SOLUTION OVERVIEW

LIVEGUARD ADVANCED

Protecție proactivă împotriva amenințărilor zero-day și celor nemaivăzute până acum

Progress. Protected.

Ce este **Advanced Threat Defense?**

O tehnologie proactivă bazată pe cloud, care utilizează scanare adaptivă avansată, machine learning de top, sandboxing în cloud și analiză comportamentală aprofundată pentru prevenirea atacurilor direcționate, precum și a noilor tipuri de amenințări nemaivăzute până acum, mai ales de tip ransomware.

ESET LiveGuard Advanced oferă încă un nivel de securitate pentru produsele ESET precum Mail Security, Endpoint și Cloud Office Security. Tehnologia avansată bazată pe cloud constă din mai multe tipuri de senzori care completează analiza statică a codului, inspecția profundă a eșantioanelor prin machine learning, introspecție în memoria stocată și detecție bazată pe comportament.

De ce să folosiți **protecția împotriva amenințărilor bazată pe cloud?**

RANSOMWARE

Atacurile de tip ransomware au fost o preocupare constantă pentru industriile 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. În zilele noastre, 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.

Un produs proactiv de detecție a amenințărilor, bazat pe cloud, oferă un nivel suplimentar de apărare în afara rețelei companiei pentru a preveni ca ransomware-ul să fie executat într-un mediu de producție.

ATACURILE CU ȚINTĂ DIRECȚIONATĂ ȘI BREȘELE DE SECURITATE A DATELOR

Peisajul securității cibernetice de astăzi este în continuă evoluție cu metode noi de atac și amenințări nemaivăzute până acum. Când are loc 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.

Abordarea unei soluții de securitate de tip sandbox în cloud este mult mai eficientă. Aceasta nu doar privește forma sub care apare o potențială amenințare, dar observă și cum poate acționa un astfel de element potențial malițios. Acest lucru ajută ca analiza să fie mult mai concludentă atunci când se determină dacă este vorba despre un atac direcționat, o amenințare persistentă avansată sau un eveniment benign.

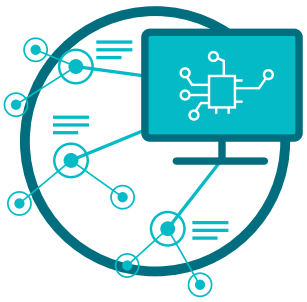
Analiza statică și dinamică este realizată de o varietate de algoritmi de învățare automatizată, care folosesc tehnici precum învățare profundă - deep learning.

O soluție de securitate de tip sandbox în cloud exterioară rețelei utilizatorului doar privește forma sub care apare o potențială amenințare dar observă și cum poate acționa un astfel de element potențial malițios.

Produsele și tehnologiile noastre se bazează pe 3 piloni

ESET LIVEGRID®

Când apare o amenințare de tip zero-day, cum ar fi ransomware, fișierul este trimis către sistemul nostru de protecție împotriva malware-ului bazat pe cloud – LiveGrid®, unde amenințarea este derulată și comportamentul este monitorizat. Rezultatele sunt furnizate tuturor endpoint-urilor la nivel global în câteva minute, fără a necesita actualizări.



MACHINE LEARNING

Utilizează puterea combinată a rețelelor neuronale și a algoritmilor selectați pentru a eticheta corect mostrele primite ca fiind curate, potențial nedorite sau malițioase.

EXPERTIZĂ UMANĂ

Cercetătorii de clasă mondială în domeniul securității împărtășesc know-how și expertiză de top pentru a asigura în mod continuu cele mai bune informații despre amenințări.

Cu ce diferă ESET

PROTECȚIE MULTISTRATIFICATĂ

ESET LiveGuard Advanced este soluție de securitate bazată pe cloud care execută toate mostrele suspecte prezentate într-un mediu de testare securizat la sediul central ESET, unde comportamentul lor este evaluat folosind feed-uri de cercetare, unele dintre multiplele instrumente interne ale ESET pentru analiză statică și dinamică și date despre reputație pentru a detecta amenințările zero-day. Pentru analiza eșantioanelor sunt folosite patru niveluri, care pot fi desfășurate dinamic în funcție de rezultatele apărute. ESET LiveGuard Advanced combină toate verdictele din straturile de detecție și evaluează statusul fiecărei probe. Rezultatele sunt livrate mai întâi către produsul de securitate ESET folosit de utilizator și către infrastructura IT a companiei.

VIZIBILITATE COMPLETĂ

Pentru fiecare probă analizată, puteți vizualiza rezultatul final în consola ESET PROTECT. Pe deasupra, clienții cu licențe pentru mai mult de 100 de stații primesc un raport complet bazat pe comportament cu informații detaliate despre probele și comportamentul lor observat în timpul analizei în sandbox – totul livrat într-o formă ușor de înțeles. Nu sunt afișate doar mostrele trimise către ESET LiveGuard Advanced, cât și toate informațiile transmise către ESET Cloud Malware Protection System - ESET LiveGrid®.

MOBILITATE

În zilele noastre, angajații din organizații apelează tot mai mult la stilul de lucru de la distanță și nu se află la sediu. Ca adaptare la noul mediu de lucru, ESET LiveGuard Advanced poate analiza fișierele indiferent unde se află utilizatorii. Vestea bună este că, dacă este detectat orice element malițios, întreaga companie este protejată imediat.

CONFIDENȚIALITATE

ESET ia foarte în serios confidențialitatea și conformitatea. Prin intermediul setărilor specifice, utilizatorul poate configura soluțiile ESET să șteargă probele imediat după analiză.

VITEZĂ FĂRĂ EGAL

Fiecare minut contează, motiv pentru care ESET LiveGuard Advanced este capabil să analizeze majoritatea mostrelor în mai puțin de 5 minute. Dacă o probă a fost analizată anterior, este vorba de doar câteva secunde până când toate dispozitivele din organizația dvs. sunt protejate.

TESTAT ȘI DE ÎNCREDERE

ESET este prezent în industria securității de peste 30 de ani, și continuă să dezvolte tehhnologia pentru a rămâne cu un pas înaintea celor mai noi amenințări. Drept urmare, 1 miliard de utilizatori de internet din întreaga lume sunt acum protejați de ESET. Soluțiile și tehnologiile sunt verificate și validate în mod constant de către testeri terți care arată cât de eficientă este abordarea ESET pentru a opri cele mai recente amenințări.

APĂRARE PROACTIVĂ

Dacă se constată că o probă este suspectă, aceasta este blocată de la execuție, în așteptarea analizei de către ESET LiveGuard Avansat. Acest lucru previne potențialele pagube pe care amenințările le pot provoca în sistemul unui utilizator. În plus, când analiza este completă și dacă este detectată o amenințare pe un singur dispozitiv endpoint conectat la rețea, informațiile respective sunt comunicate în câteva minute către toate celelalte endpoint-uri din rețea, protejând astfel imediat orice utilizator care ar fi putut fi pus în pericol.

Studii de caz

Ransomware

IPOTEZĂ

Programele ransomware au tendința să se infiltreze în căsuțele poștale ale utilizatorilor nesuspicioși prin mesajele de tip e-mail.

SOLUȚIE

- ✓ ESET Mail Security trimite automat fișierele suspecte atașate la e-mail către ESET LiveGuard Advanced.
- ✓ Apoi, ESET LiveGuard Advanced analizează proba și trimite rezultatul înapoi la Mail Security de obicei în mai puțin 5 minute.
- ✓ ESET Mail Security detectează și remediază automat fișierele atașate care conțin elemente malițioase.
- ✓ Fișierul atașat malițios nu ajunge, astfel, niciodată la destinatar.

Protecție granulară pentru diferite roluri în cadrul companiei

IPOTEZĂ

Fiecare rol în companie necesită niveluri diferite de protecție. Developerii sau angajații IT necesită restricții de securitate diferite față de office manager sau CEO.

SOLUȚIE

- ✓ Configurați în ESET LiveGuard Advanced o politică personalizată unică pentru fiecare computer sau fiecare server.
- ✓ Aplicați automat o politică diferită bazată pe grupuri diferite de utilizatori, de exemplu grup de utilizatori static sau grup Active Directory.
- ✓ Schimbați automat setările de configurare prin simpla mutare a unui utilizator dintr-un grup în altul.

Fișiere necunoscute sau dubioase

IPOTEZĂ

Uneori, angajații sau departamentul IT pot primi un fișier pe care vor să-l verifice, pentru a determina dacă este sigur.

SOLUȚIE

- ✓ Orice utilizator poate trimite direct o mostră pentru analiză, opțiune prezentă în toate produsele ESET.
- ✓ Eșantionul este analizat de ESET LiveGuard Avansat.
- ✓ Dacă se determină că un fișier este malițios, toate computerele din organizație sunt protejate.
- ✓ Administratorul IT are vizibilitate deplină asupra utilizatorului care a trimis eșantionul și asupra statusului fișierului analizat, curat sau rău intenționat.

Caracteristicile ESET LiveGuard Advanced

PROTECȚIE AUTOMATĂ

Odată ce totul este configurat, nu este necesară nicio acțiune suplimentară din partea administratorului de rețea sau a utilizatorului. Produsul de securitate instalat pe dispozitivul endpoint sau pe server decide automat dacă un eșantion este bun, rău sau necunoscut. Dacă proba este necunoscută, aceasta este trimisă către ESET LiveGuard Advanced pentru analiză. Odată ce analiza este finalizată, rezultatul este partajat și soluția de securitate acționează în consecință.

PERSONALIZARE PE COMANDĂ

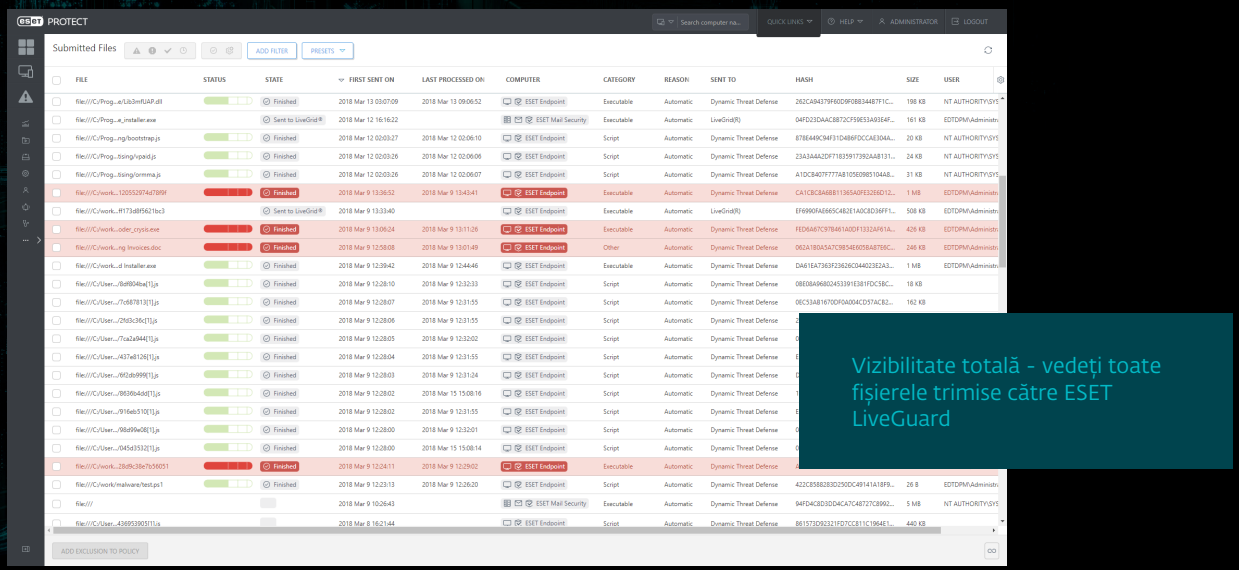
ESET permite configurarea detaliată a politicii de securitate pentru fiecare computer în parte pentru soluția ESET LiveGuard Advanced, astfel încât administratorul de rețea să poată controla ce este trimis și ce ar trebui să se întâmple pe baza rezultatul primit. În plus, setările nu pot fi aplicate doar per computer, dar și pe grup de computere.

DEPUNEREA MANUALĂ

În orice moment, un utilizator sau un administrator de rețea poate trimite mostre pentru analiză prin intermediul unui produs compatibil ESET și poate obține un rezultat complet. Administratorii vor vedea direct în consola ESET PROTECT cine și ce anume a trimis și ce rezultat a fost găsit în analiză.

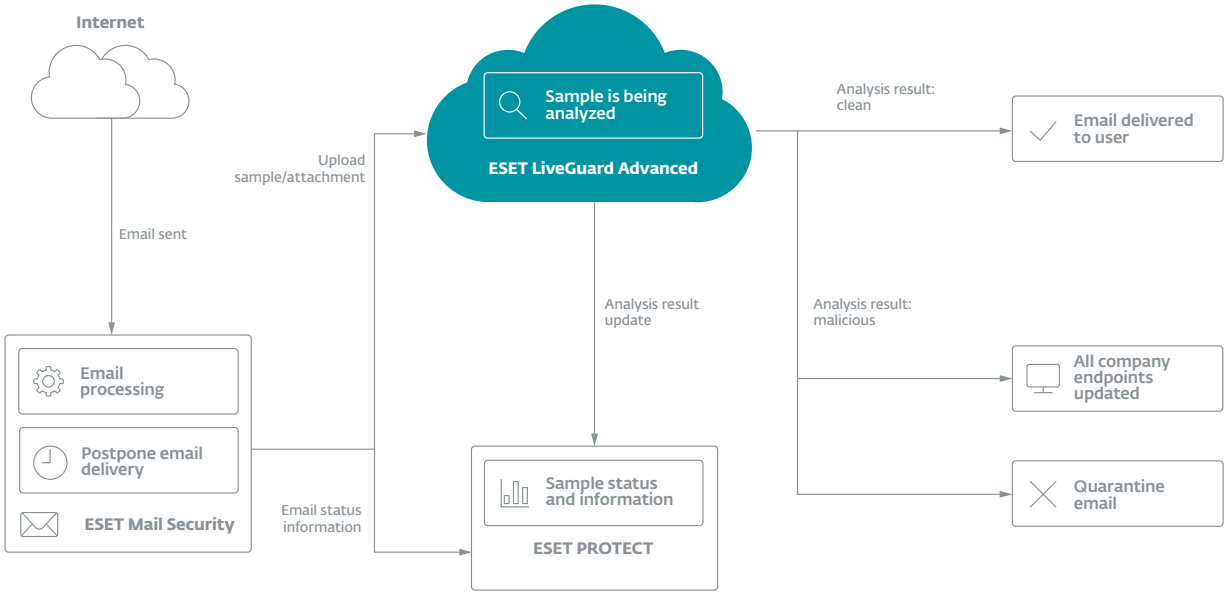
PROTECȚIE PRIN MAIL SECURITY

ESET LiveGuard Advanced nu funcționează numai pentru fișiere simple, ci funcționează și direct cu ESET Mail Security pentru a se asigura că e-mailurile rău intenționate nu sunt livrate către organizația dvs. Pentru continuitatea afacerii, doar e-mailurile care provin din afara organizației pot fi trimise către ESET LiveGuard Advanced pentru inspecție.



Cum funcționează **ESET LiveGuard Advanced**

With ESET Mail Security



ESET LiveGuard Advanced este compatibil cu ESET Endpoint, Server și produsele de securitate din aplicația Cloud (Microsoft 365) și este complet integrat în consolele de management ESET:

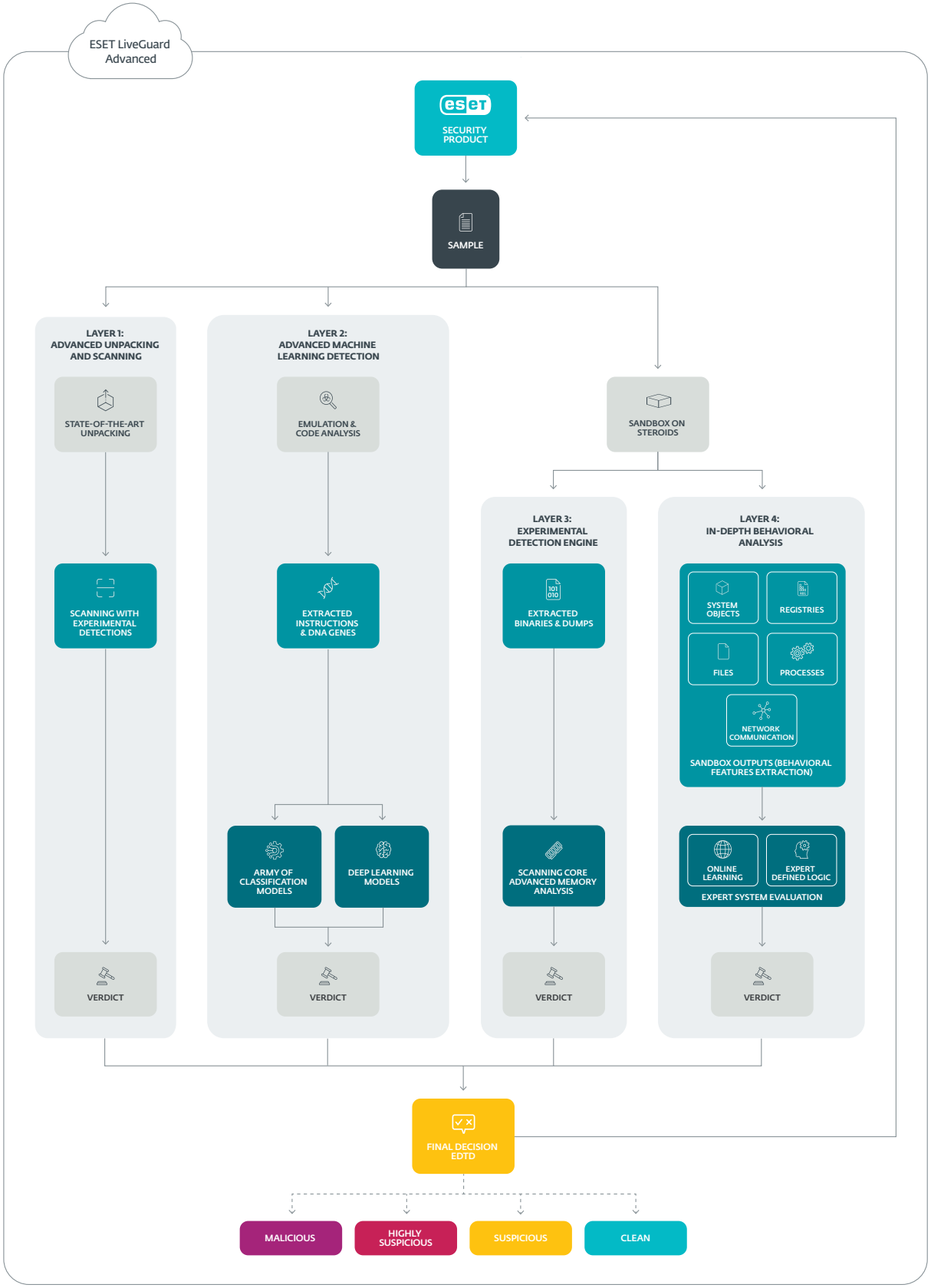
„Este un produs uimitor!"

Ce îți place cel mai mult?

„Îmi place cât de ușor a fost să îl instalez pe toate stațiile mele de lucru și cât de repede mi-a securizat rețeaua. Depistează software-ul nedorit și trimite e-mailuri zilnice despre cum oprește daune ale bug-urilor din rețea. Mă odihnesc mai bine, știind că rețeaua mea este protejată de ESET."

— Michael P. / Network manager / Mid-market (51-1,000 emp.)

Cum funcționează analiza noastră avansată



ESET LiveGuard Advanced utilizează 4 niveluri separate de detecție pentru a asigura cea mai înaltă rată de detecție. Fiecare nivel folosește o abordare diferită și oferă un verdict propriu pentru proba analizată. Evaluarea finală cuprinde rezultatele tuturor informațiilor despre mostră.

LAYER 1

Scanare și unpacking avansate

Probele sunt supuse analizei statice și procedeului de unpacking de ultimă generație, iar apoi sunt comparate cu o bază de date variată de amenințări cunoscute.

LAYER 2

Detecție avansată prin machine learning

Analiza statică și dinamică este efectuată de o serie de algoritmi de machine learning, folosind diverse tehnici, inclusiv deep learning.

LAYER 3

Motor de detecție experimentală

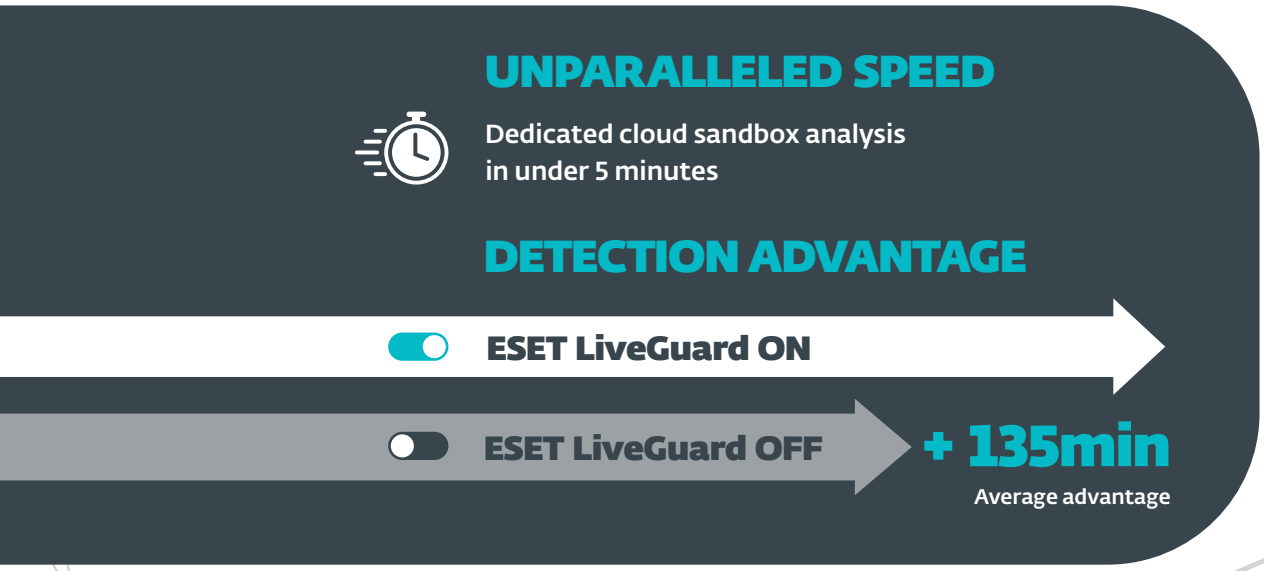
Mostrele sunt introduse într-un „sandbox la putere maximă" care seamănă foarte mult ca și scară cu dispozitivele utilizatorului. Ele sunt ulterior monitorizate pentru orice semn de comportament rău intenționat.

LAYER 4

Analiză de comportament în profunzime

Toate elementele care ies din sandbox sunt supuse apoi unei analize comportamentale în profunzime care identifică modelele malițioase cunoscute și posibile reacții în lanț.

SOLUȚIA COMBINĂ TOATE VERDICTELE OBȚINUTE ÎN URMA NIVELURILOR DE DETECȚIE ȘI EVALUEAZĂ STATUSUL FIECĂRUI EȘANTION. REZULTATELE SUNT LIVRATE ÎNT I PRODUSULUI DE SECURITATE ESET FOLOSIT DE UTILIZATOR ȘI INFRASTRUCTURII IT A COMPANIEI.



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 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

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.

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".