PREHĽAD

LIVEGUARD ADVANCED

Proaktívna cloudová ochrana pred novovznikajúcimi hrozbami s možnosťami autonómnej nápravy

Progress. Protected.

Čo je **pokročilá ochrana pred hrozbami?**

Proaktívna technológia, ktorá využíva pokročilú adaptívnu konzolu, špičkovú umelú inteligenciu, cloudový sandboxing a hĺbkovú analýzu aktivity s cieľom predchádzať cieleným útokom a doposiaľ neznámym druhom hrozieb, najmä ransomvéru. ESET poskytuje pokročilú cloudovú prevenciu hrozieb s možnosťami autonómnej nápravy a vyhľadávania hrozieb na báze cloudu. Podrobný prehľad o globálnom prostredí malvéru zaisťuje rezidentnú ochranu pred neustále sa vyvíjajúcimi kybernetickými hrozbami.

ESET LiveGuard Advanced poskytuje ďalšiu vrstvu zabezpečenia pre produkty ESET Mail Security, ESET Endpoint Security a ESET Cloud Office Security. Cloudová pokročilá technológia tohto riešenia pozostáva z viacerých typov senzorov, ktoré vykonávajú statickú analýzu kódu, hĺbkovú kontrolu vzorky s využitím strojového učenia, sledovanie vlastnej pamäte a detekciu na základe správania.

Prečo využívať **proaktívnu cloudovú ochranu pred hrozbami?**

RANSOMVÉR

Od objavenia hrozby Cryptolocker v roku 2013 predstavuje ransomvér neustále nebezpečenstvo pre rôzne odvetvia na celom svete. Hoci ransomvér existuje oveľa dlhšie, nikdy nepatril medzi významné hrozby, ktorým by firmy venovali pozornosť. V súčasnosti však aj jediný ransomvérový útok dokáže zašifrovať dôležité či kritické súbory firmy, a tak úplne znemožniť jej činnosť. V niektorých prípadoch firma po ransomvérovom útoku príde na to, že jej existujúce zálohy nie sú dostatočne aktuálne a rozhodne sa zaplatiť výkupné.

Proaktívna cloudová detekcia hrozieb s autonómnou nápravou predstavuje ďalšiu vrstvu ochrany mimo firemnej siete, vďaka ktorej sa ransomvér nikdy nespustí priamo v produkčnom prostredí firmy.

CIELENÉ ÚTOKY A ÚNIKY ÚDAJOV

Súčasný svet IT zabezpečenia sa neustále vyvíja, pribúdajú nové spôsoby útokov a doposiaľ neznáme hrozby. Keď dôjde k útoku alebo úniku údajov, organizácie bývajú prekvapené, že ich ochranné mechanizmy boli kompromitované, prípadne ani len netušia, že k útoku vôbec došlo. V reakcii na jeho odhalenie sa snažia implementovať opatrenia na zmiernenie rizík, aby sa v budúcnosti nič podobné neopakovalo. To ich však neochráni pred ďalším útokom, ktorý použije úplne nový vektor infekcie.

Cloudový sandbox je oveľa efektívnejší než obyčajné sledovanie povahy možnej hrozby, keďže sa navyše pozoruje aj jej správanie. Vďaka tomu sa dá oveľa presnejšie určiť, či ide o cielený útok, pokročilú pretrvávajúcu hrozbu alebo niečo neškodné.

Statickú a dynamickú analýzu vykonáva celý rad algoritmov strojového učenia, pričom sa využívajú rôzne techniky vrátane hĺbkového učenia.

Cloudový sandbox mimo siete používateľa neanalyzuje len povahu možnej hrozby, ale pozoruje aj jej správanie.

V čom je ESET iný

AUTONÓMNA NÁPRAVA HROZIEB

ESET LiveGuard Advanced je cloudové riešenie na ochranu pred hrozbami, ktoré všetky odoslané podozrivé vzorky spúšťa v bezpečnom testovacom prostredí v rámci cloudu ESET (v sandboxe). Vyhodnocuje ich správanie, pričom využíva informačné kanály o aktuálnych hrozbách, početné interné nástroje spoločnosti ESET na statickú a dynamickú analýzu, ako aj údaje o reputácii súborov s cieľom zachytiť malvér či zero-day hrozby. Funguje okamžite a správca ani používateľ nemusia nič nastavovať. Ak je vzorka na úrovni koncového zariadenia identifikovaná ako neznáma, odošle sa na analýzu. Po dokončení analýzy a identifikácii hrozby sa táto automaticky odstráni, čím sa zabráni prípadným narušeniam.

KOMPLEXNÝ PREHĽAD

Konzola ESET PROTECT umožňuje zobraziť výsledky každej analyzovanej vzorky. Zákazníci s licenciou určenou pre viac ako 100 zariadení navyše dostanú kompletnú správu o aktivite zaslanej vzorky s podrobnými informáciami o jej správaní zaznamenanom počas analýzy v sandboxe – všetko v prehľadnom formáte. Nejde len o jednoduchý prehľad vzoriek, ktoré boli odoslané do riešenia ESET LiveGuard Advanced, ale všetkých položiek odoslaných do cloudového systému ESET LiveGrid® na ochranu pred malvérom.

VŠADEPRÍTOMNÁ OCHRANA

Technológie spoločnosti ESET podporujú pracovné postupy vašej organizácie. ESET LiveGuard Advanced dokáže analyzovať súbory bez ohľadu na to, kde sa používatelia nachádzajú – hybridní zamestnanci či zamestnanci pracujúci na diaľku sú chránení rovnako ako pracovníci nachádzajúci sa na pôde firmy. Ak sa zistí prítomnosť škodlivého kódu, zabezpečená je okamžite celá firma.

OCHRANA SÚKROMIA

Spoločnosť ESET berie ochranu osobných údajov a dodržiavanie príslušných predpisov veľmi vážne. Prostredníctvom špecifických nastavení produktu ESET môže používateľ nastaviť, aby sa vzorky po analýze okamžite odstránili.

BEZKONKURENČNÁ RÝCHLOSŤ

Z hľadiska digitálnej bezpečnosti je veľmi dôležitý čas, preto ESET LiveGuard Advanced dokáže zanalyzovať väčšinu vzoriek za menej ako päť minút.

PROAKTÍVNA OCHRANA

Podozrivé vzorky sa nebudú môcť spustiť, kým ich ESET LiveGuard Advanced neanalyzuje. To zabráni potenciálnym hrozbám napáchať v systéme používateľa škodu. Okrem toho, po dokončení analýzy a zistení hrozby na jednom koncovom zariadení sa táto informácia v priebehu niekoľkých minút odošle do všetkých koncových zariadení vo firemnej sieti, čo zabezpečí okamžitú ochranu každého používateľa, ktorý by mohol byť potenciálne ohrozený.

JEDNODUCHÉ MANUÁLNE ODOSIELANIE, JASNÉ VÝSLEDKY

Používateľ alebo správca môže kedykoľvek odoslať vzorky na analýzu prostredníctvom konzoly ESET PROTECT a získať komplexný výsledok. Správcom sa zobrazí odosielateľ, odoslaná vzorka a výsledok analýzy.

VYLEPŠENÁ E-MAILOVÁ OCHRANA

ESET LiveGuard Advanced funguje nad rámec analýzy súborov – spolupracuje priamo s produktom ESET Mail Security či ESET Cloud Office Security s cieľom zabrániť doručovaniu škodlivých e-mailov do vašej organizácie. Z dôvodu zabezpečenia plynulého chodu firmy možno do riešenia ESET LiveGuard Advanced odoslať na kontrolu len externé e-maily.

Príklady použitia

Ransomvér

PROBLÉM

Ransomvér zvyčajne prenikne k ničnetušiacim používateľom prostredníctvom e-mailu.

RIEŠENIE

- ✓ ESET Mail Security automaticky odosiela podozrivé e-mailové prílohy do riešenia ESET LiveGuard Advanced.
- ✓ ESET LiveGuard Advanced vzorku analyzuje a potom (zvyčajne do 5 minút) odošle výsledok späť do programu ESET Mail Security.
- ✓ ESET Mail Security zachytí prílohy so škodlivým obsahom a automaticky s nimi vykoná potrebnú akciu.
- ✓ Príloha so škodlivým obsahom sa nikdy nedostane k príjemcovi.

Neznáme alebo pochybné súbory

PROBLÉM

Niekedy dostanú zamestnanci alebo IT oddelenie súbor, ktorého bezpečnosť chcú dôkladne preveriť.

RIEŠENIE

- ✓ Každý používateľ môže odoslať vzorku na analýzu priamo prostredníctvom ktoréhokoľvek produktu ESET.
- ✓ ESET LiveGuard Advanced zabezpečí rýchlu analýzu vzorky.
- ✓ Ak sa zistí, že súbor je škodlivý, všetky počítače v organizácii budú chránené.
- ✓ IT správca má dokonalý prehľad o tom, ktorý používateľ vzorku odoslal a či bol súbor neškodný alebo, naopak, škodlivý.

Dôkladná ochrana pre rôzne funkcie v spoločnosti

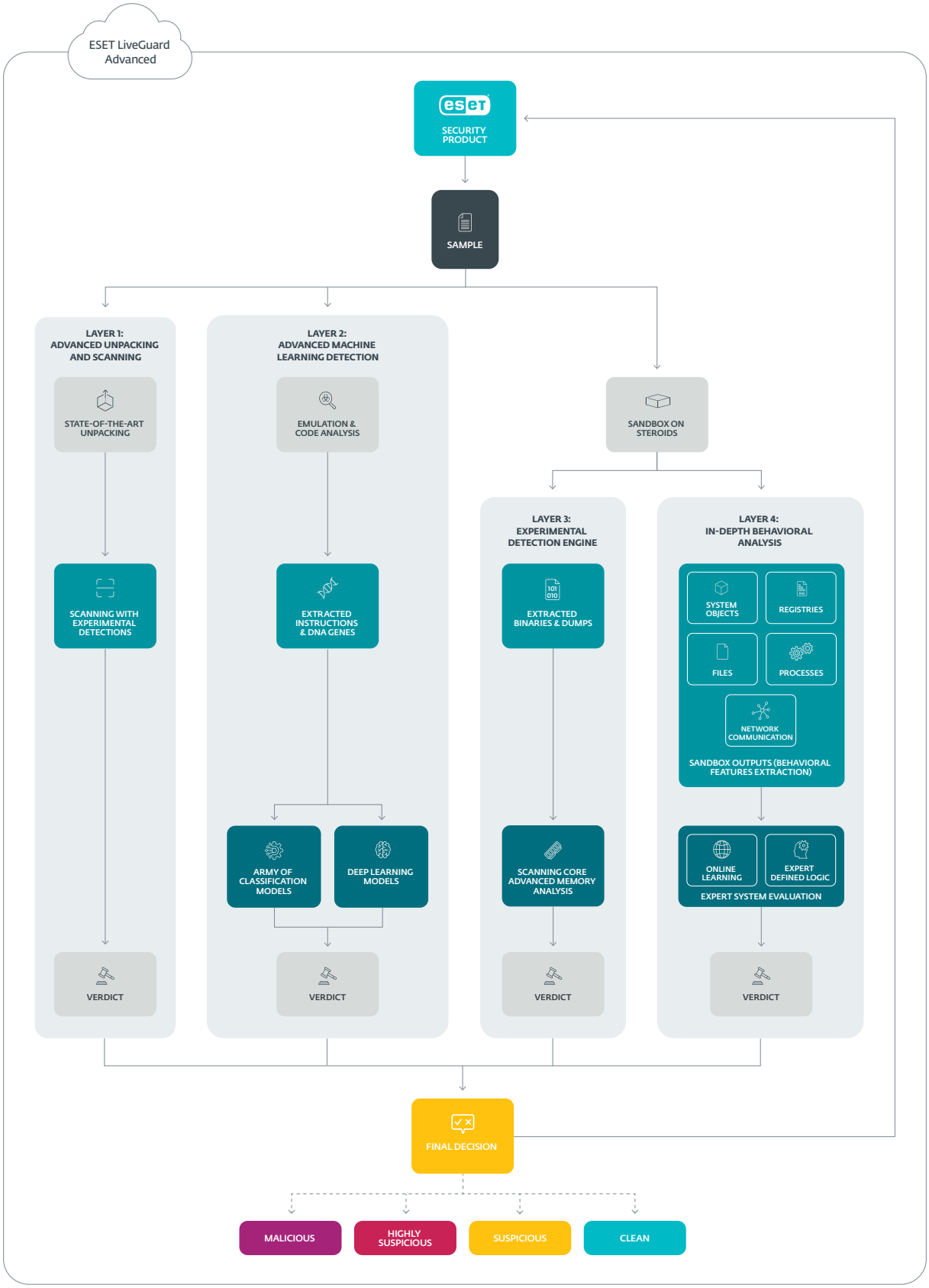
PROBLÉM

Každá funkcia v spoločnosti si vyžaduje inú úroveň ochrany. Na vývojárov či zamestnancov IT oddelenia sa musia vzťahovať iné bezpečnostné obmedzenia než na vedúceho kancelárie alebo generálneho riaditeľa.

RIEŠENIE

- ✓ Pre každý počítač alebo server nakonfigurujte jedinečnú politiku v rámci riešenia ESET LiveGuard Advanced.
- ✓ Automaticky uplatňujte rozličné politiky v závislosti od rôznych statických skupín používateľov alebo skupín služby Active Directory.
- ✓ Automaticky zmeňte nastavenia konfigurácie jednoduchým presunutím používateľa do inej skupiny.

Ako funguje naša pokročilá analýza?



ESET LiveGuard Advanced využíva štyri samostatné detekčné vrstvy na zaistenie maximálnej účinnosti detekcie. Každá vrstva uplatňuje iný prístup a prináša vlastný verdikt o vzorke. Konečné hodnotenie zahŕňa výsledky na základe všetkých informácií o vzorke.

1. VRSTVA

Pokročilá extrakcia a kontrola

Vzorky sú podrobené statickej analýze a pokročilej extrakcii, aby sa mohli následne porovnať s databázou hrozieb doplnenou aj o dosiaľ nezverejnené detekcie.

2. VRSTVA

Detekcia pokročilého strojového učenia

Statickú a dynamickú analýzu vykonáva celý rad algoritmov strojového učenia, pričom sa využívajú rôzne techniky vrátane hĺbkového učenia.

3. VRSTVA

Experimentálne detekčné jadro

Vzorky sa vložia do sústavy systémov, akýchsi „sandboxov na steroidoch“, ktoré sú veľmi podobné skutočným zariadeniam používateľov. Následne sa monitorujú, aby sa zachytil akýkoľvek náznak nebezpečnej aktivity.

4. VRSTVA

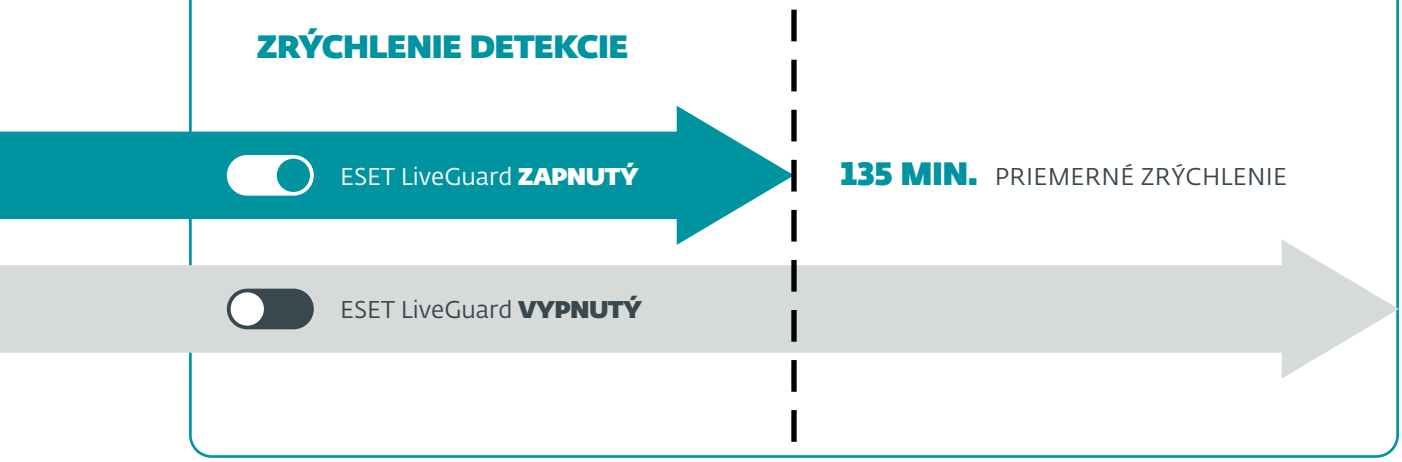
Hĺbková analýza aktivity

Všetky výstupy zo sandboxu sú podrobené hĺbkovej analýze aktivity, pri ktorej sa identifikujú známe škodlivé vzorce a reťazce akcií.

RIEŠENIE ZOHĽADNÍ VŠETKY VERDIKTY JEDNOTLIVÝCH DETEKČNÝCH VRSTIEV A VYHODNOTÍ STAV KAŽDEJ VZORKY. VÝSLEDKY SA NAJPRV ODOŠLÚ DO BEZPEČNOSTNEJ APLIKÁCIE ESET A FIREMNEJ INFRAŠTRUKTÚRY, PRIČOM ZMIERŇOVANIE RIZÍK ZAPOČNE AUTOMATICKY.

BEZKONKURENČNÁ RÝCHLOSŤ

Špecializovaná analýza v cloudovom sandboxe za menej ako 5 minút



Digital Security
Progress. Protected.

Toto je ESET

Proaktívna ochrana. Minimalizujte riziká vďaka prevencii.

Buďte o krok vpred pred známymi aj novými kybernetickými hrozbami vďaka nášmu prístupu, ktorý je založený na umelej inteligencii a zameraný na prevenciu. Kombinovaním sily umelej inteligencie a odborných znalostí našich pracovníkov dokážeme poskytovať jednoduchú a efektívnu ochranu.

ESET PROTECT, naša cloudová platforma kybernetickej bezpečnosti s podporou XDR, kombinuje next-gen schopnosti prevencie, detekcie a proaktívneho vyhľadávania hrozieb so širokou škálou bezpečnostných služieb vrátane riadenej detekcie a reakcie (MDR). Naše vysoko prispôsobiteľné riešenia zahŕňajú podporu v lokálnom jazyku, majú minimálny vplyv na výkon zariadenia, identifikujú a zneškodnia známe aj nové hrozby ešte v zárodku, podporujú plynulý chod prevádzky a znižujú náklady na implementáciu a správu.

ESET chráni vašu firmu, aby ste mohli naplno využívať potenciál technológií.

ESET V ČÍSLACH

1 mld.+
chránených používateľov internetu

400-tis.+
firemných zákazníkov

200
krajín a teritórií

13
globálnych centier výskumu a vývoja

NIEKTORÍ Z NAŠICH ZÁKAZNÍKOV

MITSUBISHI MOTORS
Drive your Ambition

Viac než 9 000 koncových zariadení chránených spoločnosťou ESET od roku 2017

Allianz Suisse

Viac než 4 000 e-mailových schránok chránených spoločnosťou ESET od roku 2016

Canon
Canon Marketing Japan Group

Viac než 32 000 koncových zariadení chránených spoločnosťou ESET od roku 2016

Bezpečnostný partner v oblasti poskytovania internetových služieb 2 miliónom zákazníkov od roku 2008

UZNANIE

AV comparatives APPROVED Business Security DEC 2023

V nezávislých testoch AV-Comparatives dosahuje ESET stabilne najlepšie výsledky a najlepšiu mieru detekcie bez falošných poplachov alebo len s minimálnym počtom nesprávne detegovaných položiek.

G2 Leader WINTER 2024

Spoločnosť ESET neustále dosahuje najvyššie hodnotenia od používateľov na globálnej platforme G2 a jej riešenia oceňujú zákazníci po celom svete.

kuppingercole ANALYSTS

ESET je podľa spoločnosti KuppingerCole celkovým a trhovým lídrom v hodnotení MDR Leadership Compass 2023.