



ENDPOINT ENCRYPTION

Criptare simplă și puternică pentru
organizații de toate dimensiunile



ENJOY SAFER
TECHNOLOGY™



30 YEARS OF
CONTINUOUS
IT SECURITY
INNOVATION



Ce este un produs **Endpoint Encryption**

Endpoint Encryption este un instrument esențial pentru securitatea datelor ce permite criptarea fișierelor și a hard-diskurilor pe sistemele endpoint ale organizației. Acest lucru împiedică citirea și utilizarea neautorizată a datelor, dacă acestea ajung pe mâini greșite.

ESET Endpoint Encryption asigură o soluție de securizare a datelor pe care le dețin companiile, indiferent de dimensiune. Soluția permite criptarea facilă a datelor stocate în: hard-disc-uri, fișiere / foldere, email-uri și stick-uri USB.

De ce Endpoint Encryption?

BREŞE DE DATE

Zona cybersecurity de astăzi înregistrează un număr tot mai mare de breșe de date care au loc în fiecare zi. Când aceste surgeri de date se petrec, iar criptarea acestor date nu a fost în prealabil implementată, datele sunt expuse riscului de a fi publicate sau utilizate în scopuri dăunătoare. Unele companii nu tratează cu seriozitate valoarea datelor pe care le dețin, însă toate companiile au un set de date sensibile, format din liste de clienți, informații proprietare și date legate de vânzări.

Prin implementarea unei soluții de criptare a acestora, companiile împiedică accesul la datele furate de către hackeri. Industriile de top vizate de atacurile soldate cu pierderi ale datelor sunt în mod tradițional cele care dețin date valoroase: finanțier, retail, asistență medicală și sectorul public. Nu înseamnă că alte industrii sunt într-un context mai sigur - doar că hackerii cântăresc în mod obișnuit efortul depus pentru un atac de succes cu câștigurile potențiale rezultante.

ANGAJAȚI CARE LUCREAZĂ REMOTE

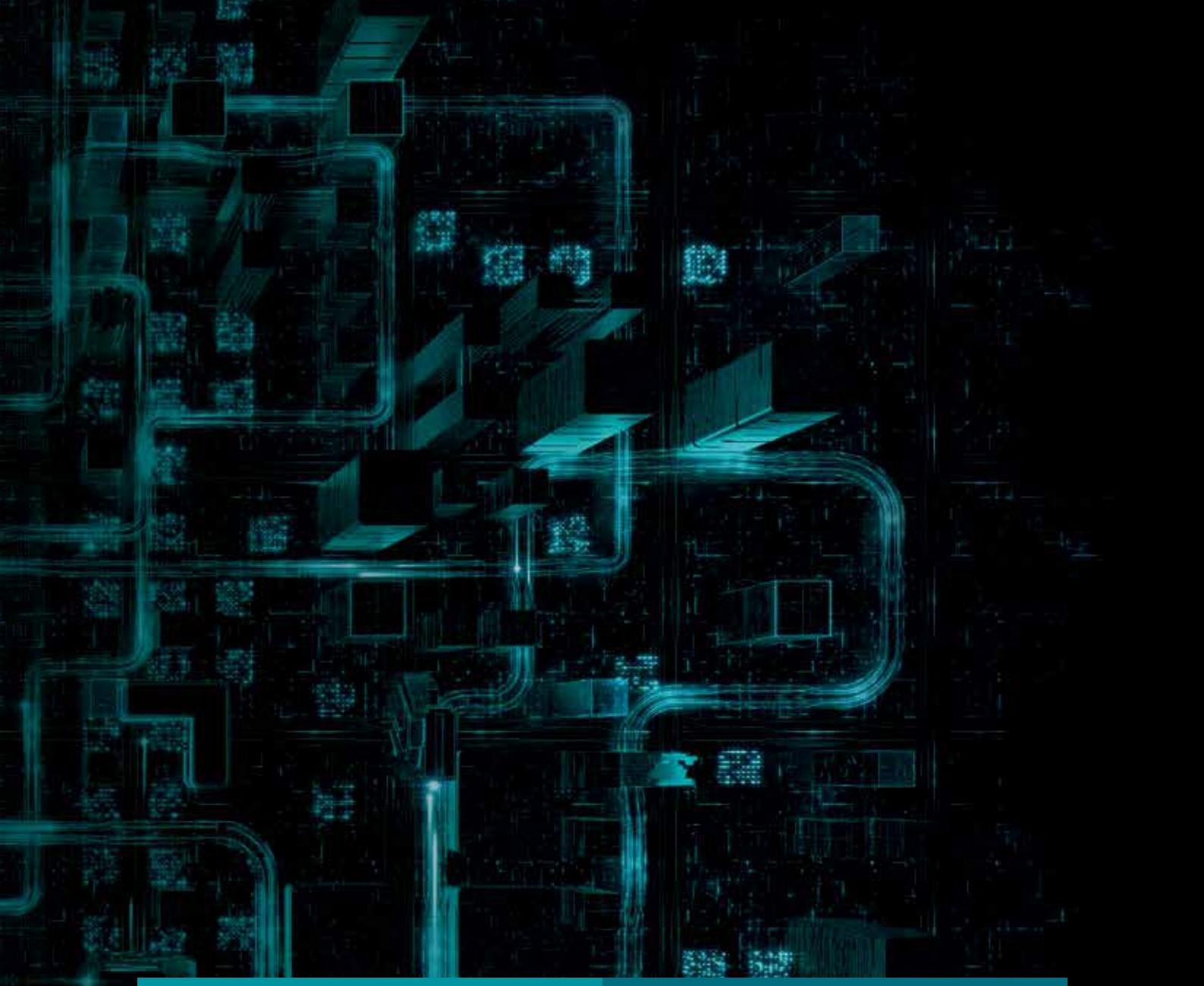
Forța de muncă care călătoresc a devenit predominantă în cadrul companiilor. Angajații lucrează acum remote, din cafenele sau din aeroporturi. Cu toate acestea, cu cât angajații acceseză datele companiei din afara perimetrlui acesteia, cu atât crește riscul de pierdere sau de furt al laptop-urilor, smartphone-urilor, stick-urilor sau altor medii de stocare. Nu numai că organizațiile trebuie să-și facă griji cu privire la dispozitivele furate, ei trebuie să se gândească și la procesul blocare a utilizatorilor remote.

Adăugarea unei soluții de criptare Endpoint face mult mai dificil pentru persoanele care fură sau găsesc dispozitivele dvs. să aibă acces la sisteme. În plus, majoritatea soluțiilor Endpoint permit dezactivarea la distanță a dispozitivelor angajaților sau a dispozitivelor pierdute / furate.

CONFORMITATE

Când vine vorba de conformitate, majoritatea întreprinderilor trebuie să înțeleagă mai întâi dacă trebuie să respecte cerințe de conformitate sau nu. În continuare, trebuie să analizeze ce fel de cerințe recomandă și mandatează conformitatea necesară pentru activitatea desfășurată. Când vine vorba de criptare, multe reglementări și legi, cum ar fi GDPR, PCI-DSS, HIPAA, SOX și GLBA, necesită implementarea proceselor de criptare a datelor.

Endpoint Encryption nu mai reprezintă o soluție opțională pentru majoritatea întreprinderilor care gestionează cărți de credit sau informații de sănătate, ci mai degrabă un nivel de securitate necesar. Toate companiile trebuie să cerceteze și evaluate dacă trebuie să respecte anumite cerințe de conformitate.



Cu cât aveți mai mulți angajați care lucrează de la distanță, cu atât aveți un risc mai ridicat din direcția echipamentelor pierdute sau furate.

Endpoint Encryption nu mai este o soluție opțională pentru majoritatea întreprinderilor care gestionează cărți de credit sau informații de sănătate, ci mai degrabă o soluție necesară.



Diferență ESET

GESTIONAȚI DISPOZITIVELE ORIUNDE

ESET Endpoint Encryption poate gestiona dispozitivele oriunde în lume fără a necesita VPN-uri sau excepții de tip firewall. Managementul este gestionat prin utilizarea conectivității HTTPS prin intermediul unui proxy. Acest lucru elimină nevoie de conexiuni de intrare riscante, ceea ce face ca gestionarea criptării să fie sigură și simplă pentru întreprinderile de toate dimensiunile. Toate conexiunile client și server sunt criptate SSL și toate comenzi și datele sunt criptate AES sau RSA.

ZERO IMPACT ASUPRA PRODUCTIVITĂȚII

Implementarea criptării este complet transparentă pentru utilizatori și nu necesită nicio acțiune din partea lor, pentru atingerea conformității. Nu se creează cheltuieli suplimentare pentru departamentele IT și nu este nevoie de instruire pentru utilizatori.

SISTEM UNIC DE CHEI DE CRIPTARE

Utilizarea cheilor de criptare partajate, gestionate la nivel central, evită problemele întâmpinate de soluțiile de criptare, care de obicei utilizează fie parole comune, fie chei publice. Sistemul folosit de ESET Endpoint Encryption reflectă modul în care cheile fizice sunt utilizate pentru a bloca casele, apartamentele, mașinile etc. Personalul înțelege deja acest concept și are

nevoie doar de o singură explicație. Cuplat cu un sistem premium de management la distanță, cheile de criptare comune sunt foarte sigure și practice.

MEDIU AMOVIBIL SECURIZAT

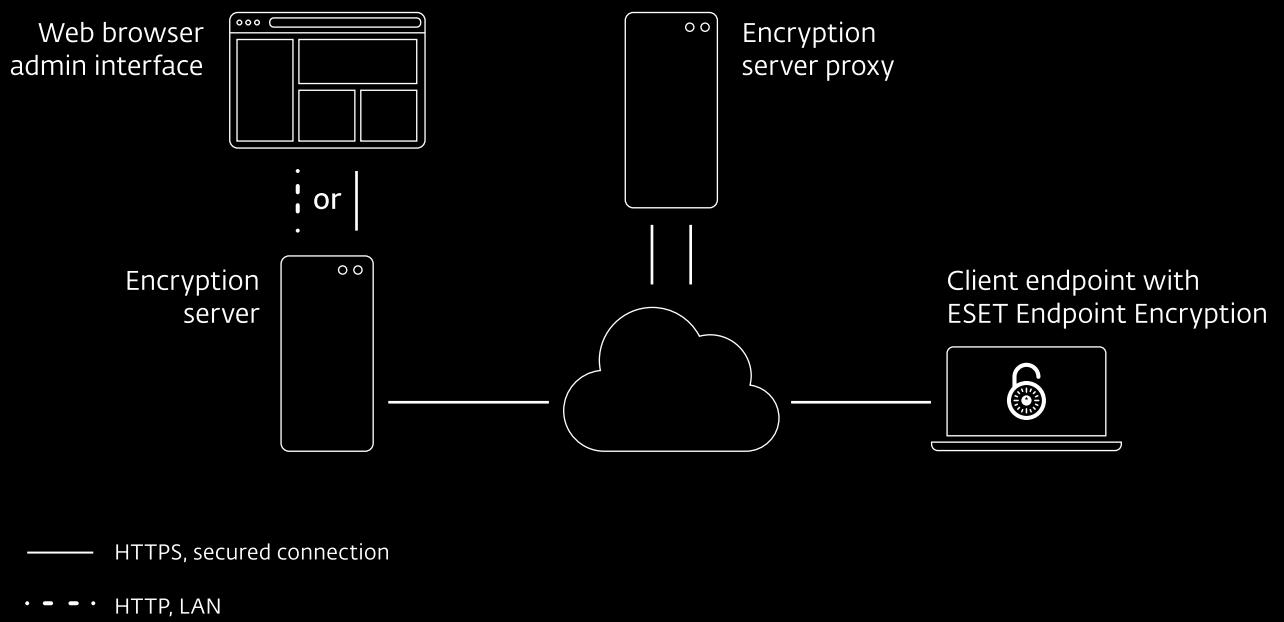
Gestionarea dispozitivelor media amovibile într-un mediu sigur poate fi uneori o muncă grea. ESET Endpoint Encryption creează automat partii pe un dispozitiv media amovibil și permite accesul la partitia securizată doar atunci când se află în mediul securizat, iar partitia nesigură atunci când este în altă parte. Acest lucru îl păstrează extrem de simplu pentru end-users. Fără nicio interacțiune cu utilizatorul, datele legate de domiciliu se mențin la domiciliu, iar datele legate de afaceri rămân la întreprindere.

DEZACTIVĂȚI DISPOZITIVE DE LA DISTANȚĂ

Tot mai multe companii se îndreaptă către o forță de muncă mobilă, unde angajații lucrează din aeroporturi, acasă sau din cafenele. Din această cauză, companiile au nevoie să poată dezactiva sau bloca de la distanță dispozitivele în cazul în care acestea sunt pierdute sau furate.

ESET Endpoint Encryption oferă o modalitate simplă de a face acest lucru și din nou nu necesită excepții VPN sau firewall pentru a face acest lucru.

Sistemul de chei de criptare utilizat de ESET Endpoint Encryption reflectă modul în care cheile fizice sunt utilizate pentru a proteja casele, apartamentele, mașinile etc. Personalul înțelege deja acest concept și are nevoie doar de o singură explicație pentru a se lămuri.



Gestionarea endpoint-urilor via proxy nu necesită conexiuni de intrare, ceea ce îl face sistemul extrem de sigur și ușor de configurat. Nu sunt necesare excluderi de firewall sau porturi deschise. Serverul de criptare poate rula pe orice PC sau server Windows.



Instalarea serverului ESET Endpoint Encryption durează mai puțin de 10 minute.

Configurarea completă a soluției durează de obicei mai puțin de o oră. Acest lucru accelerează semnificativ timpul de adoptare în întreaga organizație.



Cazuri de utilizare

Preveniți breșele de date

CAZ DE UTILIZARE

În fiecare zi la știri aflăm de noi companii care sunt nevoie să își notifice clienții că s-a produs o scurgere de date care a vizat informații legate de aceștia.

SOLUȚIE

- ✓ Protejați datele sensibile cu ESET Endpoint Encryption prin criptare full disk (FDE).
- ✓ Protejați comunicațiile vulnerabile, cum ar fi Remote Desktop, prin adăugarea de autentificare multi-factor.
- ✓ Solicitați autentificarea multi-factor pentru a vă conecta la dispozitive care conțin date sensibile.

SOLUȚIILE RECOMANDATE ESET

- ✓ ESET Endpoint Encryption
- ✓ ESET Secure Authentication

Gestionăți angajații remote

CAZ DE UTILIZARE

Companiile au nevoie de capacitatea de a proteja datele sensibile în cazul demisiei angajaților sau atunci când dispozitivele sunt pierdute sau furate.

SOLUȚIE

- ✓ Restricționați accesul la resursele companiei prin utilizarea autentificării multi-factor.
- ✓ Utilizați funcția de blocare remote pentru a proteja dispozitivele care pot fi pierdute sau furate.
- ✓ Folosiți abilitatea de a elimina utilizatorii remote de la dispozitive pentru a proteja datele în cazul terminării contractelor cu angajații.

SOLUȚIILE RECOMANDATE ESET

- ✓ ESET Endpoint Encryption
- ✓ ESET Secure Authentication

“Ca furnizor de servicii, este linistitor faptul că putem recomanda, procura, comanda și susține o soluție de criptare care ajută la menținerea continuității în instituțiile de învățământ din Staffordshire, reducând costurile totale”.

Andy Arnold, CS Team Leader of System Solutions,
Staffordshire Learning Technologies (SLT), UK

Preveniți scurgerea de date

CAZ DE UTILIZARE

Fiecare companie utilizează dispozitive media amovibile pentru a muta date de la un computer la altul, dar majoritatea companiilor nu au o modalitate de a verifica dacă datele se află numai pe dispozitivele companiei.

SOLUȚIE

- ✓ Implementați user-proof removable media care protejează utilizatorul pentru a restricționa deplasarea datelor în afara companiei.
- ✓ Restricționați accesul la dispozitive media amovibile utilizatorilor selectați..

SOLUȚIILE RECOMANDATE ESET

- ✓ **ESET Endpoint Encryption**

“Implementarea pilot a fost instalată într-un mediu de lucru real și s-a dovedit a fi extrem de ușor de utilizat de către utilizatori, cu interfață sa web. Serverul a fost foarte eficient, permitând chiar și controlul dispozitivelor prin internet, independent de structura rețelei.”

Simon Goulding, Aster's Network Services Analyst, UK



Caracteristici tehnice ESET Endpoint Encryption

TIPURI DE CRIPTARE ACCEPTE

Criptare completă de disk (FDE), criptare fișier/folder, criptare stick USB și email.

COMPLET VALIDATĂ

ESET Endpoint Encryption este validată FIPS 140-2 cu criptare AES pe 256 de biți.

ALGORITMI ȘI STANDARDE

AES 256 biți, AES 128 biți, SHA 256 biți, SHA1 160 biți, RSA 1024 biți, Triple DES 112 biți, Blowfish 128 biți.

SUSTINERE SISTEM DE OPERARE

Suport pentru Microsoft® Windows® 10, 8, 8.1 inclusiv UEFI și GPT, 7, Vista, XP SP 3; Microsoft Windows Server 2003-2012; Apple iOS.

NU ESTE NEVOIE DE HARDWARE SPECIAL

Cipurile TPM sunt opționale, dar nu sunt necesare pentru utilizarea criptării full disk.

NU ESTE NECESAR NICIU SERVER

ESET Endpoint Security nu are nevoie de niciun server și poate susține fără probleme criptarea utilizatorilor remote.

CRIPTAREA DE E-MAIL ȘI ATAŞAMENTE

Trimiteți și primiți cu ușurință e-mailuri și atașamente criptate prin Outlook.

CRIPTARE TEXT & CLIPBOARD

Criptați în totalitate sau parțial ferestre text din: browsere web, câmpuri memo de baze de date sau web-mail.

MANAGEMENT CENTRALIZAT

Control complet al licențierii și al caracteristicilor software, al politicii de securitate și al cheilor de criptare.

DISCURI VIRTUALE ȘI ARHIVE CRIPTATE

Creați un volum securizat, criptat pe PC sau într-o altă locație sau o copie criptată a unui întreg arbore de directoare și a fișierelor acestuia.

Toate companiile au date sensibile, cum ar fi liste de clienți, informații de proprietate și date referitoare la vânzări.

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

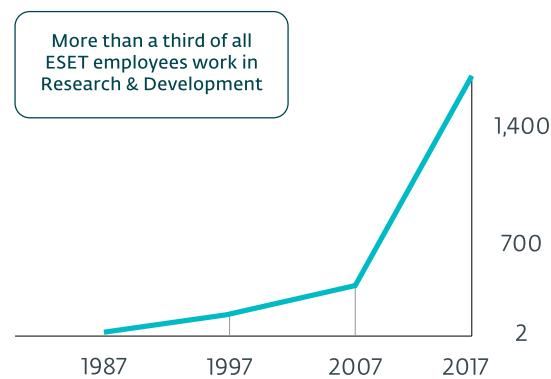
110m+
utilizatori în
întreaga lume

400k+
clienti
business

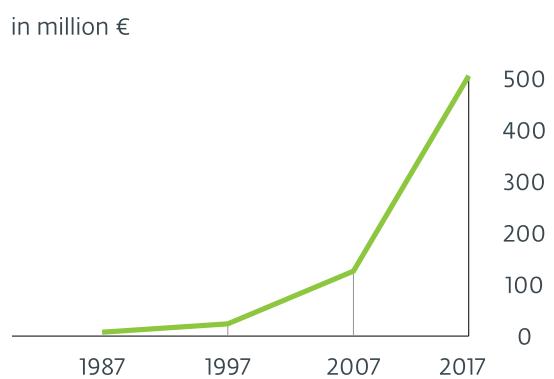
200+
țări &
teritorii
acoperite

13
centre
globale de
R&D

ANGAJAȚII ESET



VENITURI ESET



*Gartner nu aproba niciun furnizor, produs sau serviciu descris în publicațiile sale de cercetare. Publicațiile Gartner de cercetare constau în opinile organizației de cercetare Gartner și nu ar trebui interpretate ca declarații de fapt. Gartner declină toate garanțiile, exprimate sau implicate, cu privire la această cercetare, inclusiv orice garanție de vandabilitate sau de adevarare 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 scurta de soluții anti-malware pe care și o construiesc companiile din segmentul enterprise."

KuppingerCole Leadership Compass
Enterprise Endpoint Security: Anti-Malware Solutions, 2018

