www.eset.sk

MAIL SECURITY

PRE MICROSOFT EXCHANGE SERVER

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE

MAIL SECURITY

PRE MICROSOFT EXCHANGE SERVER

ESET Mail Security pre Microsoft Exchange Server predstavuje silnú antivírusovú a antispywarovú ochranu, ktorá zabezpečí spoľahlivé odfiltrovanie e-mailov so škodlivým obsahom už priamo na serverovej úrovni. Navyše vďaka nízkej záťaži systému budete môcť aj naďalej pracovať naplno.

S týmto riešením získate kompletnú ochranu serverov vrátane serverového file systému. Pomocou nástroja vzdialenej správy ESET Remote Administrator môžete nastavovať bezpečnostné politiky na základe špecifického obsahu, prípadne typu reálnej prípony daného súboru. Samozrejmosťou je možnosť monitorovania nasadených politík, ako aj jemného dolaďovania nastavení produktu.

Antimalvérová ochrana a Antispam

Antivírus a Antispyware	Eliminuje rozličné typy hrozieb vrátane vírusov, rootkitov, červov a spywaru s voliteľnou možnosťou cloudovej kontroly pre lepší výkon a detekciu. **Voliteľná cloudová kontrola:** Vytváraním zoznamov bezpečných súborov v cloudovej reputačnej databáze zabezpečuje lepšiu detekciu a rýchlejšiu kontrolu. Do cloudu sa zasielajú iba informácie o spustiteľných a archívnych súboroch. Tieto dáta sa nedajú spätne priradiť k používateľovi.
Antispam a Anti-Phishing	Chráni pred spamovými a phishingovými útokmi. Prináša vysokú mieru detekcie, a to aj bez potreby manuálneho nastavenia Spam Conficence Level (SCL). Antispamový modul je pripravený na spustenie hneď po inštalácii – netreba ho manuálne nastavovať.
Lokálna správa karantény	Každý majiteľ mailboxu môže prostredníctvom samostatného prehliadača interagovať so správami, ktoré boli označené ako podozrivé a neboli preto doručené do mailboxu. Na základe privilégií nastavených administrátorom môže používateľ rozdeliť správy v karanténe, vyhľadávať v nich a vykonávať povolené akcie, po jednotlivých správach, alebo skupinách. Všetko cez internetový prehliadač. Akcie sa líšia na základe dôvodu, z ktorého bola správa umiestnená do karantény. Používateľovi môže byť zaslaný pravidelný e-mailový report, ktorý sumarizuje správy v karanténe. Prostredníctvom priložených linkov je následne možné vykonať akciu.
On-demand skenovanie databáz	Administrátori si môžu vybrať, ktoré databázy či samostatné mailboxy majú byť skontrolované. Kontrola môže byť špecifikovaná na základe „time stamp" označenia správ, ktoré majú byť preverené. Zaťaženie servera sa tak pri tejto úlohe znižuje na minimum.
Pravidlá spracovania správ	Pravidlá spracovania správ ponúkajú veľké množstvo kombinácií, akými sa môže so správami narábať. Vyhodnocované parametre obsahujú štandardné polia ako predmet, odosielateľ, samotný text správy a špecifická hlavička. Navyše ponúkajú ďalšie podmienené spracovania na základe predošlých výsledkov antispamových a antivírusových kontrol. Na kontrolu príloh poškodených alebo heslom chránených archívov sa nepoužíva len súborová prípona, ale na účely posúdenia skutočného typu súboru prebieha kontrola reálnej dátovej štruktúry. Pravidlá sa môžu meniť podľa potreby.
Exploit Blocker	Zlepšuje zabezpečenie aplikácií, ktoré bývajú častými terčami útokov. Medzi takéto aplikácie patria napríklad internetové prehliadače, PDF čítačky, e-mailoví klienti alebo komponenty MS Office. Sleduje správanie procesov a hľadá podozrivé aktivity, typické pre zneužitia. Chráni pred cielenými útokmi a zatiaľ nezaznamenanými hrozbami, tzv. zero-day útokmi.
Pokročilá kontrola pamäte	Monitoruje správanie škodlivých procesov a kontroluje ich priamo v pamäti. Poskytuje tak lepšiu detekciu hrozieb, ktoré sa skrývajú pod viacerými vrstvami šifrovania.
Host-Based Intrusion Prevention System (HIPS)	Umožňuje vám definovať pravidlá pre systémové registre, procesy, aplikácie a súbory. Poskytuje ochranu pred zmenami nastavení a zaznamenáva hrozby na základe správania systému.
Správa zariadení	Chráni váš server pred pripojením neoprávnených vymeniteľných zariadení. Umožňuje vám zostať v súlade s firemnými smernicami vytvorením pravidiel pre používateľské skupiny. V prípade, že je na zariadenie aplikovaná funkcionalita tzv. jemného blokovania (soft blocking), zariadenie je možné používať, ale jeho aktivita bude monitorovaná.

Komplexná infraštruktúra v bezpečí

Snapshot nezávislosť	Aktualizácie ESET a programové moduly môžu byť uložené mimo prednastaveného úložiska. Nie sú tak ovplyvnené prechodom na starší stav virtuálneho zariadenia. To znamená, že aktualizácie a moduly nemusia byť stiahnuté vždy, keď sa virtuálne zariadenie vráti do staršieho stavu. Navyše takto obnovené zariadenie môže využiť nedotknuté aktualizácie a vyhnúť sa tak veľkému objemu sťahovaných dát. Výsledkom sú rýchlejšie časy obnovy stavu.
Natívna podpora klastrovania	Umožňuje vám nastaviť riešenie tak, aby automaticky replikovalo nastavenia pri inštalácii v klastrovom prostredí. Vďaka intuitívnemu prostrediu sprievodcu nastavení je prepojenie jednotlivých inštalovaných uzlov v klastri veľmi jednoduché. Môžete ich tak riadiť naraz a zmeny už nemusíte opakovane manuálne konfigurovať na ostatných uzloch v klastri.
ESET Shared Local Cache	ESET Shared Local Cache porovnáva metadáta súborov s metadátami už uložených súborov a automaticky vynecháva už preverené súbory. V prípade, že sa pri kontrole objaví ešte nepreverený súbor, automaticky je pridaný do cache. To znamená, že súbory kontrolované na virtuálnom zariadení nebudú opakovane kontrolované na iných virtuálnych zariadeniach v rovnakom virtuálnom prostredí, čo zvyšuje výkonnosť kontroly. Keďže komunikácia prebieha na fyzicky tom istom hardvéri, v skenovaní nie sú prakticky žiadne omeškania, čím sa výrazne šetria zdroje.
Windows Management Instrumentation (WMI) Provider	Poskytuje možnosť sledovať hlavné funkcie ESET Mail Security prostredníctvom rozhrania Windows Management Instrumentation. Umožňuje to integrovať ESET Mail Server do SIEM riešení tretích strán, ako napríklad Microsoft System Center Operations Manager, Nagios a iné.

MIESTNA TECHNICKÁ PODPORA ZDARMA

Dosiahnite viac s pomocou našich špecialistov, ktorí vám poradia, keď to budete potrebovať. Navyše v slovenčine.

Používanie

Výnimky procesov	Administrátor môže definovať procesy, ktoré sú modulom rezidentnej ochrany ignorované. Všetky súborové operácie súvisiace s týmito procesmi budú následne považované za bezpečné. Je to šikovný nástroj hlavne pri procesoch, ktoré prichádzajú do konfliktu s rezidentnou ochranou, ako je zálohovanie alebo migrácie vo virtuálnom prostredí. Procesy s bezpečnostnou výnimkou môžu pristupovať aj k nezabezpečeným prvkom a súborom a nespustiť pri tom poplach.
Inkrementálne mikrodefinície	Časté aktualizácie sú sťahované a uplatňované inkrementálne v malých balíčkoch. Šetria sa tak systémové zdroje a internetové pásmo bez badateľného vplyvu na rýchlosť celej sieťovej infraštruktúry, serverov, alebo požiadavky koncových zariadení na pamäť, alebo CPU.
Modulárna inštalácia	Okrem požadovaných komponentov vám ESET umožňuje výber a inštaláciu len tých komponentov, ktoré potrebujete: – ochrana súborového systému v reálnom čase – webová a e-mailová ochrana – správa zariadení – grafické rozhranie (GUI) – ESET Log Collector – a iné
Vzdialená správa	Riešenia ESET Endpoint sú plne ovládateľné cez technológiu ESET Remote Administrator. Webová konzola vám umožní spúšťať úlohy, meniť nastavenia, zbierať logy a získavať správy o celkovom bezpečnostnom stave vašej siete.
ESET Log Collector	Jednoduchý nástroj zbiera všetky logy súvisiace s riešením problémov a spája ich do jednotlivých archívov. Tie môžu byť zaslané prostredníctvom e-mailu alebo nahraté na zdieľaný sieťový disk a zrýchliť tak proces riešenia problémov.
ESET License Administrator	Umožňuje transparentné narábanie so všetkými licenciami z jedného miesta cez internetový prehliadač. Licencie môžete spájať, delegovať a všetky centrálne riadiť v reálnom čase, a to aj v prípade, že nepoužívate ESET Remote Administrator.