



SERVER SECURITY

Protejează serverele, utilizând o soluție
multistratificată de încredere, fără compromisuri

CYBERSECURITY
EXPERTS ON YOUR SIDE



Ce este o soluție de securitate a fișierelor?

Un produs de securitate a fișierelor este conceput pentru a proteja serverele centrale ale unei organizații în fața amenințărilor. Acest produs trebuie instalat pe orice server nespecializat pentru a vă asigura că resursele organizaționale nu sunt infectate. În zilele noastre companiile își supun infrastructurile unor riscuri specifice, permițându-le utilizatorilor să salveze fișierele într-o rețea comună, dar fără a proteja de obicei accesul fișierelor compromise, malițioase. Un singur utilizator care salvează unui fișier infectat pe o unitate de rețea poate provoca instantaneu o reacție în lanț prin care, în anumite scenarii de infectare, fișierele organizației pot să devină inaccesibile.

ESET Server Security oferă protecție avansată serverelor generale, fișierelor stocate în rețea și serverelor multifuncționale. Soluția se asigură că serverele rămân stabile și lipsite de conflicte, păstrând ferestrele de mentenanță și restarturile la un nivel minim pentru a nu perturba continuitatea afacerii.

De ce o soluție de securitate a fișierelor?

RANSOMWARE

Ransomware-ul a fost o preocupare constantă pentru industriile din întreaga lume încă de la apariția Cryptolocker în 2013. În ciuda faptului că ransomware-ul a existat de mult mai mult timp, nu a fost de la început amenințarea majoră care preocupă astăzi companiile. Cu toate acestea, un singur incident ransomware poate bloca acum complet o afacere prin criptarea fișierelor importante sau necesare. Atunci când o companie se confruntă cu un atac ransomware își poate da seama rapid că backup-urile pe care le deține nu sunt suficient de recente, așa că deseori oamenii responsabili de business încep să se gândească la opțiunea de a plăti răscumpărarea.

La nivel de servere, ransomware-ul poate fi o problemă și mai acută din cauza riscului ca utilizatorii să salveze fără să își dea seama cod ransomware pe o unitate de stocare din rețea. ESET Server Security oferă multiple nivele de apărare nu doar pentru a preveni apariția ransomware, dar și pentru a detecta dacă acesta a existat vreodată în cadrul unei organizații. Prevenția și detecția ransomware este foarte importantă pentru că de fiecare dată când cineva plătește o răscumpărare criminalii cibernetici devin și mai determinați să atace din nou.

ATACURI DIRECȚIONATE ȘI BREȘE DE DATE

Peisajul de securitate cibernetică de astăzi evoluează constant, apărând noi metode de atac și amenințări neidentificate încă de nimeni. Când are loc un atac sau o breșă de date, organizațiile sunt de obicei surprinse de faptul că securitatea lor a fost compromisă sau nu au fost decât târziu conștienți de faptul că se confruntă cu un atac. După ce incidentul este descoperit în cele din urmă, organizațiile implementează apoi reactiv metode de atenuare, pentru a împiedica un al doilea atac. Cu toate acestea, această măsură nu îi protejează pe deplin, pentru că atacatorii își schimbă regulat vectorii de atac.

Soluțiile ESET Server Security utilizează informații Threat Intelligence despre amenințări pe baza prezenței lor globale, pentru a prioritiza și bloca eficient cele mai noi amenințări, înainte de apariția lor oriunde altundeva în lume. Serverele sunt de obicei una dintre țintele cele mai căutate, întrucât conțin de regulă date sensibile sau confidentiale. Pentru o mai bună protecție împotriva acestor tentative de intruziune, soluțiile ESET Server Security oferă detecție bazată pe cloud pentru a răspunde rapid în cazul unei potențiale identificări ratate, fără a fi nevoie să se aștepte o nouă actualizare.

ATACURI FILELESS

Amenințările mai noi, din categoria malware-ului fileless, persistă exclusiv în memoria computerului, fiind imposibil de detectat în timpul scanării fișierelor. Unele atacuri fileless se vor folosi de aplicațiile deja instalate, ce sunt integrate în sistemul de operare, pentru a face mai dificilă detecția unei sarcini payload rău intenționate. De exemplu, utilizarea PowerShell în decursul acestor atacuri este o practică foarte frecventă.

Soluțiile ESET Server Security pun la dispoziție nivele distincte de detecție pentru a identifica aplicațiile malformate sau deturnate și a le proteja împotriva atacurilor fileless. Soluțiile ESET File Security au fost întotdeauna adapteze să reziste și să rămână cu un pas înaintea celor mai noi amenințări malware.

Soluțiile ESET oferă straturi de protecție menite nu doar să prevină intruziunile malware, dar și să descopere dacă a existat vreodată o astfel de amenințare în cadrul unei organizații.

Când are loc un atac sau o breșă de date, organizațiile sunt de obicei surprinse de faptul că securitatea lor a fost compromisă sau nu sunt complet conștienți de faptul că se confruntă cu un atac.

Amenințările mai noi, din categoria malware fileless, există exclusiv în memoria computerului, fiind imposibil de detectat în timpul scanării fișierelor.

“ESET oferă de ani buni soluția de securitate în care avem încredere. Fac tot ce trebuie să facă, iar noi nu trebuie să ne facem griji pentru nimic. Pe scurt, ESET înseamnă: fiabilitate, calitate și servicii.”

—Jos Savelkoul, Team Leader al Departamentului ICT; Spitalul Zuyderland, Olanda; 10.000+ stații



OneDrive



Office 365



Azure

vmware®

Soluțiile ESET Server Security

ESET Server Security pentru Microsoft Windows Server

ESET Server Security pentru Linux

ESET Server Security pentru Microsoft Azure

Diferența ESET

PROTECȚIE MULTI-STRATIFICATĂ

La ESET combinăm tehnologia de detecție multistrat, machine learning-ul și expertiză umană pentru a le oferi clienților cel mai bun nivel de protecție posibil. Tehnologia noastră este îmbunătățită constant și adaptată pentru a oferi cel mai bun echilibru între detecție, rezultate fals pozitive și performanță.

SUPPORT TRANS-PLATFORMĂ

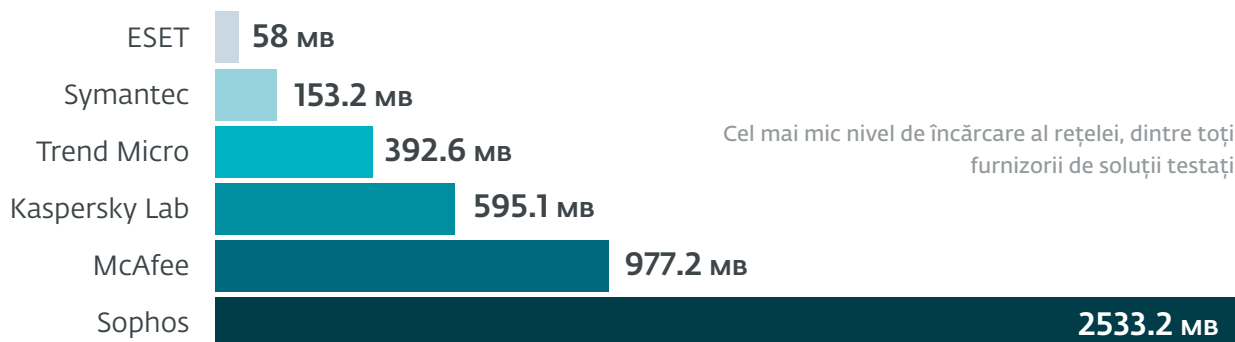
Soluțiile ESET Server Security sunt compatibile cu mai multe sisteme de operare și platforme, inclusiv Windows Server, Office 365 OneDrive, Linux/FreeBSD și Microsoft Azure. Soluțiile ESET pot fi gestionate cu ușurință din fața unui singur panou unificat de instrumente.

PERFORMANȚĂ DE NEEGALAT

Deseori, una din preocupările majore ale unei organizații este impactul pe care îl are soluția de protecție endpoint asupra performanței. Produsele ESET continuă să exceleze la nivel de performanță și câștigă în testele terților, care dovedesc cât de redus este impactul soluțiilor noastre asupra sistemelor.

PREZENȚĂ GLOBALĂ

ESET are birouri în 22 de țări din întreaga lume, laboratoare de cercetare și dezvoltare în 13 state și o prezență globală, în peste 200 de țări și teritorii. Acest lucru ne ajută să colectăm date pentru a opri eficient codul malware înainte ca acesta să se răspândească pe tot globul, dar și să prioritizăm dezvoltarea de noi tehnologii bazate pe cele mai recente amenințări sau pe vectorii noi de atac.



Sursa: AV-Comparatives: Network Performance Test, Business Security Software

"...cel mai clar testimonial? Iată ce indică statisticile din biroul nostru de asistență: după ce am implementat ESET, colegii de la suport tehnic nu mai înregistrează niciun apel - legate de probleme antivirus sau incidente malware!"

— Adam Hoffman, Manager de infrastructură IT; Mercury Engineering, Irlanda; 1.300 de stații

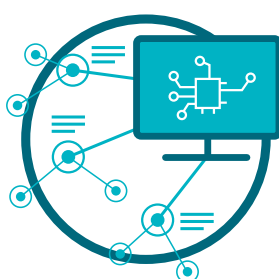
Tehnologia

Produsele și tehnologiile noastre se bazează pe 3 piloni



ESET LIVEGRID®

Ori de câte ori se descoperă o potențială amenințare zero-day așa cum este ransomware-ul, fișierul este trimis către LiveGrid®, sistemul nostru de protecție anti-malware bazat pe cloud, unde amenințarea este lansată, iar comportamentul său este monitorizat. Rezultatele sunt trimise către toate stațiile endpoint la nivel global, în câteva minute, fără a fi nevoie de actualizări.



MACHINE LEARNING

Folosește puterea combinată a rețelelor neurale și algoritmi selectați manual pentru etichetarea corectă a eșantioanelor primite în curate, potențial nedorite sau rău intenționate.



EXPERTIZA UMANĂ

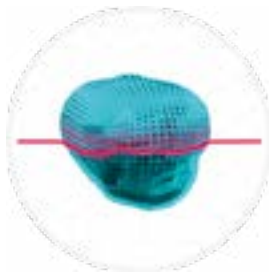
Cercetătorii de securitate de talie mondială împărtășesc know-how de elită pentru a oferi cea mai bună tehnologie threat intelligence.

Un singur strat de apărare nu este suficient în contextul unui peisaj cibernetic în continuă evoluție. Toate produsele de securitate ESET au capacitatea de a detecta malware-ul înainte, în timpul și după execuție. Concentrându-ne pe mai mult decât pe o singură parte a ciclului de viață al malware-ului, putem oferi cel mai înalt nivel de protecție posibil.



MACHINE LEARNING

Toate produsele ESET Endpoint utilizează învățarea automatizată în plus față de utilizarea celorlalte straturi de apărare, încă din 1997, până în prezent. ESET folosește în prezent tehnologia machine learning în combinație cu toate celelalte straturi de protecție. În mod specific, învățarea automatizată este utilizată sub formă de rețele consolidate și rețele neurale.



SCANER AVANSAT DE MEMORIE

Monitorizează comportamentul unui proces rău intenționat și îl scanează odată ce acesta se dezvoltă în memorie. Malware-ul fileless rulează fără a avea nevoie de componente persistente în sistemul de fișiere, ce pot fi detectate în mod convențional. Numai scanarea în memorie poate detecta și opri cu succes astfel de atacuri rău intenționate.



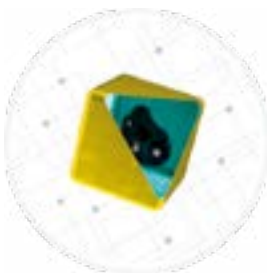
RANSOMWARE SHIELD

ESET Ransomware Shield este un strat suplimentar care protejează utilizatorii de ransomware. Această tehnologie monitorizează și evaluează toate aplicațiile executate pe baza comportamentului și reputației acestora. Acesta este conceput pentru a detecta și a bloca procesele care seamănă cu comportamentul ransomware-ului.



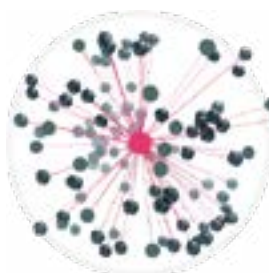
EXPLOIT BLOCKER

Monitorizează aplicațiile care sunt cel mai des exploatare de atacatori (browsere, cititoare de documente, clienți de e-mail, Flash Player, Java și altele) și în loc de a ținti doar identificatorii CVE se concentrează pe tehnicile de exploatare. Atunci când este declanșată, amenințarea este blocată imediat.



SANDBOXING INTEGRAT

Malware-ul de astăzi este adesea disimulat cât mai avansat pentru a trece nedetectat cât mai mult timp posibil. Ca să înțelegem cât mai bine ce se petrece și pentru a identifica comportamentul real din spatele codului aparent legitim, folosim sistemul de sandbox integrat în produs. Cu ajutorul acestei tehnologii, soluțiile ESET imită diferite componente ale hardware-ului și software-ului, pentru a executa o mostră suspectă într-un mediu virtual izolat.



PROTECȚIE BOTNET

Protecția Botnet ESET detectează comunicarea specifică folosită de rețelele botnet și, în același timp, identifică procesele rău intenționate. Orice modalitate de comunicare periculoasă este blocată și raportată utilizatorului.



PROTECȚIA LA ATAC A REȚELEI

Această extensie a tehnologiei firewall îmbunătățește detectarea vulnerabilităților cunoscute la nivel de rețea. Constituie un strat important de protecție împotriva răspândirii malware-ului, a atacurilor derulate în rețea și a exploatării vulnerabilităților pentru care un patch nu a fost încă lansat sau propus spre implementare.



SEMNĂTURILE ADN

Tipurile de semnături ce variază de la hash-uri foarte specifice la semnăturile ADN ESET, care reprezintă definiții complexe ale comportamentului și ale caracteristicilor malware. În timp ce codurile malițioase pot fi modificate ușor sau disimulate de către atacatori, comportamentul obiectelor nu poate fi schimbat atât de ușor, iar semnăturile ADN ESET sunt proiectate tocmai pentru a beneficia de acest principiu.



DETECȚIE COMPORTAMENTALĂ - HIPS

ESET Host-Based Intrusion Prevention System monitorizează activitatea sistemului și utilizează un set predefinit de reguli pentru a detecta un comportament suspect al sistemului. Mai mult decât atât, mecanismul de autoapărare HIPS oprește procesul de desfășurare al unei activități dăunătoare.



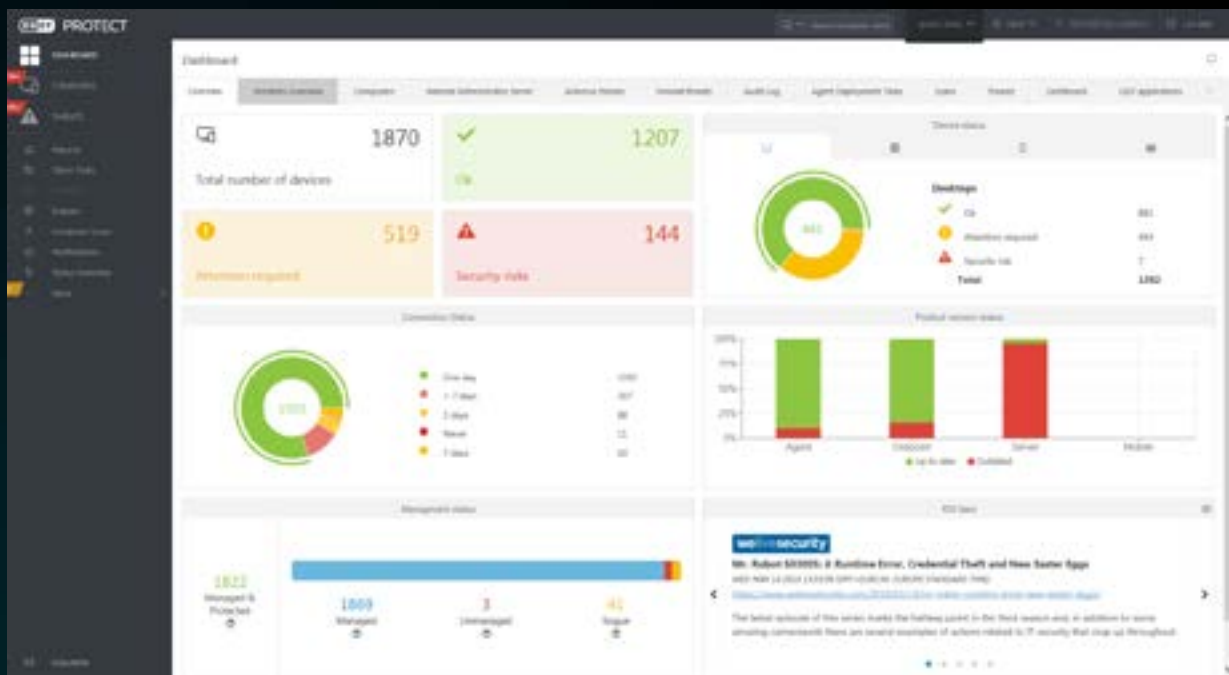
AMSI/SCRIPT SCANNING

Soluțiile ESET utilizează interfața de scanare Antimalware (AMSI) pentru a oferi protecție îmbunătățită împotriva malware-ului pentru utilizatori, date, aplicații și volumul de lucru. În plus, folosește interfața de servicii protejată, care este un nou modul de securitate încorporat în Windows, care permite doar încărcarea codului de încredere, semnat și protejarea mai bună împotriva atacurilor de injectare a codului.

“Cel mai important lucru care se remarcă este avantajul său tehnic puternic față de alte produse de pe piață. ESET ne oferă securitate sigură, ceea ce înseamnă că pot lucra la orice proiect în orice moment știind că există soluții de protecție de încredere care protejează sistemele noastre.”

— Fiona Garland, Business Analyst Group IT; Mercury Engineering, Ireland;

1.300 stații



ESET PROTECT

Toate soluțiile endpoint ESET sunt gestionate dintr-o singură consolă cloud cu un panou unificat de instrumente, ESET PROTECT, asigurând vizibilitate completă asupra rețelei.

“Când am descoperit ESET, am știut că este alegerea corectă: tehnologie de încredere, detecție robustă, prezență locală și suport tehnic excelent, exact ce aveam nevoie.”

— Ernesto Bonhoure, Manager de infrastructură IT; Spitalul Alemán, Argentina,
1.500+ stații



Cazuri de utilizare

Fileless malware

Caz de utilizare: Malware-ul care nu se bazează pe fișiere este o amenințare relativ nouă și din cauza faptului că persistă doar în memoria de lucru a sistemului necesită o abordare diferită pentru identificare, față de malware-ul tradițional bazat pe fișiere.

SOLUȚIE

- ✓ Tehnologia ESET unică Advanced Memory Scanner, ce protejează împotriva acestui tip de amenințare prin monitorizarea comportamentului proceselor rău intenționate și scanarea lor odată ce apar în memorie.
- ✓ Dacă ESET Server Security nu este sigur de o potențială amenințare, are capacitatea de a încărca eșantionul în mediul de sandbox din cloud, Dynamic Threat Defense, pentru a decide dacă mostra este rău intenționată.
- ✓ Dacă se confirmă o amenințare, reduce timpul viitor de analiză prin încărcarea amenințării în ESET Threat Intelligence, care primește informații despre mecanismul de funcționare al eșantionului.

Amenințări de tipul zero-day

Caz de utilizare: Amenințările de tipul zero-day reprezintă o preocupare majoră pentru companii, acestea având dificultăți semnificative în a se proteja față de forme de atac nemaiîntâlnite până acum.

SOLUȚIE

- ✓ Soluțiile Endpoint ESET folosesc euristica și machine learning-ul, ca parte a abordării multistrat pentru a preveni și a proteja împotriva malware-ului nemaivăzut până acum.
- ✓ 13 laboratoare globale de cercetare și dezvoltare vă ajută să răspundeți repede atacurilor malware, după prima lor incidență, oriunde pe glob.
- ✓ Vă puteți baza pe sistemul de protecție anti-malware Cloud de la ESET pentru vă proteja împotriva noilor amenințări, fără a mai fi nevoie să așteptați actualizări de detecție.

Ransomware

Caz de utilizare: Unele companii doresc asigurări suplimentare cu privire la protecția împotriva atacurilor Ransomware.

SOLUȚIE

- ✓ Network Attack Protection are capacitatea de a împiedica infectarea cu ransomware a unui sistem, prin oprirea exploit-urilor la nivelul rețelei.
- ✓ Apărarea noastră multistratificată are caracteristici de tipul sandbox și în interiorul produsului, care au capacitatea de a detecta malware-ul.
- ✓ Sistemul de protecție anti-malware bazat pe Cloud al ESET vă protejează împotriva noilor amenințări, fără a fi nevoie să așteptați actualizările de detecție.
- ✓ Toate produsele conțin protecție Ransomware Shield pentru a se asigura companiile sunt protejate față de criptarea nedorită a fișierelor.
- ✓ Dacă ESET Server Security nu este sigur de o potențială amenințare, acesta are capacitatea de a încărca eșantionul în Cloud Sandbox ESET, Dynamic Threat Defense, pentru a lua decizia de cea mai înaltă calitate dacă ceva este rău intenționat.

Despre ESET

De mai bine de 30 de ani, ESET® se ocupă cu dezvoltarea de software și servicii de securitate IT, oferind o protecție instantanee și completă împotriva amenințărilor cibernetice aflate în continuă dezvoltare, pentru companii și clienți din întreaga lume.

ESET este o companie privată, fără datorii și împrumuturi, ce are libertatea de a asigura o protecție absolută, fără compromisuri, pentru toți clienții.

ESET ÎN CIFRE

110m+

utilizatori,
global

400k+

clienți
business

200+

țări și
teritorii

13

centre
globale R&D

CÂȚIVA DINTRE CLIENȚII NOȘTRI



protejat de ESET încă din 2017,
peste 14.000 stații

Canon

Canon Marketing Japan Group

protejat de ESET încă din 2016,
peste 9000 stații



protejat de ESET încă din 2016,
peste 4.000 casuțe e-mail



Partener de securitate ISP încă din
2008 - bază de peste 2 milioane
clienți

De ce să alegeți ESET



ESET este conform cu [ISO/IEC 27001:2013](#), un standard de securitate recunoscut la nivel internațional și aplicabil în implementarea și gestionarea securității informațiilor. Certificarea este acordată de către un organism terț de certificare acreditat [SGS](#) și demonstrează conformitatea deplină a ESET cu cele mai bune practici din industrie.

PREMIILE ESET



RECUNOAȘTERI DIN PARTEA INDUSTRIEI

Gartner

ESET a fost numit unicul Challenger în Raportul Gartner Magic Quadrant pentru Platforme de Protecție Endpoint din 2019,

FORRESTER®

ESET a fost evaluat ca Strong Performer în Forrester Wave (TM): Endpoint Security Suites, T3 2019.

THE RADICATI GROUP, INC. A TECHNOLOGY MARKET RESEARCH FIRM

ESET a fost numit Top Player în raportul Radicati Endpoint Security 2019 pentru două criterii principale: funcționalitate și viziune strategică.

Gartner Inc, Cadranul magic pentru platformele de protecție endpoint, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. Gartner nu susține niciun furnizor, produs sau serviciu prezentat în publicațiile despre cercetările sale, și nu sfătuiește utilizatorii de tehnologie să aleagă doar acei furnizori care au rating-urile cele mai bune sau alte nominalizări. Publicațiile despre cercetările Gartner se compun din opiniile organizației de cercetare a companiei Gartner și nu ar trebui interpretate ca situații de fapt. Gartner nu oferă nicio garanție expresă sau implicată cu privire la această cercetare/ investigație/studiu, inclusiv orice garanții de vandabilitate sau adevărate pentru un scop special.

Gartner Peer Insights este o platformă gratuită care colectează evaluări și recenzii, concepută pentru factorii de decizie din segmentul enterprise care sunt responsabili de achizițiile de software și servicii conexe. Recenziile sunt procesate și moderate într-un regim strict, pentru a se asigura autenticitatea informației. Recenziile Gartner Peer Insights constituie opiniile subiective ale unor utilizatori finali individuali, pe baza propriilor experiențe, și nu reprezintă opiniile Gartner sau ale afiliaților săi.



ENJOY SAFER
TECHNOLOGY™