Příloha č. 1

Technické požadavky na antivirový SW

Základní funkce AV:

- Antivirus
- Antispyware
- Umožní odinstalovat konkurenční bezpečnostní software
- Ochrana poštovních klientů
- Cloud technologie (white listing na základě reputace)
- Možnost kontroly výměnných médií (kontrola po připojení, nebo volba na uživateli)
- Možnost definovat pravidla pro systémové registry, procesy, a plikace a soubory
- Multiplatformní ochrana (Windows 10 - 11, Linux, Mac)
- Tvorba pravidel pro konkrétní USB a klienty
- Whitelist / Blacklist na konkrétní www stránky
- Prezentační režim (blokuje nevyžádaná upozornění a zprávy při fullscreen aplikacích)
- Detekce důvěryhodné zóny
- Roamingový provoz (při mobilním připojení notebooku se nestahují velké aktualizace)
- šetřící režim při provozu na mobilních zařízeních
- Modulární instalace
- Ochrana proti Botnetu
- Podpora virtualizace
- Podpora Windows File Serveru
- Podpora Windows Server 2012 a vyšší
- Správa zařízení pro Windows, macOS a Linux umožňující blokaci médií s podporou whitelistování na základě definování: výrobce, modelu nebo sériového čísla, uživatelů nebo skupin (např. administrátorů) v AD
- Provádění kontrol při nečinnosti zařízení: vypnuté obrazovce, aktivním spořiči obrazovky, uzamčení počítače, odhlášení uživatele.

Centrální správa:

- Podporované systémy Windows, Linux.
- Profily přístupů (víceúrovňová práva správců pro jednotlivé organizace)
- Šablon reportů pro různé události s možností nastavení hraniční hodnoty pro odeslání upozornění
- Vzdálená instalace na více koncových bodů současně
- Vzdálená instalace / odinstalace konkrétních .msi balíčků
- Export / Import politik v xml souboru
- Vzdálená správa modulů
- Možnost správy vzdálené podsítě z jedné konzoly vzdálené správy
- Webový dashboard
- Protokoly v různých formátech (CSV, text, Win event. protokol – čitelné pomocí SIEM)
- Komplexní protokoly a zprávy o kontrole výměnných zařízení
- Náhodné spuštění úloh (spouštění naplánovaných úlohy v náhodných intervalech z důvodu snížení zatížení sítě)
- Rollback aktualizací
- Odložené aktualizace – až o 12 hodin (možnost použít více aktualizačních serverů)
- Lokální aktualizační server s podporou protokolu HTTPS)
- Možnost udělat mirror aktualizací na klientovi
- Možnost definovat parametry interní MDB databáze, tak aby nedocházelo ke zbytečnému ukládání dat
- Podpora Microsoft NAP
- Kompletní správa karantény na klientských počítačích
- Synchronizace s Active Directory adresářem
- Automatické zasílání reportů administrátorům

- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
- Možnost navazování úloh pro zautomatizování činností bez zásahu administrátora. Například: Automatická detekce antiviru 3. strany > automatická odinstalace > automatický zpožděný restart pro možnost uložení rozdělané práce klienta > automatická instalace nového bezpečnostního programu > automatická aktivace nového bezpečnostního programu.

Technická podpora

- Implementační podpora v rozsahu 1MD
- Zaškolení administrátorů organizací presenčně nebo pomocí online školení
- Provozní technická podpora v Českém jazyce v pracovní dny od 8 do 17hod na tel, email a webový formulář
- Možnost vzdáleného připojení
- Roční reporty o počtu licencí