SOLUTION OVERVIEW

PROTECT

Platformă unificată de management a securității, cu o vizibilitate superioară asupra rețelei

Progress. Protected.

Ce este o **consolă de management pentru protecția endpoint?**

ESET PROTECT este o consolă UEM versatilă, care poate fi implementată on-premise sau în cloud, care asigură vizibilitate în timp real pentru stațiile endpoint on-premise și off-premise, plus raportare completă și management al securității pentru toate sistemele de operare.

Are integrat un panou unificat de instrumente pentru soluțiile ESET implementate în rețea. Acesta controlează prevenirea, detectarea și răspunsul final pe toate platformele - acoperind desktop-uri, servere, mașini virtuale și chiar dispozitivele mobile gestionate.

De ce este nevoie de **management al securității?**

VIZIBILITATE

Amenințările zero-day, APT-urile, atacurile direcționate și botneturile reprezintă o preocupare pentru industriile din întreaga lume. O vizibilitate asupra acestor amenințări în timp real este extrem de importantă pentru a-i permite personalului IT să răspundă prompt și să atenueze orice risc ce s-ar putea dezvolta. Datorită presiunii continue asupra companiilor de a dezvolta o forță de muncă mobilă, vizibilitatea nu mai este necesară doar on-premise, ci și off-premise.

ESET PROTECT oferă informații actualizate pentru personalul IT, despre starea tuturor stațiilor endpoint instalate on-premise sau off-premise. De asemenea, oferă vizibilitate asupra tuturor sistemelor de operare deținute de o companie. În cele mai multe cazuri, vizibilitatea este îmbunătățită prin afișarea de informații la nivel de dispozitiv cum ar fi inventare hardware sau software, pentru a se asigura conștientizarea completă a situației.

MANAGEMENT

Peisajul securității cibernetice de astăzi este în continuă evoluție, cu noi metode de atac și amenințări nemaivăzute. Când are loc un atac sau o breșă de date, organizațiile sunt de obicei surprinse că au fost compromise mecanismele lor de apărare sau nu sunt complet conștienți că a avut loc un atac. După ce atacul este descoperit, organizațiile pot dori apoi să execute sarcini specifice pe diferite dispozitive, cum ar fi scanarea. Acest lucru poate conduce organizațiile să-și schimbe complet politicile de configurare pentru a se proteja mai bine împotriva unui atac viitor.

ESET PROTECT vine cu politici predefinite puternice și inteligente, dar le permit organizațiilor să ajusteze politicile sau configurațiile securității endpoint în orice moment. În plus, sarcinile pot fi automatizate pentru a salva din timpul personalului IT, care ar fi trebuit să le execute pe fiecare calculator individual.

RAPORTARE

Pe lângă faptul că trebuie să îndeplinească reglementările de conformitate, cele mai multe organizații au la rândul lor protocoale interne legate de raportare. Indiferent de organizație, vor exista rapoarte ce trebuie generate la intervale programate și furnizate părților relevante sau stocate pentru utilizare ulterioară.

ESET PROTECT poate să genereze rapoarte la intervale programate, să le salveze în dosare specifice sau să le trimită direct prin e-mail celui care l-a solicitat. Există zeci de modele utile de rapoarte, iar acestea pot fi folosite fie imediat sau personalizat, pentru a furniza solicitantului datele de care are nevoie. Acest proces este primordial pentru a le salva administratorilor IT din timp în munca asociată cu raportarea continuă.

„Avantajul major al ESET este că ai toți utilizatorii pe o singură consolă și poți gestiona și revizui corect starea lor de securitate."

Jos Savelkoul, Team Leader ICT-Department; Spitalul Zuyderland, Olanda, peste 10.000 de stații

Vizibilitatea asupra acestor amenințări în timp real este extrem deimportantă pentru a permite personalului IT să răspundă prompt și să atenueze orice risc ce ar putea să se dezvolte.

Indiferent de organizație, vor exista rapoarte ce trebuie generate la intervale programate și furnizate părților relevante sau stocate pentru utilizare ulterioară.

Diferența ESET

PREVENȚIE LA RĂSPUNS

Într-o singură consolă, ESET PROTECT combină gestionarea mai multor soluții de securitate ESET. De la prevenirea amenințărilor până la depistare și răspuns, acestea acoperă întreaga organizație pe mai multe nivele, pentru cea mai solidă protecție.

REMEDIERE INCIDENTE CU UN SINGUR CLICK

Din tabloul de bord principal, un administrator IT poate evalua rapid situația și răspunde la probleme. Acțiuni precum crearea unei excluderi, trimiterea unui fișier spre analiză sau inițierea unei scanări sunt disponibile într-un singur click. Excluderile pot fi făcute prin numele amenințării, URL, hash sau combinație.

RBAC AVANSAT

Începând cu accesul protejat cu MFA, consola este echipată cu un Sistem de control al accesului (RBAC), bazat pe roluri. Asociați administratorii și utilizatorii de consolă la anumite sucursale ale rețelei, grupuri de obiecte și specificați seturi de permisiuni cu un grad ridicat de granularitate.

SISTEM DE NOTIFICARE COMPLET PERSONALIZABIL

Sistemul de notificare vine cu un editor „what you see is what you get", unde veți putea configura de la zero notificările pentru a fi alertat cu exactitate despre informațiile cu care vreți să rămâneți la curent.

RAPORTARE DINAMICĂ ȘI PERSONALIZATĂ

ESET PROTECT oferă peste 170 de rapoarte încorporate și vă permite să creați rapoarte personalizate din peste 1000 de puncte de date. Acest lucru le permite organizațiilor să creeze rapoarte, care să arate exact așa cum își doresc. Odată create, rapoartele pot fi configurate pentru a fi generate și trimise prin e-mail la intervale programate.

AUTOMATIZARE CADRU

Grupurile dinamice pot sorta calculatoarele în funcție de starea curentă a dispozitivului sau includerea criteriilor definite. Sarcinile pot fi atunci configurate pentru a declanșa acțiuni precum scanări, modificări de politică sau instalări/dezinstalări de software bazate pe modificările de membri în cadrul grupurilor dinamice.

SUPORT VDI COMPLET AUTOMATIZAT

Un hardware cuprinzător cu algoritm de detectare este folosit pentru a determina identitatea

mașinii în funcție de hardware-ul său. Acest lucru permite re-imaging automat și clonarea de medii hardware nepersistente. Prin urmare, suportul VDI de la ESET nu necesită interacțiune manuală și este complet automatizat.

PROTECȚIE DOVEDITĂ ȘI DE ÎNCREDERE

ESET se află în industria de securitate cibernetică de peste 30 de ani și continuă să-și dezvolte tehnologia pentru a rămâne cu un pas înaintea cele mai noi amenințări. Acest lucru a făcut ca peste 110 milioane utilizatori din întreaga lume să aibă încredere în noi. Tehnologia noastră este verificată și validată în mod constant de către testeri terți care arată cât de eficientă este abordarea noastră în oprirea celor mai recente amenințări.

ADAPTAT LA MSP-URI

Dacă sunteți un furnizor de servicii gestionate (MSP), răspunzător pentru rețelele clienților, veți aprecia capabilitățile multi-tenancy ale ESET PROTECT. Licențele MSP sunt detectate automat și sincronizate cu serverul de licențiere, iar consola vă permite să faceți acțiuni avansate, cum ar fi să instalați/eliminați orice aplicație terță, să rulați scripturi, să dați comenzi de la distanță, să listați procesele care rulează, Configurații HW etc.

„Companie remarcabilă, suport tehnic excelent, care oferă o protecție puternică împotriva amenințărilor și management centralizat.”

Dave, Manager IT, Districtul școlar unificat Deer Valley, SUA,
peste 15.500 de stații

Cazuri de utilizare

Ransomware

Un utilizator deschide un e-mail rău intenționat care conține un formular nou de ransomware

SOLUȚIE

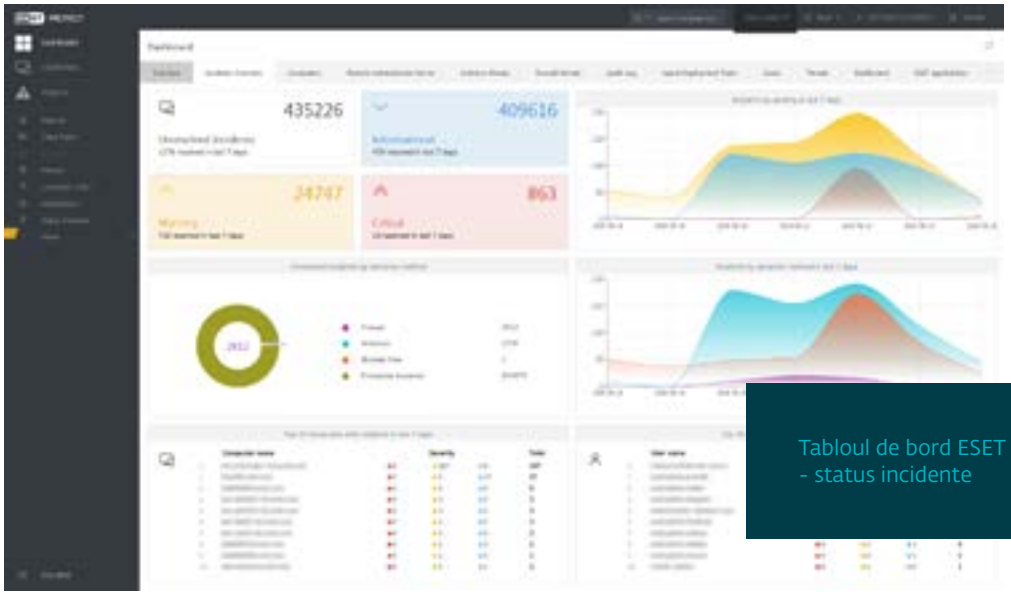
- ✓ Departamentul IT primește o notificare prin e-mail și SIEM că s-a detectat o nouă amenințare pe un anumit computer.
- ✓ O scanare este inițiată cu un singur click pe calculatorul infectat.
- ✓ Fișierul este trimis către ESET LiveGuard Advanced cu un alt click.
- ✓ După confirmarea că amenințarea este sub control, avertismentele din consola ESET PROTECT sunt șterse automat

Dezvoltatorii de cod

Programatorii care lucrează cu cod pe computerele lor ar putea crea rezultate false pozitive din cauza software-ului de compilare.

SOLUȚIE

- ✓ Departamentul IT primește o notificare prin e-mail și SIEM că a fost găsită o nouă amenințare.
- ✓ Notificarea arată că amenințarea provine din computerul unui dezvoltator.
- ✓ Cu un singur click, fișierul este trimis către ESET LiveGuard Advanced pentru a confirma că fișierul nu este rău intenționat.
- ✓ Departamentul IT, cu un singur click, crează o excludere pentru a preveni ca viitoarele fals pozitive să fie afișate în acest folder.



Tabloul de bord ESET PROTECT - status incidente

Implementări VDI

Mediile hardware nepersistente necesită de obicei interacțiune manuală din partea unui departament IT și crează dificultăți la nivel de raportare și vizibilitate..

SOLUȚIE

- ✓ După implementarea unei imagini master pe computerele deja prezente în ESET PROTECT, computerele vor continua raportarea la instanța anterioară în ciuda unui proces de re-imaging completă al sistemului.
- ✓ Mașinile care revin la starea inițială la sfârșitul un schimb de lucru nu vor cauza mașini duplicate și, în schimb, vor fi corelate într-o singură înregistrare.
- ✓ La implementarea de imagini nepersistente, puteți crea o imagine care include agentul, deci ori de câte ori o nouă mașină este creată cu altă amprenta hardware, se creează automat noi înregistrări în ESET PROTECT.

Inventar hardware și software

Organizațiile trebuie să știe ce software este instalat pe fiecare computer, dar și cât de vechi este fiecare computer.

SOLUȚIE

- ✓ Vizualizați fiecare bucată de software instalată, inclusiv numărul versiunii, în înregistrarea computerului.
- ✓ Vizualizați detaliile hardware ale fiecărui computer, cum ar fi tipul dispozitivului, producător, model, număr de serie, procesor, RAM, spațiu HD și multe altele.
- ✓ Rulați rapoarte pentru a avea o viziune mai holistică a unei organizații în vederea luării deciziilor bugetare privind upgrade-urile hardware în anii următori pe baza mărcilor și modelelor actuale.

Remediere software

Organizațiile trebuie să știe când a fost instalat software neaprobat și să remedieze ulterior acel soft.

SOLUȚIE

- ✓ Configurați un grup dinamic în ESET PROTECT pentru a căuta o anumită bucată de software nedorită.
- ✓ Creați o notificare pentru a alerta departamentul IT atunci când un computer îndeplinește acest criteriu.
- ✓ Configurați o sarcină de dezinstalare a software-ului în consola ESET PROTECT pentru a se executa automat atunci când un computer îndeplinește criteriile de grup dinamic.
- ✓ Configurați o notificare de utilizator care apare automat pe ecranul utilizatorului, indicând că acesta a comis o încălcare a instalării software-ului prin instalarea software-ului în cauză.

ESET PROTECT poate rula ca o consolă cloud, poate fi instalată on-prem pe Windows sau Linux, ori poate fi implementată ca un aparat virtual.

Suportul multi-tenancy și autentificarea securizată 2FA permit raționalizarea completă a responsabilităților în cadrul echipelor mari din companii.

„Securitatea gestionată centralizat pe toate stațiile endpoint, servere și dispozitive mobile a fost un beneficiu cheie pentru noi."

Manager IT, Diamantis Masoutis S.A., Grecia, peste 6.000 stații

Caracteristici tehnice

PANOU UNIFICAT DE INSTRUMENTE

Toate produsele ESET endpoint pot fi gestionate din consola ESET PROTECT. Aceasta include stațiile de lucru, dispozitivele mobile, servere și mașini virtuale și următoarele sisteme de operare: Windows, macOS, Linux și Android.

SUPORT PENTRU XDR

Pentru a contribui în continuare la conștientizarea statusului securității și a oferi vizibilitate în cadrul rețelei, ESET PROTECT funcționează împreună cu ESET Inspect, componenta de activare XDR a platformei ESET PROTECT. ESET Inspect este de tip multiplatformă (Windows, macOS și Linux), permite threat-hunting avansat și remediere și se poate integra perfect cu centrul de operațiuni de securitate al fiecărei organizații.

CRIPTARE FULL DISK (FDE)

Criptarea completă a discului este nativă pentru ESET PROTECT. Gestionează criptarea datelor atât pe Windows, cât și pe endpointuri Mac (FileVault), îmbunătățind securitatea datelor, și ajută organizațiile în atingerea conformității cu reglementările privind datele

ADVANCED THREAT DEFENSE

Suportul pentru apărarea avansată împotriva amenințărilor îmbunătățește detecția amenințărilor zero-day, cum ar fi ransomware, analizând rapid fișierele suspecte în instanța de sandboxing în cloud al ESET. În plus, rulează o baterie de scanări de programe malware, printre care și „cloud detonation”.

INVENTARUL HARDWARE/SOFTWARE

ESET PROTECT nu numai că raportează toate instalările de aplicații software din cadrul unei organizații, dar oferă și rapoarte despre hardware-ul instalat.

MULTITENANT

Se pot crea mai mulți utilizatori și grupuri de permisiuni pentru a permite accesul la o porțiune limitată a consolei ESET PROTECT. Acest lucru permite eficientizarea completă a responsabilităților în echipele mari ale întreprinderilor.

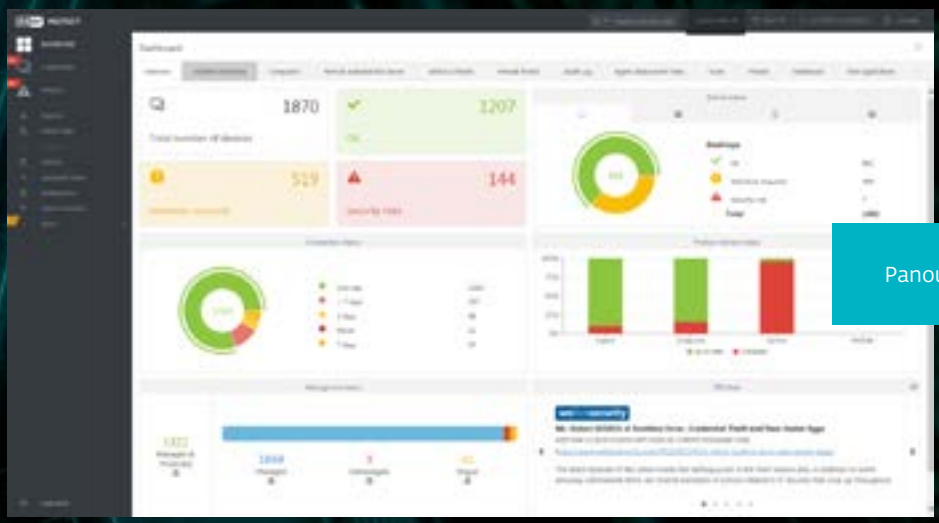
În plus, vă permite să faceți mai mult dintr-o singură locație prin gruparea dinamică a calculatoarelor în funcție de marcă, model, sistem de operare, procesor, RAM, spațiu HD și multe alte articole.

CONTROL GRANULAR DE POLITICĂ

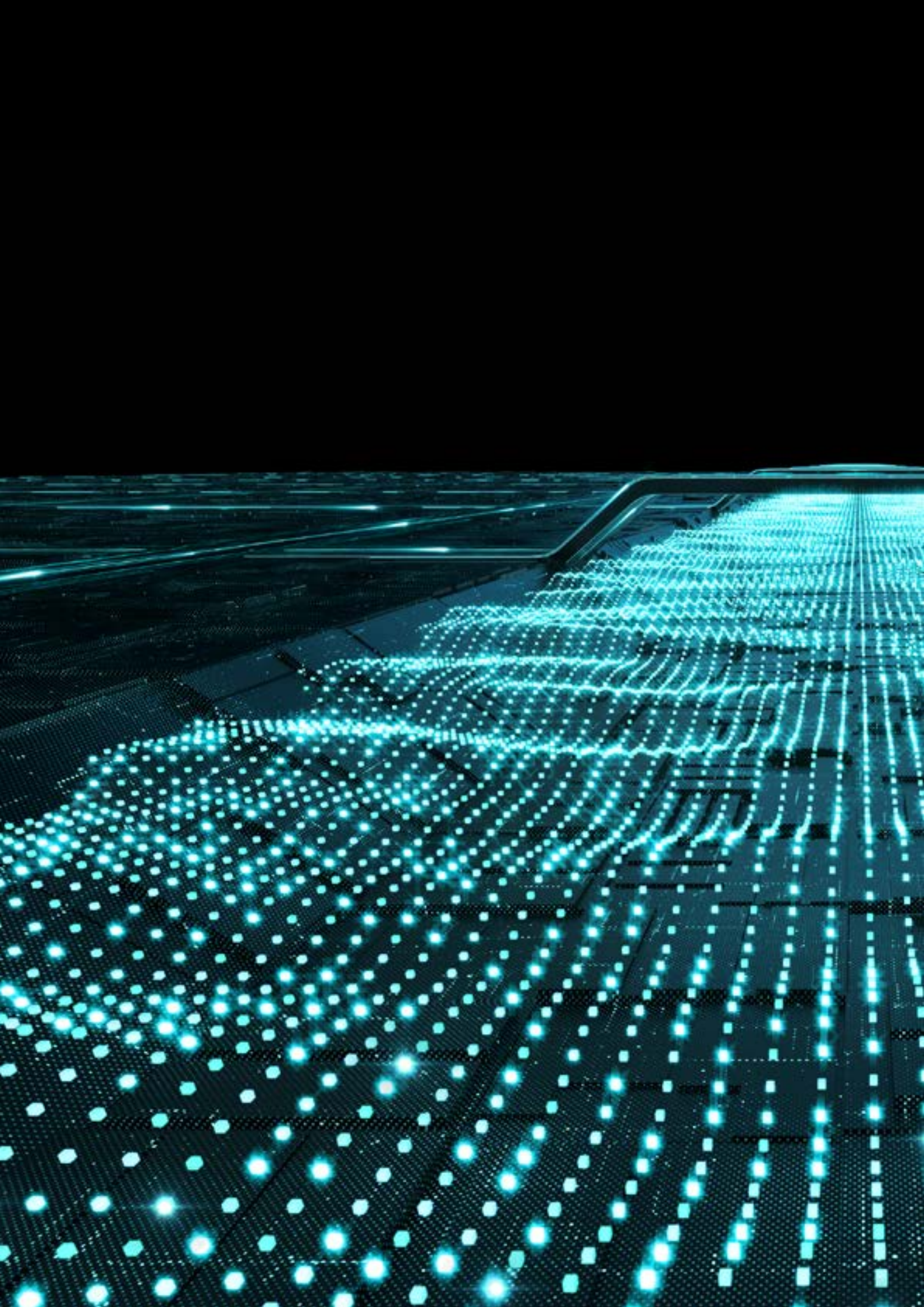
Organizațiile pot configura mai multe politici pentru același computer sau grup și pot crea politici pentru permisiunile moștenite. În plus, organizațiile pot configura setările politicii ca fiind configurabile de către utilizator, astfel încât să puteți reduce orice număr de setări de la utilizatorii finali.

SUPORT SIEM ȘI SOC

ESET PROTECT suportă pe deplin instrumentele SIEM și poate scoate toate informațiile de jurnal în formatele JSON sau LEEF, permițând integrarea cu Centrele de operațiuni de securitate (SOC).



Panou al ESET PROTECT



Următorul pas

Cum cumpărați:
Puteți alege oricare dintre soluțiile business direct din *site-ul nostru web dedicat.*

Începeți perioada de trial de 30 de zile acum.
Deblocați cele 30 de zile de testare gratuită pentru a vă bucura pe deplin de funcțiile soluției, inclusiv de protecție a stațiilor endpoint.

30-DAY TRIAL

Migrarea de la consola ESET locală:
Utilizați în prezent consola locală ESET? Contactați suportul tehnic ESET pentru a vă ajuta cu migrația. *https://www.eset.ro/*

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".


Digital Security
Progress. Protected.