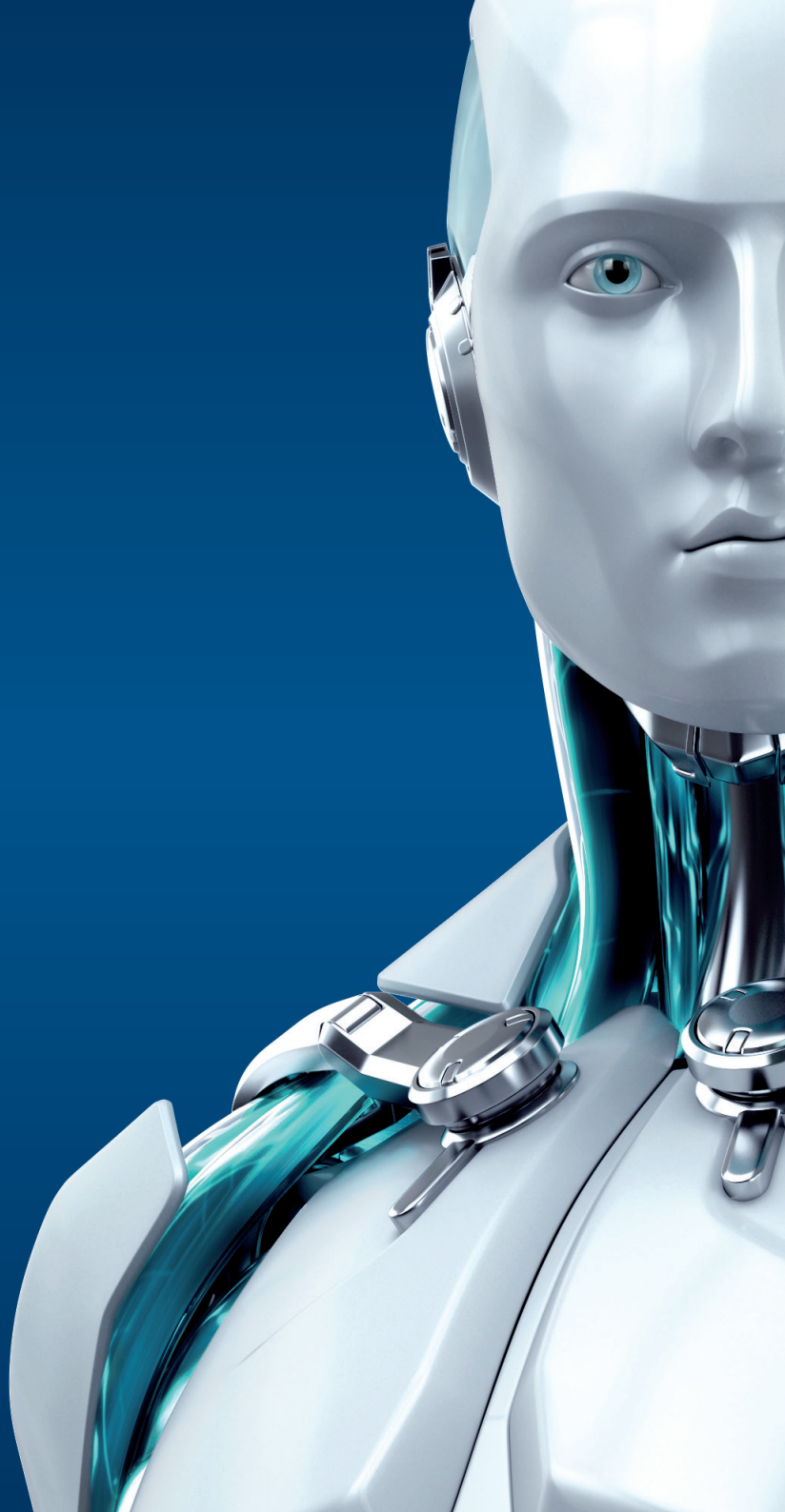
MAIL SECURITY

PRO MICROSOFT EXCHANGE SERVER

ENJOY SAFER TECHNOLOGY™



MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER

ESET Mail Security pro Microsoft Exchange Server integruje rychlou antivirovou a antispamovou ochranu, která filtruje příchozí poštu již na úrovni serveru. Díky nízké systémové zátěži může systém pracovat s maximální efektivitou.

S tímto řešením získáte kompletní ochranu serveru, včetně ochrany serverových souborů. Můžete aplikovat politiky pro filtrování obsahu dle typu souboru a zároveň monitorovat bezpečnostní situaci pomocí nástroje vzdálené správy ESET Remote Administrator.

Anti-malware a Antispam ochrana

Antivirus a Antispyware	Odstraňuje všechny typy hrozeb, včetně virů, rootkitů, červů a spyware. **Volitelná cloud kontrola souborů:** Pro lepší a rychlejší kontrolu souborů je možné využít whitelisting - porovnání s cloudovou databází souborů, kam se umisťují soubory na základě reputace. Do cloudu se odesílá pouze informace o spustitelných souborech a archivech.
Antispam a Anti-Phishing	Blokuje nevyžádanou poštu a phishing pokusy s vysokou úspěšností bez potřeby manuálně upravovat SCL (Spam Confidence Lecel) hodnoty. Po instalaci je antispam plně funkční a není potřeba větší konfigurace.
Správa lokální karantény	Každý uživatel poštovní schrány může pracovat, pomocí samostatného prohlížeče, se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do poštovní schránky. V závislosti na povolených právech může uživatel třídit/ prohledávat zprávy v karanténě a provádět povolené akce. Dostupné akce se liší v závislosti na důvodu uložení do karantény. Uživateli je také možné poslat pravidelný report se seznamem zpráv zařazených do karantény.
Volitelná kontrola databáze	Administrátor může vybrat, jakou databázi nebo poštovní schránky chce zkontrolovat. Kontroly je možné dále upřesnit, tak aby docházelo k co nejmenšímu využití systémových zdrojů.
Pravidla zpracování zpráv	Nabízejí široké možnosti kombinací, jak se mají zprávy zpracovat. Hodnotící parametry obsahují standardní volby jako jsou předmět, odesílatel, tělo a hlavička, ale umožňují zvolit u další podmínky v závislosti na předchozím antispam filtrování a výsledcích antivirové kontroly. Porušené nebo heslem chráněné archivy jsou detekovány a obsah příloh je kontrolován pro nalezení skutečného typu souboru. Pravidla je možné měnit, tak aby bylo dosaženo ideálního výsledku.
Exploit Blocker	Chrání často zneužívané aplikace, jako jsou internetové prohlížeče, čtečky PDF, poštovní klienti nebo MS Office. Sleduje chování procesů a hledá podezřelou aktivitu, která je pro exploity typická. Zajišťuje ochranu stanic před dosud neznámými hrozbami tzv. zero day útoky.
Pokročilá kontrola paměti	Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti. Takto je schopná detekovat i těžce šifrované hrozby.
HIPS (Host-Based Intrusion Prevention System)	Umožňuje definovat pravidla pro systémové registry, procesy, aplikace a soubory. Chrání soubory před neautorizovanou změnou a detekuje hrozby na základě chování systému.
Kontrola zařízení	Blokuje neautorizovaná přenosná zařízení při pokusu o připojení na server. Umožňuje vytvořit pravidla pro uživatelské skupiny v souladu s firemní politikou. Nabízí i „podmíněnou" variantu blokování, kdy je uživatel upozorněn, že zařízení bylo zablokováno, zapne se logování aktivity a uživatel může na zařízení přistoupit.

Pokrytí kompletní infrastruktury

Nezávislost na snapshotu	Aktualizace a programové moduly je možné ukládat mimo defaultní lokaci. Proto nejsou ovlivněny použitím uložených snapshotů virtuálních strojů. Výsledkem je, že se aktualizace a moduly nemusí stahovat znovu při každém vracení k předchozímu stavu systému.
Nativní podpora clusterů	Umožňuje nastavit řešení tak, aby docházelo k automatické replikaci nastavení při instalaci v prostředí clusterů. Jednoduchý průvodce propojí jednotlivá řešení v rámci jednoho clusteru, která lze potom spravovat jako celek bez nutnosti manuální konfigurace.
ESET Shared Local Cache	ESET Shared Local Cache ukládá metadata o čistých souborech z již kontrolovaných počítačů. Při kontrole na dalším počítači porovná ESET Local Cache metadata z počítače s již uloženými metadaty a automaticky přeskočí soubory z whitelistu. Každý nově skenovaný soubor se automaticky přidává do cache paměti. Jednou kontrolované soubory na virtuálním stroji se tedy už podruhé v rámci jednoho virtuálního prostředí na jiném stroji nekontrolují, což má značný dopad na rychlost skenování souborů. V případě komunikace na stejném fyzickém hardwaru prakticky nedochází při kontrole ke zpoždění, čímž se znatelně šetří systémové prostředky.
Windows Management Instrumentation (WMI) Provider	Poskytuje možnost monitorovat klíčové funkce produktu pomocí Windows Management Instrumentation frameworku. To umožňuje integrovat ESET File Server do nástrojů třetích stran a SIEM, jako je Microsoft System Center Operations Manager, Nagios a další.

SLUŽBY ZDARMA PRO ZÁKAZNÍKY S PLATNOU LICENCÍ

Technická podpora

K dispozici je nejen možnost konzultace po telefonu nebo e-mailem, ale také online pomocí vzdáleného připojení* a databáze znalostí.

Návštěva technika

V rámci platné licence nabízíme všem firemních zákazníkům s licencí na 25 počítačů a více jednou ročně návštěvu našeho technika. Zahrnuje max. 4 hodiny práce technika na místě + cestu. Možno čerpat jako školení, konzultaci nebo pomoc s instalací a nasazením.

Antivirová ambulance

Služba je poskytována online pomocí vzdáleného připojení po předchozí dohodě s technikem. Služba neslouží k odvirování všech počítačů ve firemním prostředí, ale jako konzultace, kdy je na základě vzorku postižených stanic technikem navržen optimální postup pro odvirování ostatních počítačů.

Školení a konzultace

Školení a konzultace vedené certifikovaným technikem v sídle společnosti ESET v maximálním rozsahu 4 hodiny.

* Po předchozí domluvě s technikem.

Použitelnost

Výjimky na procesy	Administrátor může definovat procesy, které bude rezidentní ochrana ignorovat – všechny operace se soubory, které se pojí s danými procesy, budou považovány za bezpečné. To se hodí pro procesy, které velmi často rezidentní ochrana kontroluje, jako je záloha nebo migrace virtuálního stroje v reálném čase. Vyloučené procesy mohou přistupovat i k nebezpečným souborům nebo objektům bez spuštění upozornění.
Inkrementální aktualizace	Pravidelné aktualizace jsou staženy a aplikovány v malých přírůstkových balíčcích. Šetří se tím nejen systémové prostředky a internetové připojení, ale také celá síťová infrastruktura a servery.
Instalace jednotlivých modulů	Dovoluje nainstalovat vybrané komponenty: - Rezidentní ochranu - Ochrani webu a pošty - Kontrolu zařízení - Graficeké uživatelské prostředí (GUI) - ESET Log Collector - a další
Vzdálená správa	Podporuje připojení do nástroje vzdálené správy ESET Remote Administrator, který umožňuje nastavit a spravovat bezpečnostní politiky, sbírat logy, dostávat upozornění a mít přehled nad celkovou bezpečnostní situací v síti – vše pomocí jedné webové konzole.
ESET Log Collector	Jednoduchý nástroj, který sbírá všechny protokoly pro případ, kdy si je vyžádá technická podpora ESET. Logy se ukládají do jednoho archívu, který je možné poslat e-mailem nebo sdílet.
ESET License Administrator	Umožňuje transparentně spravovat/spojovat/ delegovat všechny licence z jednoho místa pomocí webového prohlížeče v reálném čase, i mimo ESET Remote Administrator.