Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux.

Obsahem je:
dodání min. 450 kusů licencí pro zabezpečení koncových bodů

Řešení musí mít zajištěnu podporu výrobce v českém jazyce telefonicky i písemně. Podpora poskytovaná prostřednictvím telefonní linky musí být dostupná min. PO-PÁ od 9 do 17 hodin.
Garantovaný přístup do knowledge databáze.

Výrobce řešení musí mít sídlo v Evropské unii nebo v zemi, která je součástí společenství NATO.
ICT produkt nebo služba podstatná pro funkčnost spravovaného či provozovaného informačního systému není dodávána prostřednictvím pobočky dodavatele v Ruské federaci.
ICT produkt nebo služba podstatná pro funkčnost spravovaného či provozovaného informačního systému nemá svůj vývoj či výrobu lokalizované v Ruské federaci.
Dodavatel nemá sídlo v Ruské federaci nebo není závislý na dodávkách z území Ruské federace.

Konzole pro centrální správu řešení:

Základní vlastnosti

- Všechny funkcionality řešení musí být možné spravovat pomocí správcovské webové aplikace
- Řešení musí obsahovat správu dodanou výrobcem a umístěnou v cloudu výrobce, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí
- Řešení musí umožňovat kdykoli zmigrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení
- Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu
- Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem

Úlohy správy bezpečnosti

- Řešení musí umožnit integraci s více strukturami Microsoft Active Directory a VMware vCenter a importovat inventáře těchto struktur za účelem správy ochrany zařízení v těchto inventářích.
- Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery
- Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity
- Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy
- Možnost restartování serveru nebo desktopu přímo z konzole centrální správy
- Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)

Nastavení úrovně bezpečnosti

- Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD
- Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně dle sekcí a subsekcí nastavení bezpečnostních pravidel

Reportování

- Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě

- Možnost zasílání vygenerovaných reportů e-mailem
- Možnost stáhnout vygenerované reporty minimálně ve formátech .pdf či .csv
- Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen

Karanténa

- Vzdálená obnova či smazání souboru v karanténě
- Možnost nastavit tzn. centrální karanténu, pro dostupnost souborů v karanténě i v případě odpojení koncové stanice
- Možnost automaticky přidat soubor do výjimky při obnově z karantény

Uživatelé

- Více předdefinovaných rolí – Root (spravuje komponenty řešení), Administrátor (spravuje bezpečnostní pravidla a inventář koncových zařízení), Reportér (spravuje a vytváří reporty)
- Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)
- Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny
- Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení
- Možnost lokálních uživatelů a uživatelů synchronizovaných z Active Directory, možnost přihlašování uživatelů z AD, možnost přiřazení uživatelských rolí členům bezpečnostních skupin v AD

Správa a instalace ochrany

- Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány
- Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN
- Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů
- Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou
- Konzole správy obsahuje detailní informace o chráněných strojích: mimo jiné název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích
- Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti

Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux):

Základní vlastnosti

- Podpora operačních systémů
  - Windows 11, 10, 8, 7
  - Windows Server 2022, 2019, 2016, 2012 R2, 2012
  - Ubuntu 14.04 LTS a vyšší
  - Red Hat Enterprise Linux
  - CentOS 6.0 a vyšší
  - SUSE Linux Enterprise Server 11 SP4 a vyšší
  - OpenSUSELeap 42.x
  - Fedora 25 a vyšší
  - Debian 8.0 a vyšší
  - Oracle Linux 6.3 a vyšší
  - Amazon Linux AMI 2016.09 a vyšší
  - Mac OS X El Capitan (10.11) a vyšší včetně MAC s procesory M1
- Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
- Aktualizace bezpečnostního obsahu alespoň jednou za hodinu

- Detekce na základě virových definicí (tzn. signatur)
- Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
- Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
- Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
- Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
- Detekce O-day útoků na základě odhalování anomálního chování
- Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
- Detekce 0-day bezsouborových útoků
- Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
- Ochrana souborů proti zašifrování Ransomware spuštěném na chráněné stanici – automatické ukončení procesu ransomware a obnovení zašifrovaných souborů do původního stavu
- Ochrana sdílených složek/souborů proti zašifrování Ransomwarem spuštěném na jiné stanici s přístupem k těmto sdíleným složkám/souborům – automatické ukončení spojení z nakažené stanice a obnovení zašifrovaných souborů do původního stavu
- Možnost automatické detonace podezřelých souborů v Sandboxu
- Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne
- Možnost ručního vložení vzorku do Sandboxu
- Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
- Možnost skenování poštovního provozu přímo na poštovním serveru (scenovací motor)
- Řešení musí obsahovat funkce EDR/XDR integrované do jedné klientské aplikace spolu s EPP
- Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
- Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
- Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
- Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
- Řešení umožňuje analýzu vektoru útoku
- Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování, kontrola https komunikace
- Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3, IMAP, MAPI)
- Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
- Ochrana proti podvodným a phishingovým webovým stránkám
- Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
- Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
- Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na různých webech, používání stejného hesla v interních a externích aplikacích, apod.)

Patch management

- Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
- Možnost hromadně vyhledávat, stahovat a vzdáleně instalovat záplaty (patche) na OS i na další aplikace třetích stran např. Windows, Apple, Adobe, Cisco, Mozilla, Opera, VMware a dalších.
- Možnost managovat instalace jednotlivých patchů na konkrétní stroje.
- Řešení musí umožňovat přehled dostupných CVE včetně podrobných informací o něm.
- Možnost volby instalace formou Slow/Fast ring.

Šifrování

- Možnost centrálně spravovat klíče pro šifrování disku na cca 90 NTB/PC bez nutnosti instalace dalšího agenta/serveru.
- Podpora systémů Windows (BitLocker) a Mac (FileVault)

Firewall

- Možnost blokovat skenování portů
- Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS
- Firewall obsahuje systém IDS včetně funkce odhalování neznámých hrozeb
- Možnost vypnout IDS
- Možnost nastavit profily známých sítí
- Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu

Karanténa

- Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě
- Možnost obnovy souboru do originální či do nově zadané lokality
- Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní)

Kontrola přístupu k internetu

- Zablokování přístupu na internet pro specifické stanice / skupiny stanic
- Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic
- Zablokování přístupu k internetu v určený čas
- Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (např. násilí, hazard a jiné)
- Zamezení přístupu ke konkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)

Ochrana virtualizovaných koncových bodů (Windows, Linux)

Základní vlastnosti

- Produkt podporuje tzv. bezenginové skenování – režim, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale není nutné aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen
- „Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením
- „Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže
- Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení

- Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace)
- Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (LAN, WAN, sdílené úložiště, přenosná média, pevný disk...)
- Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů
- Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru
- Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
- Detekce na základě virových definicí (tzn. signatur)
- Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
- Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
- Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
- Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
- Detekce 0-day útoků na základě odhalování anomálního chování
- Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
- Detekce 0-day bez souborových útoků
- Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
- Ochrana souborů proti zašifrování Ransomware spuštěném na chráněné stanici – automatické ukončení procesu ransomware a obnovení zašifrovaných souborů do původního stavu
- Ochrana sdílených složek/souborů proti zašifrování Ransomwarem spuštěném na jiné stanici s přístupem k těmto sdíleným složkám/souborům – automatické ukončení spojení z nakažené stanice a obnovení zašifrovaných souborů do původního stavu
- Možnost automatické detonace podezřelých souborů v Sandboxu
- Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne
- Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
- Možnost ručního vložení vzorku do Sandboxu
- Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení
- Řešení musí obsahovat funkce EDR/XDR integrované do jedné klientské aplikace spolu s EPP
- Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy
- Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
- Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
- Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
- Řešení umožňuje analýzu vektoru útoku
- Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
- Možnost prověřovat http provoz
- Možnost prověřovat provoz šifrovaný pomocí SSL
- Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3)

- Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
- Ochrana proti podvodným a phishingovým webovým stránkám
- Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
- Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
- Řešení musí umožňovat připojení na konzoli koncové stanice s možností výpisu procesů, registrů a souborů, vytvoření, změnu či výmaz souborů či registrů a ukončení procesu

Implementace systému musí zahrnovat

- Konzultace a návrh konkrétní implementace (Příprava na implementaci, dodání dokumentací a nutných technologických požadavků pro správný návrh a funkčnost řešení)
- Zprovoznění cloudové konzole a dalších komponent potřebných pro správný chod (včetně nastavení dle domluveného zadání vydefinovaného v bodě 1)
- Vzorová instalace na cca 10% koncových bodů (40 ks PC a 15 ks serverů včetně Linux), testovací provoz s plnou podporou dodavatele po dobu 20-ti dnů
- Nastavení vzorové bezpečnostní politiky (Nastavení dle doporučení výrobce, nastavení dle potřeb zákazníka, včetně konzultací a doporučení)
- Základní zaškolení administrátorů v rozsahu 2 pracovních dnů
- Předání kompletní dokumentace nastavená systémů (servery, stanice , EDR, karanténa,..)