



ENDPOINT SOLUTIONS

O tehnologie multistratificată, machine learning și o expertiză umană ce lucrează împreună într-un echilibru dinamic, totul pus la dispoziție de cel mai important vendor de securitate la nivel mondial din Uniunea Europeană



ENJOY SAFER
TECHNOLOGY™



30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION



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, detecția și numărul redus de rezultatele fals pozitive.

De ce e nevoie de solutii de Endpoint Protection?

RANSOMWARE

Ransomware-ul a reprezentat o preocupare constantă pentru industriile din întreaga lume încă de la Cryptolocker, din 2013. În pofida faptului că ransomware-ul a existat de mai mult timp, niciodată nu a reprezentat o amenințare atât de severă care să preocupe întreprinderile, ca în acești ultimi ani. Cu toate acestea, ransomware-ul poate face acum cu ușurință o afacere inoperabilă prin criptarea fișierelor importante sau necesare ale acesteia. Atunci când o companie este victima unui atac de ransomware, aceasta își dă seama rapid că backup-urile pe care le are nu sunt suficient de eficiente, iar compania se simte deseori forțată să plătească suma cerută.

Soluțiile ESET Endpoint Protection oferă nivele multiple de apărare nu numai pentru a preveni atacurile ransomware, ci și pentru a detecta existența acestora într-o organizație. Este important să prevenim și să detectăm ransomware-ul, pentru că de fiecare dată când cineva cedează și plătește șantajul convinge infractorii să continue să folosească acest tip de atac.

ATACURILE TARGETATE ȘI BREȘELE DE SECURITATE

Peisajul de securitate cibernetică de astăzi evoluează în mod constant prin noi metode de atac și amenințări nemaîntâlnite până acum. Atunci când apare un nou atac sau o nouă breșă de securitate, organizațiile sunt de obicei surprinse de faptul că apărarea lor a fost compromisă sau nu știu că atacul a avut loc. După ce atacul este în cele din urmă descoperit, organizațiile implementează în mod reactiv măsuri de atenuare pentru a opri repetarea acestui atac. Cu toate acestea, acest lucru nu le protejează de următorul atac care ar putea folosi un vector nou.

Soluțiile ESET Endpoint Protection utilizează informații de tipul threat intelligence, folosind ca referință feedback-ul lor. Se utilizează endpoint-urile drept senzori globali - care verifică la nivel mondial, prioritizează și blochează în mod eficient cele mai noi amenințări depistate, înainte de a se răspândi oriunde altundeva. În plus, majoritatea platformelor de protecție endpoint au funcții de actualizare bazate pe cloud pentru a răspunde rapid în cazul unei detecții pierdute fără a trebui să așteptați o actualizare normală.

ATACURI FILELESS

Noile amenințări, numite fileless malware, există exclusiv în memoria computerului, ceea ce face imposibilă detectarea acestora prin protecția bazată pe scanarea fișierelor. În plus, unele atacuri de tip fileless vor folosi aplicațiile deja instalate, încorporate în sistemul de operare, pentru a face chiar mai dificilă detectarea pericolelor. De exemplu, utilizarea PowerShell în aceste atacuri este foarte frecventă.

Platformele ESET Endpoint Protection folosesc tehnici speciale pentru a detecta aplicațiile afectate sau deturnate și pentru a proteja calculatorul dvs. împotriva atacurilor fileless. ESET a creat, de asemenea, scanere dedicate pentru a verifica constant memoria calculatorului față de orice comportament suspect. Folosind această abordare multistratificată, ne asigurăm că vom rămâne mereu cu un pas înaintea celui mai nou program malware.

Soluțiile ESET Endpoint Protection oferă straturi de apărare nu numai pentru a preveni ransomware-ul, ci și pentru a detecta existența acestora într-o organizație.

Atunci când apare un atac sau o breșă de securitate, organizațiile sunt de obicei surprinse de faptul că apărarea lor a fost compromisă sau nu știu că atacul a avut loc.

Noile amenințări, numite fileless malware, există exclusiv în memoria computerului, ceea ce face imposibilă detectarea acestora prin protecția bazată pe scanarea fișierelor.

“ESET este soluția noastră de securitate de încredere de ani de zile. Ea face ceea ce are de făcut; nu trebuie să îți faci griji. Pe scurt, ESET reprezintă: fiabilitate, calitate și servicii. ”

—Jos Savelkoul, Team Leader ICT-Department; Zuyderland Hospital, Netherlands;
10.000+ seats



Soluțiile ESET Endpoint Protection

ESET Endpoint Security pentru Windows/Mac/Android

ESET Endpoint Antivirus pentru Windows/Mac/Linux Desktop

ESET File Security pentru Windows Server/Linux/FreeBSD/Azure

ESET Mobile Device Management pentru Apple iOS

Diferența ESET

PROTECȚIE MULTISTRATIFICATĂ

ESET combină tehnologia multistratificată premiată, învățarea automată și expertiza umană pentru a oferi clienților cel mai înalt nivel de protecție posibil. Tehnologia noastră se adaptează în mod constant și se transformă pentru a oferi cel mai bun echilibru de detecție, rezultate fals pozitive reduse și performanță.

SUPORT TRANS PLATFORMĂ

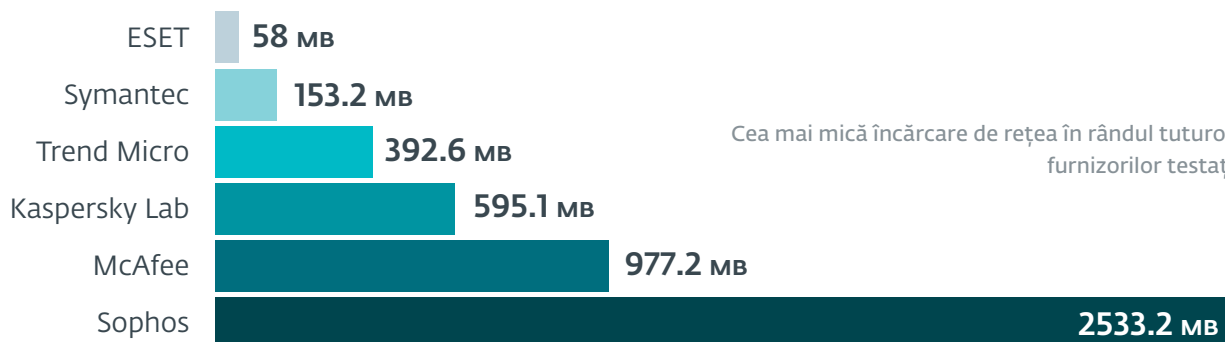
Produsele ESET Endpoint Protection sprijină toate sistemele de operare, inclusiv Windows, Mac, Linux și Android. Toate produsele endpoint pot fi gestionate complet dintr-un punct central; Mobile Device Management pentru iOS și Android reprezintă o caracteristică complet integrată de asemenea.

PERFORMANȚĂ FĂRĂ PRECEDENT

De nenumărate ori, cea mai mare preocupare a unei organizații este performanța unei soluții de protecție endpoint. Produsele ESET continuă să exceleze ca performanță și să câștige teste derulate de entități independente, prin care demonstrează cât redus este impactul lor asupra parametrilor de performanță de sistem.

PREZENȚĂ GLOBALĂ

ESET are birouri în 22 de țări din întreaga lume, 13 laboratoare de cercetare și prezență în peste 200 de țări și teritorii. Acest lucru ne ajută să furnizăm date pentru a opri malware-ul înainte de a se răspândi în întreaga lume, precum și pentru a acorda prioritate noilor tehnologii menite să blocheze cele mai recente amenințări sau vectori de atac.



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

“... cel mai relevant testimonial? Statisticile furnizate de la serviciul nostru de asistență: după introducerea produselor ESET, persoanele care se ocupă de suportul tehnic al organizației nu mai înregistrează apeluri legate de probleme antivirus sau de malware! ”

— Adam Hoffman, IT Infrastructure Manager; Mercury Engineering, Ireland; 1.300 seats

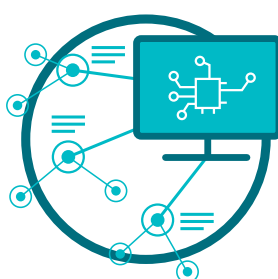
Tehnologia

Produsele și tehnologia noastră au la bază 3 piloni



ESET LIVEGRID®

Când se observă o amenințare de tipul zero-day (ca de exemplu, ransomware), fișierul este trimis la sistemul nostru de protecție împotriva malware-ului (LiveGrid®), unde amenințarea este declanșată și monitorizată. Rezultatele sunt furnizate tuturor endpoint-urilor la nivel global în câteva minute fără a fi nevoie de actualizări.



MACHINE LEARNING

Învățarea automată utilizează puterea combinată a rețelelor neurale și a algoritmilor atent aleși pentru a clasifica corect eșantioanele primite ca fiind curate, potențial nedorite sau rău intenționate.



EXPERTIZA UMANĂ

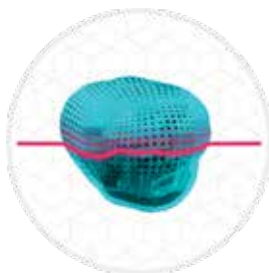
Cercetători de securitate de clasă mondială împărtășesc know-how-ul de elită și inteligența necesară pentru a asigura cele mai bune și complete informații despre amenințări.

Un singur strat de apărare nu este suficient pentru a contracara peisajul amenințător aflat în continuă evoluție. Toate produsele ESET Endpoint Security au capacitatea de a detecta pre-execuția, execuția și post-execuția malware-ului. Concentrarea pe mai multe părți ale ciclului de viață malware ne permite să oferim cel mai înalt nivel de protecție posibil.



MACHINE LEARNING

Toate produsele ESET Endpoint utilizează învățarea automată în plus față de utilizarea celorlalte straturi de apărare încă din 1997 până în prezent. În mod specific, învățarea automată este utilizată sub formă de rețele consolidate și rețele neurale.



SCANNER AVANSAT DE MEMORIE

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



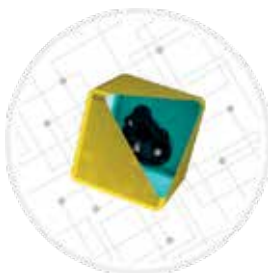
RANSOMWARE SHIELD

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.



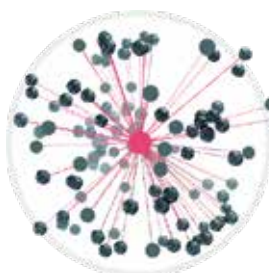
EXPLOIT BLOCKER

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 declanșat, comportamentul procesului este analizat și, în cazul în care acesta este considerat suspect, amenințarea poate fi imediat blocată pe aparat.



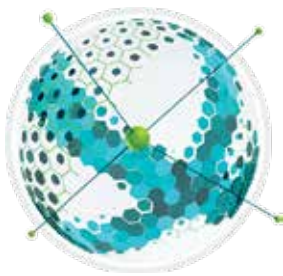
IN-PRODUCT SANDBOX

Malware-ul de astăzi este adesea disimulat cât mai avansat pentru a trece nedetectat cât mai mult timp posibil. Ca să înțeleagă cât mai bine ce se petrece și pentru a identifica comportamentul real din spatele codului aparent legitim, folosim sandboxing 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, atacurilor realizate în rețea și a exploatării vulnerabilităților pentru care un patch nu a fost încă lansat sau propus spre implementare.



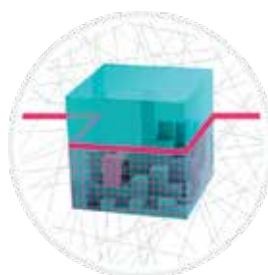
SEMNĂTURILE ADN

Tipurile de semnături 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.



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.

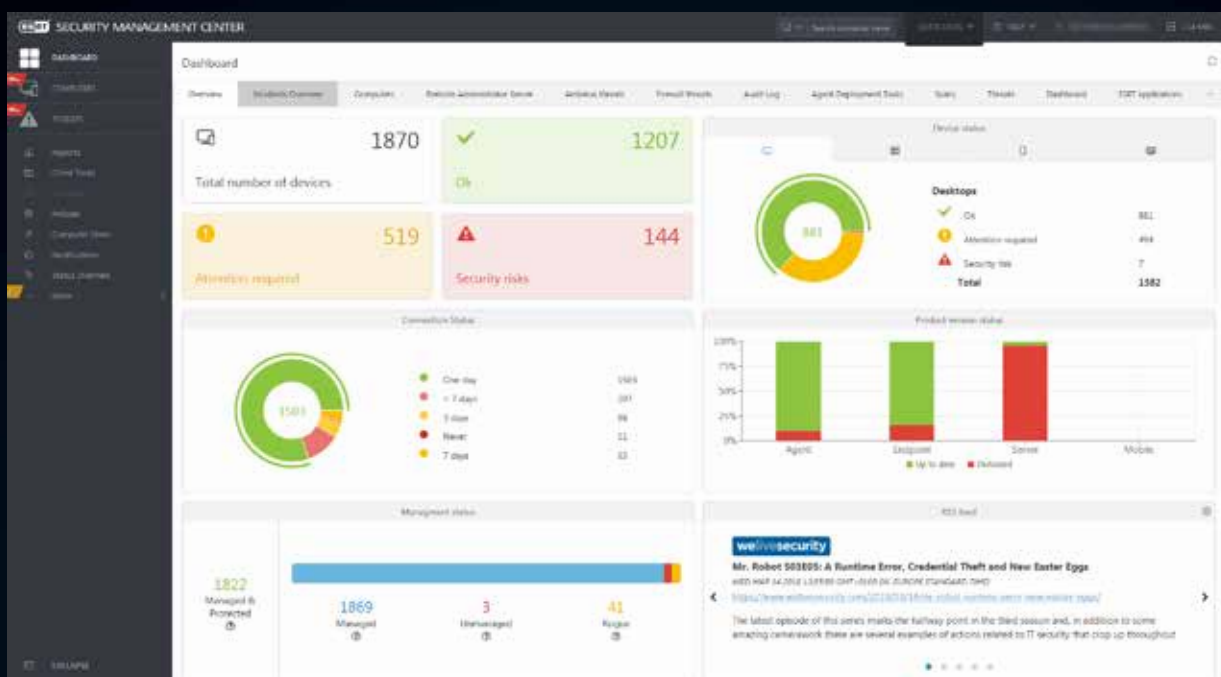


SCANNER UEFI

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.

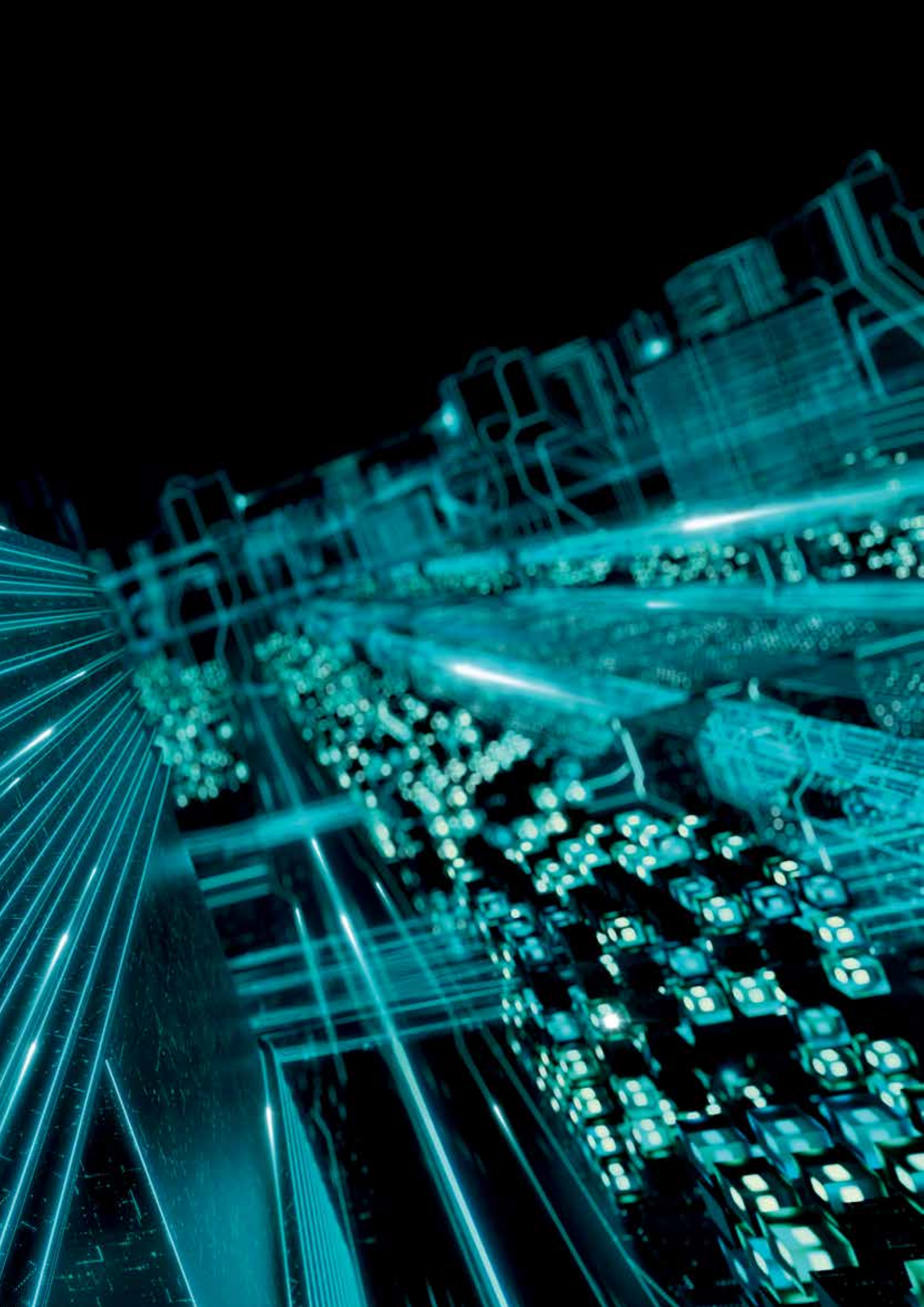
“Cel mai important lucru care se remarcă este avantajul său tehnic puternic față de alte produse de pe piață. ESET ne oferă securitate sigură, ceea ce înseamnă că pot lucra la orice proiect în orice moment știind că există soluții de protecție de încredere care vizează calculatoarele noastre.”

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



Security Management Center

Toate soluțiile ESET sunt gestionate dintr-un singur loc - ESET Security Management Center - care poate fi instalat pe Windows sau Linux. În plus față de versiunea instalată, ESET oferă un virtual appliance pe care îl puteți importa cu ușurință pentru o configurare rapidă.



Cazuri de utilizare

Ransomware

Unele companii doresc asigurări suplimentare cu privire la protecția împotriva atacurilor Ransomware.

SOLUȚIE

- ✓ Network Attack Protection are capacitatea de a împiedica infectarea de către un ransomware a unui sistem, prin oprirea exploit-urilor la nivelul rețelei.
- ✓ Apărarea noastră multistratificată are caracteristici de tipul sandbox în interiorul produsului, care au capacitatea de a detecta malware-ul.
- ✓ Folosiți sistemul de protecție anti-malware bazat pe Cloud al ESET pentru vă proteja împotriva noilor amenințări, fără a fi nevoie să așteptați actualizările de detectare.
- ✓ Toate produsele conțin protecție Ransomware Shield pentru a se asigura că firmele sunt protejate de criptarea nedorită a fișierelor.

Amenințări de tipul zero-day

Amenințările de tipul zero-day reprezintă o preocupare majoră a companiilor deoarece acestea au dificultăți în a se proteja față de ceva nemaîntâlnit până acum.

SOLUȚIE

- ✓ Soluțiile Endpoint ESET folosesc euristica și machine learning-ul, ca parte a abordării noastre multilaterale 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.
- ✓ Folosiți sistemul de protecție anti-malware Cloud de la ESET pentru vă proteja împotriva noilor amenințări, fără a fi nevoie să așteptați actualizările de detecție.

Fileless malware

Fileless malware-ul reprezintă o amenințare nouă și datorită faptului că rezidă doar în memorie necesită o abordare diferită de cea a malware-ului bazat pe fișiere.

SOLUȚIE

- ✓ Tehnologia unică ESET Advanced Memory Scanner, protejează împotriva acestui tip de amenințare prin monitorizarea comportamentului proceselor malware și scanarea acestora în memorie.
- ✓ Reduceți timpul de investigare al unui incident prin încărcarea amenințărilor în ESET Threat Intelligence pentru a vă furniza informații despre modul în care funcționează amenințarea propriu-zisă.
- ✓ Tehnologia multistratificată, învățarea automatizată și expertiza umană oferă clienților noștri cel mai bun nivel de protecție posibil.

“Când am descoperit ESET am știut ca este alegerea potrivită: tehnologie de încredere, detecție solidă, prezență locală și un suport tehnic excelent. Pe scurt, tot ceea ce ne trebuia.”

— Ernesto Bonhoure, IT Infrastructure Manager;
Hospital Alemán, Argentina,
1.500+ seats

Despre ESET

ESET - un lider global în domeniul securității informațiilor - a fost numit singurul Challenger în Gartner Magic Quadrant pentru platformele de protecție Endpoint 2018.*

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 în continuă dezvoltare, pentru întreprinderi și clienți din întreaga lume.

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

STATISTICI ESET

110m+
utilizatori în
întreaga lume

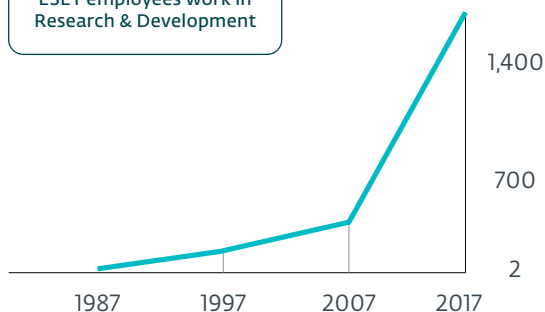
400k+
clienți
business

200+
țări &
teritorii
acoperite

13
centre
globale de
R&D

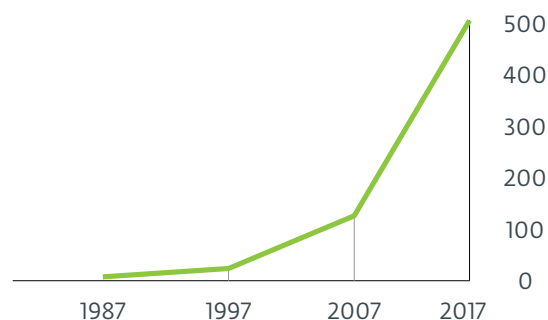
ANGAJAȚII ESET

More than a third of all
ESET employees work in
Research & Development



VENITURI ESET

in million €



*Gartner nu aprobă niciun furnizor, produs sau serviciu descris în publicațiile sale de cercetare. Publicațiile Gartner de cercetare constau în opiniile organizației de cercetare Gartner și nu ar trebui interpretate ca declarații de fapt. Gartner declină toate garanțiile, exprimate sau implicite, cu privire la această cercetare, inclusiv orice garanție de vandabilitate sau de adecvare pentru un anumit scop.

UNII DINTRE CLIENȚII NOȘTRI

HONDA

protejat de ESET din 2011

licență prelungită de 3x, extinsă de 2x

GREENPEACE

protejat de ESET din 2008

licență prelungită/extinsă de 10x

Canon

protejat de ESET din 2016

peste 14,000 stații de lucru

T ..

partener ITP din 2008

bază de clienți - 2 milioane

UNELE DINTRE PREMIILE NOASTRE DE TOP



"Având în vedere funcționalitățile anti-malware de top și ușurința în administrare oferită, alături de acoperirea globală a suportului asigurat clienților, ESET merită să fie plasat pe lista scurtă de soluții anti-malware pe care și o construiesc companiile din segmentul enterprise."

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018



ENJOY SAFER
TECHNOLOGY™

