PREGLED REŠITVE

ENDPOINT SOLUTIONS

Večplastna tehnologija, strojno učenje in človeško znanje, ki delujejo skupaj v dinamičnem ravnotežju, ki ga zagotavlja prvi globalni varnostni partner za končne točke iz Evropske unije.

CYBERSECURITY
EXPERTS ON YOUR SIDE

Kaj je **Endpoint Protection Platform?**

Platforma za zaščito končne točke (EPP) je rešitev, nameščena na delovnih napravah, da prepreči napade zlonamerne programske opreme, ki temeljijo na datotekah, odkrije zlonamerno dejavnost ter zagotovi preiskovalne in sanacijske zmogljivosti, ki so potrebne za odziv na dinamične varnostne incidente in opozorila.

ESET-ove rešitve za zaščito delovnih postaj izkoriščajo večplastni pristop, ki uporablja več tehnologij katere delujejo v dinamičnem ravnovesju, ki lahko uravnoteži zmogljivost, zaznavanje in lažne pozitivne učinke.

Zakaj **rešitve za zaščito končnih točk?**

IZSILJEVALSKA PROGRAMSKA OPREMA

Izsiljevalska programska oprema je že od Cryptolockerja leta 2013 stalna skrb industrije po vsem svetu. Čeprav izsiljevalska programska oprema obstaja že dlje časa, prej ni bila nikoli velika grožnja podjetij. Zdaj pa lahko en sam pojav izsiljevalske programske opreme zlahka onemogoči poslovanje s šifriranjem pomembnih ali bistvenih datotek.

Ko podjetje doživi napad izsiljevalske programske opreme, lahko hitro ugotovi, da varnostne kopije, ki jih ima, niso dovolj nedavne, zato plača odkupnino.

ESET-ove rešitve za zaščito končnih točk zagotavljajo več obrambnih slojev, ki ne le da preprečijo izsiljevalsko programsko opremo, temveč jo tudi zaznajo, če se kdaj pojavi v organizaciji. Pomembno je preprečiti in odkriti izsiljevalsko programsko opremo, ker vsakič, ko nekdo plača odkupnino, to spodbudi zločince, da še naprej uporabljajo ta način napada.

CILJNI NAPADI IN KRŠITVE PODATKOV

Današnja krajina kibernetske varnosti se nenehno razvija z novimi
metodami napadov in še nikoli videnih groženj. Ko pride do napada ali kršitve podatkov, so organizacije običajno presenečene, da je bila njihova obramba ogrožena, ali pa se sploh ne zavedajo,
da se je napad zgodil. Ko je napad končno odkrit, organizacije nato uvedejo ukrepe, s katerimi preprečijo, da bi se podobni napadi ponovili. Vendar jih to ne varuje pred naslednjim napadom, ki lahko uporabi povsem nov prenašalec.

ESET-ove rešitve za zaščito končnih točk uporabljajo informacije o grožnjah, ki temeljijo na njihovi globalni prisotnosti, za prednostno obravnavo in učinkovito blokiranje najnovejših groženj, preden so bile dostavljene kjer koli drugje na svetu. Poleg tega imajo naše rešitve posodobitve v oblaku, ki omogočajo hiter odziv ob nezaznavanju, ne da bi morali čakati na običajno posodobitev.

NAPADI BREZ DATOTEK

Novejše grožnje, imenovane zlonamerna programska oprema brez datotek, obstajajo izključno v računalniškem pomnilniku, zato jih zaščita na podlagi skeniranja datotek ne more zaznati.
Poleg tega bodo nekateri napadi brez datotek vplivali na trenutno nameščene aplikacije, ki so vgrajene v operacijski sistem, da bo zlonamerno obremenitev še težje zaznati. Na primer, uporaba PowerShell v teh napadih je zelo pogosta.

ESET-ove platforme za zaščito končnih točk imajo ublažitve za odkrivanje nepravilno oblikovanih ali ugrabljenih aplikacij za zaščito pred napadi brez datotek. ESET je ustvaril tudi namenske optične bralnike, ki nenehno preverjajo pomnilnik, če je kaj sumljivega. Z uporabo tega večplastnega pristopa
smo vedno korak pred najnovejšo zlonamerno programsko opremo.

ESET-ove rešitve za zaščito končnih točk nudijo več slojev obrambe, ki ne le da preprečijo škodljivo programsko opremo, ampak jo tudi zaznajo, če se kdaj pojavi v organizaciji.

Ko pride do napada ali kršitve podatkov, so organizacije običajno presenečene, da je bila njihova obramba ogrožena, ali pa sploh ne vedo, da se je napad zgodil.

Novejše grožnje, imenovane zlonamerna programska oprema brez datotek, obstajajo izključno v računalniškem pomnilniku, zato jih zaščite na osnovi skeniranja datotek ne zaznajo.

»ESET je že leta naša zanesljiva varnostna rešitev. Naredi, kar mora; vam ni treba skrbeti. Skratka, ESET pomeni: zanesljivost, kakovost in storitev.«

-Jos Savelkoul, vodja oddelka za IKT; Bolnišnica Zuyderland, Nizozemska; 10.000+ sedežev

ESET rešitve za zaščito končnih točk

ESET Endpoint Security za Windows/Mac/Android ESET Endpoint Antivirus za Windows/Mac/Linux ESET File Security za Windows Server/Linux/Azure

ESET-upravljanje mobilne naprave za Android in Apple iOS

Kako je ESET drugačen

VEČPLASTNA ZAŠČITA

ESET združuje večplastno tehnologijo, strojno učenje in človeško znanje, da našim strankam zagotavlja najboljšo mogočo raven zaščite. Naša tehnologija se nenehno prilagaja in spreminja, da zagotovi najboljše ravnovesje med zaznavanjem, lažnimi pozitivnimi učinki in zmogljivostjo.

ZMOGLJIVOST BREZ PRIMERE

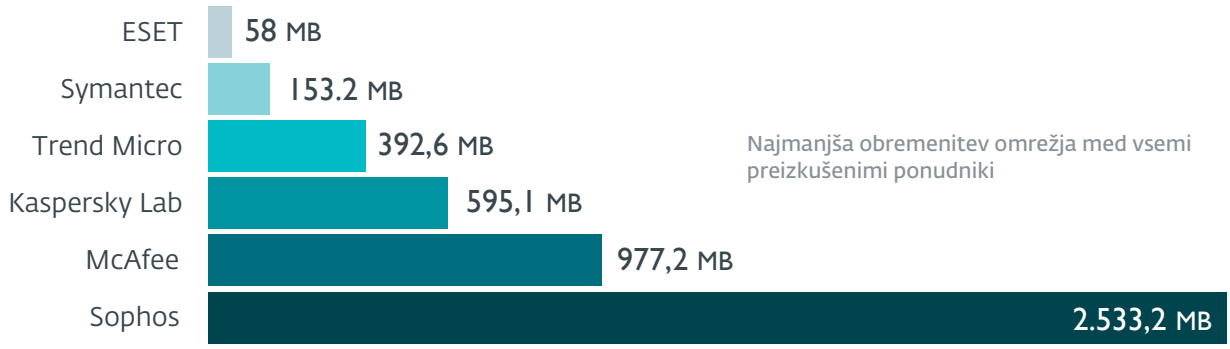
Številne organizacije skrbi učinek njihove rešitve za zaščito končnih točk. Izdelki ESET še naprej dosegajo odličnost na področju zmogljivosti in zmagujejo na testih tretjih oseb, ki dokazujejo, kako enostavne so naše končne točke na sistemih.

PODPORA CROSS PLATFORM

Izdelki ESET za zaščito končnih točk podpirajo vse operacijske sisteme, vključno z Windows, Mac, Linux in Android. Vse naše izdelke za zaščito končnih točk je mogoče v celoti upravljati z enega samega stekla; upravljanje mobilnih naprav za iOS in Android je v celoti vgrajeno.

PRISOTNOST PO SVETU

ESET ima pisarne v 22 državah po vsem svetu, raziskovalne in razvojne laboratorije v 13 državah ter je prisoten v več kot 200 državah in ozemljih. To nam omogoča, da dobimo podatke, s katerimi zaustavimo zlonamerno programsko opremo, preden se razširi po vsem svetu, in dajemo prednost novim tehnologijam, ki temeljijo na najnovejših grožnjah ali možnih novih prenašalcih.



Najmanjša obremenitev omrežja med vsemi preizkušenimi ponudniki

Vir: AV-Comparatives: Network Performance Test, Business Security Software

»Najboljši dokaz? Statistični podatki naše službe za pomoč: po uvedbi ESET-a naše osebje za podporo ne beleži nobenih klicev – ni jim treba reševati nobenih težav s protivirusnimi programi ali z zlonamerno programsko opremo.«

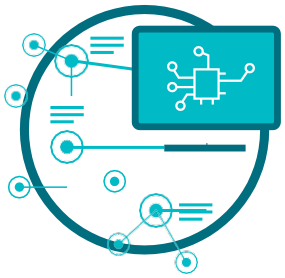
– Adam Hoffman, vodja informacijske infrastrukture; Mercury Engineering, Irska; 1.300 sedežev

Tehnologija

Naši izdelki in tehnologije temeljijo na treh stebrih

ESET LIVEGRID®

Kadar koli opazimo grožnjo ničtega dne, kot je izsiljevalska programska oprema, je datoteka poslana v naš sistem za zaščito pred zlonamerno programsko opremo v oblaku – LiveGrid®, kjer se grožnja sproži in se nadzoruje njeno vedenje. Rezultati tega sistema so na voljo vsem končnim točkam po vsem svetu v nekaj minutah, ne da bi bile potrebne posodobitve.



STROJNO UČENJE

Uporablja kombinirano moč nevronskih mrež in izbranih algoritmov za pravilno označevanje vhodnih vzorcev kot čistih, potencialno neželenih ali zlonamernih.

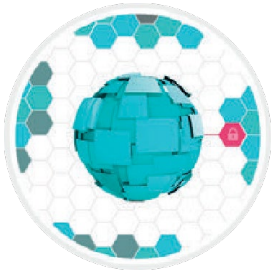
ČLOVEŠKO STROKOVNO ZNANJE

ESET-ovi svetovni raziskovalci na področju varnosti delijo elitno strokovno znanje in informacije, da našim uporabnikom zagotavljajo optimalno, neprekinjeno informacijo o grožnjah.

Ena obrambna plast ni dovolj za nenehno razvijajočo se pokrajino groženj. Vsi izdelki ESET za zaščito končnih točk lahko zaznajo zlonamerno programsko opremo pred izvajanjem, med izvajanjem in po izvajanju. Ko se osredotočamo na več kot določen del življenjskega cikla zlonamerne programske opreme, nam to omogoča najvišjo mogočo raven zaščite.

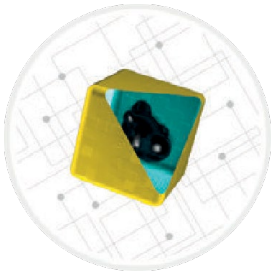
STROJNO UČENJE

Vsi izdelki ESET za zaščito končnih točk od leta 1997 poleg preostalih obrambnih slojev uporabljajo tudi strojno učenje. Natančneje, strojno učenje se uporablja v obliki trdne izhodne in nevronske mreže. Za globok pregled omrežja lahko skrbniki vklopijo poseben agresiven način strojnega učenja, ki deluje tudi brez internetne povezave.



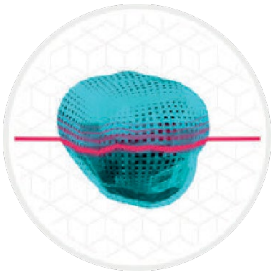
ŠČIT PRED IZSILJEVALSKO PROGRAMSKO OPREMO

ESET-ščit pred izsiljevalsko programsko opremo je dodatna plast, ki ščiti uporabnike pred izsiljevalsko programsko opremo. Ta tehnologija spremlja in ocenjuje vse izvedene aplikacije glede na njihovo vedenje in ugled. Zasnovan je tako, da zazna in blokira procese, ki spominjajo na obnašanje izsiljevalske programske opreme.



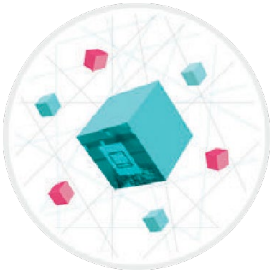
VGRAJEN PESKOVNIK

Današnja zlonamerna programska oprema je pogosto močno zamegljena in se skuša čim bolj izogniti zaznavanju. Da bi videli skozi in prepoznali resnično vedenje, skrito pod površino, uporabljamo vgrajen peskovnik. S pomočjo te tehnologije rešitve ESET posnemajo različne komponente računalniške strojne in programske opreme za izvedbo sumljivega vzorca v izoliranem virtualnem okolju.



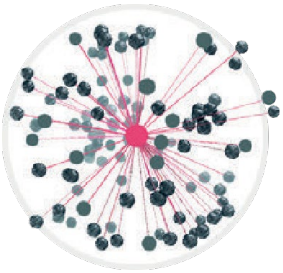
NAPREDNI OPTIČNI BRALNIK POMNILNIKA

ESET-napredni optični čitalnik pomnilnika spremlja obnašanje zlonamernega procesa in ga optično prebere, ko se ta razkrije v pomnilniku. Zlonamerna programska oprema brez datotek deluje brez stalnih komponent v datotečnem sistemu, ki jih je mogoče zaznati na običajen način. Samo optično branje pomnilnika lahko uspešno odkrije in ustavi takšne zlonamerne napade.



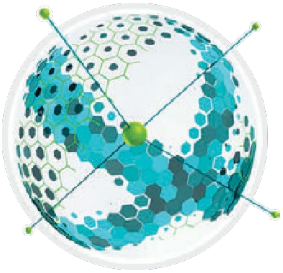
EXPLOIT BLOCKER

ESET Exploit Blocker nadzira običajno izkoriščene programe (brskalnike, bralnike dokumentov, e-poštne odjemalce, Flash, Java in druge) in se osredinja na tehnike izkoriščanja, namesto da bi le ciljal na določene CVE-identifikatorje. Ko se sproži, se grožnja takoj blokira na napravi.



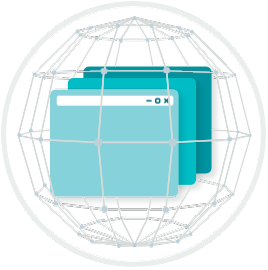
ZAŠČITA »BOTNET-a«

ESET Botnet Protection zazna zlonamerno komunikacijo, ki jo uporabljajo »botneti«, in hkrati prepozna kršitve. Vsakršna zaznana zlonamerna komunikacija je blokirana in prijavljena uporabniku.



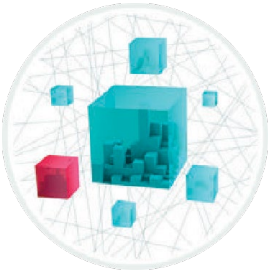
ZAŠČITA MREŽNIH NAPADOV

Ta tehnologija izboljša odkrivanje znanih ranljivosti na omrežni ravni. Predstavlja še eno pomembno plast zaščite pred širjenjem zlonamerne programske opreme, napadi, ki jih izvaja omrežje, in izkoriščanjem ranljivosti, za katere zaščita še ni bila sproščena ali uporabljena.



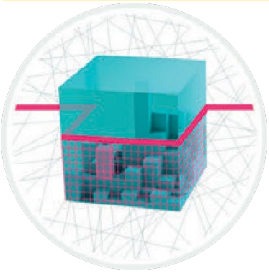
ZAŠČITEN BRSKALNIK

Zasnovan za zaščito premoženja organizacije s posebno plastjo zaščite, ki se osredinja na brskalnik, ki je glavno orodje za dostop do kritičnih podatkov znotraj intranetnega obsega in v oblaku. Varen brskalnik zagotavlja izboljšano zaščito pomnilnika za postopek brskanja skupaj z zaščito tipkovnice in omogoča skrbnikom, da dodajo url-je za zaščito



HIPS

ESET-ov sistem za preprečevanje vdorov na osnovi gostitelja spremlja sistemsko aktivnost in uporablja vnaprej določen nabor pravil za prepoznavanje sumljivega vedenja sistema. Poleg tega mehanizem samoobrambe HIPS prepreči, da bi postopek kršitve izvajal škodljivo dejavnost.

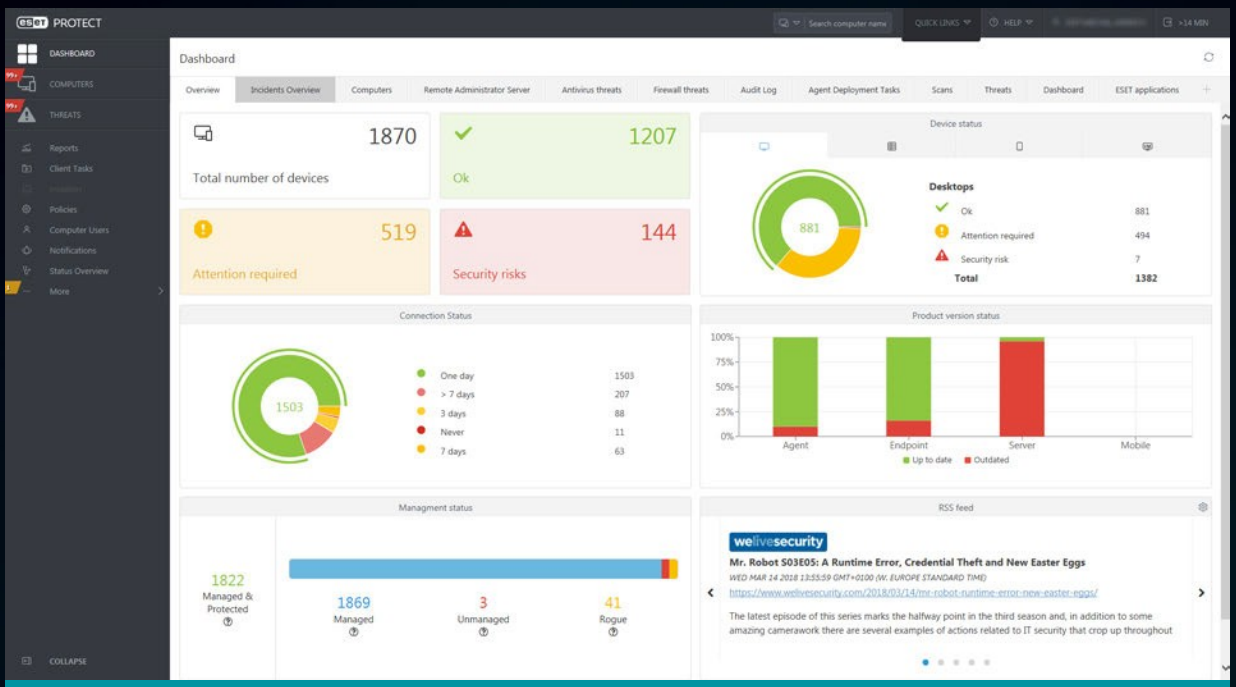


OPTIČNI BRALNIK UEFI

ESET je prvi ponudnik za zaščito končne točke, ki je v svojo rešitev dodal namensko plast, ki ščiti enotni razširljivi vmesnik strojne programske opreme (UEFI). Optični bralnik ESET UEFI preverja in uveljavlja varnost okolja pred zagonom in je zasnovan za spremljanje celovitosti strojne programske opreme. Če je sprememba zaznana, o tem obvesti uporabnika.

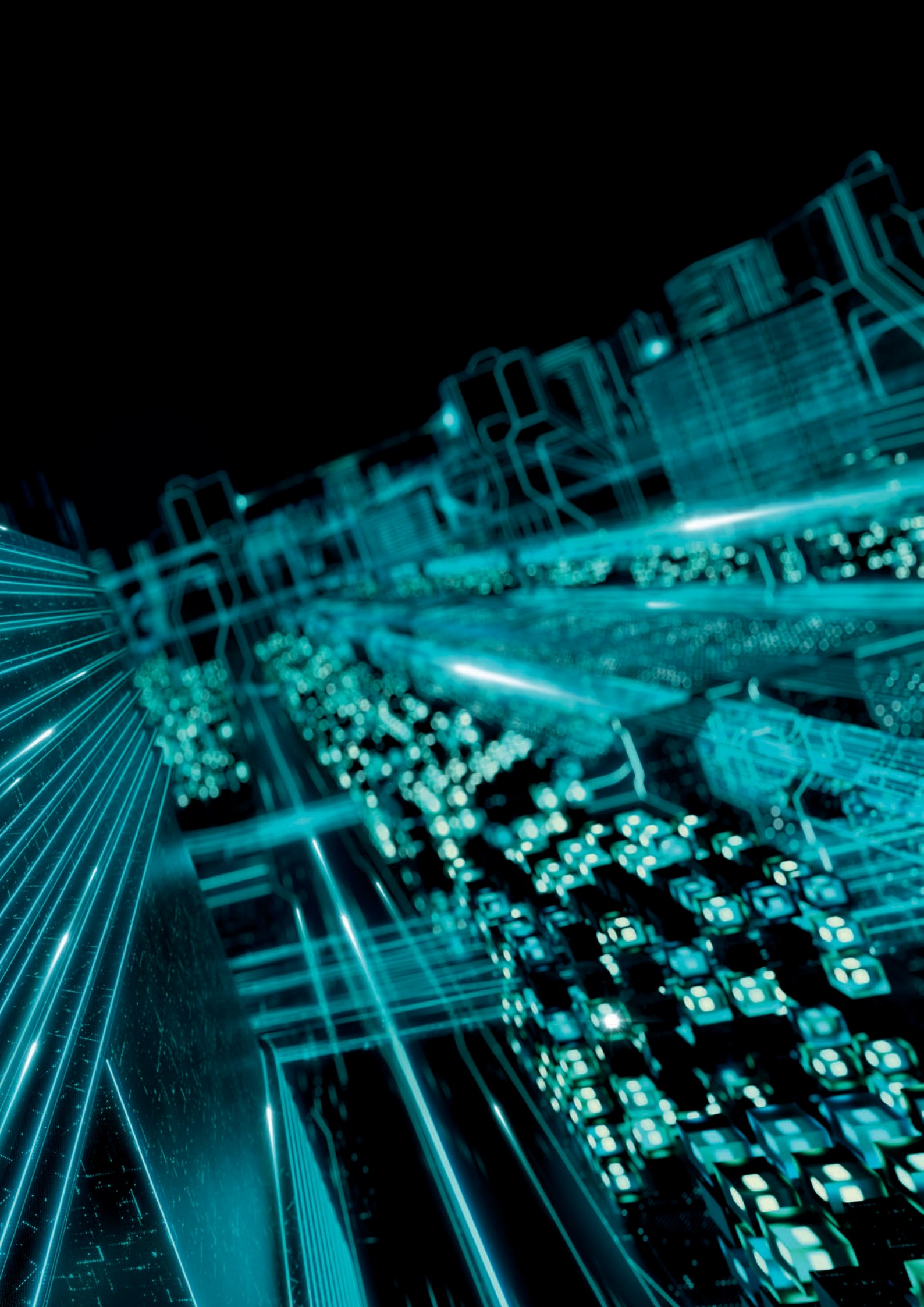
»Najbolj izstopa močna tehnična prednost pred drugimi izdelki na trgu. ESET nam nudi zanesljivo varnost, kar pomeni, da lahko kadar koli delam pri katerem koli projektu, saj vem, da so naši računalniki stoodstotno zaščiteni.«

– Fiona Garland, poslovna analitična skupina IT; Mercury Engineering, Irska; 1.300 sedežev



ESET PROTECT

Vse ESET-ove rešitve za zaščito končnih točk se upravljajo iz oblačne konzole z enim steklom ESET PROTECT, ki zagotavlja popoln pregled vašega omrežja.



Primeri uporabe

Izsiljevalska programska oprema

Nekatera podjetja želijo dodatno zagotovilo, da bodo zaščitena pred napadi izsiljevalske programske opreme.

REŠITEV

- ✓ Network Attack Protection lahko prepreči, da bi izsiljevalska programska oprema kdaj okužila sistem, tako da ustavi izkoriščanje na ravni omrežja.
- ✓ Naša večplastna obramba ima vgrajen peskovnik, ki ima zmožnost zaznavanja zlonamerne programske opreme, ki se s pomočjo zakrivanja poskuša izogniti zaznavanju.
- ✓ Izkoristite ESET-ov sistem za zaščito pred zlonamerno programsko opremo v oblaku za samodejno zaščito pred novimi grožnjami, ne da bi morali čakati na naslednjo posodobitev zaznavanja.
- ✓ Vsi izdelki vsebujejo zaščito v obliki ščita pred izsiljevalsko programsko opremo, ki zagotavlja, da so uporabniki ESET zaščiteni pred zlonamernim šifriranjem datotek.

Zlonamerna programska oprema, brez datotek

Zlonamerna programska oprema brez datotek je razmeroma nova grožnja in, ker obstaja le v pomnilniku, zahteva drugačen pristop v primerjavi s tradicionalno zlonamerno programsko opremo, ki temelji na datotekah.

REŠITEV

- ✓ Edinstvena ESET-ova tehnologija, Advanced Memory Scanner, ščiti pred tovrstnimi grožnjami, tako da spremlja obnašanje zlonamernih procesov in jih optično prebere, ko se ti razkrijejo v pomnilniku.
- ✓ Zmanjšajte čas za zbiranje podatkov in preiskave, tako da naložite grožnjo v ESET Threat Intelligence, da dobite informacije o tem, kako deluje.
- ✓ ESET združuje večplastno tehnologijo, strojno učenje in človeško znanje, da našim strankam zagotavlja najboljšo mogočo raven zaščite.

Grožnje

Grožnje so glavna skrb podjetij, ker nimajo preprostega načina zaščite pred nečim, česar še nikoli niso videli.

REŠITEV

- ✓ Izdelki ESET za zaščito končnih točk uporabljajo hevristiko in strojno učenje kot del našega večplastnega pristopa za preprečevanje in zaščito pred še nikoli videno zlonamerno programsko opremo.
- ✓ Naših 13 laboratorijev za raziskave in razvoj po vsem svetu nam omogoča hiter odziv na zlonamerno programsko opremo, ko se ta prvič pojavi kjerkoli po vsem svetu.
- ✓ ESET-ov sistem za zaščito pred zlonamerno programsko opremo v oblaku samodejno zaščiti pred novimi grožnjami, ne da bi morali čakati na naslednjo posodobitev zaznavanja.

»Ko smo odkrili ESET, smo vedeli, da je to prava izbira: zanesljiva tehnologija, zanesljivo zaznavanje, lokalna prisotnost in odlična tehnična podpora, vse, kar potrebujemo.«

– Ernesto Bonhoure, vodja informacijske infrastrukture; Bolnišnica Alemán, Argentina, 1.500+ sedežev

O podjetju ESET

ESET® že več kot 30 let razvija vodilno programsko opremo in storitve za informacijsko varnost, ki zagotavljajo takojšnjo celovito zaščito pred vedno večjimi grožnjami kibernetske varnosti za podjetja in uporabnike po vsem svetu.

ESET je v zasebni lasti. Brez dolgov in brez posojil lahko storimo, kar je treba storiti za popolno zaščito vseh naših strank.

ESET V ŠTEVILKAH

110m+
uporabnikov po vsem svetu

400k+
poslovnih strank

200+
držav in ozemelj

13
globalnih centrov za raziskave in razvoj

NEKAJ NAŠIH STRANK

MITSUBISHI MOTORS
Drive your Ambition

ESET je od leta 2017 zaščitil več kot 14.000 končnih točk.

Canon
Canon Marketing Japan Group

ESET je od leta 2016 zaščitil več kot 9.000 končnih točk.

Allianz Suisse

ESET je od leta 2016 zaščitil več kot 4.000 nabiralnikov.

Varnostni partner ISP od leta 2008, 2 milijona strank.

Zakaj izbrati ESET

ESET je skladen z ISO/IEC 27001:2013, mednarodno priznanim in veljavnim varnostnim standardom za izvajanje in upravljanje informacijske varnosti. Certifikat podeli neodvisni akreditirani certifikacijski organ SGS in dokazuje, da ESET v celoti izpolnjuje najboljše prakse v industriji.

NAGRADE ESET

PRIZNANJE ANALITIKA

ESET je bil že drugo leto zapored imenovan za edinega izzivalca v Gartnerjevem čarobnem kvadrantu 2019 za platforme za zaščito končnih točk.

ESET je bil v Forrester Wave ocenjen kot močan izvajalec(TM): Endpoint Security Suite, tretje četrtletje 2019.

ESET je bil v poročilu Radicati Endpoint Security 2019 ocenjen kot »najboljši igralec« po dveh glavnih merilih: funkcionalnost in strateška vizija.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20. avgust, 2019. Gartner ne promovira nobenega prodajalca, izdelka ali storitve, ki so opisani v raziskovalnih publikacijah. Raziskovalne publikacije sestavljajo mnenja raziskovalne organizacije Gartner in se jih ne sme razlagati kot navedbe dejstev. Gartner zavrača vsa jamstva, izražena ali implicitna, v povezavi s to raziskavo, vključno z vsemi jamstvi za prodajo ali primernost za določen namen.

Gartner Peer Insights je brezplačna platforma za medsebojne preglede in ocene, namenjena podjetjem, ki odločajo o programski opremi in storitvah. Mnenja gredo skozi strog postopek preverjanja in moderiranja, kar zagotavlja verodostojnost informacij. Mnenja družbe Gartner Peer Insights so subjektivna mnenja posameznih končnih uporabnikov na podlagi lastnih izkušenj in ne predstavljajo stališč podjetja Gartner ali njegovih povezanih podjetij.


ENJOY SAFER
TECHNOLOGY™