**Specifikace předmětu VZ**

Předmětem plnění této zakázky je dodávka a upgrade licencí pro endpoint zabezpečení s podporou na 36 měsíců, instalace a konfigurace software endpoint protection zabezpečení rozšířené o funkce EDR ochrany koncových Windows/Mac/Linux stanic a Windows/Linux serverů, zabezpečení poštovních schránek v prostředí MS 365, výkonově optimalizovaného řešení pro zabezpečení virtuálních serverů v prostředí VMware/Hyper-V a licence pro zabezpečení a správu mobilních zařízení s Android/iOS, v dále uvedené konfiguraci:

* **Upgrade na Kaspersky EDR Optimum (310 lic., podpora na 3 roky)**
* **Prodloužení Kaspersky Endpoint Security SELECT (40 lic., podpora na 3 roky)**
* **Prodloužení Kaspersky Hybrid Cloud Security (30 lic., podpora na 3 roky)**
* **Nová licence Kaspersky Security for Microsoft Office 365 (450 lic., podpora na 3 roky)**

K výše uvedenému software Zadavatel dále vyžaduje technické zaškolení IT administrátorů a poskytování služeb lokální technické podpory v ČJ v režimu 5x8 po celou dobu platnosti zakoupené licence.

Uchazeč předloží nabídku na plně funkční a nakonfigurovaný systém ochrany zařízení Zadavatele (počítače, notebooky, mobilní telefony, servery, virtuální prostředí, MS 365 pošty) dle svých nejlepších znalostí a svědomí, splňující veškeré minimální požadavky na technické parametry a funkce zabezpečení.

**Názvy produktů a popisy uvedené v této zadávací dokumentaci specifikují požadované plnění v případě výrobce aktuálně používaného řešení s tím, že Zadavatel připouští i jiná, avšak kvalitativně a technicky obdobná řešení za podmínky, že nedojde ke zhoršení technických parametrů kladených na požadované řešení a bude současně zachována kompatibilita se stávajícími zařízeními a infrastrukturou Zadavatele.**

1. **Obecné požadavky**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Nabízené Endpoint Protection řešení splňující dále požadovaná kritéria pro ochranu stanic, serverů, virtuálního prostředí, BYOD mobilních zařízení včetně MS 365 pošty (v případě MS 365 lze nabídnout SaaS od stejného výrobce jako je nabízené řešení) je vzájemně plně integrováno a je od stejného výrobce. |  |  |
| Nabízená technologie byla testována v nezávislých testech AV Comparatives, [www.av-comparatives.org](http://www.av-comparatives.org), kategorie Enterprise/Real-World Protection Test za rok 2023 |  |  |
| Plná lokalizace GUI rozhraní aplikace na koncových zařízeních typu PC, notebook nebo BYOD mobilní zařízení v češtině. |  |  |
| Bezpečnostní cloud infrastruktura výrobce nabízeného řešení využívaná pro detekci malware mimo prostředí klienta je na území EU nebo některého z přidružených států v Evropě. |  |  |

1. **Pokročilá endpoint ochrana pracovních stanic a serverů rozšířená o funkce EDR (XXX Windows/Linux/Mac desktop OS, XX Windows/Linux serverů)**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Podpora pro OS Windows 7 a výše, Windows Server 2008 a výše, Linux (CentOS, Debian, RedHat, Ubuntu, SUSE), Mac. |  |  |
| Rozhraní klientské části endpoint protection je plně lokalizováno do ČJ |  |  |
| APT ochrana (viry, červy, trojské koně, backdoors, spyware, adware, ransomware, keyloggery, crimeware, phishing, rootkit), skripty (PowerShell, WSH, Java, VB, …) vč. Zero Day útoků. |  |  |
| Ochrana před exploitací instalovaných aplikací a OS |  |  |
| Pokročilá detekce malware prostřednictvím technologií virových signatur, heuristiky, behaviorální analýzy a strojového učení (Machine Learning) |  |  |
| Detekce malwaru na bázi reputace a cloudové kontroly (lokální i globální služby výrobce) |  |  |
| Kontrola paměti a detekce Fileless Threats ve Windows. |  |  |
| Podpora MS AMSI Protection Provider. |  |  |
| Antiransomware - detekce pokusů o neoprávněné šifrování dat na úrovni Windows serverů. |  |  |
| Roll-back nechtěných změn v systému v reakci na detekované aktivity malware. |  |  |
| Automatická integrovaná cloud Sandbox ochrana od stejného výrobce jako je dodané řešení |  |  |
| Funkce EDR a rozšíření informací o zjištěných detekcích a další související systémové události jako je vizualizace incidentu formou grafického znázornění vývoje a realizace bezpečnostní hrozby (kill chain), informace o zařízení (IP, MAC, Users, OS, …), způsobu detekce, změnách v registru, stažených souborech, provedených reakcích, informace o procesech, síťových spojeních, atd. |  |  |
| Možnost generování IoC informací na základě zjištěných detekcí s možností spuštění IoC scanu na všechny endpointy a rychlé reakce na zjištěné detekce |  |  |
| Možnost doplnění vlastních IoC detekcí |  |  |
| Podpora rychlé reakce z centrální konzole na zjištěné incidenty a detekce např. blokování spuštění aplikace, izolace zařízení, smazání podezřelého souboru, ukončení procesu, odeslání do karantény, spuštění systémového scanu, provedení CMD příkazu, spuštění IoC scanu. |  |  |
| Možnost konfigurovat firewall pravidla ve Windows Server a Linux prostřednictvím centrální konzole nabízeného řešení |  |  |
| Manuální a plánované spouštění skenování, blokování skriptů, kontrola Windows registrů, Buffer overflow ochrana a skenování na pozadí |  |  |
| Self-Defense ochrana heslem před neoprávněnou deaktivací endpoint protection & EDR ochrany včetně blokování neoprávněné vzdálené správy |  |  |
| Kontrola archivů (ZIP, ARJ, CAB, RAR, LHA, JAR, ICE) |  |  |
| Pravidelná automatická aktualizace systému (v závislosti na síťovém prostředí se aktualizace stahují buď z centrálního uložiště, nebo přímo z Internetu). Lokální aktualizační servery (mirrory) si mohou vzájemně replikovat data. Pro externí pracovníky lze nastavit sekundární profil aktualizace z internetu. |  |  |
| Centrálně konfigurovaný personální firewall + Host Intrusion Prevention (HIPS). Pravidla firewallu lze automaticky měnit v závislosti na prostředí |  |  |
| Ochrana elektronické pošty na úrovni protokolů (POP3, IMAP) vč. plug-in pro MS Outlook |  |  |
| Inspekce síťového provozu HTTP(S) a FTP |  |  |
| Blokování uživatelských přístupů na webové stránky s nechtěným nebo škodlivým obsahem na základě URL, webové kategorie, uživatele a času přístupu |  |  |
| Kontrola URL vůči globální cloudové službě výrobce |  |  |
| Uživatelské bezpečnostní politiky zvlášť na zařízení, web a aplikace. |  |  |
| Application Control – možnost povolovat/blokovat spouštění vybraných aplikací dle nastavené firemní politiky (blacklisty/whitelisty) |  |  |
| Whitelist aplikací na základě digitálního certifikátu, HASH, souborového umístění nebo výrobcem předdefinovaných kategorií |  |  |
| Device Control - možnost blokovat vybraná USB a jiná přídavná zařízení na úrovni sběrnice s možností whitelist zařízení a řízení oprávnění (read/write) |  |  |
| Automatická kategorizace připojovaných USB zařízení dle jejich typu, možnost blokace upravených USB zařízení emulujících standardní klávesnici |  |  |
| Automatická kontrola výměnných zařízení a blokace spuštění spustitelných souborů |  |  |
| Možnost skenování stanice na vyžádání, možnost definovat vytížení koncového bodu a vynechat již dříve zkontrolované a nezměněné objekty |  |  |
| Umožňuje uložit protokoly o činnostech v běžných formátech (CSV, text, Windows event log) |  |  |
| Vlastní šifrování celého disku vč. OS (Full Disk Encryption), výměnných paměťových úložišť a/nebo správa nativního šifrování ve Windows MS BitLocker a v MacOS FileVault. |  |  |
| Data Recovery šifrovaných zařízení v případě havárie včetně centrální správy šifrovacích klíčů |  |  |
| Podpora multifaktorové autentizace v preboot režimu u šifrovaných zařízení |  |  |
| Patch Management - přehled zranitelností u min. 100+ aplikací, včetně možnosti automatické instalace příslušných oprav a aktualizací s podporou jejich agregace |  |  |
| Možnost instalace pouze administrátorem schválených aktualizací s možností využít testovací režim na nastavitelném vzorku zařízení |  |  |
| EDR agent je integrální součást endpoint protection klienta |  |  |
| EDR agent podporuje ovládání prostřednictvím CMD rozhraní |  |  |
| Funkčnost systému ochrany bez nutnosti připojení k centrální správě či internetu, přičemž nedochází k významné degradaci detekčních schopností endpoint protection zabezpečení |  |  |

1. **Ochrana a správa mobilních zařízení typu SmartPhone/tablet (XX mobilních zařízení s Android/iOS)**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Podpora pro OS Android a iOS |  |  |
| Podpora cloud centrální správy a nasazení |  |  |
| Antimalware ochrana Android zařízení na úrovni souborů a síťové komunikace (virové signatury, heuristika, cloud reputace, strojové učení) |  |  |
| Detekce root/jailbreak zařízení |  |  |
| SMS/MMS AntiSpam a filtr nevyžádaných hovorů |  |  |
| Anti-Theft funkce (vzdálené uzamčení, smazání, SIM kontrola, foto a GPS lokace) |  |  |
| Zabezpečení on-line komunikace (firewall) |  |  |
| Správa přístupu uživatelů na web umožňující blokovat škodlivé nebo nevhodné webové stránky také na základě jejich kategorií |  |  |
| Ochrana uživatelů před phishingovými weby, které hrozí krádeží informací a identifikačních údajů |  |  |
| Konfigurace správy aplikací umožňující určit, které aplikace bude možné spouštět |  |  |
| Správa zařízení - povolení/blokování použití paměťových karet, kamery, WiFi, Bluetooth, IR, … |  |  |
| Příprava zařízení, centrální nastavení politik |  |  |

1. **Optimalizovaná ochrana pro virtuální prostředí (XX virtuálních serverů VMware/Hyper-V)**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Optimalizované skenování ve virtuálních prostředí VMware, Hyper-V, Citrix |  |  |
| Antimalware kontrola za využití virových signatur, heuristiky, strojového učení a behaviorální analýzy |  |  |
| Zabezpečení pomocí napojení na cloud reputační službu výrobce a ochrana před exploitací instalovaných aplikací |  |  |
| Kontrola poštovní (IMAP, SMTP, POP3, NNTP) a síťové komunikace HTTP(S) a FTP(S) |  |  |
| Podpora MS AMSI Protection Provider |  |  |
| Kontrola integrity systémových souborů, logů a kritických aplikací |  |  |
| Přenesení skenovacích úloh a tím i zatížení na samostatnou virtuální appliance a eliminace opakovaného skenování nezměněných objektů |  |  |
| Application Control – možnost omezit oprávnění běžících aplikací na základě jejich reputace |  |  |
| Roll-back nechtěných změn v systému v reakci na detekované aktivity malware. |  |  |
| Vestavěný firewall a Host Intrusion Prevention (HIPS) |  |  |
| Device Control – správa připojování výměnných zařízení |  |  |
| Podpora integrace s EDR řešením od stejného výrobce |  |  |

1. **Zabezpečení pošty MS 365 (XXX mailových schránek, možnost SaaS od stejného výrobce)**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Plně cloudové nasazení s MS Exchange Online integrací nebo služba typu SaaS od stejného výrobce jako je nabízené řešení |  |  |
| Antimalware, antiphishing a antispam ochrana elektronické pošty |  |  |
| Podpora poštovních autentizačních metod SPF, DKIM a DMARC |  |  |
| Detekce Office souborů s makry a možnost blokace |  |  |
| Antimalware kontrola schránky na vyžádání |  |  |

1. **Centrální správa**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Konzole centrální správy v provedení cloud webové konzole |  |  |
| Společná konzole pro administraci a analýzu informací jak pro endpoint protection, tak i EDR |  |  |
| Podpora Windows Server 2008 R2 a výše, MS SQL Server 2014 (Express) a výše, MySQL 5.7 a výše |  |  |
| Možnost vzdálené instalace, odinstalace a konfigurace všech komponent na PC a serverech včetně mobilních zařízení typu SmartPhone a tablet |  |  |
| Deployment klientů na koncová zařízení pomocí RPC, GPO, síťový agent popř. standalone instalačního balíčku |  |  |
| Instalace endpoint aplikace na serverech bez nutnosti restartu |  |  |
| Zabezpečené spojení mezi serverem centrální správy a endpoint agenty včetně EDR |  |  |
| Podpora manuální/automatické instalace/odinstalace nekompatibilních aplikací (vč. současné ochrany Kaspersky) |  |  |
| Podpora Active Directory a IPv6 |  |  |
| Tvorba politik s jednotlivým nastavením komponent řešení a jejich aplikace na úrovni skupin. |  |  |
| Přidělování práv administrátorů na úrovni skupin nebo serverů s předdefinovanými security právy pro role auditor, supervisor a security officer. |  |  |
| Centrální správa a nastavení jednotlivých klientů na úrovni skupin nebo hierarchie |  |  |
| Správa zařízení na základě dynamických profilů a tagů (síť, OS, AD, virtualizace, aplikace). |  |  |
| Možnost stahování aktualizací z centrálního serveru nebo Internetu na základě kvality sítě |  |  |
| Možnost distribuovat události z vybrané skupiny PC prostřednictvím vybraného počítače v síti. |  |  |
| Podpora virtuálního prostředí (VMware, Hyper-V, Citrix) |  |  |
| Možnost prohlížení všech bezpečnostních událostí na spravovaných zařízeních v síti. |  |  |
| Notifikace pomocí e-mail, syslog, SIEM. |  |  |
| Možnost generovat a odesílat reporty e-mailem ve formátu .PDF nebo .CSV včetně možnosti jejich přizpůsobení. |  |  |

1. **Služby lokální technické podpory**

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splněno**  **(ANO / NE)** | **Poznámka**  **(jakým způsobem řešeno)** |
| Instalace a konfigurace SW v prostředí Zadavatele. Nastavení centrální správy (včetně pravidel a politik pro všechna zařízení, reporting, alerting, revize aktuálních výjimek) |  |  |
| Revize stávajícího nastavení a přenesení do nabízeného řešení |  |  |
| Nastavení optimalizovaného skenování s ohledem na nízké systémové zatížení ve virtuálním prostředí VMware / Hyper-V dle doporučení výrobce a dostupných funkcí dodaného řešení |  |  |
| Úvodní zaškolení obsluhy na správu a používání dodaného systému |  |  |
| Lokální technická podpora dodavatele nabízeného řešení v ČJ v rozsahu HOT LINE (e-mail/telefon) v pracovních dnech od 8:00 hod. – 16:00 hod. |  |  |