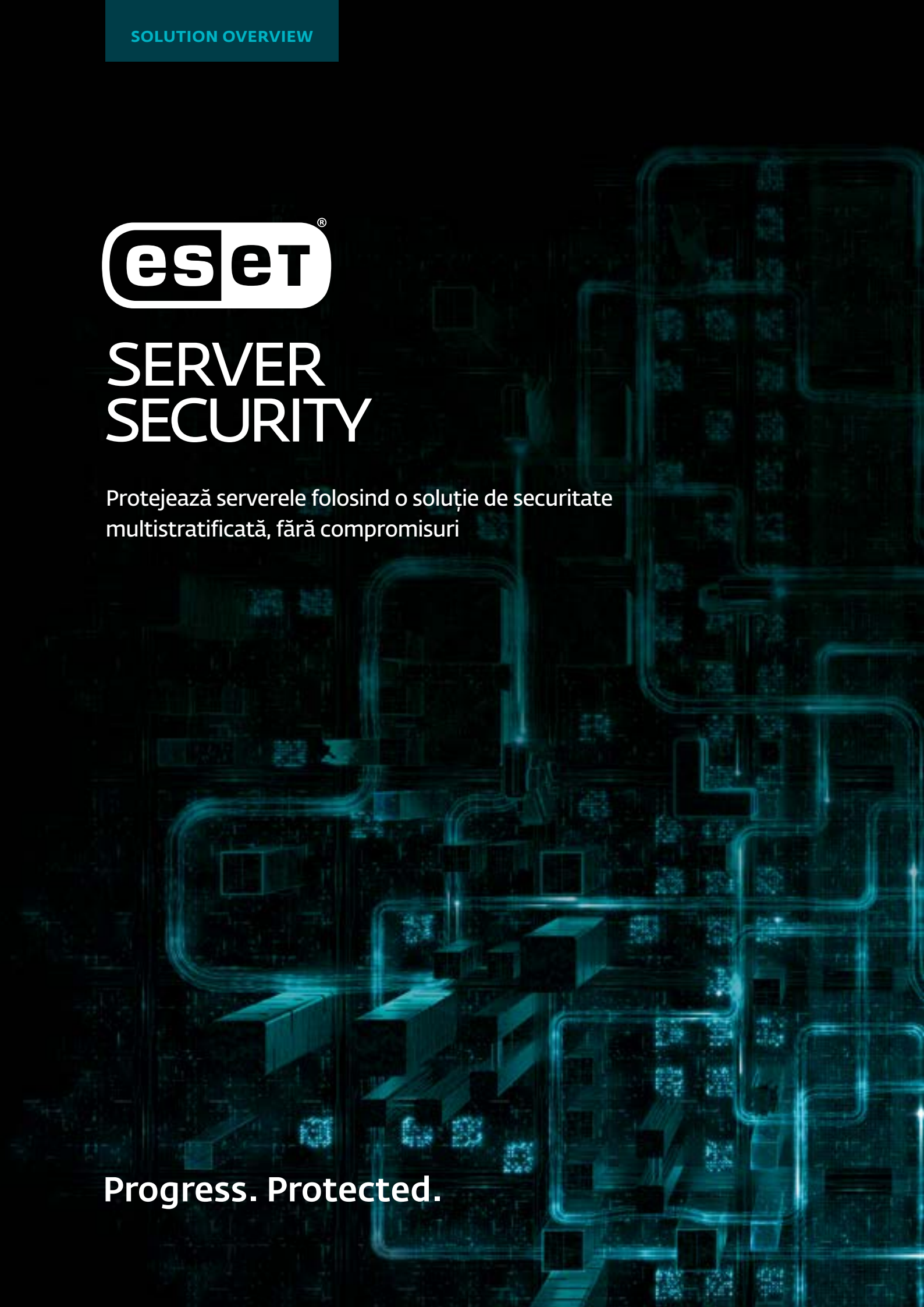
SOLUTION OVERVIEW



# SERVER SECURITY

Protejează serverele folosind o soluție de securitate multistratificată, fără compromisuri

Progress. Protected.

# Ce este o **soluție de securitate a fișierelor?**

**Un produs de securitate a fișierelor este proiectat pentru a proteja serverele centrale ale unei organizații de amenințări. Această soluție ar trebui instalată pe orice server nespecializat, pentru a vă asigura că resursele organizatorice nu sunt infectate. În zilele noastre, companiile își pun securitatea organizației în pericol, permițând utilizatorilor să salveze fișiere într-o rețea de partajare a companiei, fără să protejeze în mod adecvat informațiile partajate de fișierele rău intenționate. Un singur utilizator care salvează un fișier rău intenționat pe un drive din rețea poate provoca instantaneu un efect de cascadă prin care toate fișierele organizației dvs. devin inaccesibile.**

**ESET Server Security** oferă servicii avansate de protecție pentru toate serverele generale, pentru soluțiile de stocare ale fișierelor din rețea și pentru serverele multifuncționale. Acesta se concentrează pe asigurarea unor servere stabile și fără conflicte de sistem, pentru a menține perioadele de întreținere și numărul de reporniri de sistem la un nivel minim, pentru a nu perturba continuitatea afacerii.

# De ce aveți nevoie de o **soluție de securitate a fișierelor?**

## 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 suficient 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 FĂRĂ FIȘIERE

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 scanerele 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.

ESET Server Security 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 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

# Soluțiile ESET Server Security

ESET Server Security pentru Microsoft Windows Server
ESET Server Security pentru Linux
ESET Server Security pentru Microsoft Azure

# Diferența adusă de 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.

## PERFORMANȚĂ FĂRĂ EGAL

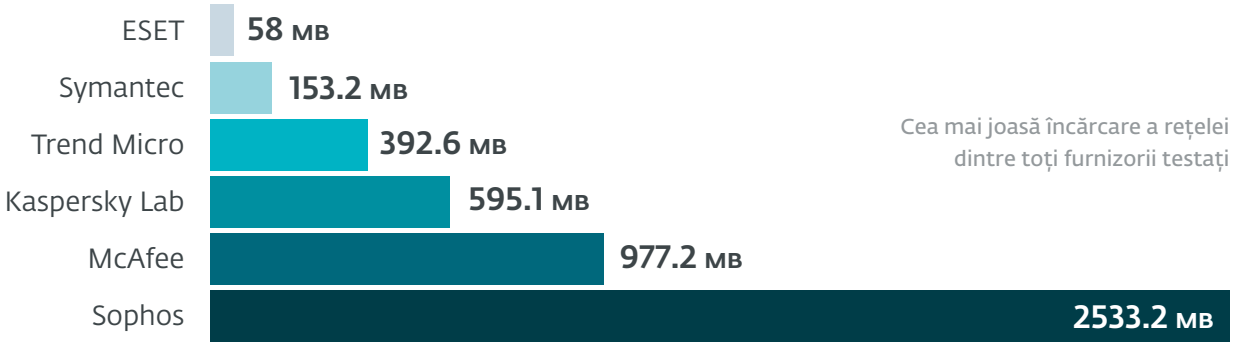
De nenumărate ori, cea mai mare preocupare a unei organizații este impactul asupra performanței al unei soluții de protecție endpoint. Produsele ESET continuă să exceleze în domeniul performanței și dovedesc în cardul testelor independente cât de noninvazive sunt soluțiile pentru sistemele de endpoint-uri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

## 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.

## 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 joasă încărcare a rețelei dintre toți furnizorii testați

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

*„... 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!"*

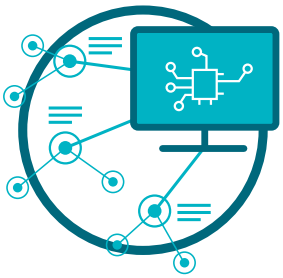
Adam Hoffman, Manager de Infrastructură IT, compania Mercury Engineering, Irlanda - 1.300 de stații

# Tehnologia

## 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.

### EXPERTIZA UMANĂ

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.

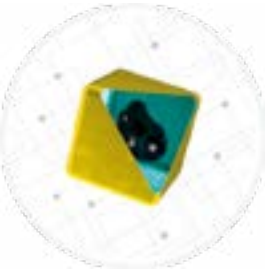
Un singur nivel de apărare nu este suficient pentru peisajul amenințărilor în continuă evoluție. Toate produsele de securitate ESET au capacitatea de a detecta programele malware înaintea execuției, în timpul execuției și după execuție. Concentrându-se pe mai mult de o anumită parte a ciclul de viață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

## ÎNVĂȚARE AUTOMATIZATĂ

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.

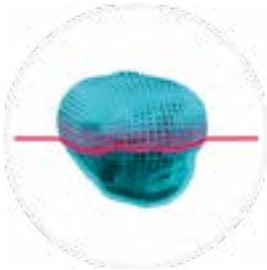
## SCUT ÎMPOTRIVA RANSOMWARE

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 blocheze procesele care se seamănă cu comportamentul de ransomware.



## 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 încoporată 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.

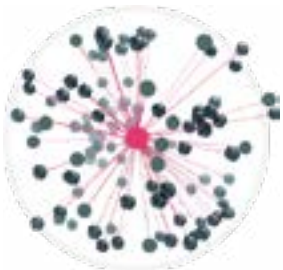


## SCANNER DE MEMORIE AVANSAT

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.

## EXPLOIT BLOCKER

ESET Exploit Blocker monitorizează aplicațiile predispuse la a fi exploatate (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.



## 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.

## DETECȚII ADN

Varietatea de tipuri de detecție variază de la valori hash foarte specifice până la ESET DNA Detections, care sunt definiții complexe ale comportamentul rău intenționat și ale caracteristicilor programelor malware. În timp ce codul rău intenționat poate fi ușor modificat sau ascuns de către atacatori, comportamentul obiectelor nu poate fi schimbat atât de ușor și ESET DNA Detections eset conceput pentru a exploata acest principiu.

## DETECȚIA COMPORTAMENTALĂ – HIPS

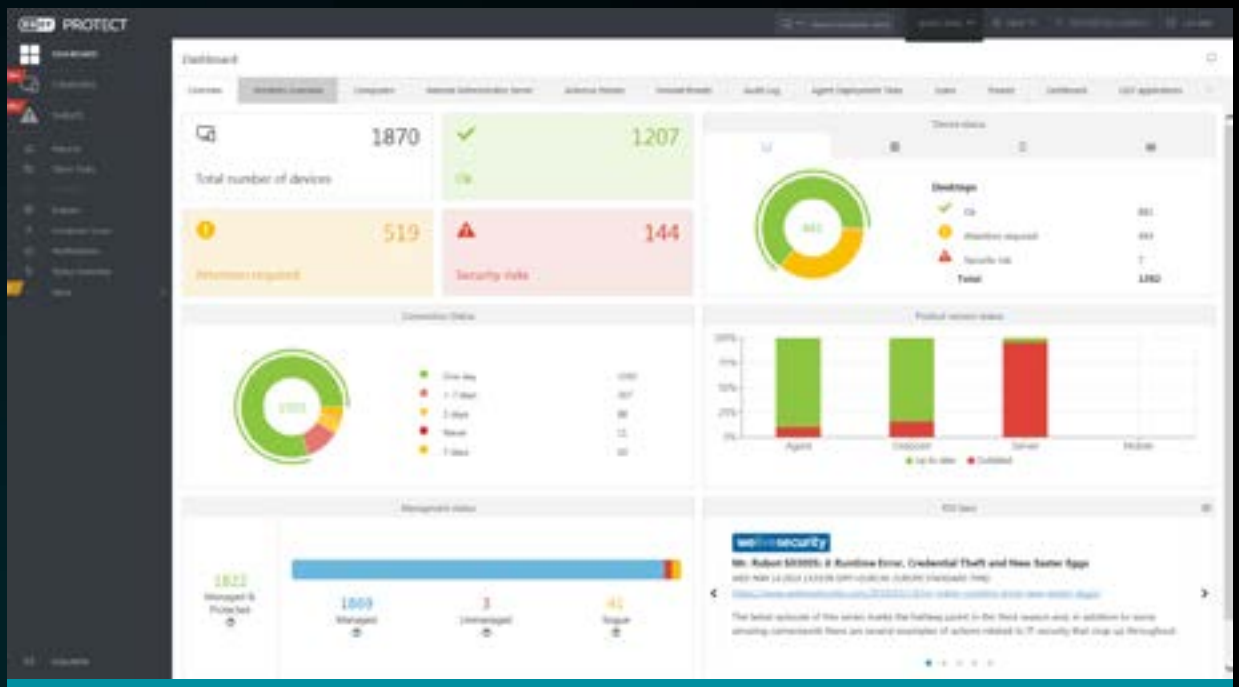
ESET HIPS (Host-Based Intrusion Prevention System) monitorizează activitatea sistemului și utilizează un set predefinit de reguli pentru a recunoaște comportamentul suspect al sistemului. În plus, mecanismul de autoapărare HIPS oprește procesul ofensator din desfășurarea activității dăunătoare.

## SCANARE SCRIPT/AMSI

Soluțiile ESET folosesc interfața de scanare antimalware (AMSI) pentru a oferi protecție îmbunătățită împotriva programelor malware pentru utilizatori, date, aplicații și volum de lucru. În plus, folosește interfața de serviciu protejată, un nou modul de securitate încorporat în Windows care permite doar încărcarea de cod de încredere, semnat și pentru protekează și mai bine împotriva atacurilor prin injectare de cod.

*„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, Irlanda - 1.300 de stații




## ESET PROTECT

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

*„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

# Cazuri de utilizare

## Fileless malware

**Caz de utilizare:** Fileless malware este o amenințare relativ nouă iar existența ei doar la nivelul memoriei de sistem necesită a 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 o dată ce se dezvăluie în memorie.
- ✓ Dacă ESET Server Security nu este sigur de o potențială amenințare, are capacitatea de a încărca eșantionul în ESET Advanced Threat Defense și ESET LiveGuard Advanced, pentru a lua cea mai bună decizie dacă vreun element este sau nu rău intenționat.
- ✓ Dacă o amenințare este confirmată, reduceți colectarea de date și timpul de investigare prin încărcarea amenințării în ESET Threat Intelligence pentru a oferi informații despre cum funcționează.

## Amenințări zero-day

**Caz de utilizare:** amenințările zero-day sunt o preocupare majoră pentru afaceri, din cauza că nu sunt pregătite pentru protecție împotriva a ceva ce nu au mai văzut până acum.

### SOLUȚIE

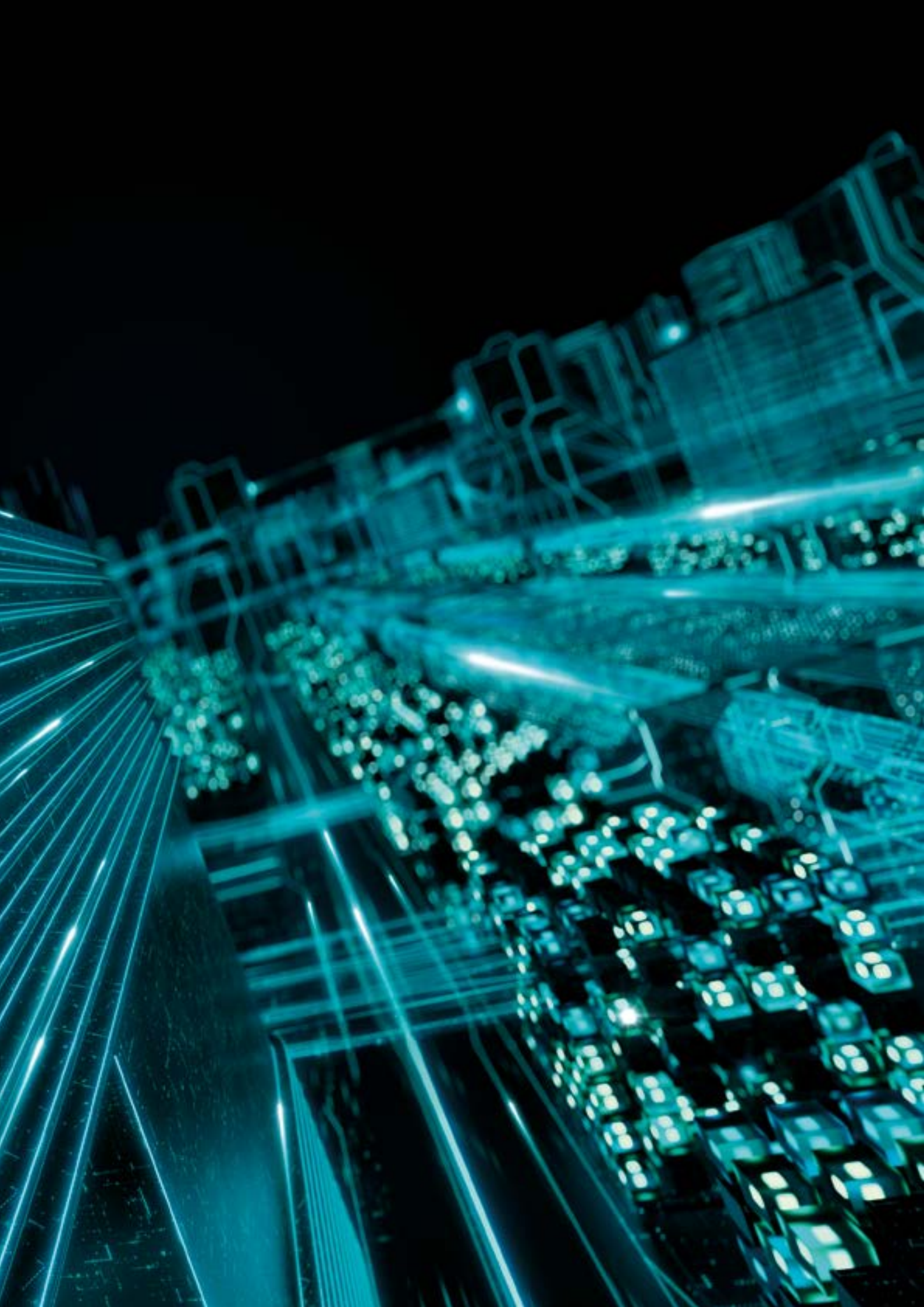
- ✓ ESET Threat Intelligence oferă date despre cele mai noi amenințări și tendințe, precum și despre atacurile direcționate, pentru a ajuta companiile să prezică și să prevadă cele mai noi amenințări.
- ✓ Produsele ESET endpoint valorifică tehnici precum trial&error sau machine learning ca abordare a sistemului multi-stratificat pentru a preveni și a proteja împotriva niciodată programelor malware nemaivăzute până acum.
- ✓ Sistemul ESET de protecție împotriva malware-ului în cloud protejează automat împotriva noilor amenințări fără necesitatea de a aștepta următoarea actualizare de detectare.

## Ransomware

**Caz de utilizare:** 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 ransomwarea 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.
- ✓ Dacă ESET Server Security nu este sigur de o potențială amenințare, are capacitatea de a încărca eșantionul în ESET Advanced Threat Defense și ESET LiveGuard Advanced, pentru a lua cea mai bună decizie dacă vreun element este sau nu rău intenționat.



# 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 unul dintre pionierii folosirii de machine learning și de tehnologii cloud care previn, detectează și răspund față de programele malware. ESET este o companie privată care promovează global cercetarea științifică și dezvoltarea.

## ESET ÎN CIFRE

**1bn+**
utilizatori, global

**400k+**
clienți business

**200+**
țări și teritorii

**13**
centre globale R&D

## CÂȚIVA DINTRE CLIENȚII NOȘTRI

MITSUBISHI MOTORS
Drive your Ambition

protejat de ESET încă din 2017, peste 9.000 stații

Allianz Suisse

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

Canon
Canon Marketing Japan Group

protejat de ESET încă din 2016, peste 32.000 stații

T

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

## PREMIILE ESET

AV comparatives APPROVED Business Security DEC 2021

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

G2 Leader WINTER 2022

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.

FORRESTER®

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".


eset
Digital Security
Progress. Protected.