



# ENDPOINT SOLUTIONS

Spolehlivá a ověřená technologie ochrany proti  
všem druhům hrozeb



ENJOY SAFER TECHNOLOGY™



# Co je řešení **ESET Endpoint?**

**Jde o bezpečnostní produkty, které se instalují na koncová zařízení. Obsahují několik vrstev ochrany počítače, včetně prověřené technologie detekce škodlivého kódu ESET NOD32, které chrání proti všem druhům hrozeb na internetu.**

Produkty umožňují detailní nastavení parametrů jednotlivých bezpečnostních modulů. Díky nízkým systémovým nárokům, podpoře virtualizace a volitelné cloudové kontrole souborů zařízení nabízejí počítače s nainstalovaným řešením ESET koncovému uživateli dostatek výkonu k rychlé a plynulé práci. Kompletní přehled o bezpečnosti koncových stanic lze získat s pomocí uživatelsky příjemného nástroje pro vzdálenou správu.

# Proč ESET?

## RANSOMWARE

Ransomware není v oblasti kyberkriminality ničím novým, v minulosti však nepatřil mezi hlavní hrozby. To se zásadně změnilo v roce 2013, kdy masivně zaútočil Cryptolocker. I jeden úspěšný ransomwarový útok může zcela ochromit chod firmy, způsobit obrovské finanční škody a zničit její dobrou pověst. A pokud neexistuje proces pravidelných záloh, pak podnikům mnohdy nezbyvá nic jiného, než zaplatit výpalné.

Produkty ESET obsahují několik na sobě nezávislých vrstev ochrany proti ransomwaru. Vedle cloudového systému ESET LiveGrid a DNA detekcí i samotný modul ochrany proti ransomwaru, který v reálném čase sleduje veškeré běžící procesy a pomocí behaviorální analýzy odhaluje škodlivý kód podle jeho typického chování – změny existujících souborů. Díky tomu detekuje i nový, dosud neznámý šifrovací malware.

## CÍLENÉ ÚTOKY A ÚNIKY DAT

Moderní hrozby se objevují každý den, neustále dochází k vývoji nového malwaru a způsobů útoku. Postižená firma reaguje na většinu kybernetických útoků v lepším případě pouze se zpožděním, v horším útok ani nezaznamená. Proto je velmi důležité dbát na zavedení preventivních opatření, která přispějí k co nejrychlejšímu odhalení probíhajícího útoku.

V produktech ESET je integrován systém včasného varování ESET LiveGrid, který hraje velmi důležitou úlohu v zabezpečení počítače, a především v ochraně před novými hrozbami. Neustále sbírá data o podezřelých souborech ze sensorů po celém světě. Díky tomuto systému se také významně zkracují kontroly počítače, protože nedochází ke kontrolám souborů, jejichž reputace byla v systému již jednou ověřena.

## ÚTOKY BEZ SOUBORU

Novější hrozby mohou existovat pouze v paměti počítače, takže je nemožné je detekovat pomocí standardní antivirové kontroly souborů. Některé útoky se také mohou maskovat za legitimní software, což dále znesnadňuje odhalení nákazy. Velmi obvyklé je například použití PowerShellu.

Produkty ESET obsahují technologie, které neustále monitorují chování procesů a kontrolují je ihned po rozbalení v paměti. Takto jsou schopny detekovat i těžce šifrované a dosud neznámé hrozby, takzvané „zero day“ útoky.

Řešení ESET používají technologie, které brání průniku malwaru do systému, a detekují, zda už nějaký organizaci v minulosti nenakazil.

V případech malwarových útoků nebo úniku dat jsou postižené firmy většinou velmi překvapené, že byl útok úspěšný, případně ani netuší, že se staly jeho terčem.

Novější hrozby mohou existovat pouze v paměti počítače, takže je nemožné je detekovat pomocí standardní antivirové kontroly souborů.

*“ESET používáme již roky. Dělá, co má. Nemusíme se o nic starat.  
V krátkosti, ESET je spolehlivý a kvalitní.”*

—Jos Savelkoul, Team Leader ICT-Department; Zuyderland Hospital, Netherlands;  
10.000+ licencí



# Produkty pro ochranu koncových stanic

ESET Endpoint Security for Windows/macOS/Android

ESET Endpoint Antivirus for Windows/macOS/Linux Desktop

ESET File Security for Windows Server/Linux/FreeBSD/Azure

ESET Mobile Device Management for Apple iOS

# Výhody

## MODERNÍ TECHNOLOGIE

Společnost ESET kombinuje moderní bezpečnostní technologie ochrany, strojové učení a analýzu ve výzkumných centrech, aby zákazníkům zajistila nejvyšší možnou úroveň ochrany proti kybernetickým hrozbám. Výsledkem je perfektní kombinace rychlosti detekce, malé míry falešných poplachů a nízkých nároků na systém. Své technologie ESET neustále inovuje v závislosti na vývoji IT bezpečnostního průmyslu resp. jeho hrozeb a útoků.

## OCHRANA NAPŘÍČ PLATFORMAMI

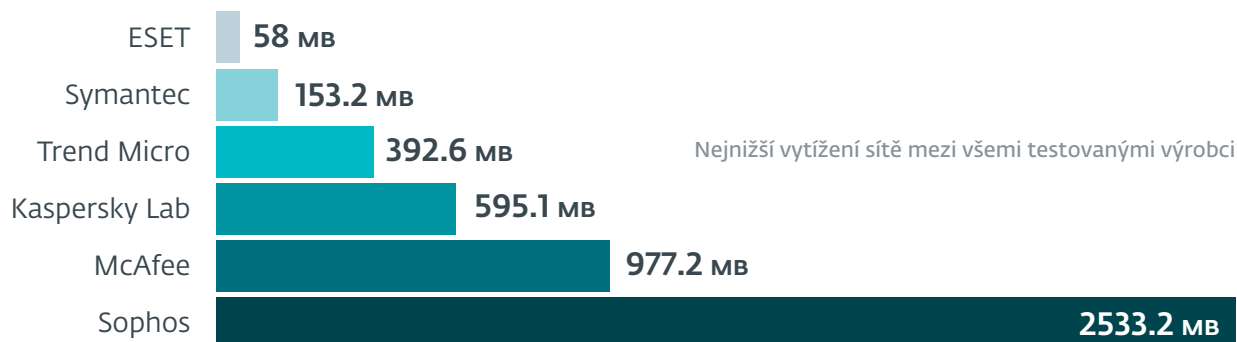
Produkty ESET podporují všechny používané operační systémy, včetně Windows, macOS, Linuxu a Androidu. Webová konzole vzdálené správy umožňuje administrátorovi spravovat veškerá zařízení z jednoho místa. Samozřejmostí je i správa mobilních zařízení s iOS a Androidem.

## NÍZKÉ SYSTÉMOVÉ NÁROKY

Při výběru bezpečnostního řešení hrají významnou roli i nároky produktů na systém. Produkty ESET prošly v průběhu let mnoha nezávislými testy, ve kterých byly jednoznačně potvrzeny jedny z nejnižších nároků a dopadů na systém.

## CELOSVĚTOVÁ PŮSOBNOST

Společnost ESET má pobočky ve 22 zemích, provozuje 13 výzkumných center a působí ve více než 200 zemích po celém světě. Díky tomu může globálně sledovat a analyzovat nově vznikající malware a aktivně bránit jeho šíření z místa prvního výskytu.



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

*“Nejlepší důvod? Statistiky z naší podpory ukazují, že po nasazení ESETu nejsou žádné hovory, které by se týkaly problému s antivirem nebo škodlivými kódy.”*

— Adam Hoffman, IT Infrastructure Manager; Mercury Engineering, Ireland; 1.300 licencí

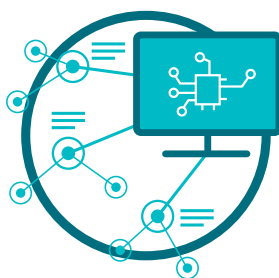
# Technologie

## 3 základní pilíře našich produktů



### ESET LIVEGRID®

Při nalezení nového druhu škodlivého kódu, resp. podezřelé činnosti na počítači s instalovaným produktem ESET, se podezřelé soubory odešlou do cloudového systému ESET LiveGrid, kde dojde k pokročilé analýze. Pokud je vzorek detekován jako škodlivý, odešle se informace o nově nalezené hrozbě do všech počítačů po celém světě. To vše v řádu minut.



### STROJOVÉ UČENÍ

ESET používá sílu neurálních sítí a pokročilých algoritmů k analýze podezřelých souborů, které vyhodnotí jako čisté, potenciálně nechtěné nebo škodlivé.



### LIDSKÁ ODBORNOST

Odborníci ve 13 výzkumných centrech analyzují každý den tisíce nových nalezených hrozeb. Získané informace se ihned odesílají prostřednictvím ESET LiveGrid do všech počítačů s nainstalovaným řešením ESET.

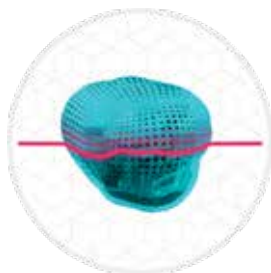
Standardní antivirová ochrana už v dnešní době na pokročilé IT hrozby nestačí. Moderní hrozby obvykle kombinují několik způsobů útoku a mohou se dobře maskovat za legitimní činnost v systému. Proto je nutné, aby moderní bezpečnostní řešení dokázalo zabránit probíhajícímu malwarovému útoku a detekovat ho ve všech jeho fázích (před, v průběhu i po nakažení počítače). Produkty ESET obsahují pokročilé technologie ochrany, které pokrývají celý cyklus malwarového útoku, a poskytují tak velmi vysokou úroveň ochrany.





## STROJOVÉ UČENÍ

Od roku 1997 všechny produkty ESET obsahují technologii strojového učení. ESET ji používá v kombinaci s ostatními vrstvami ochrany. Strojové učení se používá ve formě konsolidovaných výstupů a neurálních sítí.



## POKROČILÁ KONTROLA PAMĚTI

Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti. Takto je schopna detekovat i šifrované hrozby.



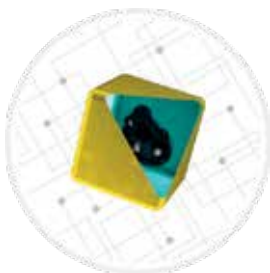
## OCHRANA PROTI RANSOMWARU

Je to bezpečnostní vrstva, která chrání počítač před ransomwarem. Monitoruje a vyhodnocuje všechny spuštěné aplikace na základě jejich chování a reputace. Pokud dojde k chování shodnému s ransomwarem, dojde k blokadě daného procesu.



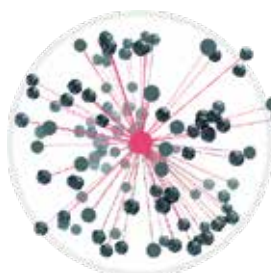
## EXPLOIT BLOCKER

Zajišťuje ochranu stanic před dosud neznámými hrozbami, takzvanými zero day útoky. Sleduje chování procesů a hledá podezřelou aktivitu, která je pro exploity typická. Chrání často zneužívané aplikace, jako jsou internetové prohlížeče, čtečky PDF, poštovní klienti nebo MS Office.



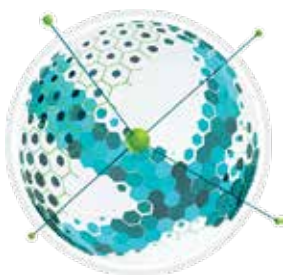
## INTEGROVANÝ SANDBOX

Moderní malware používá techniky, které mají za úkol maximálně ztížit detekci bezpečnostním řešením. Pro nalezení a identifikaci opravdového chování takové hrozby produkty ESET používají integrovaný sandbox. V izolovaném virtuálním prostředí dochází k emulaci různých hardwarových komponent počítače a softwaru a ke spuštění podezřelých vzorků.



## OCHRANA PROTI ZAPOJENÍ DO BOTNETU

Chrání před infiltrací malwarem, který zapojuje infikované počítače do botnetové sítě. Tu může útočník využívat například k šíření spamu, síťovým útokům na jiná zařízení či k dalšímu šíření škodlivého kódu.



## OCHRANA PŘED SÍŤOVÝMI ÚTOKY

Rozšiřuje schopnosti firewallu a zlepšuje detekci takzvaných CVE (Common Vulnerabilities and Exposures) neboli běžných zranitelností v síti na protokolech SMB, RPC a RDP. Přidává důležitou vrstvu ochrany před škodlivým kódem, který se šíří zneužíváním chyb v síťových protokolech.



## DNA DETEKCE

Pracují s komplexními definicemi škodlivého chování a charakteristikami malwaru. Škodlivý kód lze jednoduše modifikovat, nicméně chování v systému tak lehce změnit nelze. A právě tohoto principu využívá DNA detekce.



## HIPS

Umožňuje definovat pravidla pro systémové registry, procesy, aplikace a soubory a detekuje hrozby na základě chování systému.

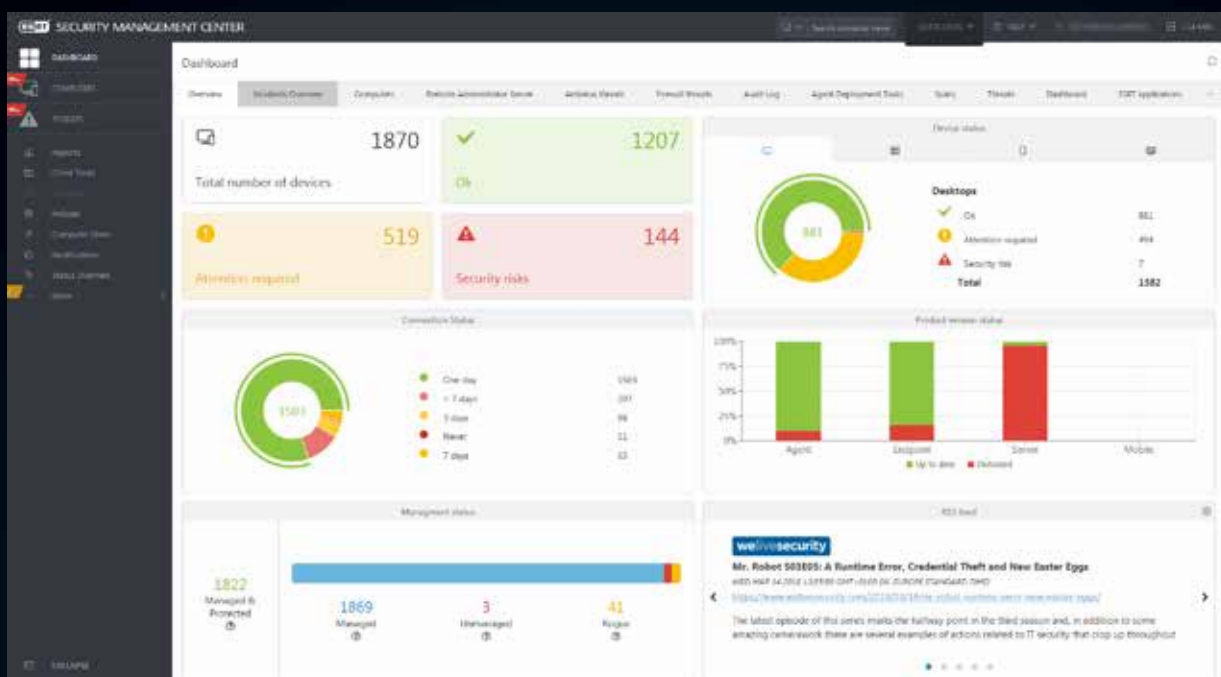


## SKENER UEFI

Chrání počítač před útoky již před startem Windows – na systémech s rozhraním UEFI. Uživatel je informován o případné změně firmwaru.

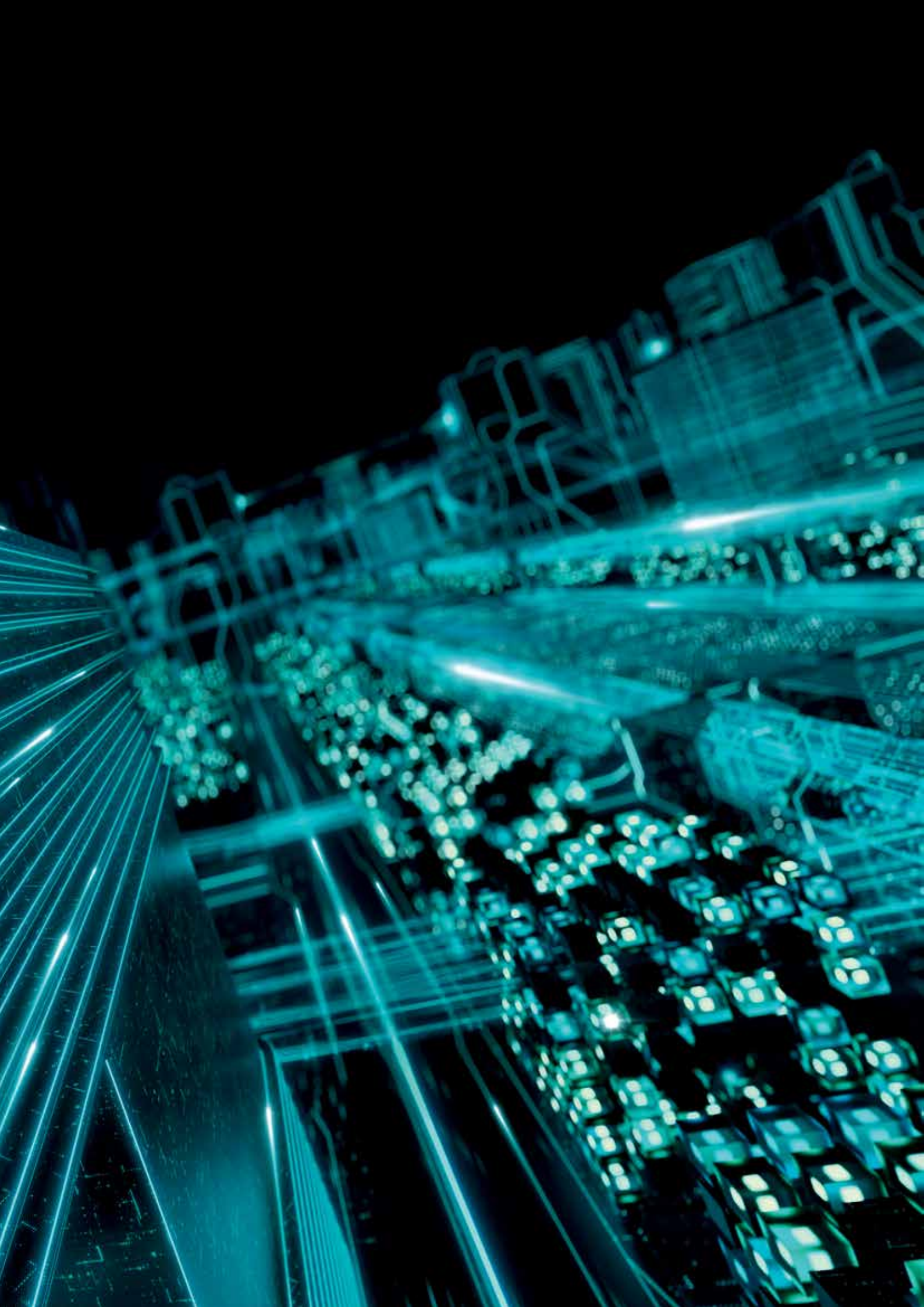
*“Největší věcí, kterou ESET vybočuje, je silná technická výhoda nad všemi dalšími produkty na trhu. ESET nabízí spolehlivé zabezpečení, což znamená, že mohu pracovat na dalších projektech s vědomím, že jsou počítače chráněny na 100 procent.”*

— Fiona Garland, Business Analyst Group IT; Mercury Engineering, Ireland;  
1.300 licencí



## Vzdálená správa

Administrátor může všechny produkty spravovat z jediného místa, konzole vzdálené správy ESET Security Management Center. Vzdálenou správu je možné nainstalovat nejen na zařízení s Windows, ale také na linuxové servery nebo využít již připravenou Virtual Appliance.



# Příklady použití

## Ransomware

Firmy chtějí mít jistotu, že jsou proti ransomwarovému útoku maximálně chráněné.

### ŘEŠENÍ

- ✓ Ochrana před síťovými útoky brání nakažení systému přes zranitelnosti na síťové úrovni.
- ✓ Produkty ESET obsahují integrovaný sandbox, který dokáže detekovat malware, jenž se snaží maskovat svou činnost a vyhýbá se detekci standardními AV technikami.
- ✓ Cloudová technologie ESET LiveGrid automaticky chrání počítač ještě před uvolněním další aktualizace virové databáze.
- ✓ Všechny produkty obsahují ochranu proti ransomwaru, která brání v zašifrování souborů a složek.

## Útoky bez souboru

Novější hrozby mohou existovat pouze v paměti počítače, takže obvykle nejdou detekovat pomocí standardní antivirové kontroly souborů.

### ŘEŠENÍ

- ✓ Unikátní technologie pokročilé kontroly paměti chrání počítač před novými hrozbami tak, že monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti.
- ✓ Nahráním hrozby do ESET Threat Intelligence správce získá informace potřebné k eliminaci dané hrozby.
- ✓ Kombinace technologií chránících počítač ve více vrstvách, strojového učení a lidské odbornosti poskytuje zákazníkům nejvyšší možnou ochranu.

## Zero day hrozby

Dosud neznámé hrozby z principu znamenají pro firmy jedno z největších rizik. Reakce na neznámý útok je velmi obtížná.

### SOLUTION

- ✓ Produkty ESET používají heuristickou analýzu a strojové učení jako prevenci a ochranu před neznámými hrozbami.
- ✓ 13 výzkumných laboratoří neustále monitoruje nově vznikající hrozby na celém světě. Při výskytu neznámé hrozby ihned probíhá analýza a získané informace se odesílají na koncové stanice prostřednictvím ESET LiveGrid.
- ✓ ESET LiveGrid chrání počítače před novými hrozbami bez nutnosti stažení nové aktualizace detekčního jádra.

*“Když jsme našli ESET, věděli jsme, že jde o správnou volbu. Spolehlivá technologie, silná detekce, přítomnost na lokálním trhu a vynikající technická podpora bylo vše, co jsme potřebovali.”*

— Ernesto Bonhoure, IT Infrastructure Manager;  
Hospital Alemán, Argentina,  
1.500+ licencí

# O ESETu

**Společnost ESET byla ve zprávě Magic Quadrant společnosti Gartner\* pro rok 2018 jmenována vyzyvatelem v segmentu Endpoint Protection. ESET byl v této zprávě uveden jako jediný vyzyvatel pro danou oblast a oceněn byl zejména za schopnost vytvářet a naplňovat své vize.**

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností, která

díky dlouhodobě vysoké úrovni ochrany získala více než 100 ocenění prestižního magazínu Virus Bulletin VB100. Za těmito úspěchy stojí zejména dlouhodobé investice do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

## ESET V ČÍSLECH

**110m+**  
uživatelů po celém světě

**400k+**  
firemních zákazníků

**200+**  
zemí a teritorií

**13**  
vývojových center

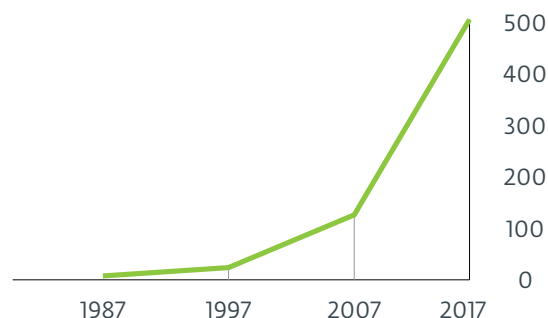
## ZAMĚŠTNANCI ESETU

Více než třetina zaměstnanců pracuje v oblasti vývoje a výzkumu.



## OBRAT ESETU

V milionech eur.



\*Společnost Gartner nepodporuje žádného prodejce, produkt ani službu, které uvádí ve svých výzkumných publikacích, a jejím cílem není doporučit uživatelům technologií jen prodejce s nejlepším hodnocením. Výzkumné publikace společnosti Gartner obsahují názory výzkumných organizací Gartner a neměly by vyznít jako tvrzení faktu. Gartner se zřiká všech záruk, vyjádřených nebo předpokládaných s ohledem na výzkum, včetně záruk obchodovatelnosti nebo vhodnosti pro konkrétní účel.

---

## NAŠI ZÁKAZNÍCI

---

# HONDA

Zákazníkem od roku 2011

3x prodloužení licence, 2x rozšíření

# GREENPEACE

Zákazníkem od roku 2008

10x prodloužení a rozšíření licence

# Canon

Zákazníkem od roku 2016

více než 14 000 licencí



ISP partnerem od roku 2008

2 miliony zákazníků

---

## NĚKTERÁ OCENĚNÍ

---



*“Vzhledem ke kvalitě antimalwarové technologie, možnostem správy a globálnímu dosahu by měl být ESET v každém seznamu při výběru nového firemního bezpečnostního řešení.”*

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

