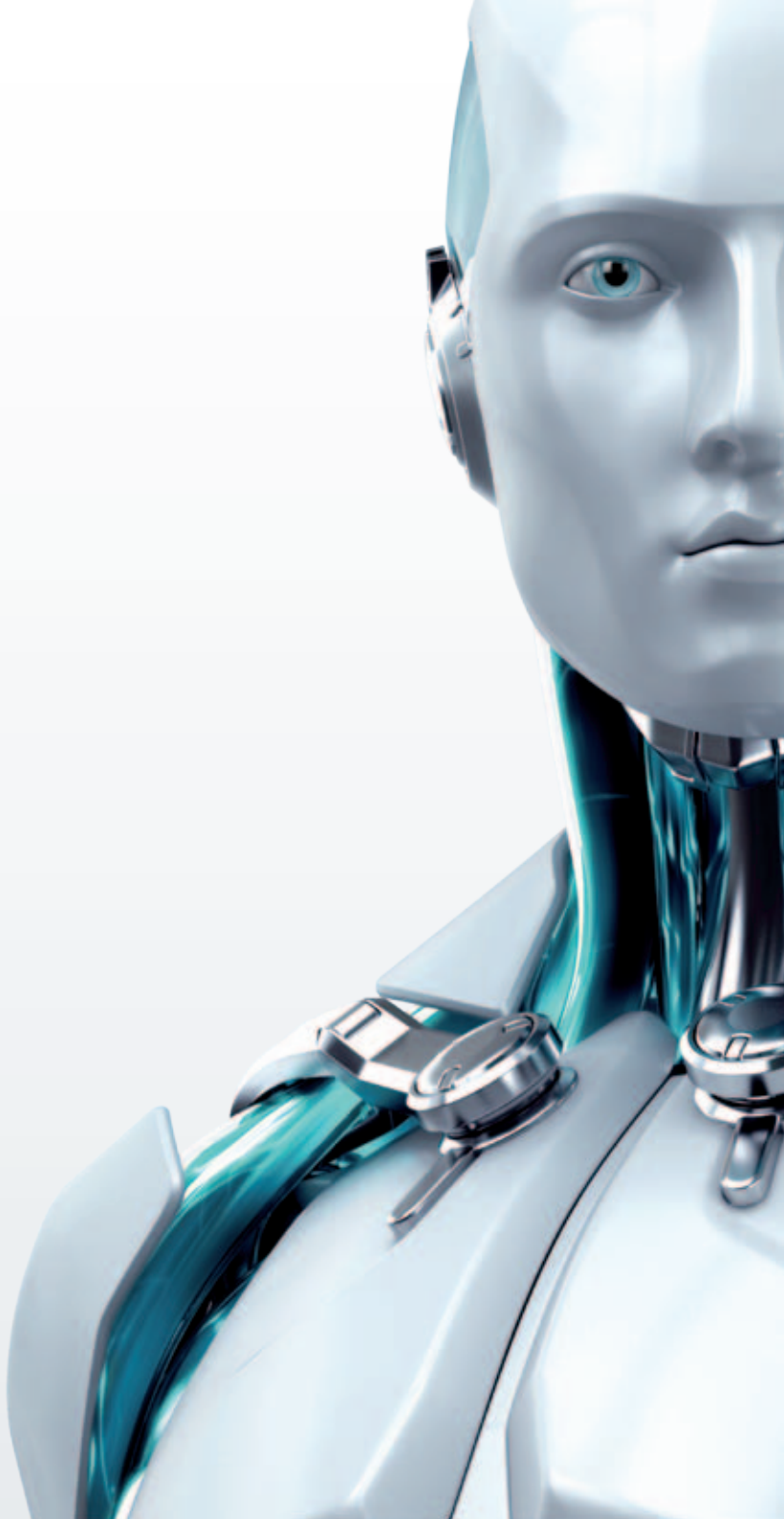
ESET ENDPOINT RIEŠENIA

Vlastnosti z pohľadu IT špecialistu



www.eset.sk

20 ROKOV

PRINÁŠAME ŠPIČKOVÉ BEZPEČNOSTNÉ RIEŠENIA

Ochrana koncových zariadení

FUNKCIA	AKO FUNGUJE	AKÉ VÝHODY PRINÁŠA
Antivírus a antispyware	Eliminuje všetky typy hrozieb vrátane vírusov, rootkitov, červov a spyware. **Voliteľná cloudová kontrola:** Povolenie bezpečných súborov na základe cloudovej databázy reputácie súborov. Do cloudu sa odosielajú len informácie o spustiteľných súboroch a archívoch.	Čisté koncové zariadenia znamenajú bezproblémovú prácu. S riešeniami od spoločnosti ESET nasadenými v podnikových koncových zariadeniach sú vaše údaje v bezpečí a chránené. Vyberte si zo širokej škály možností prispôsobenia a nastavte automatické akcie v prípade zistenia hrozieb. Cloudová kontrola od spoločnosti ESET zaručuje rýchlejšiu kontrolu a lepšiu detekciu aktuálne sa šíriacich (in-the-wild) vírusov, pričom minimalizuje chybné vyhodnotenia. Do cloudu sa neodosielajú žiadne dôverné údaje, len informácie o spustiteľných a archívnych súboroch. Odoslané údaje navyše neumožňujú identifikáciu konkrétnej osoby.
Nástroj Host-based Intrusion Prevention System (HIPS)	Umožňuje definovať pravidlá pre systémové registre, procesy, aplikácie a súbory. Poskytuje ochranu pred neoprávnenou manipuláciou. Rozpoznáva hrozby na základe správania systému.	Prispôsobenie správania celého systému a jednotlivých častí. Blokovanie neoprávnených činností a používanie podrobných protokolov funkcie HIPS na kontrolu a vykazovanie súladu. Integrovaná funkcia Self-Defence zaručuje ochranu súčastí softvéru od spoločnosti ESET pred neoprávnenou manipuláciou a maximálnu ochranu systémov.
Automatická kontrola vymeniteľných médií	Umožňuje kontrolovať zariadenia a médiá na prítomnosť malvéru okamžite po vložení. Možnosti kontroly: automatické spustenia/upozornenie (výzva pre používateľa)/ bez kontroly.	Automatická kontrola vymeniteľných ukladacích médií zaručuje rozšírenú ochranu voči offline hrozbám prenášaným v zariadeniach USB, na diskoch CD, DVD a v iných zariadeniach.
Modulárna inštalácia ★	Umožňuje nainštalovať len niektoré alebo všetky nasledujúce komponenty zabezpečenia: firewall, antispam, kontrola webu, ovládanie zariadení, podpora funkcie Microsoft NAP a ochrana prístupu na web.	Nasadenie len požadovaných modulov ochrany pre každú skupinu koncových zariadení, aby vaše systémy mohli fungovať na plný výkon bez premrhaných prostriedkov. Aktivácia a deaktivácia nainštalovaných modulov na diaľku vždy, keď potrebujete jemne doladiť koncové zariadenia.
Klientský antispam ★	Účinne filtruje nevyžiadanú poštu v koncovom zariadení používateľa. Kontroluje všetku prichádzajúcu poštu na prítomnosť malvéru.	Výkonný antispam so zoznamom povolených a zakázaných položiek a vlastným učením možno nastaviť samostatne pre každého klienta alebo skupinu. Natívna podpora programu Microsoft Outlook vylepšuje ochranu (protokolov POP3, IMAP, MAPI, HTTP) pred online hrozbami bez dodatočnej námahy z vašej strany.
Nízke nároky na systém	Poskytuje overenú ochranu a zároveň ponecháva viac systémových prostriedkov pre pravidelne používané programy.	Minimalizuje spomalenia pozorované pri iných antivírusových riešeniach náročných na systém a zachováva vysoký výkon podnikových počítačov. Predlžuje životnosť hardvéru nasadením riešení od spoločnosti ESET do starších počítačov bez nutnosti inovácie. Šetrenie výdrže batérie notebookov mimo pracoviska s režimom batérie.
Multiplatformová ochrana	Rozpoznáva a eliminuje malvér útočiaci na operačné systémy Windows, Mac a Linux.	Poskytuje lepšiu ochranu v multiplatformovom prostredí, pretože riešenia zabezpečenia od spoločnosti ESET pre systém Windows dokážu zistiť hrozby pre systém Mac OS a naopak.
ESET SysRescue	Umožnuje vytvorit spustitelný obraz operacného systému s predinštalovaným bezpečnostným riešením ESET. Napomáha tak efektívnejšiemu idvíreniu infikovaných počítačov.	Zvyšuje pravdepodobnosť záchrany dát z veľmi infikovaných počítačov.

★ Vlastnosti označené hviezdičkou sú dostupné v ESET Endpoint Security.
Všetky ostatné sú dostupné aj pre ESET Endpoint Antivirus.

Kontrola prístupu k údajom

FUNKCIA	AKO FUNGUJE	AKÉ VÝHODY PRINÁŠA
Web control ★	Obmedzuje prístup k webovým stránkam podľa kategórií. Umožňuje vytvárať pravidlá pre skupiny používateľov v súlade s politikami spoločnosti.	Riadenie a monitorovanie prístupu používateľov alebo skupín k webovým stránkam s možnosťou kategategorizácie (hry, sociálne siete, nakupovanie atď.). Webové stránky sa automaticky zaraďujú do kategórií prostredníctvom cloudovej služby. Blokovanie stránok, ktoré vytvárajú vysoký objem dátových prenosov, šetrenie kapacity podnikovej siete a súlad s podnikovými politikami prijateľného používania internetu.
Správa zariadení	Blokuje prístup neoprávnených médií a zariadení k systému. Umožňuje nastaviť pravidlá/parametre pre konkrétne médiá, zariadenia, používateľov a klientov.	Centrálne spravované pravidlá a politiky pre médiá a zariadenia podľa vopred nastavených atribútov, ako sú napríklad sériové číslo, výrobca alebo model. Nastavenie prístupu len na čítanie, na čítanie aj zápis alebo blokovanie prístupu pre jednotlivých používateľov a skupiny. Podrobné protokoly o prístupe a kontrole zjednodušujú presadzovanie politík a vykazovanie súladu.
Detekcia dôveryhodných zón ★	Poskytuje prísnejšiu ochranu pri pripájaní klientov k novej alebo neautorizovanej sieti.	Vytváranie prísnejších politík pre prístup k neautorizovaným sieťam, ako sú napríklad verejné Wi-Fi. Definovanie dôveryhodných sietí a predvolené vynútenie všetkých ostatných pripojení v prísnom režime. Používatelia a údaje v ich notebookoch budú chránené pred internetovými hrozbami pri pripájaní používateľov k verejným prístupovým bodom v kaviarňach, na letiskách alebo v hoteloch.
Obojsmerný firewall ★	Zabraňuje neoprávnenému prístupu k podnikovej sieti. Poskytuje ochranu proti hakerom a zabraňuje odhaleniu údajov.	Brána firewall s jednoduchým nastavením, rozsiahlou možnosťou prispôsobenia a inteligentným režimom učenia. Program ESET Remote Aministrator obsahuje sprievodcu na zjednodušenie zlúčení pravidiel firewallu. vďaka tomu budete môcť jednoducho vytvárať skupiny pravidiel a použiť ich na rôznych miestach v sieti.

★ Vlastnosti označené hviezdičkou sú dostupné v ESET Endpoint Security.
Všetky ostatné sú dostupné aj pre ESET Endpoint Antivirus.

Vzdialená správa

FUNKCIA	AKO FUNGUJE	AKÉ VÝHODY PRINÁŠA
Centralizovaná správa	Umožňuje spravovať všetky bezpečnostné riešenia od spoločnosti ESET z centrálneho nástroja na správu.	Program ESET Remote Administrator umožňuje spravovať všetky bezpečnostné riešenia od spoločnosti ESET z jednej konzoly bez ohľadu na to, či používate systém Windows, Mac alebo Linux. Toto riešenie podporuje infraštruktúru IPv6 a z tej istej konzoly možno spravovať aj virtuálne počítače a smartfóny.
Dynamické klientské skupiny	Umožňuje vytvárať dynamické klientské skupiny a napĺňať ich podľa rôznych parametrov.	Vytváranie skupín používateľov s rôznymi parametrami, ako sú napríklad operačný systém, maska názvu klienta, maska adresy IP, nedávno zistené hrozby atď. Nastavenie osobitných politík pre rôzne skupiny, automatické preradenie klienta do príslušnej skupiny v prípade zmeny parametrov.
Správa na základe rolí	Udeľuje rôzne privilégiá jednotlivým používateľom programu ESET Remote Administrator. Audit používateľov s programom ESET Remote Administrator. Vynútenie zložitosti hesla.	Delegovanie zodpovedností medzi jednotlivých užívateľov a skupiny. Podrobné protokoly auditu zjednodušujú vykazovanie súladu a integrovaný nástroj na kontrolu sily hesla zaručuje náležitú ochranu správcovských kont.
Vzdialená inštalácia	Vykonáva vzdialenú inštaláciu softvéru od spoločnosti ESET na viacero koncových zariadení naraz.	Program ESET Remote Administrator umožňuje vykonávať vzdialene spúšťané inštalácie riešení ESET Endpoint Solutions pre Windows ako i novej generácie koncových riešení pre systémy Mac, Linux a ľubovoľných inštalačných súborov formátu msi.
Exportovanie a importovanie politík	Umožňuje importovať, exportovať a upravovať politiky vo formáte XML.	Šetrenie času, predchádzanie chybám spojeným s definovaním konfiguračných súborov a možnosť exportu s následným použitím v koncových zariadeniach.
Vzdialená správa modulov	Vzdialená aktivácia alebo deaktivácia modulov ochrany nainštalovaných na konkrétnom klientovi vrátane brány firewall, technológie anti-stealth, rezidentnej ochrany, kontroly prístupu na web a ochrany e-mailového klienta. Automatickú opätovnú aktiváciu možno nastaviť o: 10 minút, 30 minút, 1 hodinu, 4 hodiny alebo nikdy.	Zjednodušenie údržby systému alebo ladenia problémov vzdialenou aktiváciou alebo deaktiváciou nainštalovaných modulov. Nastavenie automatického časovača na obnovenie predchádzajúcich nastavení zabraňujúcich neúmyselnej zraniteľnosti systému. Všetky moduly okrem technológie Anti-stealth sa automaticky prepnú naspäť po reštartovaní koncového zariadenia.

Hlásenia, protokoly a upozornenia

FUNKCIA	AKO FUNGUJE	AKÉ VÝHODY PRINÁŠA
Web Dashboard	Zaručuje kompletný dohľad nad podnikovou sieťou a umožňuje odkiaľkoľvek skontrolovať stav zabezpečenia.	Prístup k webovému rozhraniu z konzoly alebo ľubovoľného miesta v sieti na získanie rýchleho prehľadu o stave zabezpečenia. Prispôsobenie zobrazovaných informácií prostredníctvom rozhrania programu ESET Remote Administrator. Monitorovanie stavu zabezpečenia siete a štatistík zaťaženia serverov pomocou živého prenosu požadovaných údajov.
Viacero formátov protokolov	Umožňuje ukladať protokoly v bežných formátoch – CSV, obyčajný text, denníku udalostí systému Windows – čitateľných pre nástroje SIEM. Ukladá protokoly na strane koncového zariadenia na neskoršie vyzdvihnutie.	Riešenia spoločnosti ESET podporujú viacero formátov protokolov, čím zjednodušujú využívanie nástrojov na správu informácií a udalostí zabezpečenia (SIEM) tretích strán. Uľahčuje tak triedenie a uchovávanie dôležitých údajov vo vyhovujúcej forme pre vašu firmu.
Upozornenia na udalosti	Umožňuje upravovať parametre zapisovania protokolov a hlásení, alebo vybrať si spomedzi viac než 50 šablón dostupných pre rôzne systémové/klientské udalosti. Samozrejmosťou je možnosť nastaviť prah pre upozornenia na udalosti.	Pomáha rýchlo identifikovať potenciálne problémy, zjednodušuje monitorovanie siete a dodržiavanie firemných politík. Nastavenie priority a času na prebiehajúce upozornenia, odosielanie okamžite alebo dávkovo v preddefinovaných intervaloch. Vytváranie pravidiel upozornení, prispôsobenie obsiahlosti protokolov a preposielanie každého upozornenia na udalosť pomocou e-mailu, funkcie syslog, pasce protokolu SNMP alebo textového súboru.
Hlásenia zo správy zariadení	Hlásenia ovládania zariadení poskytujú komplexné protokoly a hlásenia pre všetky udalosti týkajúce sa zariadenia.	Podrobné protokoly o používaní vymeniteľných médií a zariadení je možné sledovať z jedného centrálneho miesta. Hlásenia obsahujú údaj o dátume, čase, používateľské meno, názov počítača, názov skupiny, triedu zariadenia a podrobnosti o vyvolanej udalosti.
Podpora platformy RSA enVision	Integrácia s nástrojom RSA enVision prostredníctvom doplnku.	Podpora platformy RSA enVision zaručuje jednoduchú integráciu s týmto obľúbeným SIEM nástrojom tretej strany.
ESET SysInspector	Vykonáva hĺbkovú analýzu koncových systémov na identifikáciu možných rizík zabezpečenia.	Identifikácia všetkých spustených procesov, nainštalovaného softvéru a hardvérovej konfigurácie vo všetkých koncových zariadeniach. Odhaľovanie potenciálnych bezpečnostných rizík porovnávaním posledných dvoch protokolov koncového zariadenia.

Rýchlosť a stabilita siete

FUNKCIA	AKO FUNGUJE	AKÉ VÝHODY PRINÁŠA
Randomizácia vykonávaných úloh	Nastaví náhodný čas spustenia pre plánované úlohy zabezpečenia.	Nastavenie náhodného času vykonávania úloh. Minimalizácia veľkého počtu simultánnych antivírusových kontrol vo virtualizovaných prostrediach. Zabraňuje sa tak vyťaženiu hardvérových prostriedkov, takže koncoví používatelia nespozorujú spomalenie výkonu.
Rollback aktualizácií	Vráti bezpečnostné moduly a databázu vírusových vzoriek na predchádzajúcu verziu.	Riešenie nekompatibilít alebo iných narušení systému vrátením aktualizácií definícií vírusov a modulov do známeho dobrého stavu niekoľkými kliknutiami. Zamedzenie aktualizácií podľa potreby – dočasné vrátenie alebo až do manuálnej zmeny.
Oneskorenie aktualizácie	Poskytuje možnosť sťahovania z troch špecializovaných aktualizačných serverov: predbežné vydanie (beta používatelia), bežné vydanie (pravidelní používatelia) a odložené vydanie (12 hodín po bežnom vydaní).	Pomáha zaručiť plynulý proces aktualizácie so zreteľom na kontinuitu operácií užívateľa. Aktualizácie antivírusových databáz môžete najskôr otestovať na nekritických systémoch a po bezproblémovom priebehu nasadiť na produkčné počítače.
Lokálny aktualizačný server	Šetrí objem prenesených dát stiahnutím aktualizácií len raz na lokálny zrkadlový server. Je podporovaný aj zabezpečený komunikačný kanál (HTTPS).	Program ESET Remote Administrator možno používať ako zrkadlový aktualizačný server pre koncové zariadenia a minimalizovať tak objem prenesených dát cez internet. Pre mobilných zamestnancov je možné definovať sekundárny aktualizačný profil, aby sa koncové zariadenia aktualizovali priamo zo serverov spoločnosti ESET, keď interný server nie je k dispozícii. Podpora protokolu HTTPS.
Rýchlejší prístup k databázam	Poskytuje optimalizovaný a zjednodušený prístup k databáze s informáciami o bezpečnosti endpointov.	Optimalizovaný výkon databáz umožňuje vyššiu produktivitu kombinovaním údajov z koncových zariadení a rýchlejšiu tvorbu hlásení.
Premazávanie databázy	Umožňuje nastaviť atribúty ukladacieho priestoru databázy, napríklad časové obdobie a prahové hodnoty, na zachovanie položiek v databáze.	Bezproblémové fungovanie, rýchla odozva a primeraná veľkosť databázy.
Podpora Microsoft NAP	Nasadzuje doplnok System Health Validator (SHV) na strane servera a agenta System Health Agent (SHA) na strane klienta. Udeľuje úplný prístup k sieti pre vyhovujúcich klientov a len obmedzený alebo žiadny prístup k sieti pre nevyhovujúcich klientov.	Pomáha pri monitoringu zariadení pripájajúcich sa do siete. Doplnok SHA zhromažďuje informácie na strane klienta odosiela ich na server v rámci funkcie NAP. Nastavenie požiadaviek na súlad klientov, ako sú napríklad: vek databázy vírusov, verziu antivírusového programu, stav ochrany, dostupnosť antivírusovej ochrany a stav brány firewall. Dosiahnutie súladu koncových zariadení vynútením aktualizácie databázy.