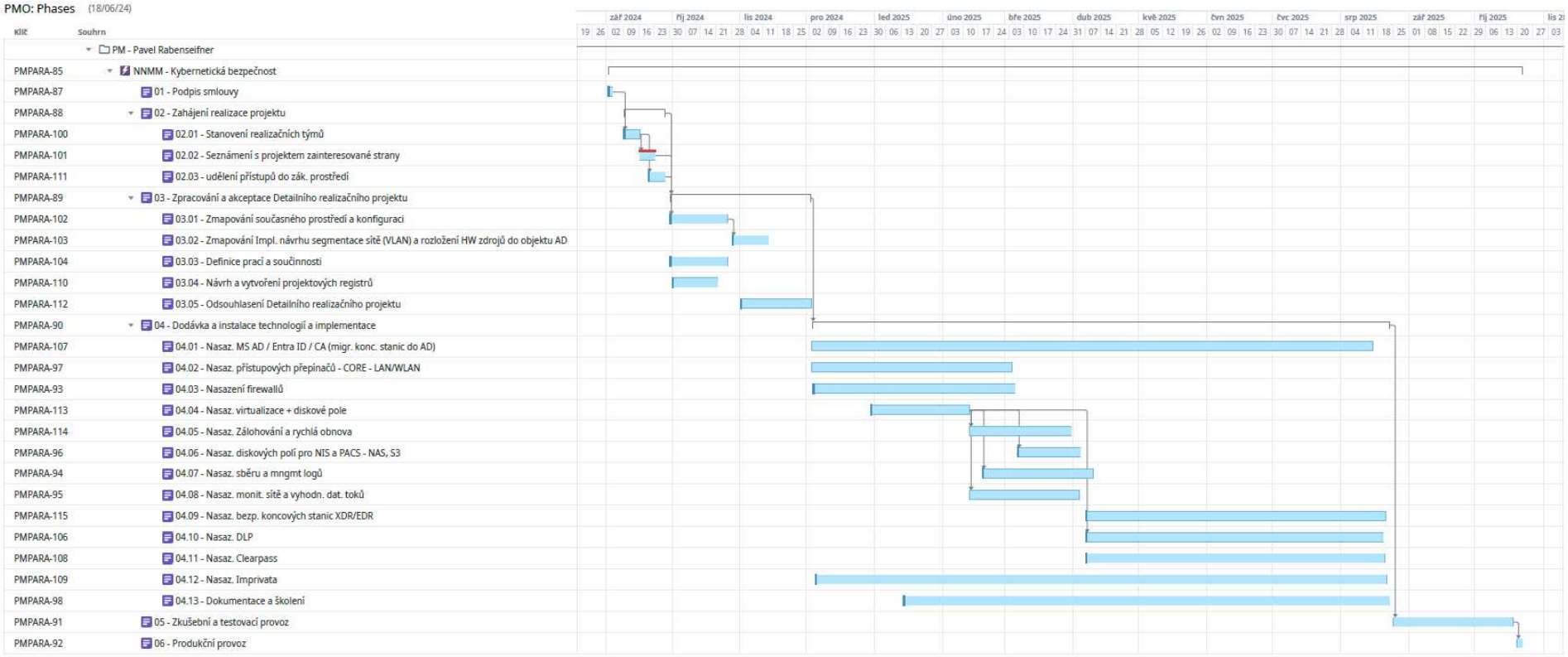
6.2. Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)

6.3. Školení

6.4. Dokumentace

Vše dle zadání a popisu v příloze č. 3b – technická specifikace Zadávací dokumentace, Fáze A – instalace a implementace.

6.5. Předpokládaný harmonogram



7. Fáze B – provozní podpora dodaných technologií

7.1. Provoz Helpdesku společnosti IXPERTA

IXPERTA provozuje vlastní pracoviště Helpdesk (Zákaznická linka, Servisní disponent, vzdálený přístup a monitoring). Helpdesk IXPERTA je dostupný pro oprávněné osoby Objednatele/Zákazníka v režimu 24/7/365 (nonstop) na svých kontaktech:

- telefon: +420 26606 3333
- email: helpdesk@ixperta.com
- webový portál ServiceDesk: https://jira.ixperta.com/servicedesk/customer/portals (doporučeno)

7.2. Zákaznická linka, Servisní disponent

Komunikace je možná v českém/slovenském nebo anglickém jazyce.
Během příjmu a potvrzení požadavku (telefonicky nebo emailem) ověřuje pracovník zákaznické linky Helpdesku IXPERTA jeho oprávněnost porovnáním s parametry platného servisního kontraktu (doba plnění, typ požadavku, priorita). Po založení zakázky do servisní aplikace IXPERTA, rozhodne Servisní disponent o přidělení zakázky na technika, který je automaticky o nasazení notifikován. V případě závad nejvyšší priority (kritická závada) je technik současně kontaktován telefonicky a možnost okamžitého nasazení na zahájení odstranění závady ověřena. V mimopracovní době je zakázka disponována přímo pracovníkem Zákaznické linky.
Jednoduší požadavky je možné s výhodou velmi rychlé reakce řešit vzdáleným přístupem přímo technickým pracovníkem Helpdesk IXPERTA. Zákazníci s platným servisním kontraktem mají přiděleného tzv. kmenového technika, kterému jsou přidělovány zakázky prioritně pro jeho znalost prostředí Objednatele/Zákazníka a provozovaného technického řešení.

7.3. Provoz elektronického webového portálu - v režimu 24/7/365

Webový portál ServiceDesk (JIRA software, výrobce Atlassian) je jednoduché, přehledné a uživatelsky přívětivé prostředí, nabízející výhody v podobě časově neomezeného zadávání požadavků v rámci a podle nastavených parametrů platného servisního kontraktu, s přístupem pouze pro oprávněné osoby Objednatele/Zákazníka (forma autentizace). Web.portál umožňuje flexibilní komunikaci mezi Zákazníkem/Objednatelem, IXPERTA Helpdesk a technikem-řešitelem požadavku. JIRA ServiceDesk poskytuje kompletní worklog všech tímto rozhraním založených požadavků, nabízí vkládání a vzájemné sdílení dokumentů upřesňující požadavek.
JIRA ServiceDesk je podporován všemi běžnými používanými webovými prohlížeči (Google Chrome, Microsoft Edge, Mozilla Firefox). IXPERTA doporučuje využití tohoto typu kontaktu pro primární komunikaci servisních požadavků ze strany Objednatele/Zákazníka.

Vše dle zadání a popisu v příloze č. 3b – technická specifikace Zadávací dokumentace Zadavatele, Fáze B – servisní a provozní podpora dodaných technologií.

8. Technická specifikace předmětu plnění

Součástí technické specifikace plnění jsou tyto přílohy:

Příloha č. 6 – Produktové_listy_materiály_5.1 a-c

Příloha č. 7 – Odkazy_na_produktovou_dokumentaci_5.2.1

Příloha č. 8 – Produktové_listy_materiály_5.2.2

Příloha č. 9 – Produktové_listy_materiály_5.2.3

Příloha č. 10 – Produktové_listy_materiály_5.3

Příloha č. 11 – Produktové_listy_materiály_5.4

Příloha č. 12 – Produktové_listy_materiály_5.5

Příloha č. 13 – Produktové_listy_materiály_5.6

Příloha č. 14 – Produktové_listy_materiály_5.7

Příloha č. 15 – Produktové_listy_materiály_5.8

Příloha č. 16 – Produktové_listy_materiály_5.8.1

Příloha č. 17 – Produktové_listy_materiály_5.9

Příloha č. 18 – Technická_specifikace_plnění,

které je nedílnou součástí této nabídky.

Uvedené přílohy jsou sočástí nabídky Prodávajícího, ke smlouvě se nepřikládají.

Příloha č. 4 Kupní smlouvy

Seznam osob realizačního týmu

(z nabídky dodavatele v souladu s požadavky zadavatele na realizační tým, uvedenými v odst. 6.3.2 Zadávací dokumentace)

IXPERTA

Platinum Solution Partner

4.4.2. Realizační tým

	Jméno a příjmení/ název	označení útvaru	Informace o vzdělání a praxi
a)	Pavel Rabenseifner	Projektový manažer	Středoškolské vzdělání, Zařízení silnoproudé elektrotechniky, SPŠE v Mohelnici, 11 let praxe ve vedení projektů v oblasti ICT. Platný certifikát PRINCE 2 V7 Foundation. Referenční zakázky vyhovující podmínkám dle článku 6.3.1 Zadávací dokumentace, na kterých se podílel jsou: 1. DLP pro endpointy pro celou infrastrukturu, Česká republika-Český statistický úřad, dodání a implementace DLP licencí od stejného výrobce, včetně školení a podpory. 2. Backup instalace a Veeam licence, disková pole, Model Obaly a. s., dodání, instalace zálohovacího systému včetně licencí Veeam a diskového pole.
b)	Milan Šereda	Bezpečnostní manažer	Vysokoškolské vzdělání, titul Ing., obor Informační technologie, Bankovní institut vysoká škola v Praze, 9 let praxe v oblasti řízení bezpečnosti ICT
c)	Ladislav Němeček	Technický konzultant na implementaci nabízených firewallů	Vysokoškolské vzdělání, titul Ing., obor Telekomunikační a informační technika, FEKT VUT v Brně, 10 let praxe v návrhu a implementaci nabízených firewallů, platný certifikát Checkpoint CCSE_R80.
d)	Jaromír Lán	Technický konzultant stávajících síťových technologií	Vysokoškolské, titul Ing. VUT Brno, 2 roky praxe v návrhu a implementaci síťových technologií Aruba Networks
d)	Josef Švihálek	Technický konzultant síťových technologií	Střední s maturitou, Obchodní akademie, 2 roky praxe v návrhu a implementaci síťových technologií Aruba Networks
e)	Jaroslav Ryšavý	Technický konzultant síťových technologií	Střední s maturitou, SPŠ Jihlava, 2 roky praxe v návrhu a implementaci síťových HP Aruba prvků a 802.1x technologii
e)	Tomáš Vohralík	Technický konzultant síťových technologií	Střední s maturitou, Střední škola a odborná škola aplikované kybernetiky, 2 roky praxe v návrhu a implementaci síťových HP Aruba prvků a 802.1x technologii
f)	Vladimír Janečka	Technický konzultant síťových technologií	Vysokoškolské, titul Ing. VUT Brno, 5 let praxe v návrhu a implementaci nabízených síťových bezdrátových technologií – HP Aruba
f)	Jiří Svoboda	Technický konzultant síťových technologií	Střední s maturitou, SPŠ Jihlava, 5 let praxe v návrhu a implementaci nabízených síťových bezdrátových technologií – HP Aruba
g)	Marcel Veselka	Technický konzultant zálohování	Středoškolské vzdělání, Mechanik elektronik pro telekomunikační zařízení, SOUT v Ostravě, 13 let praxe v návrhu a implementaci nabízeného zálohovacího software.
g)	Jakub Drábek	Technický konzultant zálohování	Vysokoškolské vzdělání, titul Ing., obor Telekomunikační a informační technika, FEKT VUT v Brně, 6 let praxe v návrhu a implementaci nabízeného zálohovacího software.
h)	Jan Plhák	Technický konzultant disková pole	Vysokoškolské vzdělání, titul Ing., obor Telekomunikační a informační technika, FEKT VUT v Brně, 10 let praxe v návrhu a implementaci nabízeného diskového pole pro nestrukturovaná data pro potřeby zálohování a uložení dat systému PACS u desítek našich zákazníků, včetně řešení servisních zásahů v rámci SLA. Pro doložení permanentní účasti v projektech na implementaci diskových polí pro nestrukturovaná data přikládáme např. následující referenci: Univerzitná nemocnica-Nemocnica svätého Michala, Zvýšení kybernetické bezpečnosti

Příloha č. 5 Kupní smlouvy

Seznam poddodavatelů

(vyplněná příloha č. 6 Zadávací dokumentace)

IXPERTA

11. Seznam poddodavatelů

Veřejná zakázka **Kybernetická bezpečnost Nemocnice Pelhřimov - 2**
Příloha č. 6 Zadávací dokumentace / Příloha č. 5 kupní smlouvy – **Seznam poddodavatelů**

Seznam poddodavatelů

pro plnění veřejné zakázky
Kybernetická bezpečnost Nemocnice Pelhřimov - 2
zadavatele
Nemocnice Pelhřimov, příspěvková organizace

Jako osoba oprávněná jednat za dodavatele IXPERTA s.r.o., IČO: 27599523, sídlo: Lihovarská 1060/12, 190 00 Praha 9 (dále jen „dodavatel"),

tímto **čestně prohlašuji**,

že dodavatel pro plnění shora uvedené veřejné zakázky

☒ **HODLÁ POUŽÍT NÁSLEDUJÍCÍ PODDODAVATELE:**[6]

Obchodní firma, název, nebo jméno a příjmení poddodavatele	Aricoma Systems a.s.
IČO poddodavatele	043 08 697
Sídlo poddodavatele	Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava
Stručný popis plnění, které je předmětem poddodávky	Týká se plnění technické specifikace 5.3, 5.7, 5.9, včetně rozsahu plnění a servisní a provozní podpory dodaných technologií pro části 5.3, 5.7 a 5.9, včetně servisní podpory individuálně objednaných služeb (po dobu 60 měsíců) u částí 5.3, 5.7 a 5.9
Finanční objem poddodávky (Kč bez DPH)	23 664 632,- Kč bez DPH

Předpokládaný procentní podíl poddodávky z nabídkové ceny dodavatele	49 %
Jedná se o poddodavatele, prostřednictvím kterého dodavatel prokazuje splnění kvalifikace?	ANO

Dále v této souvislosti prohlašuji, že plnění smlouvy na shora uvedenou veřejnou zakázku nebude probíhat za účasti poddodavatele, na kterého se vztahuje mezinárodní sankce dle § 48a zák. č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších právních předpisů,

zejména za účasti Ruska nad limit stanovený článkem 5k Nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022,

přičemž rovněž výslovně prohlašuji, že žádný ze shora uvedených poddodavatelů s plněním vyšším než 10 % nabídkové ceny dodavatele:

a) není ruským státním příslušníkem, fyzickou či právnickou osobou, ani subjektem nebo orgánem se sídlem v Rusku,
b) není právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněn některým ze subjektů uvedených v bodu a) výše,
c) není právnickou osobou jednající jménem či na pokyn subjektu uvedeného v bodech a) či b) výše.

V Praze doplnit dne dle elektronického podpisu

(el.) podpis:

Pavel Šipr

Digitálně podepsal Pavel Šipr
Datum: 2024.09.26 13:18:46 +02'00'

Pavel Šipr
Jednatel, IXPERTA s.r.o.

Příloha č. 6 kupní smlouvy

Pravidla pro zřízení a používání vzdáleného přístupu do počítačové sítě Nemocnice Pelhřimov, příspěvková organizace

1. *Kupující* umožní vzdálený přístup/připojení do své počítačové sítě nebo její části *prodávajícímu* tak, aby mohl *prodávající* vykonávat veškeré smluvní či *kupujícím* prokazatelně vyžádané/objednané služby (dále jen „služba“).

2. *Kupující* zřídí vzdálený přístup pro *prodávajícího* na dobu a v rozsahu nezbytně nutnou k plnění závazků vyplývajících z této smlouvy.

3. Technické podmínky vzdáleného připojení jsou dohodnuty takto:
   a) připojení přes SSH protokol VNC dle individuálně dohodnutých parametrů a hesel
   b) připojení přes RDP (Microsoft remote desktop klient) dle individuálně dohodnutých parametrů a hesel
   c) VPN přístup dle individuálně dohodnutých parametrů a hesel
   d) jiný typ přístupu či autentizace dle individuálně dohodnutých parametrů při podpisu smlouvy.

   Předání parametrů přístupu a přístupových hesel zajistí v předem dohodnutém termínu zaměstnanec úseku informatiky *kupujícího*.

4. *Prodávající* se zavazuje zajistit, že osoby, jim pověřené k vykonávání služeb prostřednictvím vzdáleného přístupu nezneužijí vzdálený přístup do sítě k aktivitám, které nejsou v souladu se smluvním rozsahem poskytovaných služeb, a ani neumožní tyto aktivity třetí osobě.

5. *Prodávající* je povinen vždy předem zajistit, že nedojde k nepředpokládanému narušení chodu počítačové sítě (informačního systému), ani jiných služeb a systémů v síti *kupujícího,* jakožto i řádného chodu serverů, počítačů a dalších HW komponent sítě. V případě porušení této povinnosti je *kupující* oprávněn požadovat náhradu způsobené škody.

6. *Kupující* si vyhrazuje právo službu vzdáleného přístupu dočasně pozastavit či omezit bez udání důvodu. V tomto případě bude o rozhodnutí *kupujícího prodávající* neprodleně informován telefonicky a následně obdrží písemné oznámení.

7. V případě, že *kupující* zjistí použití vzdáleného přístupu v rozporu s těmito pravidly, je *kupující* oprávněn vzdálený přístup *prodávajícímu* zcela zrušit. O tomto rozhodnutí *kupujícího* bude *prodávající* neprodleně informován telefonicky a následně obdrží písemné oznámení.

8. Kontaktní osoby pro účely poskytování služby a předávání informací dle bodů této přílohy

Za kupujícího

Jméno	Pozice	Telefon	Email
Karel Kužel	technik	731691345	intranet@nempe.cz
Lukáš Nováček	technik	734439002	intranet@nempe.cz

Za prodávajícího

Jméno	Pozice	Telefon	Email
Pavel Rabenseifner	Head of Project Office	603 200 159	pavel.rabeseifner@ixperta.com

1.1 Bezpečnostně provozní dokumentace – podmínky a požadavky

K dodanému informačnímu aktivu by měla být prodávajícím dodána i provozní dokumentace v oblastech, které jsou relevantní pro dané informační aktivum.

Níže je uveden popis provozní dokumentace a jsou popsány oblasti, které by provozní dokumentace měla pokrývat.

Cílem zpracování této dokumentace je popsat a zdokumentovat provozní postupy pro zajištění správného, bezchybného a bezpečného provozování vybavení pro zpracování informací (informačních aktiv, informačních systémů).

1.2 Bezpečnostní specifikace systému

Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.

Forma dokumentu: textový popis, buď dle metodiky ITSEM (Information Technology Security Evaluation Manual podle ITSEC) nebo v rozsahu minimálně dle následujících bodů.

Minimální rozsah:

Soupis a popis všech funkcí prosazujících bezpečnost pro:

- zajištění integrity dat při jejich přenosu a uložení,
- zajištění důvěrnosti dat při jejich přenosu a uložení,
- zajištění autentizace a session managementu,
- zajištění ošetření, filtrování a prověřování veškerých vstupních dat,
- zajištění auditní stopy a logování,
- externí rozhraní – jak uživatelská, tak pro komunikaci s externími systémy.

- Popis těchto oblastí:

- použité kryptografické funkce a algoritmy – popis přesné specifikace a použitých parametrů (typ funkce, délka klíče, mód šifrování, počet iterací, apod.),
- poloformální popis všech nestandardních algoritmů, funkcí a protokolů v oblasti bezpečnosti (např. vlastní šifrovací algoritmus, vlastní komunikační protokol, apod.),
- autentizační a autorizační model a mechanizmus (např. fáze autentizace, způsoby ověření, heslové politiky, protokoly, session management, ...),
- řízení uživatelských a privilegovaných rolí a oprávnění (včetně Access Control, Least Priviledge principy, Multi-factor autentizace, Segregation of Duties principy, Accountability principy)
- To vše z pohledu:
- Interních uživatelů
- Externích uživatelů,
- detailní popis úrovně všech přístupových oprávnění/aplikačních rolí,
- vývoj systému – použité bezpečnostní metodiky, praxe, frameworky, standardy a politiky při návrhu, plánování a vývoji,
- způsob bezpečnostního testování,
- monitoring řešení a zaznamenávání logů a auditní stopy (viz. část provozně bezpečnostní dokumentace Monitoring),
- způsob zajištění dostupnosti, důvěrnosti a integrity dat ve stavech jejich uložení/uchování, zpracování a přenosu,
- soulad s právními normami pro ochranu osobních údajů,
- bezpečnostní architektura infrastruktury,
- bezpečnostní architektura klienta/koncového zařízení,
- disaster recovery plán a strategie zálohování,
- u webových aplikací popis způsobu ošetření aplikace dle OWASP Testing guide v aktuální verzi.

1.3 Instalace systému

Cíl dokumentu: popsat a zdokumentovat postupy, kroky a činnosti vedoucí k instalaci informačního systému/aktiva nebo k přípravě prostředí pro instalaci.

- Forma dokumentu: textová, může být doplněno o návodné obrázky.

- Systémové požadavky (architektura procesoru, verze operačního systému, miminální požadavky na HW, apod.)
- Instalační média (CD, síť, soubor, …) a cesta k nim
- Konkrétní kroky vedoucí k instalaci systému, způsob instalace serverové části, způsob instalace klientské části, apod.

1.4 Základní konfigurace

Cíl dokumentu: popsat a zdokumentovat postupy, které vedou k nastavení systému do takového stavu, aby bylo možné systém po instalaci provozovat na základní úrovni.

- Forma dokumentu: textový popis (může být i např. formou okomentovaného config souboru)
- Základní konfigurace sítě (nastavení ip adresa, maska, GW, ...)
- Nastavení připojení/komunikace na další systémy (např. DB, web server, SMTP, DNS, NTP, ...), nastavení portů na kterých služba naslouchá, kam data odesílá, …
- Nastavení proxy pro komunikaci, seznam URL (nebo domén), kam systém potřebuje komunikovat (směrem do Internetu), ...
- Spuštění potřebných modulů, agentů, komponent, procesů, registrování knihoven, úprava registrů OS Windows, …
- Nastavení automatických úloh, nastavení systémových účtů, …
- Detailní popis úrovně přístupových oprávnění/aplikačních rolí

1.5 Způsob zpracování informací

Cíl dokumentu: popsat, jakým způsobem jsou zpracovávány informace v rámci informačního systému + případně v rámci ostatních systémů, na které je daný IS navázán.

- Forma dokumentu: textový popisu nebo i schéma
- Vytváření dat (datové vstupy)
- manuálně|strojově|automaticky|uživatelsky
- kdy jsou data vytvářena? (např. nějaká událost, naplánovaná událost, apod.)
- Přenosy dat
- Odkud kam (např. agent>master, do jiných systémů, mezi moduly, apod.)?
- Jakým protokolem?
- Uložení dat
- Databáze (typ?)
- File (typ?)
- Výstupy systému (dat)
- User Interface (webový formulář, GUI aplikace, konzole, …)
- E-mail|sms|voice call
- Soubor (formáty)?
- Tisk
- Datová pumpa
- Do jiných systémů (DB server, file server, ...)

1.6 Záloha, obnova, restart

Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, jakým způsobem, kdy, kam a jak často jsou zálohována data v rámci daného informačního systému a jakým způsobem se provádí obnova systému po havárii nebo ze zálohy, postupy a konkrétní kroky, které povedou k bezpečnému restartu systému.

- Forma: může být i formou zálohovacího plánu (backup schedule) a disaster recovery plánu, textový popis, návodné obrázky, okomentované příkazy, apod.
- Zálohování
    - Strategie zálohování systému navržená dodavatelem
    - Způsob zálohování – plná, přírůstková, rozdílová záloha
    - Kdy a jak často je záloha prováděna
    - Jak dlouhou dobu jsou zálohy uloženy a kde
    - Jak často se provádí testování záloh

- Obnova
    - Posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému nebo jeho části či dat ze zálohy do jeho plně funkčního stavu
    - Zpracovaný disaster recovery plán, tedy posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání do jeho plně funkčního stavu
    - Včetně potřebných zdrojů, jako je např. SW, HW, přístupové údaje, data, parametry disaster recovery prostředí, apod.
- Restart
    - Posloupnost kroků (co a jak udělat), které je třeba provést pro bezpečné restartování systému tak, aby naběhl do původního stavu
    - Např. informování uživatelů, ověření odhlášení všech uživatelů, provedení zálohy systému, restart systému (pořadí konkrétních procesů, služeb, apod.), způsob základní kontroly funkčnosti, výčet služeb, které je potřeba spustit/zkontrolovat, apod.

1.7 Postupy řešení problémů

Cíl dokumentu: popsat, jakým způsobem se řeší případ nějakého problému, typicky nefunkčnost systému, nefunkčnost části systému, chybové stavy, základní troubleshooting, apod.

- Základ dokumentace: kontakty (e-mailové adresy, telefonní čísla, url helpdesku)
- V jakém případě, koho a prostřednictvím čeho (e-mailu, helpdesku, sms, telefonu) kontaktovat a jakým způsobem
- Základní troubleshooting často řešených problémů
- Základní chybové stavy (často řešené) – jejich popis a základní způsob odstranění

1.8 Vazby na jiné systémy, rozhraní, datové vztahy a struktury

Cíl dokumentu: popsat, jakým způsobem je daný systém navázán na jaké systémy, popsat všechna rozhraní a popsat datové vztahy a struktury.

- Forma: textový popis doplněný o schéma
- Výčet systémů, na jaké je daný systém navázán (DB, aplikační servery, fileservery, UI, pracovní stanice, zdroje informací /vstupy/, výstupy, datové pumpy, jiné IS, apod.)
- Komunikační protokoly (příp. rozhraní) připojení na jiné systémy
- Porty, ip adresy, identifikátory NIC, API
- Schéma datových toků
- Schéma datových toků osobních údajů, osobních údajů zvláštních kategorií a jiných citlivých informací
- Forma a struktura dat, způsob přenášení dat (použité protokoly), toky dat z a do kterých systémů, způsob jejich uložení, apod.
- Naplánované úlohy přenosu dat (např. datové pumpy), apod.
- Forma a struktura dat, obecný popis dat

1.9 Monitoring

Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.

- Popis logů informačního aktiva
- Výčet a popis všech událostí, které jsou zaznamenávány (př. přihlášení/odhlášení uživatele, provozní/chybové stavy, přidělení/odebrání oprávnění, …)
- Včetně jejich jednotlivých identifikátorů
- Včetně popisu jednotlivých polí/atributů události
- Způsob uložení zalogovaných událostí
- Jak jsou události uloženy
- Kde
- soubor (včetně cesty k souboru)
- databáze, včetně:
- DB serveru a názvu tabulky, případně tabulek
- SQL dotazu pro sestavení view v případě, že událost je uložena do více tabulek

- vzdálený server (IP adresa, protokol)
- Jak dlouho jsou uloženy
- Jak lze konfigurovat
- Protokol logování (např. syslog, windows event log, W3C, apod.)
- Popis provozního monitoringu (např. SNMP, síťový monitoring, aplikační monitoring)
- Popsat, jakým způsobem je realizován provozní monitoring za účelem identifikace a detekce požadovaných či nestandardních provozních stavů

1.10 Základní uživatelská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání uživatelského rozhraní systému pro běžného uživatele. Zjednodušit běžnému uživateli základní orientaci v uživatelském rozhraní systému.

- Forma dokumentu: textový popis, textový popis doplněný o obrázky
- Popis provedení základních/běžných/rutinních funkcí, kroků a postupů, které uživatel může provádět

1.11 Základní administrátorská příručka

Cíl dokumentu: vytvořit základní návod pro ovládání administračního rozhraní systému pro administrátora. Zjednodušit privilegovanému uživateli základní orientaci v administračním rozhraní systému.

- Forma dokumentu: textový popis, textový popis doplněný o obrázky
- Popis provedení standardních (základních/běžných/rutinních) operací, které vedou k běžné administraci systému
- Popis provedení nestandardních (málo běžných) operací, pokud je třeba

1.12 Popis klíčových komponent

Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému

- Forma dokumentu: textový popis (může být doplněno i o schéma)
- Základní fungování, účel, úloha jednotlivých klíčových komponent + jakou platformou (softwarem) jsou jednotlivé komponenty zajištěny
  - Např. master (server), agent (klient), různé typy použitých serverů, moduly, zdroje informací, příjemci informací (systémy), apod.

Příloha č. 8 kupní smlouvy

Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv kupujícího:

- Bezpečnost přístupových oprávnění
  - Poskytovatel je povinen chránit veškeré přístupové údaje k informačním aktivům kupujícího včetně přístupů k informačním aktivům prodávajícího, které umožňují přístup k informačním aktivům kupujícího či umožnují jejich správu.
  - Prodávající je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 17 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      - malá písmena
      - velká písmena
      - číslice
      - speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1,5 roku.
  - Prodávající je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  - Pokud by Prodávající zřizoval přístupová oprávnění třetí straně, je Prodávající povinen o této skutečnosti informovat Kupujícího. Kupující má v tomto případě právo zřízení přístupu zamítnout.

- Řízení změn
  - Prodávající se zavazuje zaznamenávat všechny změny, které v informačním aktivu provedl.
  - Prodávající se zavazuje vynucovat zaznamenávání změn i u případných subposkytovatelů.
  - Záznam změny musí obsahovat minimálně tyto informace:
    - Datum a čas změny
    - Jméno osoby, která změnu provedla
    - Název, popis a účel změny
  - Kupující si vyhrazuje právo na pravidelné informace o záznamech všech změn provedených Prodávajícím i případnými subdodavateli/subposkytovateli.
  - Prodávající se zavazuje všechny jím provedené změny i změny případných subdodavatelů poskytnout Kupujícímu formou pravidelného měsíčního reportu ve formátu pdf, opatřeného elektronickým podpisem, zaslaného na email: epodatelna@nempe.cz případně DS: 9tsrjpp
  - Řízení rizik
  - Kupující si vyhrazuje právo na informace o tom, jakým způsobem Prodávající řídí rizika v souvislosti s plněním této Smlouvy, tedy o tom, jakou metodiku pro řízení rizik používá, jakým způsobem jsou rizika hodnocena a klasifikována, jakým způsobem jsou rizika ošetřována a kdo je za řízení rizik za Prodávajícího zodpovědný.

- Prodávající se zavazuje řídit rizika informační bezpečnosti minimálně v následujícím rozsahu:
    - Identifikace a ohodnocení aktiv souvisejících s plněním této Smlouvy,
    - Identifikace, analýza a ohodnocení rizik souvisejících s plněním této Smlouvy,
    - Zvládání a monitoring rizik souvisejících s plněním této Smlouvy.

- Řízení kybernetických bezpečnostních incidentů:
    - Prodávající je povinen Kupujícímu hlásit veškeré kybernetické bezpečnostní incidenty, které by mohli mít nějakou souvislost s:
        - informačními aktivy Kupujícího,
        - přístupovými údaji k informačním aktivům Kupujícího,
        - informacím Kupujícího
    - Prodávající je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kupujícího.

- Kryptografie:

a) Obecně

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá

b) Hashovací funkce

c) Ukládání otisků hesel

- pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
    - Argon2 s parametry alespoň t=1, m=221, p=4 a funkcí Argon2id
    - scrypt s parametry alespoň N=32768 (215), r=8, a p=1
    - PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2 (viz níže)
- při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
- pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

d) Elektronické podepisování e-mailů a dokumentů

- SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- délka otisku 384 bitů a vyšší

e) Ověřování integrity souborů

- SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- délka otisku 384 bitů a vyšší

f) Asymetrická kryptografie

g) SSL/TLS

- verze protokolu minimálně TLSv1.2 a vyšší
- konfigurace
    - cipher suite musí být vybrána na základě serverem preferovaného pořadí
    - vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
        - ECDHE musí mít vyšší prioritu než DHE
        - ECDSA musí mít vyšší prioritu než DSA
    - všechny EXPORT cipher suites musí být zakázány
    - algoritmy a funkce pro výměnu klíčů
        - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
            - tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
            - a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů
        - délky klíčů:
            - pro Diffie-Hellman (DH) - 3072 bitů
            - pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
        - nesmí být použita anonymní výměna klíčů
    - algoritmy a funkce pro autentizaci
        - minimální délky klíčů:
            - RSA - 3072 bitů
            - DSA – 3072 bitů
            - ECDSA - 256 bitů
    - algoritmy a funkce pro symetrické šifrování
        - nesmí být použita hodnota NULL v cipher suites
        - nesmí být použity tyto šifry:
            - DES, 3DES, RC4
        - minimální délka šifrovacího klíče - 128 bitů
        - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
    - MAC (Message Authentication Code)
        - použití SHA funkce s minimální délkou hashe 256 bitů
        - vyšší délky otisků musí mít vyšší prioritu v cipher suites

h) TLS cipher suites

- Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
- TLS1.3:

  TLS_AES_256_GCM_SHA384
  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_128_GCM_SHA256
  TLS_AES_128_CCM_SHA256

- TLS1.2:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

i) Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
    - algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to půjde)
    - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to půjde)
    - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
    - délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to půjde)
    - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

j) Symetrická kryptografie

- nesmí být použity tyto šifry:
    - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 128 bitů
    - pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
- nesmí být použity tyto módy pro ochranu integrity:
    - HMAC-SHA1, CBC-MAC-X9.19