



MOBILE PROTECTION

Tehnologie multistratificată, învățare automatizată și expertiză umană ce lucrează împreună pentru a oferi securitate cuprinzătoare, pentru toate platformele.

Progress. Protected.



Ce este o **soluție de securitate** a dispozitivelor mobile?

Un produs de protecție pentru dispozitivele mobile poate fi împărțit în două categorii distincte: securitate și management.

Caracteristicile de securitate variază de la antimalware, anti-phishing, limitarea accesului la conexiuni nesigure și multe altele.

Managementul include ștergerea de la distanță a datelor de pe dispozitive, restricționarea instalărilor de aplicații, preconfigurarea dispozitivelor pentru utilizatori și alte acțiuni legate de managementul IT.

Protecția dispozitivelor mobile acoperă terminalele Android și Apple, cele două cele mai răspândite sisteme de operare mobile. Având în vedere că aceste sisteme de operare sunt diferite, și capacitățile protecție mobilă pot varia în funcție de sistemul căruia i se adresează.

De ce aveți nevoie de o soluție de securitate a dispozitivelor mobile?

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 critice. 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.

Oferind multiple straturi de protecție, ESET Endpoint Security pentru Android asigură prevenirea și detectarea atacurilor ransomware la nivelul dispozitivelor mobile ale forței de muncă a organizației. Este deosebit de important pentru toate companiile să prevină și să detecteze ransomware-ul, pentru că de fiecare dată când o răscumpărare a accesului la date este plătită, aceasta convinge infractorii să continue să utilizeze această metodă de atac.

DISPOZITIVE FURATE SAU PIERDUTE

Lucru de acasă sau de la distanță au devenit mai degrabă regula decât excepția. Organizațiile lucrează pentru a facilita acest lucru, dar asigurarea accesului securizat de la distanță aduce cu sine un nou set de provocări, inclusiv problema dispozitivelor furate și /sau pierdute. Acestea nu conțin numai documente, fișiere și e-mailuri legate de muncă, dar pot de asemenea stoca informații care ar putea dăuna reputației organizației.

Soluțiile de securitate ESET MDM (Mobile Device Management) pentru platformele mobile permite administratorilor IT ai unei companii să blocheze de la distanță sau să șteargă date de pe anumite dispozitive. Acest lucru asigură că acea informație sensibilă nu este compromisă atunci când un dispozitiv este pierdut sau furat, și nici în cazul unui angajat concediat.

MANAGEMENTUL DISPOZITIVIELOR

Organizațiile, din motive legate de asumare a răspunderii sau a gestionării timpului, vor să se asigure că angajații lor folosesc dispozitivele furnizate de către companie, exclusiv în scop de serviciu. În plus, dispozitivele mobile devin mai riscante când au permisiunea de a se conecta la rețele nesigure sau când acestea au anumite funcții activate.

Soluțiile ESET pentru platformele mobile permit organizațiilor restricționarea accesului pentru utilizatori pentru anumite aplicații, filtrarea apelării anumitor numere, precum și activarea anumitor caracteristici ale dispozitivelor precum camere video, Wi-Fi și Bluetooth. În plus, această funcționalitate poate fi implementată pe baza unui program prestabilit, de exemplu restricțiile sunt activate numai pe perioada orelor de lucru.

În 2014 a fost identificat primul ransomware pe Android, cunoscut sub formă de Simplocker.



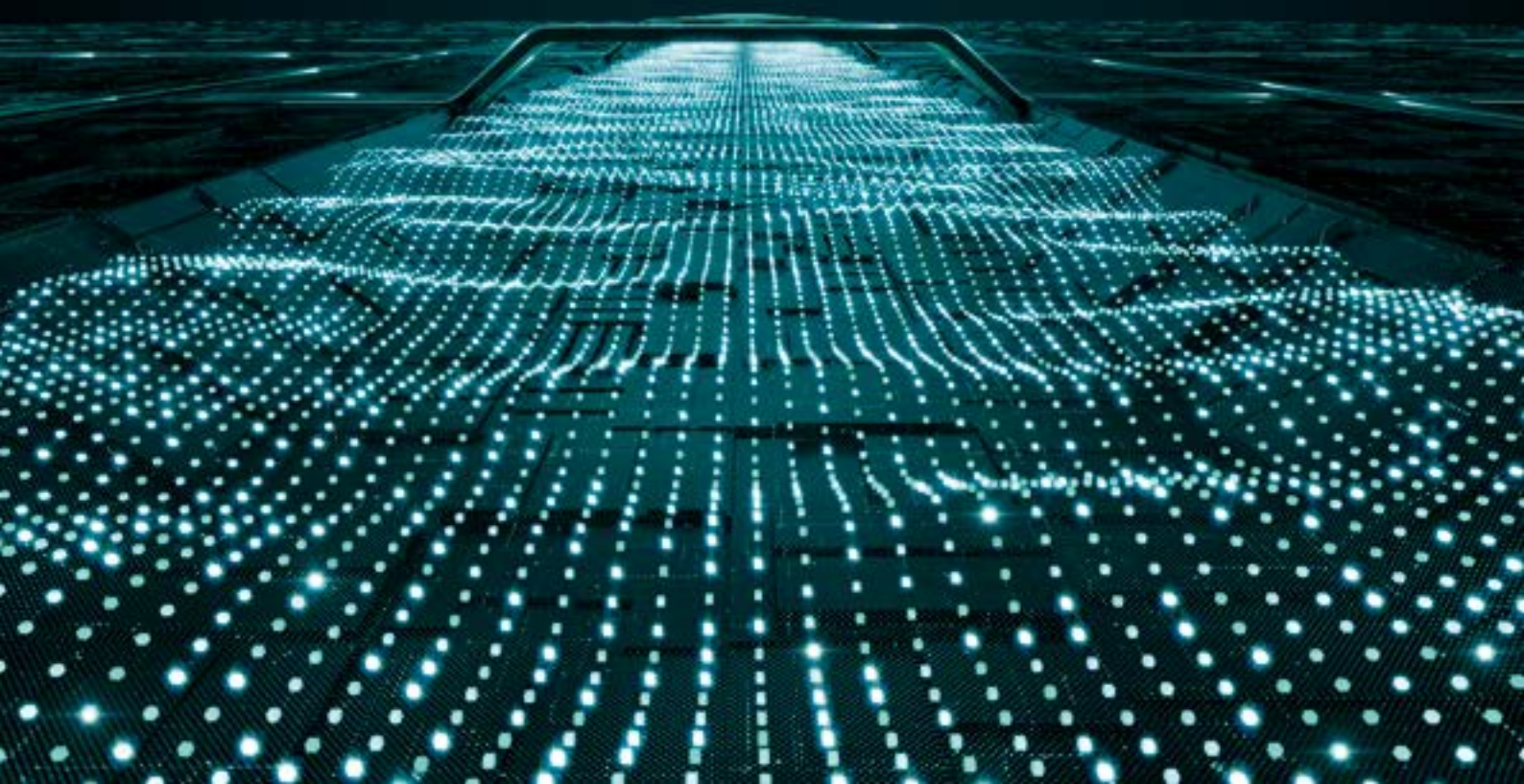
Lucrul de la distanță este acum normalitatea și organizațiile se repliază pentru a le oferi angajaților lor libertatea și confortul oferit de acesta. Dar companiile își dau seama că oferirea de acces sigur de la distanță aduce cu sine un nou set de provocări, inclusiv problema dispozitivelor pierdute și/sau furate. Acestea nu conțin doar documente, fișiere și e-mailuri legate de muncă, ci pot stoca și informații care ar putea dăuna reputației organizației.

Este important ca toate companiile să prevină și să detecteze ransomware-ul, pentru că de fiecare dată când răscumpărarea este plătită, răufăcătorii se simt motivați și vor continua astfel să dezvolte noi scheme de atac.

Nu este nevoie de soluții dedicate pentru componenta completă Mobile Device Management. Supravegheați smartphone-urile și endpoint-urile dintr-un singur panou de control cu ESET PROTECT.

„Avantajul major al ESET este că controlează toți utilizatorii dintr-o singură consolă și poate gestiona și revizui în mod corespunzător statutul lor de securitate.”

Jos Savelkoul, Team Leader în Departamentul ICT, din Spitalul
Zuyderland, Olanda - 10.000+ de stații



Diferența pe care o aduce ESET

EFICIENTIZAREA COSTURILOR

Nu este nevoie de soluții dedicate pentru componenta Mobile Device Management. Supravegheați smartphone-urile și dispozitivele endpoint dintr-un singur panou de control cu ESET PROTECT.

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 actualizează în mod constant pentru a oferi cel mai bun echilibru între detecție, nr, minim de alerte fals-pozitive și performanță.

SISTEMUL ESET DE PROTECȚIE ÎN CLOUD ÎMPOTRIVA MALWARE

Ori de câte ori o amenințare zero-day apare, de pildă noi atacuri ransomware, fișierul suspect este trimis către sistemul de protecție împotriva malware, bazat pe cloud - LiveGrid®, unde amenințarea este executată și comportamentul este monitorizat. Rezultatele acestui test sunt apoi furnizate tuturor endpoint-urilor la nivel global, în doar câteva minute, fără a necesita actualizări.

CAPABILITĂȚI DOVEDITE ȘI DE ÎNCREDERE

ESET este prezent în industria securității de peste 30 de ani și continuă să-și dezvolte tehnologia pentru a rămâne cu un pas înaintea celor mai noi amenințări. Drept urmare, ESET este acum considerabil un produs de securitate de încredere de peste 110 milioane de utilizatori din întreaga lume.

PERFORMANȚĂ FĂRĂ EGAL

De nenumărate ori, una dintre preocupările unei organizații este impactul asupra performanței de lucru pe care îl au soluțiile de securitate la nivel de endpoint. Produsele ESET continuă să exceleze în domeniul vitezei și consumului de resurse și dovedesc în cadrul testelor independente ce impact redus au asupra performanței sistemelor protejate.

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 derivate din analiza celor mai recente amenințări sau vectorii de atac. tehnologii bazate pe cele mai recente amenințări sau pe vectorii noi de atac.

„Soluțiile de securitate ESET au protejat și alertat departamentul IT de la Primoris în numeroase ocazii asupra riscului unor amenințări și infectări grave, cel mai important asupra atacurilor ransomware.”

Joshua Collins, Data Center Operations Manager pentru compania
Primoris Services Corporation, USA - 4.000+ de stații

Cazuri de utilizare

Ransomware

Programele de tip ransomware nu sunt o amenințare doar pentru desktop-uri și servere, acestea reprezintă o amenințare și pentru dispozitivele mobile. Companiile doresc să se asigure că toate datele lor sunt protejate de la atacuri de răscumpărare.

SOLUȚIE

- ✓ Implementați ESET Endpoint Security pentru Android pe toate dispozitive mobile pentru a se asigura că aceste terminale Android sunt protejat de orice tip de malware.
- ✓ Restricționați dispozitivele Android de la instalarea aplicațiilor din surse necunoscute pentru a limita riscul.

Dispozitive conforme

Fiecare organizație are politici diferite legate de utilizarea dispozitivelor mobile, iar administratorii de rețea doresc să se asigure că toate dispozitivele sunt conforme cu reglementările companiei.

SOLUȚIE

- ✓ Limitați aplicațiile care pot fi instalate pe dispozitive.
- ✓ Restricționați accesul la rețelele Wi-Fi nesecurizate.
- ✓ Asigurați-vă că funcțiile de securitate ale telefoanelor sunt activate și implementate.

Pierdere de date

Organizațiile nu sunt preocupate doar de problema dispozitivelor pierdute sau furate, dar și de scenariul de furt de date atunci când un angajat este concediat.

SOLUȚIE

- ✓ Aplicați politica de securitate care necesită ca toate dispozitivele mobile să fie criptate.
- ✓ Implementați politici de securitate care necesită ca parolele sau autentificarea prin cod PIN să fie obligatoriu setate pe toate dispozitivele.
- ✓ Blocați dispozitivele sau ștergeți datele de pe acestea de la distanță, atunci când este necesar.



„Securitatea gestionată centralizat pentru toate terminalele, serverele și dispozitivele mobile a fost un beneficiu cheie pentru noi.”

IT Manager pentru Diamantis Masoutis S.A., Greece - 6.000+ de stații

Organizațiile nu sunt preocupate doar de problema dispozitivelor pierdute sau furate, dar și de scenariul de furt de date atunci când un angajat este concediat.

Caracteristici tehnice

Android/iOS

ANTI FURT

Blocați cu ușurință de la distanță accesul, ștergeți datele stocate sau porniți rapid o alarmă atunci când un dispozitiv este pierdut sau furat. În plus, puteți trimite mesaje personalizate direct către dispozitive sau puteți configura informațiile ecranului de blocare pentru a vă asigura că dispozitivele sunt returnate proprietarilor de drept.

CONTROLUL APLICAȚIILOR

Oferă administratorilor opțiuni de monitorizare a instalării de aplicații, de blocare a accesului la anumite aplicații definite, de crearea de permisiuni sau categorii și de trimitere de solicitări către utilizatori pentru deinstalarea anumitor aplicații.

SECURITATEA DISPOZITIVULUI

Securitatea dispozitivului, gestionată de utilizator, de obicei nu este implementată în mod corespunzător. Soluția ESET permite administratorilor să definească complexitatea cerințelor privind alcătuirea parolei, să seteze temporizatoarele pentru blocarea ecranului sau să solicite prompt utilizatorilor să cripteze dispozitivul, să blocheze accesul la camera video sau altele.

CONSOLĂ FLEXIBILĂ DE MANAGEMENT

Gestionați toate endpoint-urile, dispozitivele și serverele din consola ESET PROTECT, care

poate să fie bazată pe cloud sau on-premises, în funcție de nevoile dvs.. ESET PROTECT este o consolă UEM (Unified Endpoint Management), care oferă o imagine de ansamblu completă a securității rețelei dvs..

Doar Android

PROTECȚIE MULTISTRATIFICATĂ

Un singur nivel de protecție nu este suficient pentru peisajul amenințărilor în continuă evoluție. Toate produsele de securitate ESET au capacitatea de a detecta programele malware înainte, în timpul și după execuție, toate rămânând optimizate pentru mobil.

MACHINE LEARNING

ESET folosește învățarea automatizată împreună cu toate celelalte straturi de protecție – și a făcut astfel încă din 1997. În mod specific, tehnologia machine learning este utilizată sub formă de output consolidat și rețele neuronale.

ANTI-PHISHING

Protejează utilizatorii de siteuri web false care încearcă să obțină parole, date bancare și alte informații sensibile.

AUDITUL APLICAȚIILOR

Urmărește aplicațiile și accesul acestora la datele personale/ale companiei sortate pe categorii, permițând administratorilor de rețea să monitorizeze și să controleze permisiunile aplicațiilor.

CONTROL WEB

Controlați sau restricționați site-urile web pe care utilizatorii le pot accesa de pe dispozitivele gestionate, pentru a evita conținutul inadecvat, dăunător sau care afectează productivitatea. Folosiți șabloane de rapoarte implicite, sau configurați-vă propriul raport personalizat.

Doar iOS

PANOU DE CONTROL UNIC

Nu este nevoie de soluții dedicate - supravegheați securitatea tuturor dispozitivelor iOS din cadrul companiei dintr-un singur panou de control cu ESET PROTECT.

FILTRAREA SETĂRILORE DE CONT DE LA DISTANȚĂ

Dezactivați de la distanță setări precum Wi-Fi, VPN și schimbul de informații.

COMPATIBILITATE ABM

ABM (APPLE BUSINESS MANAGER) este o metodă puternică de înregistrare a dispozitivelor iOS corporative. Prin compatibilitatea ABM puteți înscrie automat dispozitivele în consola de protecție ESET, fără a fi nevoie de contact direct cu dispozitivul și cu interacțiune minimă de la utilizator. Acest lucru permite personalizarea completă a configurației dispozitivului, economisind timp și bani.

Alegeți propria opțiune de implementare MDM

MDM ÎN CLOUD

Această opțiune vine ca o soluție gata de utilizare, integrată cu consola de management ESET bazată pe cloud, ESET PROTECT CLOUD. Este ușor de implementat pentru organizații de orice dimensiune, deoarece nu necesită cerințe prealabile precum certificate sau componente suplimentare. MDM în cloud acoperă dispozitivele Android, iOS și iPadOS.

MDM ON-PREM

Dacă preferați să implementați consola on-premises, ESET oferă suport complet pentru această opțiune. Instalare locală acoperă dispozitivele care rulează Android, iOS și iPadOS. Pentru implementare, este necesară instalarea unui conector special pentru dispozitivele mobile.



**ESET
PROTECT**



Cu ESET PROTECT, obțineți o vizibilitate completă a rețelei, de la telefoane mobile la stații de lucru și servere.



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 completă împotriva amenințărilor cibernetice care afectează companiile și consumatorii din întreaga lume.

ESET este unul dintre pionierii implementării machine learning și de tehnologii cloud care previn, detectează și răspund în fața atacurilor malware. ESET este o companie privată care promovează la nivel mondial cercetarea științifică și dezvoltarea de software.

ESET ÎN CIFRE

1bn+
utilizatori,
la nivel global

400k+
clienți
business

200+
țări și
teritorii

13
centre
globale R&D

CÂȚIVA DINTRE CLIEȚII NOȘTRI



protejat de ESET încă
din 2017, peste 9.000
stații



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



protejat de ESET
încă din 2016, peste
32.000 stații



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

PREMIILE ESET



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



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.



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”.

