SOLUTION OVERVIEW

SECURITY MANAGEMENT CENTER

Soluție enterprise-grade de management a securității oferind vizibilitate, management și raportare în toate OS-urile

ENJOY SAFER TECHNOLOGY™

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

Ce este **endpoint security management console?**

ESET Security Management Center utilizează o consolă web pentru a asigura asigură vizibilitate completă, on-premise și off-premise, în timp real asupra endpoint-urilor, precum și gestionarea integrală a rapoartelor și a securității pentru toate OS-urile.

Este un singur panou de sticlă peste toate soluțiile de securitate ESET implementate în rețea și controlează prevenirea endpoint-urilor, detectarea și răspunsul asupra tuturor platformelor - incluzând desktop-uri, servere, mașinării virtuale și dispozitive mobile gestionate.

De ce **endpoint security management?**

VIZIBILITATE

Amenințările persistente avansate de tipul zero-days, atacurile țintite și botnet-urile reprezintă preocupări pentru industriile din întreaga lume. Vizibilitatea acestor amenințări în timp real este extrem de importantă pentru a permite personalului IT să răspundă prompt și să atenueze orice risc care ar putea apărea. Datorită faptului că intreprinderile pun accentul pe o forță de muncă mobilă, vizibilitatea nu este doar necesară on-premise, ci și off-premise.

ESET Security Management Center furnizează informații actualizate referitoare la starea tuturor computerelor personalului IT, indiferent dacă on-premise sau off-premise. De asemenea, oferă vizibilitate în toate OS-urile pe care o companie le-ar putea avea. În cele mai multe cazuri, vizibilitatea este, de asemenea, îmbunătățită pentru a afișa informații la nivel de dispozitiv, cum ar fi stocurile hardware sau software.

MANAGEMENT

Peisajul de securitate cibernetică de astăzi evoluează în mod constant prin noi metode de atac și amenințări nemaiîntâlnite 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. În plus, acest lucru poate determina organizațiile să își schimbe complet politicile de configurare pentru a se proteja mai bine împotriva unui viitor atac.

ESET Security Management Center permite organizațiilor să își adapteze politicile sau configurațiile produselor de securitate endpoint în orice moment. În plus, sarcinile pot fi executate atât de la distanță, cât și automat pe dispozitive pentru a salva administratorii IT de executarea sarcinilor pe fiecare calculator în mod individual.

RAPORTARE

Majoritatea organizațiilor de astăzi, în cazul în care nu au nevoie să respecte orice conformitate, au cerințe interne legate de raportare. Indiferent de organizație, vor exista rapoarte care trebuie generate la intervale regulate și furnizate părților relevante sau stocate pentru o dată ulterioară.

ESET Security Management Center permite organizațiilor să configureze rapoartele care să fie generate la intervale regulate și să fie salvate în anumite dosare sau să fie trimise prin e-mail direct persoanei care le-a solicitat. Rapoartele pot fi personalizate pentru a oferi solicitantului rapoartele exact cum le-ar putea dori. Acest proces este esențial pentru a salva timpul administratorilor IT și pentru a îi lăsa să se ocupe de alte activități din cadrul domeniului lor de muncă.

"Avantajul major oferit de ESET este că aveți toți utilizatorii dintr-o singură consolă și puteți gestiona și examina corect starea lor de securitate."

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

Rapoartele pot fi personalizate pentru a oferi solicitantului rapoartele exact cum le dorește.

Vizibilitatea în incidente de securitate în timp real este extrem de importantă pentru a permite personalului IT să răspundă prompt și să atenueze orice risc care s-ar fi putut dezvolta.

Indiferent de organizație, vor exista rapoarte care trebuie generate la intervale regulate și furnizate părților relevante sau stocate pentru viitor.

ESET Security Management Center dispune de peste 170 de rapoarte integrate și vă permite să creați rapoarte personalizate pe baza a peste 1000 de puncte de colectare a datelor.

Grupurile dinamice pot sorta și filtra calculatoarele pe baza stării actuale a dispozitivului, care se schimbă o dată la ceva timp.

Diferența ESET

PREVENȚIE ȘI RĂSPUNS

ESET îmbină managementul produselor dedicate endpoint cu soluția de Endpoint Detection and Response - ESET Enterprise Inspector - împreună cu o soluție sofisticată de cloud sandbox - ESET Dynamic Threat Defense - într-o singură consolă de administrare, foarte ușor de folosit.

REMEDIERE A AMENINȚĂRILOR DINTR-UN SINGUR CLICK

Din tab-ul amenințări, puteți crea o excludere, încărca fișiere pentru analiză suplimentară sau puteți iniția o scanare dintr-un singur clic.

SISTEM DE NOTIFICARE COMPLET PERSONALIZABIL

Sistemul de notificare conține un editor complet, foarte ușor de folosit, unde veți putea configura în întregime notificările, pentru a primi avertismente în legătură cu informațiile exacte despre care doriți să fiți anunțat.

RAPORTARE DINAMICĂ ȘI PERSONALIZATĂ

ESET Security Management Center dispune de peste 170 de rapoarte integrate și vă permite să creați rapoarte personalizate pe baza a peste 1000 de puncte de colectare a datelor.

CADRUL DE AUTOMATIZARE

Grupurile dinamice pot sorta calculatoarele pe baza stării actuale ale dispozitivelor sau pe baza criteriilor de includere definite. Sarcinile pot fi apoi setate pentru a declanșa acțiuni, cum ar fi scanări, modificări de politică sau instalări / dezinstalări de software bazate pe modificările dinamice ale grupului.

SUPORT VDI COMPLET AUTOMATIZAT

Algoritmul complex de detectare a hardware-ului este utilizat pentru a determina identitatea dispozitivului, pe baza hardware-ului său. Acesta permite funcțiile de re-image automatizat și clonarea mediilor hardware non-persistente.

DOVEDID ȘI DE ÎNCREDERE

ESET se află în industria de securitate de peste 30 de ani și continuăm să ne dezvoltăm tehnologia pentru a rămâne cu un pas înaintea celor mai noi amenințări. Acest lucru ne-a determinat să câștigăm încrederea a peste 110 de milioane de utilizatori din întreaga lume. Tehnologia noastră este constant verificată și validată de către terții de testare care demonstrează cât de eficientă esste abordarea noastră în a opri cele mai recente amenințări.

"Companie remarcabilă, suport tehnic superb, asigură o protecție puternică a amenințărilor și un management central."

— Dave, Manager of IT; Deer Valley Unified School District, USA; 15.500+ seats

Cazuri de utilizare

Ransomware

Un utilizator deschide un e-mail rău intenționat care conține o nouă formă de ransomware.

SOLUȚIE

Departamentul IT primește o notificare prin e-mail și prin intermediul sistemului de operare SIEM conform căreia a fost detectată o nouă amenințare la un anumit computer.

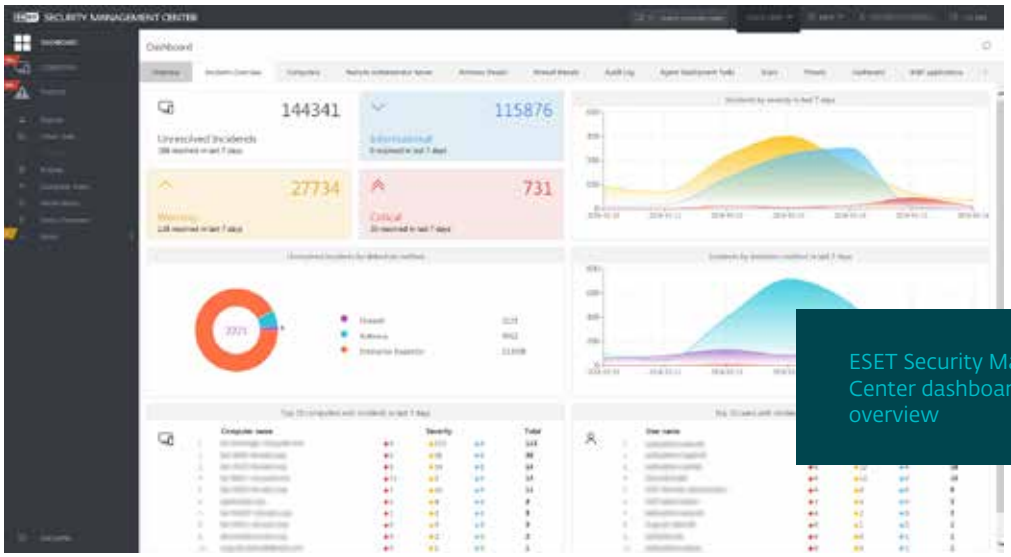
- ✓ O scanare este inițiată cu un singur click pe computerul infectat.
- ✓ Fișierul este trimis la ESET Dynamic Threat Defense cu un alt click.
- ✓ După confirmarea stării de pericol, avertismentele din ESET Security Management Center sunt șterse automat.

Programatori

Programatorii care lucrează cu coduri pe computerul de lucru pot avea tendința de a crea detecții fals - pozitive din cauza compilării software-ului.

SOLUȚIE

- ✓ Departamentul IT primește o notificare prin e-mail și prin SIEM-ul său că a fost găsită o nouă amenințare.
- ✓ Notificarea arată că amenințarea provine de la computerul unui programator.
- ✓ Cu un singur click, fișierul este trimis la ESET Dynamic Threat Defense pentru a confirma că fișierul nu este rău intenționat.
- ✓ Departamentul IT, cu un singur click, plasează o excludere pentru a preveni afișarea în acest dosar a unor detecții fals - pozitive viitoare.



ESET Security Management Center dashboard – incidents overview

VDI deployments

Non-persistent hardware environments typically require manual interaction from an IT department or create reporting and visibility nightmares.

SOLUTION

- ✓ After deploying a master image to computers already present in ESET Security Management Center, computers will continue reporting to the previous instance despite a complete re-image of the system.
- ✓ Machines that after the end of a work shift return back to their initial state will not cause duplicate machines and instead will be matched into one record.
- ✓ On deployment of non-persistent images, you can create an image that includes the agent, then whenever a new machine is created with another hardware fingerprint, it automatically will create new records in ESET Security Management Center.

Hardware and software inventory

Organizations need to know what software is installed on each computer, as well as how old each computer is.

SOLUTION

- ✓ View every installed piece of software, including version number, in the computer record.
- ✓ View every computer's hardware details, such as device, manufacturer, model, serial number, processor, RAM, HD space and more.
- ✓ Run reports to view a more holistic view of an organization to make budgetary decisions on hardware upgrades in future years based off current make and models.

Software remediation

Organizations need to know when an unapproved software has been installed, then are required to remediate the software afterwards.

SOLUTION

- ✓ Set up a dynamic group within ESET Security Management Center to look for a specific unwanted piece of software.
- ✓ Create a notification to alert the IT department when a computer meets this criterion.
- ✓ Set up a software uninstall task in the ESET Security Management Center to execute automatically when a computer meets the dynamic group criteria.
- ✓ Set up a user notification that automatically pops up on the user's screen indicating that they committed a software installation violation by installing the above software.

ESET Security Management Center poate fi instalat pe Windows, Linux sau implementat ca Virtual Appliance.

Multi-tenancy support and 2FA secured logins allow full streamlining of responsibilities across large enterprise teams.

"Siguranța administrată centralizat pentru toate terminalele, serverele și dispozitivele mobile a fost un beneficiu-cheie pentru noi."

— IT Manager; Diamantis Masoutis S.A., Greece; 6.000+ seats

Caracteristicile ESET Security Management Center

INSTALARE FLEXIBILĂ

ESET Security Management Center poate fi instalat pe Windows, Linux sau ca Virtual Appliance. După instalare, tot managementul se realizează prin intermediul unei console web, facilitând accesul și administrarea de pe orice dispozitiv sau sistem de operare.

PANOU DE INSTRUMENTE UNIFICAT

Toate soluțiile ESET Endpoint care rulează pe Windows, mac OS, Linux pot fi administrate printr-o singură consolă, ESET Security Management Center. În plus, ESET Security Management Center dispune de Mobile Device Management (MDM) complet pentru dispozitivele Android și iOS.

COMPLET MULTI-TENANT

Mulți utilizatori și grupuri de permisiune pot fi create pentru a permite accesul la o porțiune limitată a instanței ESET Security Management Center. Acest lucru permite raționalizarea completă a responsabilităților în cadrul întreprinderilor mari.

STOCARE HARDWARE/SOFTWARE

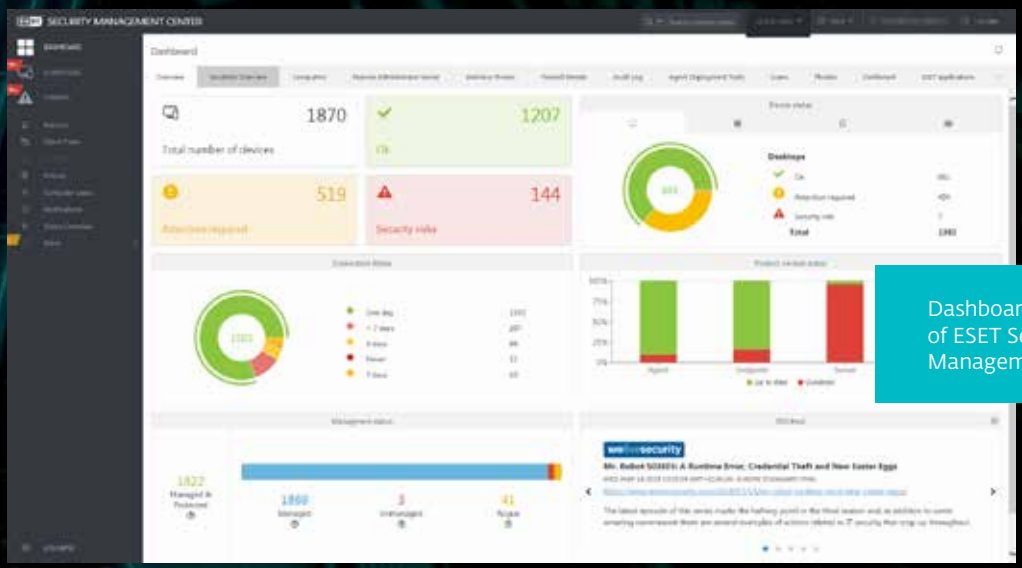
Nu numai că ESET Security Management Center raportează despre toate aplicațiile software instalate dintr-o organizație, ci și despre hardware-ul instalat. Acest lucru vă permite să faceți mai mult dintr-o singură locație prin gruparea dinamică a computerelor bazate pe marcă, model, OS, procesor, RAM, spațiu HD și multe alte elemente.

GRANULAR POLICY CONTROL

Organizațiile pot să configureze mai multe politici pentru același computer sau grup și pot impune politici pentru permisiunile moștenite. În plus, organizațiile pot selecta ca setările de politică să fie deschise configurării de către utilizatori, astfel încât să puteți bloca orice număr de setări de la utilizatorii finali.

SIEM SUPPORT

ESET Security Management Center suportă în întregime instrumentele SIEM și poate afișa toate informațiile de jurnal în formatele JSON sau LEEF, care sunt universal acceptate.



Dashboard
of ESET Security
Management Center

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

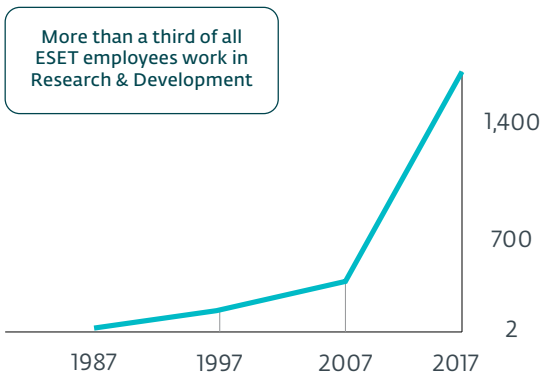
110m+
utilizatori în întreaga lume

400k+
clienți business

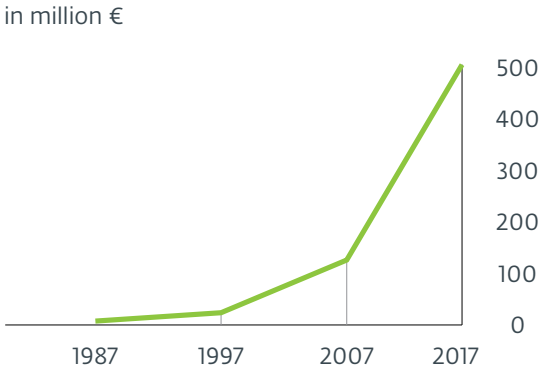
200+
țări & teritorii acoperite

13
centre globale de R&D

ANGAJAȚII ESET



VENITURI ESET



*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

protejat de ESET din 2011

licență prelungită de 3x, extinsă de 2x

protejat de ESET din 2008

licență prelungită/extinsă de 10x

protejat de ESET din 2016

peste 14,000 stații de lucru

partener ITP din 2008

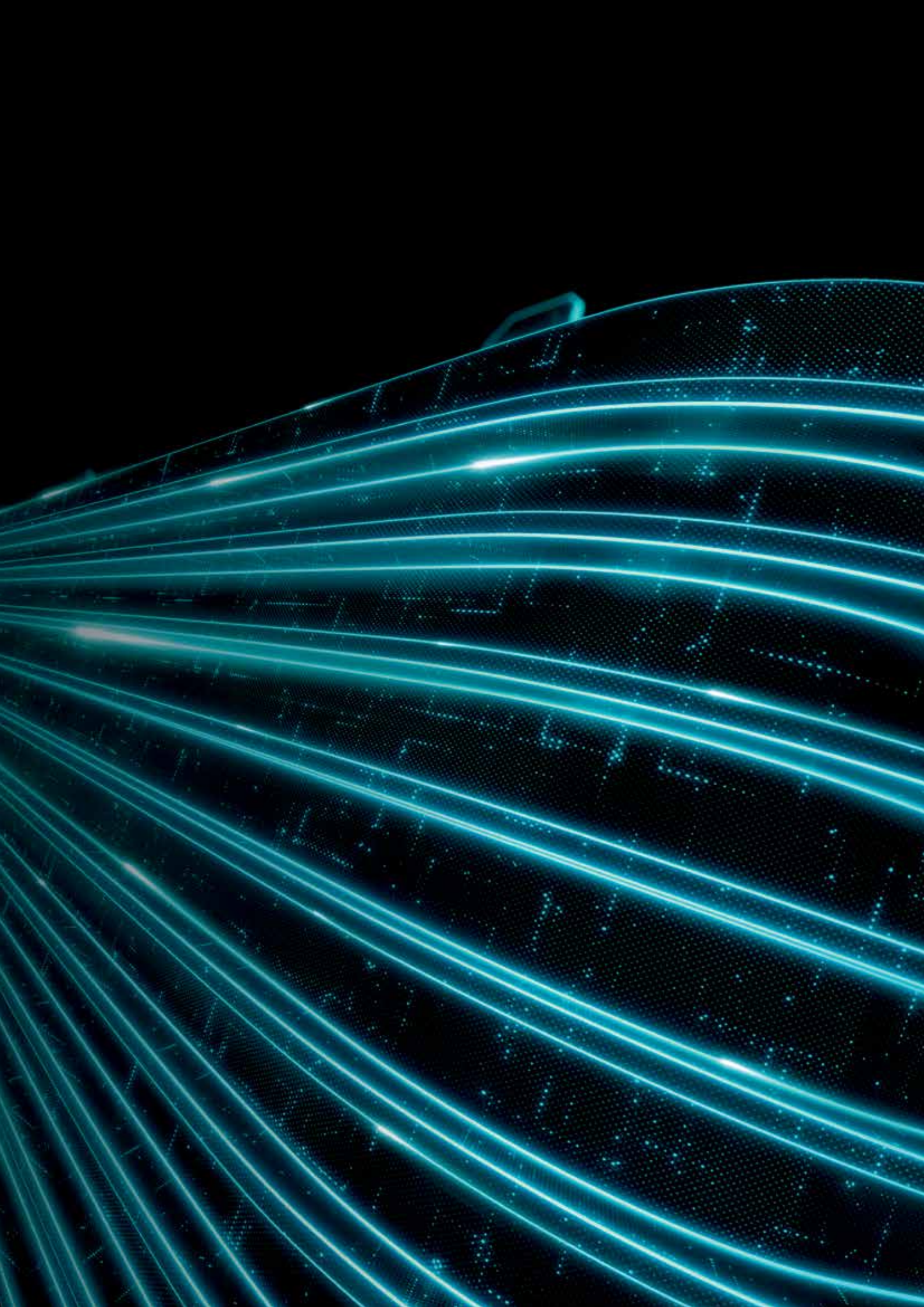
bază de clienți - 2 milioane

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



ENJOY SAFER TECHNOLOGY™