Příloha č. 1

**Technická specifikace**

k veřejné zakázce na dodávky s názvem:

**„Dodávka HW zařízení a SW aplikací – Městský úřad Hronov“**

1. **Identifikační údaje zadavatele**

|  |  |
| --- | --- |
| Název: | Město Hronov |
| Sídlo: | nám. Čs. armády 5, 549 31 Hronov |
| Zastoupený: | Petr Koleta, starosta města |
| IČO: | 00272680 |

1. **Identifikace účastníka**

|  |  |
| --- | --- |
| Název: | …………………………………… |
| Sídlo: | …………………………………… |
| Osoba oprávněná za účastníka jednat: | …………………………………… |
| IČO: | …………………………………… |

1. **Předmět veřejné zakázky – technická specifikace HW zařízení a SW aplikací**
2. **Server – 1 ks**
* rack provedení s výškou maximálně 2U
* 1x určený pro servery, skóre dle benchmark v konfiguraci dvou CPU min. 58.000 bodů dle <https://www.cpubenchmark.net/cpu_list.php>
* možnost osazení druhým procesorem
* operační paměť ve výši 384 GB RAM DDR5 PC4800, možnost rozšíření až na 3072 GB/socket
* ochrana paměti: Advanced ECC with multi-bit error protection and memory online spare mode
* integrovaný síťový adaptér 4x 1Gb port, nezabírající PCIe slot
* síťový adaptér s rozhranním 2x 10GbE SFP+
* SAN adaptér 32Gb dual port HBA ve sběrnici PCIe
* hardwarový RAID řadič minimálně s podporou RAID 0, 1, 5, 6 a 10, cache pamětí min. 4 GB a zálohou pomocí baterie
* 3x pevný disk 1,6TB NVMe Mixed Use SFF v provedení 2,5“ Hot-Plug
* možnost rozšíření až na 34 disků 2,5“ s podporou NVME Premium
* 6ks PCIe slotů ve specifikaci PCIe 5.0 X16, ve standardním provedení minimálně 3ks
* 2x redundantní napájecí zdroj min. 1000W, s účinností min. 94%
* integrovaná karta vzdálené správy včetně SW licence pro plnohodnotné využití minimálně na 3 roky
* vzdálené ovládání limitů výkonu a spotřeby zdrojů bez nutnosti instalace agentů do OS
* přímá podpora správy virtuálních serverů pro VMware, Microsoft Hyper-V – možnost min. těchto operací nad virtuálními servery: start, stop, pause, reset, move, copy, backup
* možnost přímé integrace s VMware vCenter a Microsoft System Centre Virtual Machine Manager
* záruka na server minimálně 3 roky s okamžitou telefonickou odezvou, 24x7 pokrytí na místě včetně svátků
* součástí výbavy serveru budou ližiny pro připevnění do racku a rameno pro správu (strukturalizaci) kabelů v racku
* Zadavatel požaduje dodání totožného typu serveru jako již jeden server vlastní z důvodu jednotného magamentu a z důvodu nasazení ve vysoké dostupnosti.
1. **Zálohovací pásková knihovna – 1 ks**
* Externí pásková mechanika ve standalone provedení
* SAS drive minimálně LTO-8
* SAS PCI-E host adapter do serveru s externím konektorem
* SAS kabel pro připojení mechaniky a serveru
* 20ks minimálně LTO-8 RW medií včetně čárových kódů
* 1ks čistící LTO pásky
* Záruka 3 roky garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem mechaniky. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla knihovny.
* Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
* Pro centrální management požadujeme diskové pole od totožného výrobce jako server, tak aby byla využita synergie jednotné správy takového prostředí
* Součástí dodávky musí být kompletní instalace mechaniky, včetně konfigurace a nastavení zálohovacích úloh dle požadavků zadavatele.
1. **Firewall – 1 ks**
* Za účelem zabezpečení sítě, interní segmentaci sítě a zabezpečení sítového perimetru jse poptáván 1 ks zařízení typu Next Generation Firewall (dále jen NGFW) ve formě hardware appliance s podporou výrobce v režimu 24x7 a aktualizací všech požadovaných bezpečnostních funkcí po dobu 3 roky.

**Obecné požadavky**

* hardware appliance o velikosti 1 RU s možností režimu vysoké dostupnosti (active-active, active-passive)
* Podpora virtualizace uvnitř HW appliance formou vytváření virtuálních kontextů
* Grafické konfigurační rozhraní a příkazový řádek
* Minimální počty požadovaných síťových rozhraní:
	+ 8x GE RJ 45
	+ 2x 10GE SFP+
	+ Min. 1x konzolový port a 1x management port
* Podpora plnohodnotné inspekce sítového provozu v režimech
	+ NAT/router
	+ L2 transparentní režim (dva a více sítových rozhraní)
	+ L2 interface pair (dvě sítové rozhraní)

**Výkonové požadavky**

* Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání.
* Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 26 Gbps (UDP pakety o velikosti 512 B)
* Nízké vložené zpoždění zařízení (latence) max. 5 μs
* Minimální počet současně navázaných spojení firewallu 2.5 M
* Minimální počet nových spojení za sekundu 120 k
* Propustnost firewallu v packetech min. 35 Mpps
* Propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)
	+ Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) min. 2 Gbps
	+ Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 2 Gbps
	+ Propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 4 Gbps
	+ Propustnost funkce rozpoznávání sítových aplikací na L7 min. 5 Gbps
* Propustnost IPsec VPN v konfiguraci AES256/SHA256 min. 20 Gbps
* Propustnost funkce SSL inspekce provozu min. 2.5 Gbps
* Min. počet konfigurovatelných virtuálních kontextů na každém zařízení 10

**Funkční požadavky**

* Podpora a zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) minimálně s ohledem na tyto bezpečnostní funkce:
	+ Funkce rozpoznávání kancelářských a průmyslových aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací a 700 průmyslových aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací
	+ Funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min. 10 000 signatur v databázi; podpora zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT)
	+ Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předání zkoumaných souborů pro analýzu do prostředí typu sandbox
	+ funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze.
	+ funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky z SSL inspekce požadujeme minimálně:
		- na základě administrátorem definovaných adres
		- na základě kategorie URL, brané z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.)
* Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
* Možnost nastavovat firewall politiku na základě geografických údajů
* Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace
* Detekce klientského zařízení, možnost nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, …) bez nutnosti instalovat klienty na koncové stanice
* Funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky
* Funkce QoS, traffic shaping
* Funkce klientské VPN (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál, možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů
* site-to-site IPsec VPN s podporou statického i dynamického routování
* Podpora OT/ICS/IoT protokolů (minimálně klasifikace provozu, identifikace zařízení, ochrana zařízení před sítovým útokem)
* Umístění výrobce v Gartner MQ for Network Firewalls v sekci „Leaders“ v posledních 3 letech.
1. **Zálohovací systém - soubor**
* Licence pro dva dvousocketové servery
* Zálohovací řešení musí podporovat infrastrukturu VMware ve verzích 6.x, 7.x a 8.0, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution
* Řešení musí podporovat hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele.
* Zálohovací řešení musí podporovat Windows Server Hyper-V 2012 až 2022 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server
* Řešení musí podporovat hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V
* Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech
* Řešení musí podporovat zálohování platformy Red Hat Virtualization 4.4 SP1
* Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux.
* Software musí být možné licencovat pomocí trvalé licence i formou časově omezené subscripce.
* Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy a to jak pro výpočetní část, tak pro část ukládání dat.
* Licence musí být přenositelná mezi různými fyzickými, virtuálními a cloudovými chráněnými objekty
* Všechny součásti řešení musí plně podporovat komunikaci po IPv6
* Řešení musí mít mechanismy k úspoře objemu úložného prostoru pro ukládání záloh. Jejich využití musí být volitelné a nesmí omezit žádné funkcionality zálohování a obnovy dat.
* Řešení musí poskytovat jednotnou konzoli pro přehled o zálohách fyzických, virtuálních, cloudových, NAS i Kubernetes prostředí
* Řešení musí umožnit vytvoření jednoho logického úložiště pro ukládání záloh z neomezeného počtu různorodých diskových úložišť
* Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení.
* Řešení musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru
* Výše uvedená funkce musí být konfigurovatelná na úrovni datastore virtualizační platformy
* Řešení musí umožňovat vytváření záloh integrací se snímky úložiště. Dále musí umožnit obnovu jednotlivých VM, souborů a položek aplikace z těchto snímků. Proces zálohy nemůže k připojení snímku použít dočasného hostitele. Popsaná funkce musí fungovat pro prostředí VMware vSphere a musí podporovat následující pole: Dell, NetApp, HPE, HITACHI VANTARA, IBM, Lenovo, Fujitsu, Pure Storage, CISCO, DataCore
* Řešení musí mít replikaci produkčních VM přímo z infrastruktury VMware vSphere, mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace. Řešení musí navíc umožnit jako zdroj replikačních úloh využít soubory záloh
* Řešení musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (vestavěný NFS server). Tato funkce musí být podporována pro prostředí VMware a Hyper-V a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM
* Uvedená funkce musí umožňovat spuštění zálohy vytvořené z různých platforem (různých virtuálních, fyzických a veřejných cloudových virtuálních strojů)
* Řešení musí umožňovat online migraci virtuálních počítačů, zpuštěných z úložiště záloh, do produkčního úložiště pomocí funkcí hypervizoru. Řešení musí také poskytovat svou vlastní funkci, která takové schopnosti poskytne.
* Řešení musí umožňovat prezentaci disků přímo ze záložního souboru do spuštěné VMware VM
* Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu.
* Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti
* Řešení musí podporovat gMSA účty pro zajištění aplikačně-konzistentních záloh v GuestOS bez nutnosti ukládání přístupových oprávnění na úrovni administrátora pro daný GuestOS.
* Řešení nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech
* Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran.
* Řešení musí poskytovat dohled nad chráněnou virtualizační platformou, poskytující včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí
* Řešení musí poskytovat možnost dohledu služeb a procesů provozovaných v GuestOS jednotlivých chráněných VM
* Řešení musí informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým způsobem byl naposledy vytvořen bod obnovy.
* Řešení musí poskytovat možnost automatizovaných řešení chybových stavů
* Řešení musí poskytovat funkce pro zasílání stavových hlášení do centrálního monitorovacího nástroje přes SNMP protokol
* Řešení musí podporovat monitorování virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran
* Řešení musí podporovat dohled následujících systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni pomocí vCenter serveru nebo pracovat v samostatném režimu
* Řešení musí poskytovat historická data a predikce z nich vyplývající, nezbytné pro plánování zdrojů pro provoz a ochranu virtualizovaného prostředí
* Součástí řešení musí být i možnost vytvářet detailní auditové správy o změnách v konfiguraci zálohovacího řešení a o obnovách dat ze záloh
* Řešení musí podporovat reporting virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran
* Řešení musí podporovat reporting následujících hypervisorových systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni vCenter nebo pracovat v samostatném režimu
* Řešení musí podporovat reporting následujících systémů: Microsoft Server Hyper-V 2012, 2012R2, 2016, 2019 a 2022 pro placené i bezplatné edice. Podporovaní hostitelé mohou být spravováni SCVMM nebo pracovat v samostatném režimu
* Řešení nesmí vyžadovat instalaci žádných agentů na monitorovaných hostitelích ESXi a Hyper-V a na virtuálních počítačích
1. **Bezpečnostní software**

Licence komplexního SW pro ochranu před škodlivým softwarem pro 50 uživatelů, včetně příslušenství uvedeného níže v podobě EDR a Sandboxu pro tyto licence.

Podpora operačních systémů MS:

* Windows 7 a vyšší
* Windows Server 2008 R2 a vyšší

Antivirový klient pro systémy:

* Windows
* Linux
* macOS
* Android

Real-Time ochrana před všemi typy PUA a malwaru:

* viry
* červy
* trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…)

Správa zařízení pro Windows, macOS a Linux, umožňující blokaci externích zařízení a médií, s podporou whitelistování dle:

* výrobce, modelu nebo sériového čísla,
* uživatelů nebo skupin (např. administrátorů) v AD,
* lokálního času.

Schopnost blokace přístupu na definované weby nebo skupiny webů dle kategorií s možností whitelistování dle přihlášeného uživatele/skupiny v AD nebo času.

* Lokální anti-spam s úspěšností detekce 99 % a vyšší.
* Lokální anti-spam s možností definování důvěryhodných a spamových adres.
* Nativní 64 bitové jádro.
* Ochrana komunikace e-mailovými protokoly:
	+ POP3,
	+ POP3S,
	+ IMAP,
	+ IMAPS,
	+ HTTP,
	+ MAPI.
* Antivirus, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.
* Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall.
* HIPS (Host-based Intrusion Prevention System) pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení.
* Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.
* Systém pro blokaci exploitů zneužívajících zeroday zranitelností, jenž pokrývá nejpoužívanější vektory útoku:
	+ síťové protokoly,
	+ Flash Player,
	+ Javu,
	+ Microsoft Office,
	+ webové prohlížeče,
	+ e-mailové klienty,
	+ PDF čtečky…
* Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě.
* Anti-phishing se schopností detekce homoglyph útoků.
* Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.
* Možnost jednotlivého zapnutí detekcí:
	+ potenciálně nechtěných aplikací,
	+ zneužitelných aplikací,
	+ podezřelých aplikací.
* Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů.
* Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.
* Detekce s využitím strojového učení.
* Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.
* Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.
* Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
* Lokální sandbox.
* Speciální modul behaviorální analýzy pro detekce nových typů ransomwaru.
* Systém reputace pro získání informací o závadnosti souborů a URL adres.
* Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.
* Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému.
* Skenr firmwaru BIOSu a UEFI.
* Skenování souborů v cloudu OneDrive.
* Šetření baterie notebooku – možnost odložení kontroly / provádění aktualizací, pokud je zařízení napájeno z baterie.
* Podpora dotykového ovládání.
* Ovládání bezpečnostního programu pomocí Příkazového řádku.
* Podpora ochrany na IPv6.
* Možnost řízení šířky pásma pro stahování aktualizací.
* HIPS s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
* Možnost vrácení i odložení aktualizací signatur.
* Možnost instalovat plnohodnotné antivirové řešení na virtuální stanici/server.
* Modulární instalace.
* Automatická synchronizace bezpečnostních produktů v clusteru.
* Bezagentové zabezpečení pro VMware vShield aNSX.
* Možnost importu/exportu nastavení.
* Prezentační režim umožňující potlačení méně důležitých upozornění při práciv celoobrazovkovém režimu aplikace.
* Možnost tvorby výjimek na procesy.
* Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému.
* Možnost vzdáleného definování akce při připojení výměnných médií (kontrolovat, nekontrolovat, nechat na uživateli).
* Možnost využití sdílené cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolované na jiném zařízeních a tím výrazně zrychlit kontrolu).
* Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky).
* Kontrola šifrovaných spojení (SSL, TLS, HTTPS,IMAPS…).
* Možnost odesílání e-mailových upozornění a událostí přímo z klienta.
* Integrovaný komplexní diagnostický nástroj umožňující řešit problémy s infiltrací, jakožto i jiné softwarové a hardwarové nekorektní chování (obsahuje informace procesech, službách, síťových připojeních, ovladačích a problémových položkách v registrech).
* Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.
* Využití Microsoft Antimalware Scan Interface (AMSI) pro kontrolu skriptů (PowerShell, wscript.exe a cscript.exe).
* Podpora Protected Services – službu produktu je možné chránit proti nechtěné modifikaci standardní součástí operačního systému.
* Podpora odečítače obrazovky pro zrakově postižené.
* Podpora SNMP Trap, Syslogu a qRadar SIEM.
* Podpora instalace skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…).
* Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
* Reportování stavu klientů chráněných jinými bezpečnostními programy.
* Schopnost zaslat reporty a upozornění na email.
* Přidání zařízení do vzdálené správy pomocí:
	+ synchronizace s Active Directory,
	+ ruční přidání pomocí dle IP adresy nebo názvu zařízení,
* pomocí síťového skenu nechráněných zařízení v síti.
* Je požadována dodávka licence s délkou trvání 3 let, včetně nároků na nové verze software po tuto dobu.

**Odhalení škodlivé, či podezřelé aktivity tzv. EDR**

* Podpora Windows a macOS.
* Indicators of Compromise (IOCs):
	+ MD5 hodnoty souborů,
	+ IP adresy a URL,
	+ Nesoulad názvů souborů/procesů,
	+ Neobvyklé využití aplikací a síťových portů,
	+ Neobvyklé injektování do procesů,
	+ Modifikace částí aplikací,
	+ Změny v registru.
* Indikátory útoku pracující s behaviorální detekcí.
* Indikátory útoku pracující s reputací.
* Možnost tvorby vlastních IoC.
* Řešení umožnuje analýzu vektorů útoku.
* Vizibilita do WMI.
* Vizibilita do spouštěných skriptů (PowerShellem, CScriptem, WScriptem…).
* Přehled o veškerém použitém softwaru a jeho verzích.
* Schopnost detekce škodlivých spustitelných souborů a skriptů.
* Pokročilé možnosti analýzy:
	+ exploitů,
	+ rootkitů,
	+ síťových útoků,
	+ bezsouborového malwaru.
* Schopnost analýzy RAM paměti.
* Detekce rootkitů v UEFI a MFT.
* Schopno detekovat laterální pohyb útočníka.
* Tagování objektů.
* Terminal (interaktivní Shell).
* Možnost ruční analýzy procesů a veškerých spustitelných souborů včetně DLL knihoven a skriptů.
* Prioritizace vzniklých incidentů za pomocí algoritmů strojového učení.
* Detekce více než 300 typů obecného podezřelého chování: dumpování přihlašovacích údajů, změna konfigurace firewallu, mazání logů, změna hosts souboru, smazání Shadow Copy, nainstalování nového certifikát, vypnutí aktualizací…
* Detekce s využitím modelů strojového učení a neuronových sítí.
* Schopnost zobrazení detekcí provedených antimalware produktem.
* Možnost spouštět předkonfigurované nápravné akce, které se sami spustí za při splnění definovaných podmínek.
	+ Okamžitá síťová izolace, ukončení procesu, vymazání/stažení souboru.
* Snížení počtu falešně pozitivních výsledků za pomocí algoritmů strojového a hlubokého učení.
* Řešení je schopno generovat tzv. forest / full execution tree model.
* Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty.
* Provázání s technikami popsanými v knowledge base MITRE ATT&CK.
* Možnost analyzovat
	+ veškeré události až 3 měsíce zpětně,
	+ bezpečnostní incidenty až 3 roky zpětně.
* Možnost provozu v offline prostředí.
* Možnost logování činností uživatele.
* Přihlašování do konzole za využití 2FA.
* Podpora exportu do SIEMu.
* REST API.
* Možnost provozu EDR serveru na systému Windows.
* Možnost provozu centrálního serveru on-premise.
* Možnost provozu s databázemi:
* MS SQL,
* MySQL.

**Sandboxing**

* Sandbox umožňující spuštění vzorků malwaru pro:
	+ Windows,
	+ macOS,
	+ Linux,
	+ Android.
* Možnost využití na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v emailech.
* Řešení zajišťuje neodesílání duplicitních souborů nalezených různými endpointy.
* Analýza neznámých vzorků v řádu jednotek minut.
* Schopnost ochrany klientů mimo firemní síť.
* Optimalizace pro znemožnění obejití anti-sandbox mechanismy.
* Schopnost analýzy rootkitů a ransomwaru.
* Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.
* Řešení pracuje s behaviorální analýzou.
* Manuální odeslání vzorku do sandboxu.
* Funkce cloudového sandboxu je integrována do antimalware produktu (cloudový sandbox nemá vlastního agenta).
* Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
* Neomezené množství odesílaných souborů.
* Veškerá komunikace probíhá šifrovaným kanálem.
* Webová konzole.
* Administrace v nejpoužívanějších jazycích včetně češtiny.
* Možnost nastavení typů odesílaných souborů:
	+ spustitelné soubory,
	+ skripty,
	+ spam,
	+ dokumenty.
* Přehled o veškerých odeslaných souborech ve správcovské konzoli.
* Nastavení per zařízení & per skupina.
* Možnost nastavit na výsledek sandboxu výjimku.
* Zaslání e-mailové notifikace v případě nalezení škodlivého kódu.
* Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
* Server/proxy architektura pro síťovou pružnost – snížení zátěže.

**Šifrování celých disků**

* + - Podpora platforem Windows a MacOS
		- Správa skrze centrální management
		- Unikátní technologie pro platformu Windows (nevyužívá se BitLocker)
		- Podpora Pre-Boot autentizace
		- Podpora SSO (Možnost zadání jména/hesla do OS přímo z pre-boot obrazovky)
		- Podpora TMP modulu
		- Podpora Opal samošifrovacích disků
		- Možnost definovat počet chybně zadaných pokusů
		- Možnost definovat složitost a délku autentizačního hesla
		- Možnost omezit platnost autentizačního hesla
		- Podpora okamžitého smazání šifrovacího klíče a následné uzamčení počítače
		- Recovery z centrální konzole

**Management konzole pro správu všech řešení v rámci nabízeného balíku**

* + - Webová konzole
		- Možnost instalace v on-premise prostředí na Windows nebo Linux.
		- Možnost provozu konzole v cloudu výrobce
		- Možnost instalace formou virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box připravenou výrobcem.
		- Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.
		- Možnost probuzení klientů pomocí Wake On Lan.
		- Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta
		- Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
		- Administrace v nejpoužívanějších jazycích včetně češtiny
		- Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
		- Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.
		- Informace o aktuálně přihlášených uživatelích na daném zařízení
		- Podpora štítků/tagování pro snazší správu a vyhledávání
		- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
		- Vzdálené získání zachyceného škodlivého souboru z klienta.
		- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
		- Instalace a odinstalace aplikací 3. stran.
		- Vyčítání informací o verzích softwaru 3. stran.
		- Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).
		- Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce.
		- Vzdálená odinstalace antivirového řešení 3. strany.
		- Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.
		- Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy
		- Dynamické skupiny musí umět fungovat i v konkrétních časových slotech a uplatňovat podporované klientské úlohy
		- Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).
		- Podpora SNMP Trap, Syslogu, Rest API
		- Podpora instalace agenta skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…).
		- Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
		- Reportování stavu klientů chráněných jinými bezpečnostními programy.
		- Schopnost zaslat reporty a upozornění na e-mail.
		- řešení umožňuje odesílat notifikace o vybraných událostech prostřednictvím tzv. webhooků
		- Možnost integrace s řešením třetích stran podporující MDM (např. MS Intune, Workspace One)
* Možnost řízení managementu konzole a jeho komponent prostřednictvím API, a to jak pro:
	+ - * Centrální správu samotnou
			* Komponenty antimalware řešení, jeho správy, politik a nastavení
			* správy zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů
* Přidání zařízení do vzdálené správy pomocí:
* synchronizace s Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů
* ruční přidání pomocí dle IP adresy nebo názvu zařízení,
* pomocí síťového skenu nechráněných zařízení v síti.

**Ochrana poštovních serverů MS Exchange**

* + - Společná víceúrovňová ochrana celého serveru – databáze schránek, transportu zpráv i souborového systému serveru
		- Podpora MS Exchange 2007, 2010, 2013 a 2016, 2019
		- Antivirus, antispyware a antispoofing technologie
		- Antispam s funkcí graylisting
		- Blokace nevyžádané pošty a phishingu bez potřeby manuálně upravovat SCL (Spam Confidenace Level) hodnoty
		- Možnost vytváření vlastních pokročilých antispamových pravidel (vyhodnocení více podmínek v jenom pravidlu)
		- Kontrola jednotlivých MBX databází, případně konkrétní schránky uživatele
		- Umožnit uživateli poštovní schránky pracovat pomocí samostatného prohlížeče se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do emailové schránky
		- Možnost vlastních pravidel s vlastním hodnocením obsahu
		- Podpora více serverového prostředí zajištění P2P komunikací, např. Ve skupině DAG
		- Detekce škodlivých souborů v reálném čase
		- Možnost správy přes příkazovou řádku (Podpora edice Windows Server Core)
		- Komplexní protokoly blokovaného spamu a zobrazení greylistingovaných odesílatelů, protokoly všech zpráv, nejen blokovaných
		- Sledování výkonu serveru v reálném čase
		- Možnosti pro nastavení pravidel inspekce souborů – mazání spustitelných souborů, skriptů
		- Cloudová reputační služba pro kontrolu příloh emailových zpráv
		- Možnost spravovat ochranu na Exchange Serveru samostatně nebo prostřednictvím management konzole v cloudu
		- Možnost exportu protokolu událostí produktu do protokolu operačního systému
		- Tvorba pravidla "Z hlavičky" a vyhodnocovat pole From: pro přesnější detekci podvržených e-mailů
		- Backscatter ochrana
		- Synchronizace lokální karantény zpráv napříč uzly clusteru
		- Podpora hybridního prostředí s možností kontroly poštovních schránek v Office 365
		- Možnost zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům
		- Možnost zabezpečit heslem ochranu poštovního serveru a jeho komponent proti náhodné či chtěné modifikaci neautorizovaného uživatele
		- Možnost zabezpečení heslem musí být možné přes konzoli dočasně deaktivovat pro vybrané uživatele na základě ověření administrátora vůči doméně
		- Správa karantény prostřednictvím webového portálu pro vybrané uživatele i administrátory
		- Ochrana nastavení dodatečným heslem před neoprávněnou změnou konfigurace produktu
		- Možnost editovat zasílané zprávy o stavu karantény a zachycených souborů v karanténě (editace těla emailu, předmětu a odkazu na blokovaný e-mail)
		- Funkce cloudového sandboxu je integrována do produktu pro e-mailovou ochranu MS Exchange, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě
		- Data odesílané v rámci cloudového sandboxu jsou zpracovávány v rámci EU
		- Sandbox umožňující spuštění vzorků malwaru pro:
			* Windows,
			* macOS,
			* Linux
		- Možnost využití na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v e-mailech
		- Analýza neznámých vzorků v řádu jednotek minut
		- Optimalizace pro znemožnění obejití anti-sandbox mechanismy
		- Schopnost analýzy rootkitů a ransomwaru
		- Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti
		- Řešení pracuje s behaviorální analýzou
		- Kompletní výsledek o zanalyzovaném souboru dostupný v centrálním managementu včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru
		- Možnost manuálního odeslání vzorku do sandboxu
		- Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu
		- Neomezené množství odesílaných souborů
		- Veškerá komunikace probíhá šifrovaným kanálem
		- Možnost okamžitého odstranění souboru po dokončení analýzy z cloudovém sandboxu
		- Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.)
		- Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.

**Ochrana pro cloudové kanceláře Microsoft 365 a Google Workspace**

* Řešení poskytuje komplexní ochranu pro prostředí Microsoft 365
* Exchange Online
* OneDrive
* SharePoint Online
* Microsoft Teams
* Řešení poskytuje komplexní ochranu pro prostředí Google Workspace
* Gmail
* Google Drive
	+ - Nezávislá cloudová správa pro vyhodnocení zachycených hrozeb
		- Neinvazivní technologie – nesmí při nedostupnosti ovlivnit fungování samotného MS365 nebo Google tenantu
		- Funkce Antimalware, Antispam, Antiphishing
		- Detekce útoků využívající homoflyf techniku
		- Možnost zasílání pravidelných reportů
		- Vícenásobná kontrola podezřených emailů
		- Export událostí, detekcí a audit logů přes Syslog
		- Možnost ochránit celý tenant nebo jednotlivé uživatele
		- Anti-spoofing technologie
* Možnost tvořit pokročila transportní pravidla (definice verifikačních podmínek a akcí na základě proměnných typu hlavička emailu apod.)
* Kontrola DKIM, DMARC and SPF
	+ - Automatická aplikace ochrany pro nově vzniklé uživatele v MS365 nebo Google Workspace
		- Integrovaná funkce analýzy neznámých vzorků v prostředí cloudového sandboxu

**Systém pro detekci a správu zranitelností (VAPM)**

* Řešení je součástí agenta poskytovatele bezpečnostní platformy bez nutnosti instalace dalších komponent
* Podpora operačních systémů Windows, Linux a MacOS
* Integrován v centrálním managementu bezpečnostního nástroje výrobce
* Všechny detekované zranitelnosti a jejich dostupné záplaty jsou spravované přes centrální správu výrobce bezpečnostního řešení
* informace o zranitelnosti je ve standardizovaném formátu CVE včetně data zařazení zranitelnosti, její povahy a odkaz na zdroj popisující zranitelnost
* každá zranitelnost musí mít „bezpečnostní skóre“ dle databáze CVSS 3.0 či novější
* možnost ručního spuštění záplaty podporované aplikace
* možnost automatického spuštění záplaty podporované aplikace podle časových kritérií s možností vybrání aplikací logikou blacklist/whitelist
* možnost automatizovaného spuštění záplaty vybrané aplikace podle vydefinované podmínky (např. podle skóringu zranitelnosti, podle konkrétních CVE, podle konkrétních verzí aplikací)
* V případě potřeby restartu zařízení má uživatel možnost restart odložit
* V případě potřeby restartu aplikace je uživatel informován o této potřebě a aplikace není bez vyzvání rovnou restartována
* Automatické záplatování Windows OS s možností definice typ aktualizací kritických/důležitých updatů
* Možnost definovat minimální prostor na disku pro stáhnutí a aplikaci záplat
* Vynucení instalace záplaty po uplynutí stanovené lhůty.
* Možnost spustit sken zranitelností na vyžádání

**Správa mobilních zařízení a antivirová ochrana (MDM)**

* + - Zařízení je možné centrálně spravovat pomocí management konzole výrobce bezpečnostního řešení
		- Podpora operačních systémy Android, iOS a iPadOS
		- Možnost zaregistrovat zařízení v režimu vlastníka nebo ABM
		- Application control s možností vynucení požadovaných aplikací,
		- Lokalizace zařízení
		- Podpora anti-theft akcí (siréna, zámek telefonu, vzdálené smazání dat)
		- Detekce roamingu
		- Konfigurace restrikcí
		- Vynucení složitosti zámku obrazovky zařízení
		- Správa účtů (email, LDAP, Exchange,..)
		- Integrace s managementem zařízení Microsoft Intune
		- WebControl s možností filtrování obsahu webu
		- Filtrování hovorů a SMS s definicí časových slotů pro uplatnění pravidel
		- správa aktualizací systému
		- Ochrana před výměnou SIM karty (definice důvěryhodné SIM)
		- Možnost definovat informace na zamčené obrazovce (kontaktní údaje společnosti)

**Požadavky na antivirové zabezpečení**

* + - Podpora antivirového zabezpečení pro operační systém Android
		- Rezidentní ochrana běžící a chránící zařízení v reálném čase
		- Možnost definice naplánovaných kontrol
		- Možnost kontroly výměnných zařízení
		- Detekce potenciálně nechtěných aplikací
		- Definice aktualizačního serveru
		- Antiphishing ochrana
		- Detekce phishingových URL v SMS zprávách
		- Instalace a odinstalace aplikací 3. stran.
		- Vyčítání informací o verzích softwaru 3. stran.
		- Možnost vyčítat informace o hardwaru na spravovaných zařízeních

**Connect API Gateway**

* + - Cloud API rozhraní pro ovládání a čerpání informací z centrálního managementu
		- Integrace se SIEM/SOAR nástroji. Konkrétně Artic Wolf, Elastic, MS Sentinel, IBM QRadar

**Požadavky na podporu a zaškolení**

Dodavatel musí prokázat schopnost poskytnout výše uvedené funkcionality, včetně adekvátní podpory a případného (i dodatkového v čase) školení pro koncové uživatele. Všechny funkce musí být kompatibilní s aktuálním hardwarovým a softwarovým vybavením organizace.

1. **NAC – Network Access Control**

• Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení

• Forma dodání: virtuální appliance pro VMware

• Minimální celková kapacita řešení pro autentizaci unikátních 100 koncových zařízení

• Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru

• Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance

• Podpora minimálně 20ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě)

• Požadované metody autentizace uživatelů a zařízení: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace

• Podpora RADIUS CoA dle RFC3576

• Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD

• 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

• Možnost TACACS+ autentizace správců síťových zařízení

• 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)

• Možnost integrace s MDM (Mobile Device Management) platformami třetích stran: minimálně AirWatch, Citrix, MobileIron, JAMF, InTune

• Podpora REST API pro většinu základních úkonů AAA platformy

• Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.)

• 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.

• Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran.

• 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.

• LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, 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.

• 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).

• Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí AAA platformy.

• Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací.

• Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení.

• Možnost licenčního rozšíření o kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku.

• 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

• Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem

• Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém.

• Servisní podpora na 36 měsíců garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce.

1. **NDR - Network Detection and Response**
* Monitorovací systém pro dlouhodobé a detailní monitorování veškerého provozu v počítačové síti
* Systém musí umožňovat v reálním čase vyhodnocovat objemy a struktury provozu, analyzovat příčiny provozních či výkonnostních problémů a odhalovat bezpečnostní hrozby.
* Systém musí být nezávislý na použité síťové infrastruktuře
* Systém nesmí svou funkcí monitorovanou síť ovlivňovat
* Sonda v podobně virtuální appliance pro monitoring datových toků v kombinaci s integrovaným kolektorem zajistí monitoring, sběr, uchování a reporting Flow dat. Sonda bude instalována na rozhraní WAN. V rámci dodávky bude nakonfigurováno min. 5 reportů a bude zaškolena lokální administrátor sítě v rozsahu min. 0,5 den. Součástí konfigurace bude nastavení servisních protokolů NTP, SSH, HTTPS, SNMP atd.
* Pasivní zapojení bez vlivu na monitorovanou síť a propustnost zařízeni (zapojení pomocí TAP sdružujícího obousměrný monitorovaný tok do jedné linky).
* Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
* Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí.
* Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalickém rozhraní.
* Podpora pro SNMP
* Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru a uložení dat po dobu min. 2 měsíců
* Výkon vestavěného kolektoru min. 50 000 toků/s
* Časová synchronizace zařízení proti centrálnímu zdroji času na síti (NTP).
* Minimální výkon 1 milion paketů za sekundu na každém portu.
* Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
* Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232).
* Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
* Podpora autentizace vůči LDAP (Active Directory).
* Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX.
* Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.
* Monitorování provozu v tunelu GRE.
* Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX.
* Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu.
* Detekce aplikací dle standardu NBAR2.
* Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
* Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
* Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
* Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.
* Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port.
* Podpora pro nastavení časů u aktivní a neaktivní expirace toků.
* Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků.
* Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX).
* Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky).
* Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port.
* Servisní podpora na 36 měsíců garantovaná přímo výrobcem.
1. **Monitoring IT Infrastruktury**

**Základní vlastnosti monitorovacího systému**

* Produkt je open source
* Výrobce vytváří verze s Long-term support (LTS)
* Výrobce nabízí možnost placené podpory
* Data lze uchovávat minimálně 1 rok
* Data se po určitém čase začnou průměrovat pro snížení velikosti databáze
* Systém podporuje proxy servery pro monitoring vzdálených lokalit, provoz ze vzdálených lokalit je šifrovaný
* Se systémem je možné pracovat přes API

**Podporované metody vyčítání dat**

* ICMP
* SNMP
* SNMP trap
* IPMI
* JMX
* Agent pro Windows, Linux, macOS, FreeBSD
* Web monitoring
* podpora monitoringu pomocí vlastních skriptů

**Šablony sledovaných zařízení** (Výrobce musí mít připravené šablony pro min.):

* Fortigate firewall
* HP Switche
* Aruba Switche
* Cisco Switche
* VMware Hypervizor
* HyperV Hypervizor
* HP ILO
* Synology NAS
* APC UPS
* Windows server
* Linux server
* MS Exchnage
* Možnost vytvářet vlastní šablony
* Možnost importu šablon vytvořených komunitou
* Možnost použití maker v šablonách, každé zařízení může mít nastavenou jinou hranici pro spuštění alertu

**Sledování hodnot**

* Možnost změny monitorovacího intervalu (vteřiny, hodiny, dny) = optimalizace velikosti DB
* Možnost změny délky ukládání dle typu hodnoty (text, číslo) = optimalizace velikosti DB
* Možnost přepočítání sledované hodnoty před uložením do DB (např. násobení) = změna jednotky (bit/Byte apod.)
* Možnost vytvoření vlastní hodnoty, která se vypočítá z jiných nasbíraných hodnot (např. Total Bytes - Free bytes = Used bytes)
* Možnost mapování sledovaných hodnot na textové výrazy (1=on, 2=off, 0=unknown)

**Notifikace** (Možnost posílat notifikace na min.):

* e-mail
* SMS
* MS Team
* Discord
* Telegram
* Možnost definovat vlastní strukturu textu notifikací
* Možnost posílat notifikace při problému a po vyřešení
* Možnost posílat notifikace jen pro vážnější alerty
* Možnost eskalace notifikací (pokud není opraveno do 1h, notifikace se odešle znovu a přidají se další adresáti)
* Možnost provozovat TV/monitor s dashboadem se zvukovými notifikacemi
* Možnost vytvoření návazností mezi alerty (v případě výpadku switche nebude systém hlásit nedostupnost zařízení do něj připojených)

**Uživatelské rozhraní**

* Možnost vytvářet skupiny uživatelů s různými oprávněními k různým zařízením
* Možnost napojení rozhraní na LDAP a SAML
* Jazyk rozhraní je v češtině, slovenštině a angličtině
* Každý uživatel si může vytvořit vlastní dashboard a zvolit vlastní jazyk rozhraní
* Rozhraní umožní uživatelům komentovat alerty, např. informovat, že na odstranění problému se už pracuje
* Rozhraní umožní volbu vlastního časového intervalu pro zobrazení hodnot v grafu
* Rozhraní umožní zobrazení více sledovaných hodnot v jednom grafu (možnost korelovat data)
* V grafech musí být pro lepší orientaci zvýrazněna pracovní a mimopracovní doba

**Další požadavky**

* Systém musí umožňovat automatické skenování sítě, nově objevená zařízení budou automaticky přidána ke sledování nebo bude správci odeslán e-mail s upozorněním na nové zařízení v sítí
* Systém musí umožnovat výpočet SLA pro jednotlivé sledované služby s možnosti vygenerování měsíčního/ročního reportu
* Systém musí umožňovat automatické vytváření inventáře zařízení ze sledovaných hodnot (Jméno, SN, MAC, OS apod.)
* Systém musí umožňovat uvedení skupiny zařízení do módu údržby a předejít tak posílání notifikací při údržbě zařízení
* Systém musí umožňovat vytváření vlastních „map“, kde mapy mohou ukazovat umístění porouchaného zařízení v rámci půdorysu budovy nebo v rámci racku v serverovně
* Systém musí umožňovat nahlížení do historie problému i několik měsíců zpětně
* Servisní podpora na 36 měsíců garantovaná přímo výrobcem
1. **LOG management**
* HW appliance (montáž do běžného 19‘‘ datového rozvaděče, výška max. 1U) pro zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
* Redundantní zdroje a ventilátory. Ventilátory za provozu vyměnitelné.
* 1x CPU min. 16 jader s podporou HyperThreadingu nebo Multi-Threadingu.
* Operační paměť RAM 64GB DDR-4
* 4x 1GbE RJ45 síťové rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.
* Průměrný trvalý příjem událostí/s. (průměrná délka zprávy min. 700Byte) 2000 událostí/s
* Špičkový příjem bez ztráty dat po dobu nejméně 10 minut (průměrná délka zprávy min. 700 Byte) 4000 událostí/s
* Čistá velikost integrované databáze 12 TB
* Jedna webová console pro všechny administrátorské i operátorské činnosti
* Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den.
* Příjem a zpracování logů, události a další strojově generovaná data prostřednictvím protokolů SYSLOG (RFC3164, RFC5424, RFC5425), RELP
* Bezagentový sběr událostí, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů
* Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů.
* Windows agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému tzn., že musí být centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker.
* Windows agent musí podporovat centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému.
* Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.
* Windows agent musí podporovat sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem.
* Windows agent musí ke všem odesílaným událostem automaticky doplňovat jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K významným bezpečnostním událostem musí doplňovat značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytvářet SHA256 hash.
* Počet instalací Windows agenta nesmí být licenčně a časově omezen. Pokud je Windows agent licenčně nebo časově omezen, požadujeme dodání licencí na Windows agenty v množství 450 na dobu předpokládané morální životnosti produktu – 7 let.
* Výrobcem vytvářené parsery pro běžné systémy.
* Uživatelsky definované parsery - systém umožňuje dopsání parserů pro další zdroje log zařízení uživatelem pomocí tzv. vizuální programování, bez nutnosti spolupráce s výrobcem.
* Standardizace přijatých logů do jednotného formátu a jejich normalizace (rozdělení) do příslušných polí dle jejich typu. Vytvoření vlastního důvěryhodného časového razítka ke každému logu.
* Uchování originální verze přijatých logů/zpráv včetně původní časové značky události.
* Okamžitá a automatická indexace umožňující okamžité prohledávání událostí.
* Podporované formáty RAW, Syslog (RFC5424), CEF, LEEF, JSON (RFC8259)
* Systém nesmí umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. (ani libovolnou konfigurační změnou)
* Automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy
* Nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty
* Ověřování uživatele na externím LDAP serveru resp. ověření lokálního účtu v případě výpadku LDAP.
* Grafické rozhraní musí umožňovat filtraci nerelevantních událostí, snadné vyhledávání událostí, vytváření reportů a dynamickou vizualizaci událostí.
* Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů
* Uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování
* Podpora základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.
* Výrobcem předpřipravené sety/vzory alertů a korelací.
* Monitoring stavu systému - alertování při překročení prahových hodnot SMTP nebo Syslog
* REST-API pro integraci s externím monitorovacím systémem Zabbix, Nagios, MRTG
* Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba
* Dedikované síťové rozhraní pro management HW 1x 1GE RJ45
* Uživatelské role definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému
* Aktualizace systému přes centrální webovou správcovskou konzoli v jednom balíku.
* Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.
* Podpora komprese ukládaných dat
* Podpora důvěryhodného zálohování komprimovaných dat na externí systém.
* Servisní podpora na HW s opravou v místě instalace serveru, s garantovanou NBD od nahlášení závady 36 měsíců
* Servisní podpora na SW v rozsahu aktualizaci systému a parserů, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem 36 měsíců

**Požadavky na implementaci:**

* Montáž do racku
* Připojení do LAN infrastruktury
* Aktualizace FW a OS
* Napojení a sběr všech významných log zdrojů stávající a pořizované infrastruktury zadavatele – (firewally, LAN prvky, servery, OS, aplikace atd.)
* Nastavení reportingu
* Nastavení alertů
* Zaškolení obsluhy v rozsahu 0,5MD

**Ověření kontroly funkčnosti systému:**

* Pokud zadavatel vyzve uchazeče k poskytnutí funkčního vzorku (v identické konfiguraci s nabízeným systémem) pro účely testování a ověření požadovaných funkčních vlastností, je uchazeč povinen doručit testovací vzorky na místo plnění do 5 pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně následujících 10 pracovních dní poskytne bezplatnou součinnost s testováním.
* Zadavatel v rámci testovacího provozu na dodaném testovacím vzorku, vycházeje z dodané dokumentace k nabízenému systému, provede tyto práce a vytvoří záznam o jednotlivých činnostech a jejich výsledcích. Jedná se zejména tyto testy:
* Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému
* Zapojení pěti vybraných zdrojových systémů logů odesílajících logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele a otestování následujících vlastností:
* nastavení klasifikace zdrojů
* nastavení značek (tagů) pro vybrané zdrojové systémy
* filtrování událostí
* úprava normalizace existujícího zdroje v grafickém rozhraní nástroje
* vytvoření reportů a exportu logů a vybraných údajů z logů
* Konfiguraci pěti vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému
* Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému včetně centrální instalace a centrální konfigurace Microsoft Sysmon služby pro rozšíření hodnoty logů vytvářených zdrojovými systémy dle doporučené auditní politiky.
* Konfigurace kolektoru logů z jedné databáze z prostředí zadavatele v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran
* Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
* provedení zálohy konfigurace a dat na externí systém
* vytažení dvou libovolných disků za běhu systému
* nastavení systému do továrního nastavení
* obnovení konfigurace a všech dat z vytvořených záloh
* kontrola úplnosti obnovené konfigurace a dat ze záloh
* Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat
* Kontrola, jakým způsobem se nastavuje systém ve vysoké dostupnosti (vytvoření clusteru) v jednotném webovém rozhraní systému a úplnost dokumentace k možným havarijním scénářům
* Kontrola výkonu systému v běžné zátěži – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému, po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. Dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace
* Kontrola výkonu systému v krátkodobém přetížení – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající dvounásobku výkonu nabízeného systému po dobu 10 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím době přijetí logu systémem. Dále kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR, číslo a jméno ASN a geolokace.
* Součástí ověření funkčních vlastností může být i ověření požadované funkcionality a parametrů dodaného funkčního vzorku systému dle Technické specifikace tohoto zadání.
* Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele/uchazeče, který mu poskytne potřebnou součinnost, a to maximálně do 3 pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele. Po ukončení testování budou funkční vzorky uchazeči vráceny (uchazeč si vyzvedne vzorky na vlastní náklady v místě plnění).
* Ověřování bude zakončeno vyhotovením zápisu. V případě, že testovaný systém neprojde úspěšným ověřením funkčních vlastností, neuzavře zadavatel s takovým uchazečem smlouvu a vyzve k dodání testovacích vzorků uchazeče, který se v hodnocení nabídek umístil jako další v pořadí.
1. **DLP – Data Loss Prevention**

**Obecné požadavky na řešení**

* Podpora databázového serveru MS SQL 2016 a novějších.
* Podpora OS Windows Server 2019, 2022.
* Podpora 64-bit Windows 10, 11.
* Podpora macOS Monterey (12) a novějších.
* Podpora terminálového prostředí.
* Centrální přizpůsobitelná webová administrační konzole.
* Integrace s více doménami Microsoft Active Directory, včetně bezpečnostních skupin.
* Modifikovatelná práva přístupu k výsledkům a nastavení produktu, správa přístupových práv pro administraci.
* Pokročilá sebeobrana agenta se zvláštním skrýváním kritických procesů a složek pro uživatele a místního nebo doménového správce na koncovém zařízení.
* Ochrana před převzetím systému pro agenty (včetně uživatelských účtů a místních a doménových správců).
* Ochrana proti manipulaci: ochrana proti zastavení bezpečnostních procesů, v případě vyšších uživatelských práv bude řešení restartovat zastavené procesy nebo použít jiný způsob, jak udržet své procesy v chodu.
* Ochrana proti manipulaci: ochrana proti odinstalaci řešení bez výslovného povolení.
* Ochrana proti manipulaci: ochrana proti úpravám registru, systémových komponent a knihoven DLL.
* Ochrana proti manipulaci: ochrana proti změnám nastavení z koncového zařízení.
* Zachování funkčnosti i v offline režimu, tzn. při připojení mimo síť společnosti nebo bez internetového připojení.
* Možnost pracovat s historickými záznamy.
* Automatické generování e-mailových upozornění v případě incidentů, s možností konfigurace na základě úrovní citlivosti incidentu.
* Automatické generování přehledů(reportů) a zaslání emailem.

**Audit dat a uživatelů**

* Podrobné informace o práci s citlivými soubory, tj. kdo soubory otevřel, jaký software byl použit k práci s nimi, místo uložení, odeslání e-mailem, přenos na externí zařízení nebo cloudové úložiště včetně synchronizované složky na disku.
* Obecný audit operací se soubory – kopírování, přesun, nahrávání nebo stahování z webu, tisk, přenos přes FTP, včetně identifikace zdroje a cílových umístění (cesta, typ zařízení).
* Podrobné informace o době aktivního používání softwaru.
* Informace o aktivním čase stráveném na webových stránkách, včetně podrobných informací o URL a záhlaví webových stránek, bez ohledu na typ prohlížeče.
* V produktu vestavěná kategorizace desktopových aplikací.
* V produktu vestavěná kategorizace webových stránek.
* Granulární nastavení auditu na úrovni celé organizace, skupin, uživatelů a počítačů.
* Možnost exportovat reporty do formátu XLSX.

**Komunikační Audit**

* E-mail: SMTP, POP3, IMAP, včetně šifrování SSL. Řešení dokáže monitorovat e-mail bez ohledu na typ klientské aplikace.
* Rozšířená podpora desktopových e-mailových klientů pro Microsoft Outlook a macOS Mail.app, včetně podpory MAPI (Exchange protokol).
* Monitorování souborů nahraných jako přílohy do webových e-mailových klientů.
* Monitorování souborů odeslaných prostřednictvím nástrojů pro rychlé zprávy.

## Ochrana dat / DLP (Data Loss Prevention)

* Ochrana dat při používání a přenosu pro standardní situace, bez ohledu na software, protokol, včetně šifrovaných spojení.
* Definice kategorií citlivých dat, která umožňuje omezit pohyb a práci s daty – jaká média lze použít pro přenos, na které webové stránky lze nahrávat soubory, e-mailové adresy, na které lze data odesílat, a jaký software může s daty pracovat.
* Dynamická úprava politik na základě anomálního chování se soubory a klasifikovanými daty.
* Možnost různých opatření při datovém incidentu: blokování operace uživatele, odůvodnění operace uživatelem (přepsání s uvedením důvodu), upozornění uživatele nebo pouze tiché zaznamenání incidentu.
* "Schránka (clipboard) Prevent data with sensitive content from being copied via clipboard."
* "Schránka (clipboard) Prevent data with sensitive content from being captured or recorded via screen capture tools."
* Možnost spravovat nebo blokovat přenos souborů na nežádoucí cloudové disky.
* Možnost spravovat nebo blokovat přenos souborů do Git repozitářů.
* "Schránka (clipboard) Prevent data with sensitive content from being captured or recorded via screen capture tools."
* Dočasný privilegovaný přístup pro koncové uživatele, udělení DLP dočasné vyjímky administrátorem.
* Funkce „Shadow copy“, která umožňuje administrátorovi zobrazit soubory u kterých došlo k bezpečnostnímu incidentu. Tato funkce umožnuje přístup k souborům, které byly odeslány, i těm, které byly blokovány DLP řešením.
* Schopnost stáhnout aktuální soubor DLP incidentu, když kopie není k dispozici.
* Řešení ochrany dat je odolné vůči obcházení ochrany systémových souborů v případě použití odkazů na jiné složky, včetně odkazů a podobných technologií.

**Ochrana citlivých dat**

* Detekce citlivých dat v dokumentech na platformách Windows a macOS.
* Podrobný náhled detekovaných citlivých dat v souboru, včetně počtu výsledků a jednotlivých shodných výrazů a klasifikačních pravidel.
* Schopnost definovat citlivá data pomocí vestavěných slovníků a algoritmů.
* Schopnost definovat citlivá data pomocí vlastních klíčových slov a regulárních výrazů.
* Schopnost nastavit prahové hodnoty detekce pro eliminaci nízkých čísel potenciálních výskytů citlivých údajů.
* Schopnost chránit heslem chráněné ZIP archivy vytvořené z souborů s citlivým obsahem.
* Schopnost klasifikovat citlivá data podle kontextových podmínek, např. původ dat nebo umístění.
* "Schopnost klasifikovat kompatibilní typy souborů pomocí vložených metadat dokumentu."
* Detekce citlivých údajů pomocí OCR v typech obrazových souborů a skenovaných PDF dokumentech.
* OCR funkce je dostupná, i když se počítač odpojí od firemní sítě nebo je offline.
* Podpora OCR pro dvoujazyčné prostředí (např. citlivé dokumenty v angličtině nebo španělštině).
* Dynamická omezení uplatněná na soubory nebo aplikace, když je detekován citlivý obsah.
* Zabránění úniku dat s citlivým obsahem z koncového zařízení – spravovat nejběžnější datové kanály: e-mail, webové nahrávání, externí disky, sdílení souborů prostřednictvím aplikací pro instant messaging, synchronizace s cloudovými službami.
* Objevování dat v nečinnosti, která obsahují citlivé údaje – koncová zařízení uživatelů a sdílené síťové úložiště.

**Správa zařízení**

* Globální omezení pro připojené USB úložiště, připojení mobilních telefonů, paměťových karet, přenosy souborů přes Bluetooth, optické jednotky a firewire zařízení.
* Schopnost blokovat pouze přenosy souborů přes Bluetooth, při zachování používání periferních Bluetooth zařízení (např. sluchátek).
* Možnost vynucení režimu pouze pro čtení pro připojená USB a Firewire úložná zařízení.
* Omezení USB zařízení, které jsou podporovány na systému macOS.
* Auditní záznam připojených externích zařízení k systému.
* Data mohou být chráněna před kopírováním do připojených chytrých telefonů pomocí protokolu Multimedia Transfer Protocol (např. chytré telefony), přičemž tato zařízení zůstanou dostupná pro použití s necitlivými daty.

**Správa aplikací**

* Monitorování aplikací používaných v celé organizaci a schopnost spravovat, které aplikace mohou být použity a které ne. Správa může být prováděna podle přesné specifikace nebo pomocí kategorií aplikací.
* Monitorování a správa desktopových aplikace včetně Microsoft Store a Apple Store.
* Monitorování návštěv webových stránek v celé organizaci a schopnost spravovat, které webové stránky mohou být navštěvovány a které ne. Správa může být prováděna podle přesné specifikace nebo pomocí kategorií webových stránek.

**Integrace analytiky dat**

* Možnost integrace a zobrazení protokolů a reportovacích dat řešení v Power BI.

**SIEM integrace**

* Možnost odesílat protokoly a upozornění na incidenty do SIEM systémů.

**Integrace Microsoft 365**

* Monitorování nejběžnějších akcí uživatelů prováděných na cloudových službách Microsoft 365 (OneDrive, SharePoint Online) – základní operace se soubory v cloudu, stahování a sdílení.
* Monitorování odeslaných e-mailů Microsoft 365 (Exchange Online) pro všechny uživatele, včetně uživatelů pracujících z Outlook Web App, BYOD nebo mobilních zařízení.
* Detekce porušení politiky Microsoft 365 při sdílení na SharePoint/OneDrive a e-mailové komunikaci v Exchange Online.
* Automatické nebo ruční odstranění sdílení na SharePoint/OneDrive při porušení politiky dat.
* Upozornění nebo blokování odesílání e-mailů z nové desktopové aplikace Outlook a webové verze Outlooku při porušení politiky dat.

**Integrace klasifikace dat**

* Schopnost integrace s třetími stranami pro klasifikaci dat uložených v metadatech dokumentu – schopnost rozpoznat tato data a uplatnit konfigurovatelné politiky DLP na ně.
* Schopnost integrace s Azure Information Protection, včetně šifrovaných dokumentů AIP.
1. **Instalace a konfigurace**
* Rozbalení veškerého dodaného HW, kontrola bezvadného stavu, likvidace přepravního a obalového materiálu a spolupráce s dodavatelem na evidenci HW (případné opatření evidenčními štítky);
* Instalace a zprovoznění veškerého dodaného HW do stávajících 19“ rozvaděčů a provedení funkčních testů;
* Instalace a zprovoznění veškerého dodaného SW na nově dodaný HW;
* Implementace zálohovacího SW v souladu s metodikou výrobce na odolnost diskových úložišť záloh před útoky ransomware;
* Nastavení LAN komponent tak, aby odpovídalo po konceptuální stránce stávajícímu schématu, tedy byly schopny rozšířit, popř. převzít funkci původní infrastruktury, tj. tak, aby nastavení firewallu odpovídalo aktuálnímu stavu a switche byly zapojeny v patřičné topologii tak, aby umožňovaly serverům komunikaci nutnou k následující fázi konfigurace a zprovoznění nového produkčního prostředí;
* Zavedení veškerého dodaného HW do monitoringu dodavatele i objednatele;
* Instalace veškerého dodaného SW a jeho zavedení do monitoringu objednatele;
* Provedení výkonových testů pole
* Nastavení monitoringu zálohování na úroveň jednotlivých HW a SW složek zálohovacího řešení, zálohovacích úloh a jejich průběhu;
* V případě pochybností o výkonnostních parametrech dodaného řešení diskových polí může objednatel pro akceptaci této fáze požadovat výkonnostní test.
* Konfigurací a zprovozněním nového produkčního prostředí se rozumí především výstavba virtualizační platformy v obou lokalitách datového centra se samostatně funkčním managementem a síťovými službami se zprovozněním současných produkčních virtuálních serverů Jedná se zejména o následující úkony:
* Úprava konfigurace datového centra tak, aby stávající produkční prostředí a služby jím poskytované byly provozovány, monitorovány, zálohovány a zabezpečeny na nově dodaném HW a SW;
* Instalace prostředí MS Windows dle dodaných licencí pro servery v primární i sekundární lokalitě;
* Nastavení virtualizace tak, aby užívala primární a sekundární diskové pole včetně synchronní replikace dat mezi lokalitami;
* Plné zanesení virtualizace do monitoringu objednatele;
* Provedení testu výkonu spojení mezi jednotlivými komponentami a disaster recovery při zátěži pro vyloučení SPOF;
* Integrace zálohování s virtualizační konzolí;
* Požadujeme instalaci základního zálohovacího SW (řízení, správa)
* Požadujeme instalaci všech potřebných serverů pro transport dat (data moover, media server, proxy server)
* Pokud má backup SW oddělené GUI klienty pro správu, požadujeme ukázkovou instalaci takové admin konzole na OS Linux
* Pokud má backup SW oddělené zálohovací klienty pro zálohování daných OS, požadujeme ukázkovou instalaci na vybraných OS (Windows, Linux)
* Požadujeme backup SW integraci s administračními nástroji pro virtualizované prostředí MS Windows a VMware
* Požadujeme backup SW integraci s funkcí snapshotů s nabízeným diskovým polem
* Požadujeme zviditelnění a nakonfigurování všech uvažovaných cílů záloh (VTL zařízení, D2D zařízení)
* Požadujeme konfiguraci všech rozhraní (LAN/SAN) na všech serverech sloužících pro transport zálohovaných dat (data moover, proxy servery, media servery, storage servery)s optimalizací na a) HA (vysokou dostupnost) b) propustnost (agregace více linek)
* Na všech komponentách zálohovacího eko-systému implementovat administraci a přístupy s ohledem na RBAC (Role Based Access Control) včetně napojení na centrální AD/LDAP.
* Požadujeme vytvoření automatizovaného reportovacího systému, který bude informovat o nedokončených zálohovacích úlohách
* požadujeme ukázku monitoringu:
* stavy-statusy jednotlivých komponent (řídící serever, data moover, cíl záloh)
* stavy-statusy úloh, statistiky úloh
* kapacity, využité a volné kapacity v jednotlivých cílech záloh
* Požadujeme dodání elektronické dokumentace (pdf) ke všem použitým SW komponentám (user guide, admin guide, config guide atp.)
* Požadujeme vytvoření a předání dokumentace o konkrétním provedení a nastavení celého zálohovacího prostředí. (otevřený editovatelný formát ODF např. \*.odt nebo MS Office formát např. \*.docx)
* Požadujeme zajištění instalace prostředí MS Windows dle dodaných licencí pro servery v primární i sekundární lokalitě, integraci na primární a sekundární diskové pole včetně synchronní replikace dat mezi lokalitami
* Požadujeme logickou migraci stávajícího prostředí MS Windows do nového prostředí založeného na MS Windows nezbytnou pro konfiguraci nového produkčního prostředí
* Požadujeme fyzickou migraci a konsolidaci dat fyzických serverů a jejich logickou migraci nezbytnou pro konfiguraci nového produkčního prostředí
* Zanesení dokumentace prostředí do Redmine objednatele, popř. předání formou dokumentů ve formátech odt, docx či pdf;
* Dokumentace jednotlivých HW a SW komponent musí mít část věnující se instalaci, konfiguraci, běžné administraci a užívání.
1. **Zaškolení obsluhy – soubor**
* Zaškolení 1 zaměstnance zadavatele v obsluze a údržbě zařízení v rozsahu 8 pracovních hodin na dodaném zařízení v místě plnění (s min rozsahem 4 pracovních hodin na zařízení LOG management).

**V následující tabulce účastník zadávacího řízení vyplní, zda a jakým způsobem splnil požadavky zadavatele:**

1. Zadavatel požaduje, aby dodavatelem nabízené HW zařízení, případně SW aplikace, splňovaly **veškeré** výše uvedené minimální požadavky (funkcionality a parametry) a tyto byly zahrnuty v jeho nabídce a v celkové ceně.
2. Dodavatel **jednoznačně deklaruje** splnění, popřípadě absenci každého minimálního požadavku ve výše uvedených tabulkách, a to vyplněním příslušného pole „Splněno“ jednou ze dvou nabízených možností:
* **ANO** - v případě, že dodavatelem nabízené plnění minimální požadavek splňuje,

nebo

* **NE** - v případě, že dodavatelem nabízené plnění minimální požadavek nesplňuje.

Tabulky s vyplněním polí „Splněno“ budou nedílnou součástí nabídky. V případě **nevyplnění** požadovaných údajů zadavatel **vyloučí** dodavatele z účasti v zadávacím řízení.

1. V případě, že dodavatel v příslušné položce pole neoznačí nebo v položce budou označeny obě možnosti dle bodu 2., bude taková položka posuzována jako neoznačená a bude znamenat vyloučení dodavatele z důvodu nesplnění zadavatelem požadovaného minimálního plnění.
2. V případě, že dodavatel v příslušné položce pole označí **NE**, bude taková položka posuzována jako nesplnění minimálních požadavků zadavatele a bude znamenat vyloučení dodavatele z důvodu nesplnění zadavatelem požadovaného minimálního plnění.
3. Dodavatel do sloupce „Popis řešení“ uvede, zda jím dodané HW zařízení, případně SW aplikace, splňuje jednotlivé požadavky zadavatele a **výstižně** (minimálně uvedením názvu výrobce a obchodního či typového označení nabízeného řešení) doplní, jakým způsobem je požadovaná funkčnost splněna.

| **Č.** | **Kritérium** | **Splněno** | **Popis řešení** |
| --- | --- | --- | --- |
| 1. | Host server | ANO / NE | …………………….……… |
| 2. | Zálohovací pásková knihovna | ANO / NE | …………………….……… |
| 3. | Firewall | ANO / NE | …………………….……… |
| 4. | Zálohovací systém | ANO / NE | …………………….……… |
| 5. | Bezpečnostní software | ANO / NE | …………………….……… |
| 6. | NAC - Network Access Control | ANO / NE | …………………….……… |
| 7. | NDR - Network Detection and Response | ANO / NE | …………………….……… |
| 8. | Monitoring IT Infrastruktury | ANO / NE | …………………….……… |
| 9. | LOG Management | ANO / NE | …………………….……… |
| 10. | DLP – Data Loss Prevention | ANO / NE | …………………….……… |
| 11. | Instalace a implementace | ANO / NE | …………………….……… |
| 12. | Zaškolení obsluhy | ANO / NE | …………………….……… |

**Prohlašuji**, že veškeré shora uvedené údaje (parametry) jsou úplné, pravdivé a odpovídají skutečnosti. Jsem si vědom/a právních následků v případě uvedení nesprávných nebo nepravdivých údajů (parametrů).

V **………………………..………,** dne **………….……**

**Osoba oprávněná jednat jménem/za účastníka:**

Titul, jméno, příjmení: **………………………………….…**

Funkce: **………………………………….…**