



ENDPOINT SOLUTIONS

Protecție puternică multistratificată pentru
desktop-uri, laptop-uri și smartphone-uri

Progress. Protected.



Ce reprezintă o **Platformă de Protecție Endpoint?**

Endpoint Protection Platform (EPP) este o soluție implementată pe dispozitivele endpoint pentru a preveni atacurile malware bazate pe fișiere, pentru a detecta o activitate rău intenționată și pentru investiga și remedia incidentele și alertele dinamice de securitate.

Soluțiile ESET Endpoint Protection se bazează pe o abordare multistratificată, care utilizează multiple tehnologii care funcționează într-un echilibru dinamic, având capacitatea de a echilibra în mod constant performanța,

De ce este nevoie de solutii de **Endpoint Protection**?

RANSOMWARE

Atacurile de tip ransomware au fost o preocupare constantă pentru industrie la nivel mondial încă din 2013, când a apărut Cryptolocker. În ciuda faptului că ransomware-ul există de mult mai mult timp, nu a fost considerat niciodată o amenințare majoră de către companii. Cu toate acestea, acum o singură incidență a ransomware poate face cu ușurință o afacere inoperabilă prin criptarea fișierelor importante sau a celor minime necesare. Când o afacere suferă un atac ransomware, își dă repede seama că backup-urile pe care le are nu sunt suficiente de recente, așadar ajunge în poziția de a plăti suma pretinsă ca și răscumpărare.

Soluțiile ESET Mail Security oferă un strat suplimentar de apărare pentru a preveni ca programele ransomware să ajungă la cutiile poștale ale utilizatorilor. În plus, capacitatea pentru a bloca anumite tipuri de fișiere atașate sau chiar toate tipurile de fișiere atașate limitează expunerea organizației la ransomware

ATACURI CU ȚINTĂ PRECISĂ ȘI BREȘE DE ÎNCĂLCARE A DATELOR

Peisajul securității cibernetice de astăzi este în continuă evoluție cu metode noi de atac și amenințări nemaivăzute până acum. Când are loc un atac sau o breșă de încălcare a protecției datelor, organizațiile sunt de obicei surprinse că sistemele lor de apărare au fost compromise sau nici măcar nu sunt conștiente că atacul a avut loc. După ce atacul este în sfârșit descoperit, organizațiile implementează apoi în mod reactiv măsuri de remediere pentru a împiedica repetarea unui astfel de scenariu. Cu toate acestea, acest lucru nu îi protejează de următorul atac, care poate folosi un alt vector nou-nouț.

Soluțiile ESET Server Security folosesc instrumente Threat Intelligence bazate pe prezența lor la nivel global ca să prioritizeze și să blocheze eficient cele mai noi amenințări înainte ca acestea să fie răspândite oriunde altundeva în lume. Serverele sunt de obicei o țintă mai căutată deoarece de cele mai multe ori acestea conțin date sensibile sau confidențiale. Pentru a vă proteja mai bine împotriva

acestor atacuri în creștere, soluțiile ESET Server Security sunt bazate pe actualizări în cloud, pentru a răspunde rapid în cazul unei detecții ratate fără a trebui să așteptați noua actualizare oficială.

ATACURI FILELESS

Amenințările mai noi, numite fileless malware, există exclusiv în memoria computerului, făcându-l imposibil de detectat pentru soluțiile de protecție cu scanare pe bază de fișiere. Ba chiar mai mult, unele atacuri fără fișiere vor folosi aplicațiile instalate în prezent care sunt încorporate în sistemul de operare pentru face și mai grea detectarea grupului malițios de date. De exemplu, în aceste atacuri este foarte frecventă utilizarea PowerShell.

Soluțiile ESET Server Security conțin reguli care detectează aplicațiile compromise și malformate pentru protejarea împotriva atacurilor fileless. Alte alternative sunt scanerile dedicate, pentru a verifica constant memoria pentru orice element suspect. Indiferent de situație, produsele File Security au fost mereu provocate să încerce să fie cu un pas înaintea celor mai noi malware.

Soluțiile ESET de protecție endpoint oferă niveluri de apărare nu doar pentru a preveni ransomware, dar și pentru a detecta existența acestora într-o organizație.

Când are loc un atac sau o breșă de încălcare a protecției datelor, organizațiile sunt de obicei surprinse că sistemele lor de apărare au fost compromise sau nici măcar nu sunt conștiente că atacul a avut loc

Amenințările mai noi, numite fileless malware, există exclusiv în memoria computerului, făcându-l imposibil de detectat pentru soluțiile de protecție cu scanare pe bază de fișiere.

„ESET a fost soluția noastră de securitate fiabilă de ani de zile. Face ceea ce are de făcut; nu trebuie să îți faci griji. Pe scurt, ESET înseamnă: fiabilitate, calitate și asistență.”

Jos Savelkoul, Team Leader în Departamentul ICT, din Spitalul Zuyderland, Olanda
- 10.000+ de stații



vmware®

Soluțiile ESET de protecție endpoint

ESET Endpoint Security pentru Windows/macOS/Android

ESET Endpoint Antivirus pentru Windows/macOS/Linux

ESET Server Security pentru Windows Server/Linux/Azure

ESET MDM pentru iOS și iPadOS

Product features and functionality may differ, depending on operating system.

Diferența ESET

PROTECȚIE MULTISTRATIFICATĂ

ESET combină tehnologia multistratificată, învățarea automatizată și expertiza umană pentru a oferi clienților săi cel mai bun nivel de protecție posibil. Tehnologiile ESET se adaptează și se schimbă în mod constant pentru a oferi cel mai bun echilibru între detecție, rezultate fals pozitive și performanță

SUPORT MULTIPLATFORMĂ

Soluțiile ESET Server Security acceptă mai multe sisteme de operare și platforme, inclusiv Windows Server, Office365 OneDrive, Linux/FreeBSD și Microsoft Azure. toate soluțiile ESET pot fi complet gestionate dintr-un singur panou de control.

PERFORMANȚĂ FĂRĂ EGAL

De nenumărate ori, cea mai mare preocupare a unei organizații este impactul asupra performanței al unei soluții de protecție endpoint. Produsele ESET continuă să exceleze în domeniul performanței și dovedesc în cadrul testelor independente cât de noninvazive sunt soluțiile pentru sistemele de endpoint-uri protejate.

PREZENȚĂ LA NIVEL MONDIAL

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 ca să prioritizăm dezvoltarea de noi tehnologii bazate pe cele mai recente amenințări sau pe vectorii noi de atac.

„... cea mai bună mărturie? Statisticile de la biroul nostru de asistență: după ce am introdus ESET, echipa noastră de asistență nu mai primește niciun apel – nu trebuie să se mai ocupe de nicio problemă legată de niciun antivirus sau malware!”

Adam Hoffman, Manager de Infrastructură IT, compania Mercury Engineering, Irlanda - 1.300 de stații

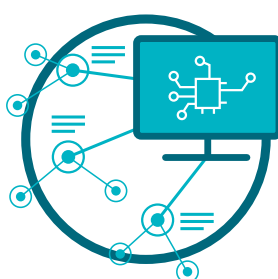
Tehnologia ESET

Produsele și tehnologiile noastre se bazează pe 3 piloni



ESET LIVEGRID®

Ori de câte ori o amenințare zero-day apare, de exemplu atacuri ransomware, fișierul este trimis către sistemul de protecție împotriva malware, bazat pe cloud - LiveGrid®, unde amenințarea este executată și comportamentul monitorizat. Rezultatele testului sunt apoi furnizate global tuturor endpoint-urilor, în doar câteva minute, fără a necesita actualizări.



MACHINE LEARNING

Utilizează puterea combinată a rețelei neuronale și a algoritmilor aleși cu mare atenție pentru a eticheta corect probele primite ca fiind curate, potențial nedorite sau malițioase.



HUMAN EXPERTISE

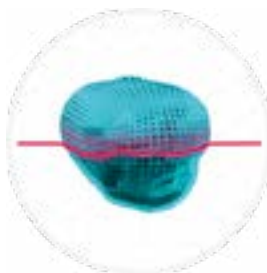
Cercetători de clasă mondială în domeniul securității împărtășesc informații și know-how de elită, pentru a asigura fără încetare cea mai bună asistență threat intelligence.

Un singur nivel de apărare nu este suficient pentru peisajul amenințărilor în continuă evoluție. Toate produsele de securitate ESET au capacitatea de a detecta programele malware înaintea execuției, în timpul execuției și după execuție. Concentrându-se pe mai mult de o anumită parte a ciclul de viață al malware-ului, soluțiile ESET pot oferi cel mai înalt nivel de protecție posibil.



MACHINE LEARNING

Toate produsele ESET endpoint au folosit învățarea automatizată pe lângă toate celelalte niveluri de protecție încă din 1997. ESET utilizează în prezent învățarea automatizată ca un nivel suplimentar de protecție, complementar cu cele de bază. În mod specific, tehnologia machine learning este utilizată sub formă de output consolidat și rețele neuronale.



SCANNER DE MEMORIE AVANSAT

ESET Advanced Memory Scanner monitorizează comportamentul unui proces malițios și îl scanează odată ce se dezvăluie în memoria de sistem. Fileless malware funcționează fără a avea nevoie de componente persistente în sistemul de fișiere, care pot fi ușor detectate în mod convențional. Numai prin scanarea memoriei puteți să descoperiți și să opriți cu succes astfel de atacuri rău intenționate.



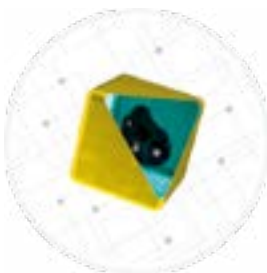
RANSOMWARE SHIELD

ESET Ransomware Shield este un strat suplimentar pentru protejarea utilizatorilor de ransomware. Această tehnologie monitorizează și evaluează toate aplicațiile executate pe baza analizei asupra comportamentului și reputației lor. Este conceput să detecteze și să blochează procesele care se seamănă cu comportamentul de ransomware.



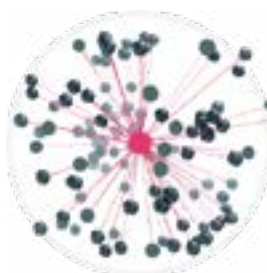
EXPLOIT BLOCKER

ESET Exploit Blocker monitorizează aplicațiile predispuse la a fi exploatare (browsere, cititoare de documente, clienți de e-mail, Flash, Java și multe altele), și în loc să țintească doar anumiți identificatori CVE, se concentrează pe tehnicile de exploatare. Când este declanșată, amenințarea este blocată imediat pe dispozitiv.



SANDBOX ÎNCORPORAT

Malware-ul actual este adesea foarte ascuns și încearcă să se sustragă cât mai mult posibil de la depistare. Pentru a scana acestea și pentru a identifica adevăratul comportament ascuns sub suprafață, folosiți opțiunea de sandbox încorporată în produs. Cu ajutorul acestei tehnologii, soluțiile ESET emulează diferite componente hardware și software pentru a executa un eșantion suspect într-un mod mediu virtualizat izolat.



PROTECȚIE BOTNET

ESET Botnet Protection detectează comunicarea malițioasă folosită de botnet și, în același timp, identifică procesele ofensatoare. Orice comunicare malițioasă detectată este blocată și raportată către utilizator.



PROTECȚIA LA ATAC A REȚELEI

Această tehnologie îmbunătățește detectarea vulnerabilităților cunoscute la nivel de rețea. Ea constituie un alt nivel important de protecție împotriva răspândirii malware, a atacurilor efectuate în rețea și a exploatării de vulnerabilități pentru care nu a fost încă eliberat sau implementat un patch.



BROWSER SIGUR

Conceput pentru a proteja activele organizației cu un nivel special de protecție care se concentrează pe browser, ca instrument principal utilizat pentru accesarea datelor critice în perimetrul intranetului și în cloud. Secure Browser oferă protecție îmbunătățită a memoriei pentru procesul browserului, împreună cu protecția tastaturii și le permite administratorilor să adauge adrese URL pentru a fi protejate de aceasta.



DETECȚIA COMPORTAMENTALĂ – HIPS

ESET HIPS (Host-Based Intrusion Prevention System) monitorizează activitatea sistemului și utilizează un set predefinit de reguli pentru a recunoaște comportamentul suspect al sistemului. În plus, mecanismul de autoapărare HIPS oprește procesul ofensator din desfășurarea activității dăunătoare.



SCANNER UEFI

ESET este primul furnizor de securitate endpoint care adaugă un strat dedicat soluției sale, prin care protejează Unified Extensible Firmware Interface (UEFI). ESET UEFI Scanner verifică și impune securitatea mediului preboot și este proiectat pentru a monitoriza integritatea firmware-ului. Dacă este detectată o modificare, aceasta notifică utilizatorul.

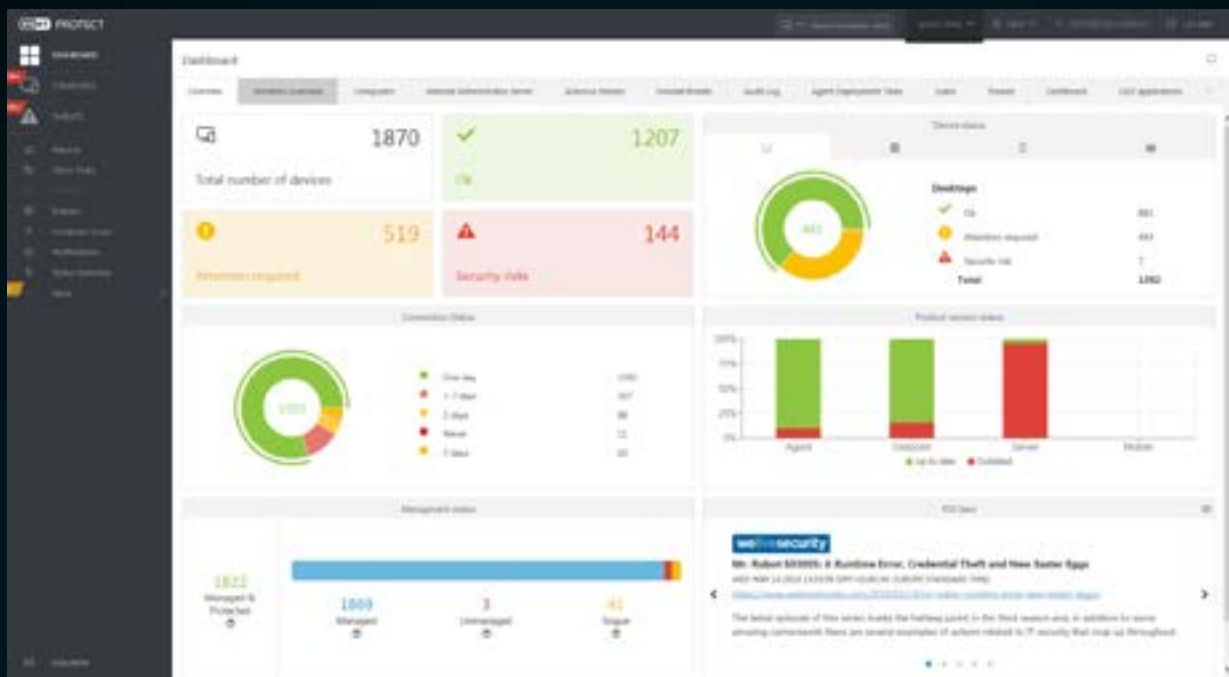


BRUTE FORCE ATTACK PROTECTION

O caracteristică de securitate care protejează dispozitivele împotriva atacurilor de ghicire a parolilor și încercărilor ilegite de stabilire a unei conexiuni de la distanță. Protecția poate fi configurată cu ușurință printr-o politică prestabilită direct din consolă, iar excluderile pot fi create atunci când ceva este blocat, dar nu ar trebui să fie.

„Cel mai important lucru prin care se remarcă este avantajul său tehnic puternic față de alte produse de pe piață. ESET ne oferă securitate de încredere, astfel pot lucra pentru orice proiect, în orice moment, știind că dispozitivele noastre sunt protejate 100%.”

Fiona Garland, Business Analyst Group IT
pentru compania Mercury Engineering, Ireland
- 1.300 de stații



ESET PROTECT

Toate soluțiile ESET de protecție endpoint sunt gestionate cu o singură consolă de management în cloud, ESET PROTECT, care asigură o imagine de ansamblu asupra rețelei dvs.

Cazuri de utilizare

Ransomware

Unele companii doresc asigurări suplimentare că vor fi protejate de atacurile ransomware. În plus, vor să se asigure că unitățile lor de rețea sunt la adăpost de criptarea malițioasă.

SOLUȚIE

- ✓ Network Attack Protection are capacitatea de a preveni infectarea cu ransomware-ul unui sistem prin oprirea exploit-urilor la nivel de rețea.
- ✓ Apărarea multistratificată conține un sandbox încorporat care are capacitatea de a detecta malware care încearcă să evite detectarea utilizând metode de derută.
- ✓ Folosiți sistemul ESET de protecție împotriva malware-ului în cloud pentru protecție automată împotriva noilor amenințări fără necesitatea de a aștepta următoarea actualizare de detectare.
- ✓ Toate produsele conțin protecție post-execuție în formă de Ransomware Shield pentru a se asigura că organizațiile sunt protejate de criptarea rău intenționată a fișierelor..

Fileless malware

Fileless malware este o amenințare relativ nouă iar existența ei doar la nivelul memoriei de sistem necesită o abordare diferită de malware-ul tradițional bazat pe fișiere.

SOLUȚIE

- ✓ O tehnologie unică ESET, Advanced Memory Scanner, protejează împotriva acestui tip de amenințare prin monitorizarea comportamentului proceselor malițioase și scanarea odată ce se dezvoltă în memorie.
- ✓ Reduceți timpul de colectare a datelor și de investigare prin încărcarea amenințării în ESET Threat Intelligence pentru a oferi informații despre modul în care funcționează.
- ✓ Tehnologia multistratificată, învățarea automatizată și expertiza umană oferă clienților noștri cel mai bun nivel de protecție posibil.

Credențiale furate

Atacurile de phishing și site-urile web false care imită organizațiile reale pentru a fura acreditările de conectare și datele financiare sunt în continuă creștere.

SOLUȚIE

- ✓ Produsele ESET endpoint sunt concepute pentru a proteja activele unei organizații cu un nivel unic de securitate, concentrându-se pe browser ca instrument principal pentru a accesa datele critice în perimetrul intranetului și în cloud.
- ✓ Caracteristica Secure Browser protejează datele sensibile în timpul navigării online.
- ✓ Cu un singur clic, administratorii pot alege să includă toate portalurile bancare și de plată și să decidă să protejeze sau nu browserul pentru anumite site-uri web

Atacuri de ghicire a parolelor

Remote Desktop Protocol (RDP) și Server Message Block (SMB) sunt vectori de atac atractivi care pot permite unui atacator să obțină controlul complet de la distanță al unui sistem.

SOLUȚIE

- ✓ Brute Force Attack Protection oferă o apărare eficientă împotriva atacurilor frontale asupra punctelor de acces de la distanță protejate cu parolă.
- ✓ Protejează dispozitivele împotriva atacurilor de ghicire a parolelor și încercărilor ilegite de stabilire a unei conexiuni de la distanță.
- ✓ Poate fi ușor configurat printr-o politică prestabilită direct din consolă; excluderile pot fi create atunci când ceva este blocat, dar nu ar trebui să fie.
- ✓ Sistem versatil: utilizatorii își pot adăuga propriile reguli sau le pot modifica pe cele existente.



„Când am descoperit ESET, am știut că este alegerea potrivită: tehnologie fiabilă, detecție robustă, prezență locală și asistență tehnică excelentă, tot ce aveam nevoie.”

Ernesto Bonhoure, Manager de Infrastructură IT pentru Spitalul German,
Argentina - 1.500+ de stații



Despre ESET

De mai bine de 30 de ani, ESET® dezvoltă software și servicii de securitate IT de top în industrie, oferind protecție instantanee și cuprinzătoare împotriva amenințărilor cibernetice care afectează companiile și consumatorii din întreaga lume.

ESET este un brand de 30 de ani, ESET® lider în dezvoltarea și distribuția de soluții de securitate IT de top în industrie, oferind protecție instantanee și cuprinzătoare împotriva amenințărilor cibernetice care afectează companiile și consumatorii din întreaga lume.

ESET ÎN CIFRE

1bn+
utilizatori,
global

400k+
clienți
business

200+
țări și
teritorii

13
centre
globale R&D

CÂȚIVA DINTRE CLIEȚII NOȘTRI



protejat de ESET încă
din 2017, peste 9.000
stații



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



protejat de ESET
încă din 2016, peste
32.000 stații



partener de securitate
ISP încă din 2008 - bază
de 2 milioane clienți

PREMIILE ESET



ESET a primit statutul APPROVED pentru soluțiile sale de protecție endpoint în testul AV-Comparative Business Security Test Decembrie 2021.



ESET este prezent constant în poziții de top pe platforma globală G2 de recenzii ale utilizatorilor iar soluțiile sale sunt apreciate de consumatori la nivel internațional.



Soluțiile ESET sunt recunoscute în mod regulat de firme de analiști de renume, fiind numit Sample Vendor în „The Forrester Tech Tide(TM): Zero Trust Threat Detection and Response, Q2 2021”.



Digital Security
Progress. Protected.

