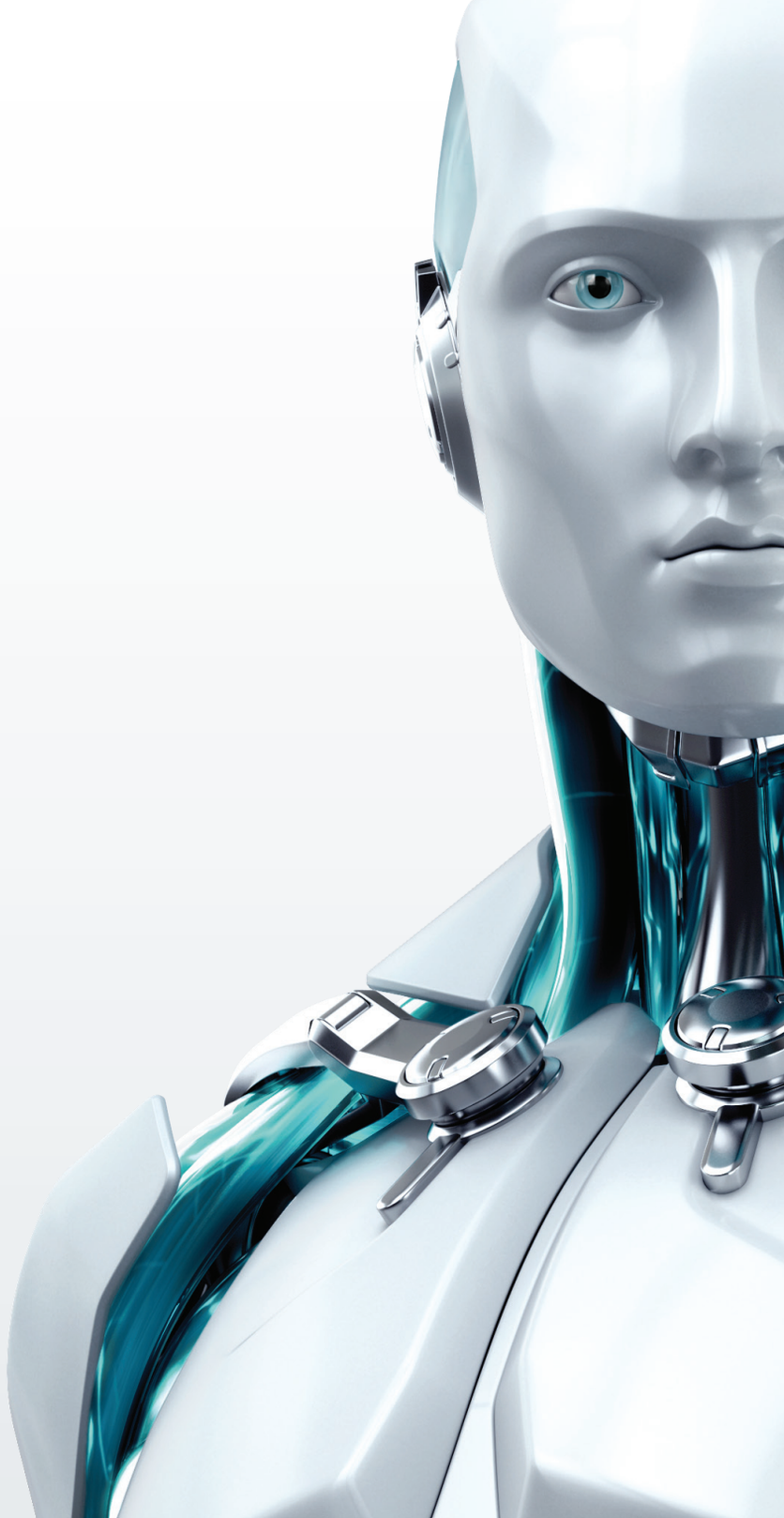
ESET ENDPOINT SOLUTIONS

Powered by ESET **NOD32 ANTIVIRUS**

Caracteristici din perspectivă IT



www.eset.ro

Protecție Endpoint

CARACTERISTICĂ	CE ANUME FACE	CARE SUNT BENEFICIILE
Antivirus / Antispyware	Elimină toate tipurile de amenințări, inclusiv virușii, rootkit-urile, viermii și spyware-ul. **Oferă scanare opțională bazată pe cloud:** presupune introducerea fișierelor sigure într-o lista albă, prin compararea lor în baza de date care stochează reputația fișierelor din cloud. Numai informațiile despre fișierele executabile și arhive sunt trimise în cloud.	Endpoint-urile neinfectate garantează o activitate lipsită de probleme. Cu soluțiile ESET instalate pe endpoint-urile din companie datele dumneavoastră sunt protejate și în siguranță. Alegeți dintr-o gama largă de opțiuni de configurare și stabiliți acțiuni automate atunci cand amenințările sunt detectate. Sistemul de scanare ESET, bazat pe cloud, asigură o viteză superioară de scanare și o detecție și mai bună a virușilor "In-the-wild", în vreme ce numărul detecțiilor fals pozitive este redus la minim. Nicio informație confidențială nu este trimisă către cloud, numai informații legate de executabile și de fișierele arhivate. În plus, datele trimise sunt complet anonim expediate.
Host-based Intrusion Prevention System (HIPS)	Vă permite să definiți reguli pentru regiștrii de sistem, pentru procese și fișiere. Asigură protecție personalizabilă. Detectează amenințările pe baza comportamentului sistemului de operare.	Puteți configura comportamentul întregului sistem și a fiecărei părți componente. Puteți bloca acțiunile neautorizate și puteți utiliza log-urile detaliate HIPS pentru a realiza un audit de conformitate dar și pentru o raportare facilă. Funcția Self-Defense se asigură că elementele și componentele software ESET sunt protejate împotriva manipulării și că sistemul dumneavoastră beneficiază de protecție maximă.
Auto-Scanarea Mediilor Amovibile de Stocare a Datelor	Vă permite să scanați dispozitive și medii de stocare portabile împotriva malware-ului, imediat după inserarea acestora. Opțiunile de scanare oferite sunt: scanează imediat/notifică utilizatorul/nu scana.	Scanarea automată a mediilor de stocare portabile asigură protecție avansată împotriva amenințărilor offline infiltrate prin memorii USB, CD-uri/DVD-uri și alte dispozitive.
★ **Instalare pe Componente**	Vă oferă opțiunea de a instala individual următoarele componente de securitate: firewall, antispam, control web, controlul dispozitivelor portabile de stocare, suport Microsoft NAP și web access protection.	Instalați doar modulele de protecție dorite pentru fiecare grup de endpoint-uri, pentru ca sistemele să ruleze la performanță de vârf, fără să irosiți în nici un fel resursele. Activați și dezactivați de la distanță modulele instalate, oricând doriți să configurați în detaliu endpoint-urile.
★ **Antispam pentru Clienți**	Filtrează eficient mesajele de tip spam, pe dispozitivele endpoint ale utilizatorilor. Scanează toate email-urile, la intrare, împotriva malware-ului.	Modul antispam puternic cu sistem self-learning și liste albe sau negre, ce poate fi configurat diferențiat pentru fiecare client sau grup. Suportul nativ pentru Microsoft Outlook mărește protecția (POP3, IMAP, MAPI, HTTP) în fața amenințărilor online, fără muncă suplimentară de configurare din partea dumneavoastră.
Cerințe reduse de Sistem	Livrează protecție dovedită în vreme ce lasă mai multe resurse sistem la dispoziția programelor pe care le utilizați cu regularitate.	Reduce la minim încetinirile pe care le-ați experimentat cu alte soluții antivirus și păstrează performanța computerelor din companie la un nivel înalt. Puteți extinde durata de viață a echipamentelor hardware instalând soluțiile ESET pe mașini mai vechi, fără să mai fie necesar un upgrade. Conservați autonomia pe baterie a laptopurilor cu modul special de lucru pe acumulator.
Protecție Trans-Platformă	Detectează și elimină malware-ul care are drept țintă sistemele de operare Windows, Mac și Linux.	Oferă o protecție mai bună în mediu de lucru multi-platformă pentru că soluțiile de securitate ESET sunt concepute să detecteze amenințările create pentru Mac OS și viceversa.
ESET SysRescue	Vă permite să creați o imagine de boot automată, cu o soluție de securitate instalată, pentru a curăța sistemele endpoint infectate sever.	Crește șansele recuperări datelor în cazul unei urgențe asigurând posibilitatea de boot-are și curățarea sistemelor endpoint puternic infectate, prin intermediul unui stick USB sau CD.

★ Caracteristicile marcate cu asterix sunt disponibile numai pentru ESET Endpoint Security; toate celelalte caracteristici listate sunt disponibile și pentru ESET Endpoint Antivirus.

Controlul Datelor Accesate

CARACTERISTICĂ	CE ANUME FACE	CARE SUNT BENEFICIILE
★ **Control Web**	Limitează accesul web în funcție de categoria site-ului Vă permite să creați reguli pentru grupurile de utilizatori, care să fie conforme cu politicile companiei.	Reglementează și controlează paginile web accesate de utilizatori sau grupuri de utilizatori pe baza unor categorii web predefinite (jocuri, rețele sociale, magazine online și altele). Site-urile sunt automat clasificate în categorii pe baza serviciului cloud. Se pot bloca site-urile care generează un volum ridicat de trafic, se conservă lățimea de bandă din companie și se aduce traficul în termeni de normalitate vis-a-vis de politicile acceptabile de utilizare a internetului pe care le are compania.
Controlul Dispozitivelor	Blochează mediile portabile de stocare a datelor, considerate neautorizate. Vă permite să stabiliți regulile și parametrii specifici de recunoaștere a dispozitivelor de stocare a datelor în funcție de tipul lor, de utilizatori și de clienți.	Controlează centralizat regulile și politicile de utilizare a dispozitivelor și mediilor portabile de stocare a datelor pe baza unor atribute presetate precum numărul serial, fabricantul sau modelul. Stabilește permisiuni de acces, de citire și scriere sau blochează permisiunile de acces pentru utilizatori sau grupuri. Log-urile detaliate, puse la dispoziție, atât de acces cât și de scanare, simplifică impunerea politicilor și raportarea de conformitate.
★ **Detecția rețelelor de încredere (Trusted)**	Asigură protecție strictă atunci când clienții se conectează la alte rețele.	Ajută la crearea de politici și mai stricte atunci când sunt accesate rețele din afara companiei, precum rețelele publice Wi-Fi. Definește rețelele de încredere, convertind în mod implicit celelalte conexiuni pe modul strict. Utilizatorii și datele lor din laptopuri vor fi protejați în fața amenințărilor provenite din Internet pe măsură ce tranzitează rețele de încredere sau hotspot-uri publice din cafenele, aeroporturi și hoteluri.
★ **Firewall bidirecțional**	Previne accesul neutorizat în rețeaua companiei Asigură protecție anti-hacker și previne expunerea datelor.	Firewall-ul este ușor de configurat și este prevazut cu un mod inteligent de învățare. ESET Remote Administrator oferă un wizard de fuzionare a regulilor pentru firewall pentru ca dumneavoastră să puteți construi ușor seturi de reguli care să fie aplicate de-a lungul rețelei.

★ Caracteristicile marcate cu asterix sunt disponibile numai pentru ESET Endpoint Security; toate celelalte caracteristici listate sunt disponibile și pentru ESET Endpoint Antivirus.

Administrare de la Distanță

CARACTERISTICĂ	CE ANUME FACE	CARE SUNT BENEFICIILE
Management Centralizat	Vă permite să administrați toate soluțiile de securitate ESET din fața unei singure console.	ESET Remote Administrator vă permite să gestionați produsele din fața unei singure console, indiferent dacă rulați Windows, Mac sau Linux. Soluția de management suportă IPv6 și mașinile dumneavoastră virtuale sau smartphone-urile pot fi administrate prin consolă.
Grupuri Dinamice de Clienți	Vă permite să creați grupuri statice și dinamice de clienți și să utilizați diferiți parametri pentru popularea acestor grupuri.	Crează grupuri de utilizatori după diferiți parametrii precum sistemul de operare, nume client, IP, amenințările recente detectate și multe altele. Stabilește politici specifice pentru grupuri diferite, mutând automat clienții în grupuri corespunzătoare dacă parametrii se schimbă.
Management Bazat pe Roluri	Atribuie privilegii diferite diverșilor utilizatori ai ESET Remote Administrator. Auditează utilizatorii cu ESET Remote Administrator. Impune necesitatea folosirii parolelor complexe.	Permite delegarea responsabilităților între diferiți indivizi sau grupuri. Log-urile detaliate de audit simplifică raportarea de conformitate iar sistemul încorporat de verificare a tăriei parolelor se asigură că protecția conturilor administratorilor este corespunzătoare.
Instalare Remote	Execută instalări simultane de software ESET pe endpoint-uri.	Instalează soluțiile ESET Endpoint și orice alt installer msi-based via push install. ESET Remote Administrator poate executa push-install al soluțiilor ESET Endpoint pentru Windows și al noilor generații pentru Mac și Linux.
Export/Import Politici	Vă permite să importați/exportați/editați politicile în XML.	Salvează timp și previne erorile prin definirea setărilor de configurare inițiale, prin exportul acestora și prin aplicarea lor către endpoint-urile și grupurile dorite.
Configurare de la distanță a modulelor	Activează sau dezactivează de la distanță modulele instalate în cazul unui anume client: funcția anti-stealth, protecția în timp real a sistemului, accesul web, protecția clienților email, inclusiv firewall-ul. Reactivarea automată poate fi ajustată pentru 10 min, 30 min, 1 ora, 4 ore sau niciodată.	Simplifică mentenanța de sistem sau depanarea prin activarea și dezactivarea de la distanță a unor module instalate. Stabilește un temporizator de reactivare automată, pentru a evita omiterea repornirii ulterioare a modulelor. Toate modulele, cu excepția Anti-Stealth, redevin automat active după restartul endpoint-ului.

Repoarte, Log-uri & Notificări

CARACTERISTICĂ	CE ANUME FACE	CARE SUNT BENEFICIILE
Consolă web based, în timp real	Asigură o privire de ansamblu asupra rețelei din companie și vă permite să verificați starea de securitate, din orice locație.	Accesați panoul de control web-based prin consolă, din orice punct al rețelei, pentru un scurt review cuprinzător. Ajustați ce informații sunt afișate în panoul de control prin intermediul interfeței de raportare a ESET Remote Administrator. Monitorizați starea de securitate a rețelei și statisticile de încărcare ale serverului utilizând fluxuri live cu datele dorite.
Multiple Formate de Log	Vă permite să salvați log-urile în formatele populare - CSV, plain text, Windows event log - accesibile prin uneltele SIEM. Stochează log-urile pentru recuperare si analiză ulterioară.	Asigură parsarea datelor via formate de date compatibile pentru a ușura colectarea informației și analizele ulterioare. Suportul ESET pentru formate de log multiple vă ajută să profitați de uneltele 3rd party de tip Security Information and Event Management (SIEM).
Notificări Evenimente	Vă oferă posibilitatea de a specifica parametrii de raportare și de creare a log-urilor sau de a alege din peste 50 de template-uri disponibile pentru fiecare eveniment de sistem/client Aveți opțiunea de a stabili pragul pentru notificările de eveniment.	Vă ajută să identificați rapid problemele potențiale, simplifică task-urile de monitorizare a rețelei și vă asistă în raportarea de conformitate. Stabilește priorități și termene pentru notificări: sunt trimise imediat sau sunt colectate în loturi și apoi expediate la intervale prestabilite de timp. Crează reguli de notificare, ordonează în funcție de cantitatea de informații afișată și expediază fiecare eveniment de notificare utilizând email, syslog, SNMP trap sau fișiere text.
Rapoarte de Control al Dispozitivelor Portabile	Rapoartele de control al dispozitivelor generează înregistrări complete pentru toate evenimentele care sunt legate de dispozitivele portabile de stocare și transfer al datelor.	Log-urile detaliate despre mediile amovibile și modul de utilizare al dispozitivelor simplifică raportarea de conformitate, fiind ușor de realizat în mod centralizat. Rapoartele includ intervalul de timp, numele de utilizator, numele computerului, numele grupului, clasa dispozitivului, detaliile evenimentului și acțiunea pe care a declanșat-o automat.
Suport RSA enVision	Se integrează, via plug-in, cu instrumentul RSA enVision SIEM.	Suportul pentru RSA enVision asigură o integrare facilă cu acest instrument popular 3rd-party de tip SIEM.
ESET SysInspector	Execută o analiză în amănunt a endpoint-urilor pentru a identifica posibile riscuri de securitate.	Identifică toate procesele care rulează, software-ul instalat și configurația hardware pe toate endpoint-urile. Descoperă posibile riscuri de securitate prin compararea ultimelor două snapshot-uri executate la nivelul endpoint-ului.

Stabilitatea și viteza rețelei

CARACTERISTICĂ	CE ANUME FACE	CARE SUNT BENEFICIILE
Executare aleatorie a task-urilor	Vă permite să stabiliți punerea în aplicare a task-urilor de securitate la intervale de timp aleatoare.	Stabilește un interval de timp în care task-urile se pot executa aleator. Minimizează efectul negativ pe care îl pot avea acțiunile derulate simultan pe endpoint-uri, precum blocarea de resurse, în cazul drive-urilor din rețea, datorită scanărilor concomitente, astfel încât utilizatorii finali să nu experimenteze încetiniri ale performanței.
Rollback-ul Update-urilor	Aveți posibilitatea să restaurați, la o stare anterioară, versiunea modulelor de protecție și baza de semnături virale.	O cale de a adresa rapid incompatibilitățile sau orice nefuncționalități de sistem prin revenirea bazei de semnături virale și a versiunii modulului de securitate la o stare anterioară de funcționare, cu doar câteva clicuri. Puteți bloca actualizările în funcție de dorință - puteți opta pentru rollback temporar sau revenire manuală.
Amânarea Update-urilor	Oferă opțiunea să descărcați actualizările din 3 servere specializate: pre-release (utilizatori beta), regular release (utilizatori obișnuiți) și postpone release (aproximativ 12 ore după lansarea de tip regular)	Ajută la asigurarea unor actualizări lipsite de probleme, cu accent pus pe continuitatea operațiunilor. Aplică actualizările antivirus mai întâi sistemelor care nu sunt critice, apoi celor care au statut critic în rețea, cu opțiunea de ștergere a cache-ului de actualizare.
Server Local de Update	Salvează lățimea de bandă a companiei, descărcând update-urile o singură dată, către un server mirror local. Se oferă suport pentru canalul de comunicare securizat (HTTPS).	Prin utilizarea ESET Remote Administrator drept server mirror de update pentru endpoint-uri se conservă lățimea benzii de Internet. Pentru forța de lucru mobilă din companie se definește un profil secundar de actualizare pentru ca endpoint-urile să realizeze update-ul conectându-se direct la serverele ESET atunci când serverul de actualizare intern nu este disponibil. Se oferă suport pentru HTTPS.
Acces rapid al Bazei de Date	Asigură un acces optimizat și neîntrerupt la baza de date care conține informațiile legate de securitatea endpoint-urilor.	Performanța optimizată a bazei de date vă asigură o productivitate ridicată prin agregarea datelor culese de la endpoint-uri și generarea rapidă a rapoartelor.
Curățarea Bazei de Date	Aveți posibilitatea de a stabili atributele de stocare a bazei de date precum perioada de timp și pragul valorii pentru intrările care sunt păstrate în baza de date.	Optimizează baza de date pentru un răspuns rapid și o dimensiune redusă.
Suport Microsoft NAP	Instalează, la nivel de server, plug-in-ul System Health Validator (SHV), iar la nivel de client, SystemHealth Agent (SHA). Oferă acces complet la rețea pentru clienții conformi și acces limitat sau acces blocat pentru clienții care nu respectă conformitatea.	Vă ajută să verificați respectarea conformității și să monitorizați rețeaua (disponibilitatea /statusul). Plug-in-ul SHA colectează informații despre client și le comunică în relația cu serverul în interiorul NAP framework. Stabilește cerințele de conformitate ale clientului precum: vechimea bazei virale, versiunea produsului antivirus, nivelul de protecție, disponibilitatea protecției antivirus și starea firewall-ului. Aduce endpoint-urile la conformitate, impunând actualizarea bazei de date.