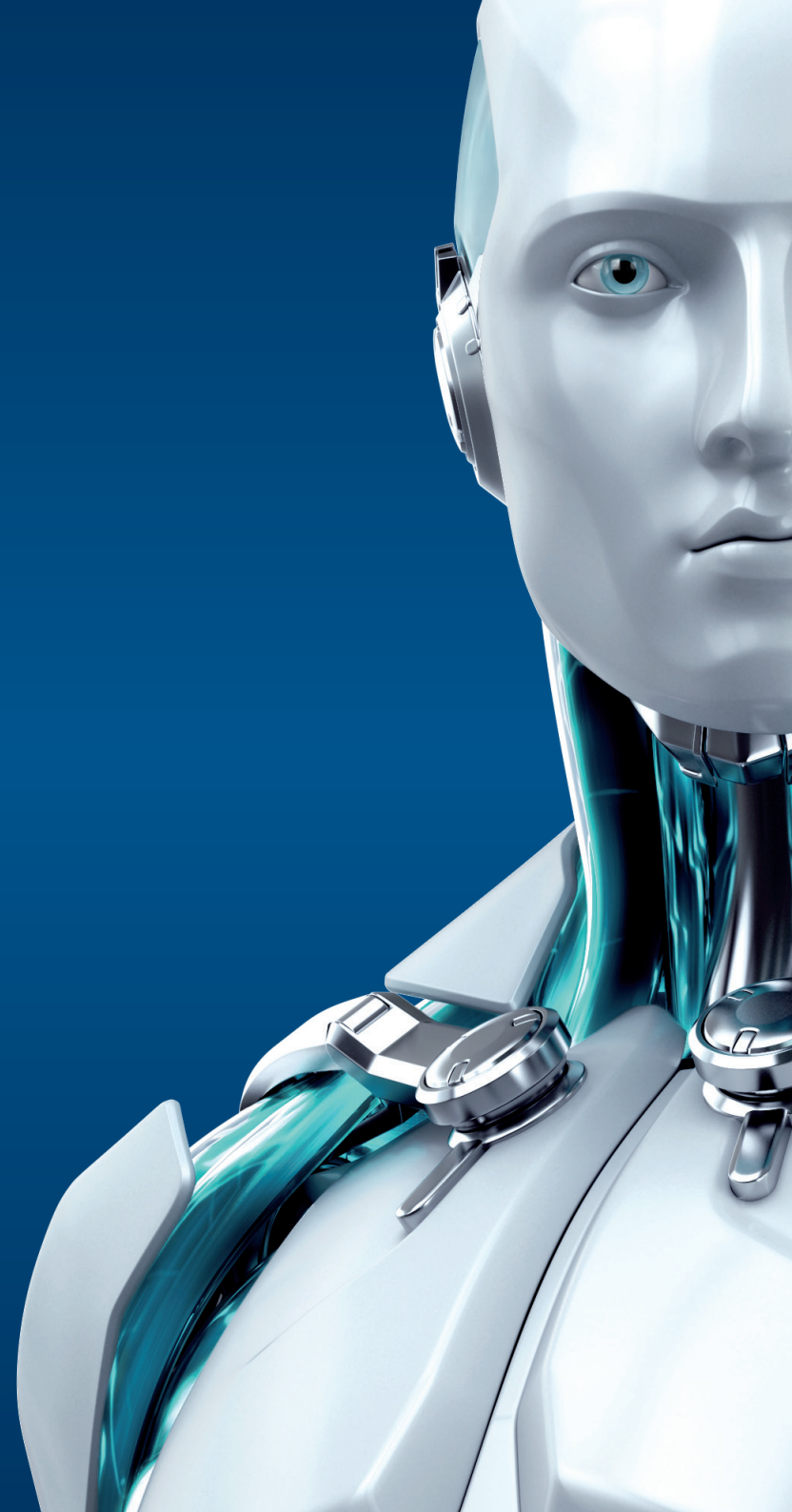




ENDPOINT SECURITY

ENJOY SAFER TECHNOLOGY™





ENDPOINT SECURITY

ESET Endpoint Security je celkové řešení IT bezpečnosti pro firmy. Obsahuje několik vrstev ochrany, včetně prověřené technologie detekce škodlivého kódu ESET NOD32, které reagují na nové trendy v počítačové kriminalitě. Produkt umožňuje detailní nastavení parametrů jednotlivých bezpečnostních modulů.

Díky nízkým systémovým nárokům, podpoře virtualizace a volitelné cloud kontrole souborů zařízení nabízí počítače s nainstalovaným ESET Endpoint Security koncovému uživateli dostatek výkonu k rychlé a plynulé práci.

Kompletní přehled o bezpečnosti koncových stanic lze získat s pomocí zcela přepracovaného, uživatelsky příjemného nástroje pro vzdálenou správu.

Ochrana koncových zařízení

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 umísťují soubory na základě reputace.

Do cloudu se odesílá pouze informace o spustitelných souborech a archivech.

Podpora virtualizace

Metadata kontrolovaných souborů se ukládají, a v rámci daného virtuálního prostředí se již znovu nekontrolují, což má pozitivní dopad na rychlost skenování systému.

Moduly aktualizací a virové databáze nejsou uloženy lokálně, takže se nebudou znovu stahovat při každém obnovení (snapshot) systému.

HIPS (Host-Based Intrusion Prevention System)

Umožňuje definovat pravidla pro systémové registry, procesy, aplikace a soubory.

Chrání soubory před neautorizovanými změnami a detekuje hrozby na základě chování systému.

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.

Antispam

Efektivně filtruje nevyžádanou poštu a kontroluje příchozí zprávy na přítomnost škodlivého kódu.

Nativně podporuje Microsoft Outlook (POP3, IMAP, MAPI).

Podpora různých platforem

Detekuje nejen malware pro Windows, ale také pro Mac OS, takže nedochází k dalšímu šíření škodlivého kódu v multiplatformním prostředí.

Ochrana přístupu k datům

Kontrola přístupu na web	Filtruje přístup k internetovým stránkám dle kategorií např. hry, sociální sítě, nakupování a další. Umožňuje vytvořit pravidla pro uživatelské skupiny v souladu s firemní politikou. Podmíněné blokování - upozorní uživatele na návštěvu blokováných stránek, dovolí je otevřít, ale veškerá aktivita je zapisována do protokolu.
Anti-Phishing	Chrání uživatele před pokusy získat jejich citlivé informace, jako jsou hesla, bankovní data nebo údaje o kreditních kartách.
Firewall	Brání neautorizovanému přístupu do firemní sítě. Chrání firemní data před zneužitím. Umožňuje definovat důvěryhodnou síť, při detekci neautorizovaného připojení se firewall přepne do administrátorského režimu.
Vulnerability Shield	Rozšiřuje schopnosti firewallu a zlepšuje detekci tzv. CVE (Common Vulnerabilities and Exposures) neboli běžných zranitelností v síti na protokolech SMB, RPC, RDP. Přidává důležitou vrstvu ochrany před škodlivým kódem, který se šíří zneužíváním chyb v síťových protokolech.
Ochrana proti botnetu	Chrání před infiltrací botnet malwarem a zabraňuje šíření spamu a síťových útoků z daného zařízení.
Kontrola zařízení	Umožňuje blokovat nebo povolit konkrétní výměnná média jako jsou CD, DVD, USB apod. Umí vytvořit pravidla pro uživatelské skupiny v souladu s firemní politikou.

Kontrola souborů a aktualizace

Kontrola při nečinnosti systému	Vylepšuje výkon systému tím, že hloubkové kontroly probíhají jen při nečinnosti počítače. Pomáhá urychlit další kontroly použitím lokální cache paměti.
Kontrola po první instalaci	Nabízí možnost automaticky spustit kontrolu počítače 20 minut po instalaci a zajistí tak bezpečnost počítače od samého počátku.
„Rollback“ aktualizace	Umožňuje návrat k předchozí verzi virové databáze. Nabízí možnost zastavit aktualizace – dočasně nebo zcela až po manuální ukončení..
Odložené aktualizace	Nabízí možnost použití tří specializovaných aktualizčních serverů: testovacího (beta uživatelé), standardního (pro nekritické systémy) a serveru s možností odložených aktualizací (až 12 hodin)..
Lokální aktualizací server	Snižuje zátěž internetového připojení při aktualizaci virové databáze tím, že ke stažení aktualizace dojde pouze jednou do lokálního mirror serveru. Pokud není lokální server dostupný, probíhá aktualizace přímo ze serverů ESET. Podporuje protokol HTTPS.



SLUŽBY ZDARMA
PRO ZÁKAZNÍKY
S PLATNOU
LICENCÍ

Technická podpora

K dispozici si 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 odvírování všech počítačů ve firemním prostředí, ale jako konzultace, kdy je na základě vzorku postižených stanic technikem navržen optimální postup pro odvírování 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.

Další funkce

Odinstalace jiných řešení	Hledá a odstraní při instalaci jiný bezpečnostní software. Podpora 32 i 64 bitových operačních systémů.
Volitelná viditelnost GUI	Umožňuje nastavit grafické rozhraní na plnou, minimální, manuální nebo „tichou“ viditelnost. Nabízí možnost kompletního zneviditelnění programu pro koncového uživatele, včetně ikony v dolní liště na hlavní obrazovce. Při této variantě vůbec neběží proces „egui.exe“, což pozitivně přispívá k rychlosti počítače.
Správce licencí	Umožňuje transparentně spravovat/spojovat/ delegovat všechny licence z jednoho místa pomocí webového prohlížeče v reálném čase, i mimo ESET Remote Administrator.
Podpora dotykové obrazovky	Podporuje dotykové obrazovky a displeje s vysokým rozlišením. Nabízí často používané možnosti nastavení v hlavním menu. Kompletně byly přepracovány grafické prvky.
Nízké systémové nároky	Přispívají k vysokému výkonu počítače. Hodí se do jakéhokoli systémového prostředí, včetně starších strojů. Nezatěžují zbytečně síťový provoz.
Vzdálená správa	Díky webové konzoli 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.

Copyright © 1992 – 2015 ESET, spol. s r. o. ESET, ESET logo, ESET android postava, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo a/nebo jiné uvedené produkty ESET, spol. s r. o., jsou registrované ochranné známky společnosti ESET, spol. s r. o. Windows® a Windows logo jsou registrované ochranné známky společnosti Microsoft Corporation v USA a dalších zemích. Ostatní zde uvedené společnosti nebo produkty mohou být registrovanými ochrannými známkami příslušných vlastníků. Vyrobeno dle norem jakosti ISO 9001:2000.