ENDPOINT SOLUTIONS

Spolehlivá a ověřená technologie ochrany proti všem druhům hrozeb

Progress. Protected.

Co je řešení **ESET Endpoint?**

Platforma ochrany koncových bodů (EPP) je bezpečnostní řešení pro koncová zařízení, které chrání firemní zařízení proti útokům kybernetických hrozeb všeho druhu, odhaluje škodlivé aktivity a poskytuje možnosti vyšetřování a nápravy potřebné k reakci na vzniklé bezpečnostní situace.

Řešení využívá různé bezpečnostní technologie, které spolupracují na různých vrstvách, se schopností neustále vyvažovat výkon, detekci a falešné poplachy.

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 nezbývá 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

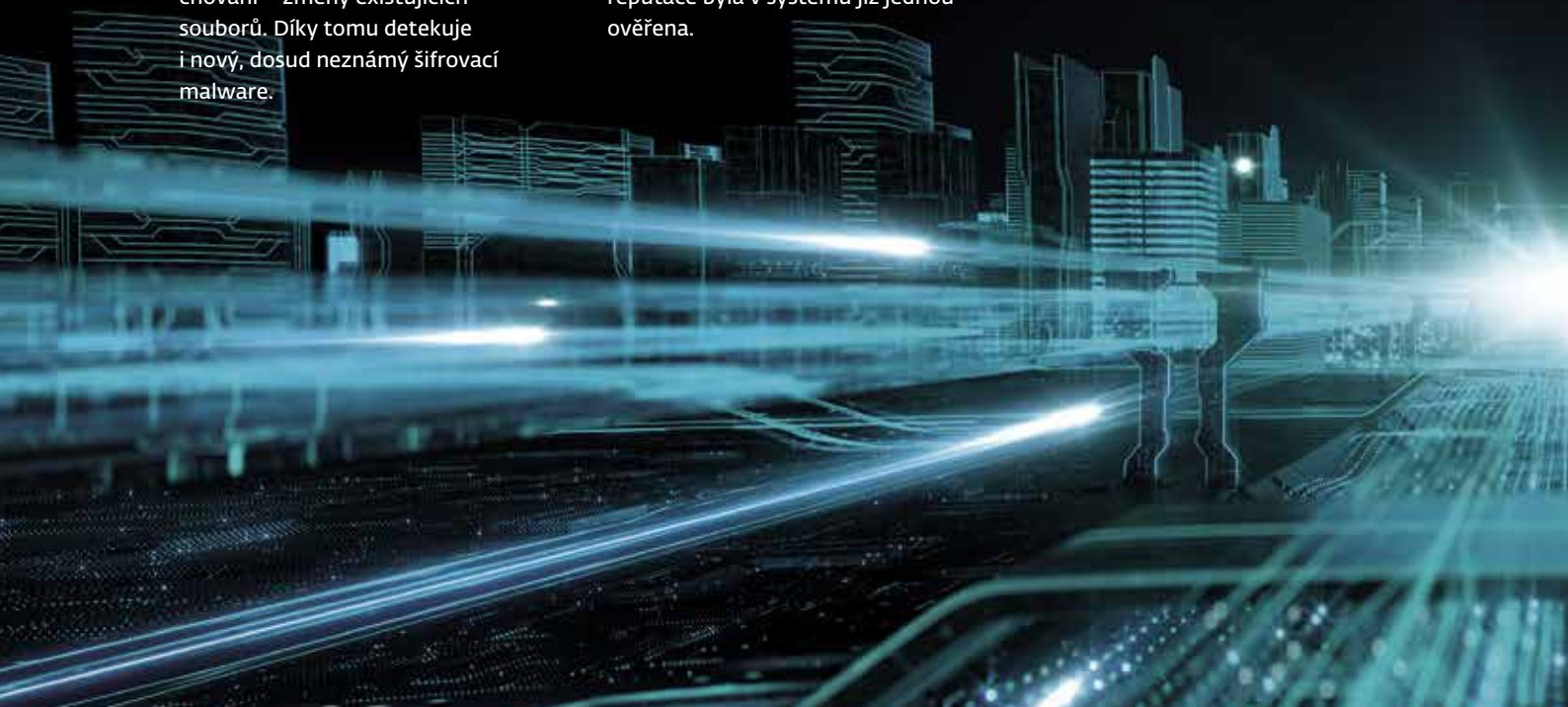
Moderní hrozby se objevují každý den, neustále dochází k vývoji nového malwaru a způsobů útoku. Postižená firma reaguje na většinu kybernetických útoků v lepším případě pouze se zpožděním, v horším útok ani nezaznamená. Proto je velmi důležité dbát na zavedení preventivních opatření, která přispějí k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



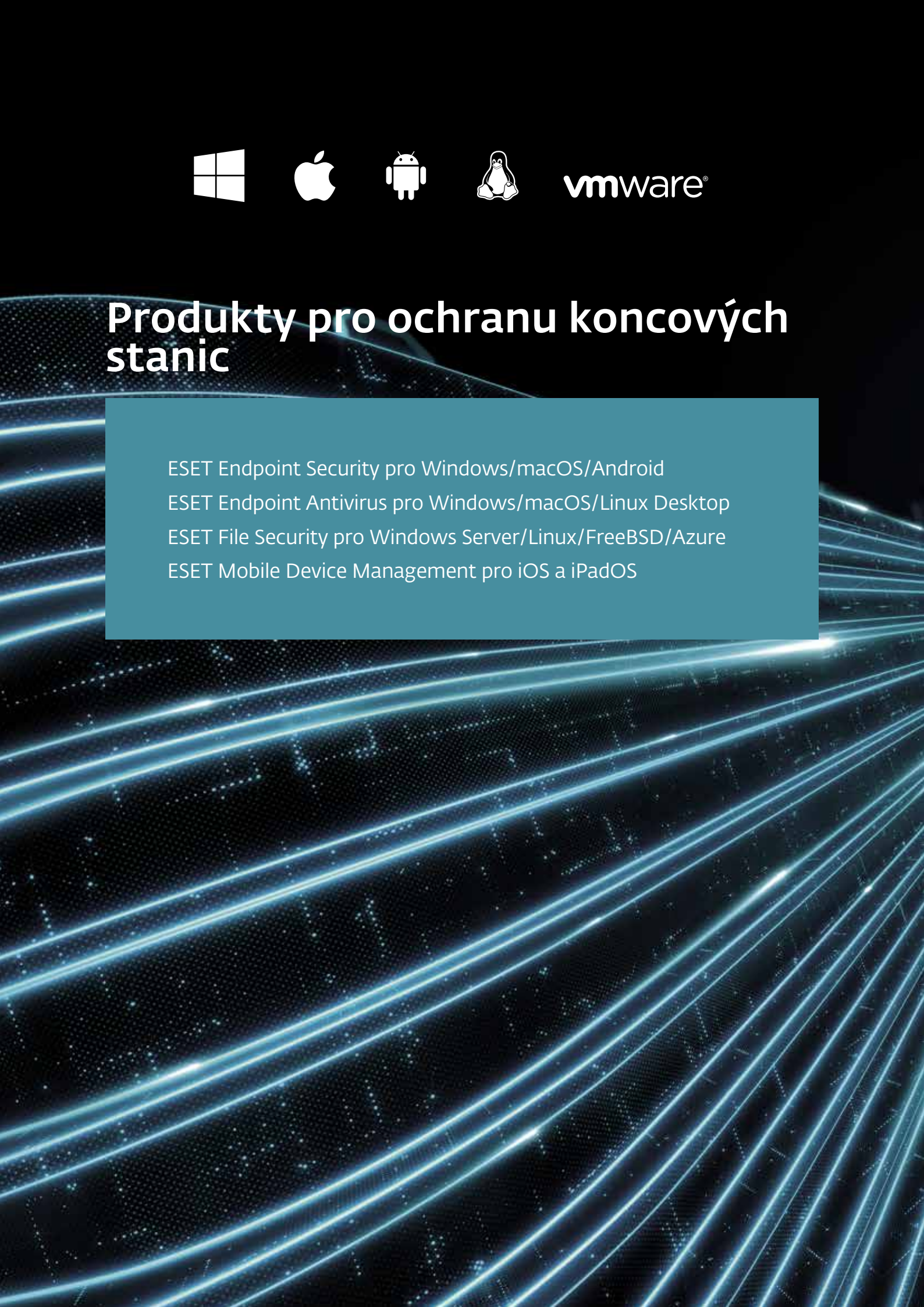
Řešení ESET používají technologie, které brání průniku malwaru do systému a detekují, zda už nějaký organizaci v minulosti nenakazil.

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 pro Windows/macOS/Android
ESET Endpoint Antivirus pro Windows/macOS/Linux Desktop
ESET File Security pro Windows Server/Linux/FreeBSD/Azure
ESET Mobile Device Management pro iOS a iPadOS

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.

„Nejlepší důvod? Statistiky z naší podpory ukazují, že po nasazení ESETu nejsou žádné hovory, které by se týkaly problému s antiviry nebo škodlivými kódy."

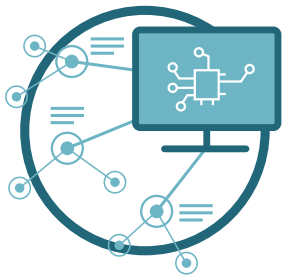
— Adam Hoffman, IT Infrastructure Manager; Mercury Engineering, Ireland; 1 300 licencí

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.

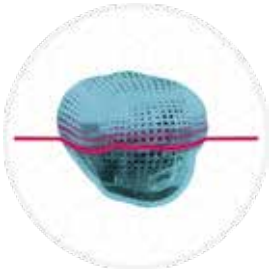
LIDSKÁ ODBORNOST

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.

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

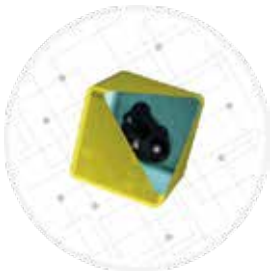
Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti. Takto je schopna detekovat i šifrované hrozby.

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 blokaci daného procesu.

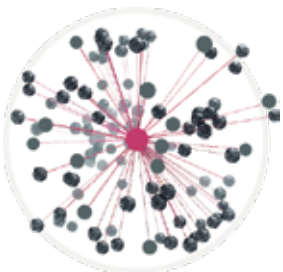
EXPLOIT BLOCKER

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.



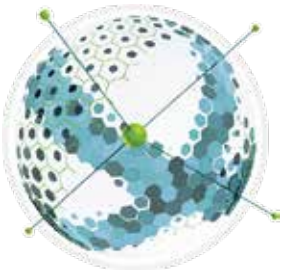
INTEGROVANÝ SANDBOX

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.

ZABEZPEČENÝ PROHLÍŽEČ

Chrání webové prohlížeče před ostatními procesy běžícími v počítači. Zabezpečení prohlížeče pracuje na základě nulové důvěry s předpokladem, že počítač je kompromitován, aby nemohlo dojít k manipulaci s pamětí prohlížeče a změně zobrazovaného obsahu. Funkce není standardně zapnutá, abyste měli jako administrátor dost času na využití jejího potenciálu a implementaci v bezpečnostní politice.

HIPS

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

SKENER UEFI

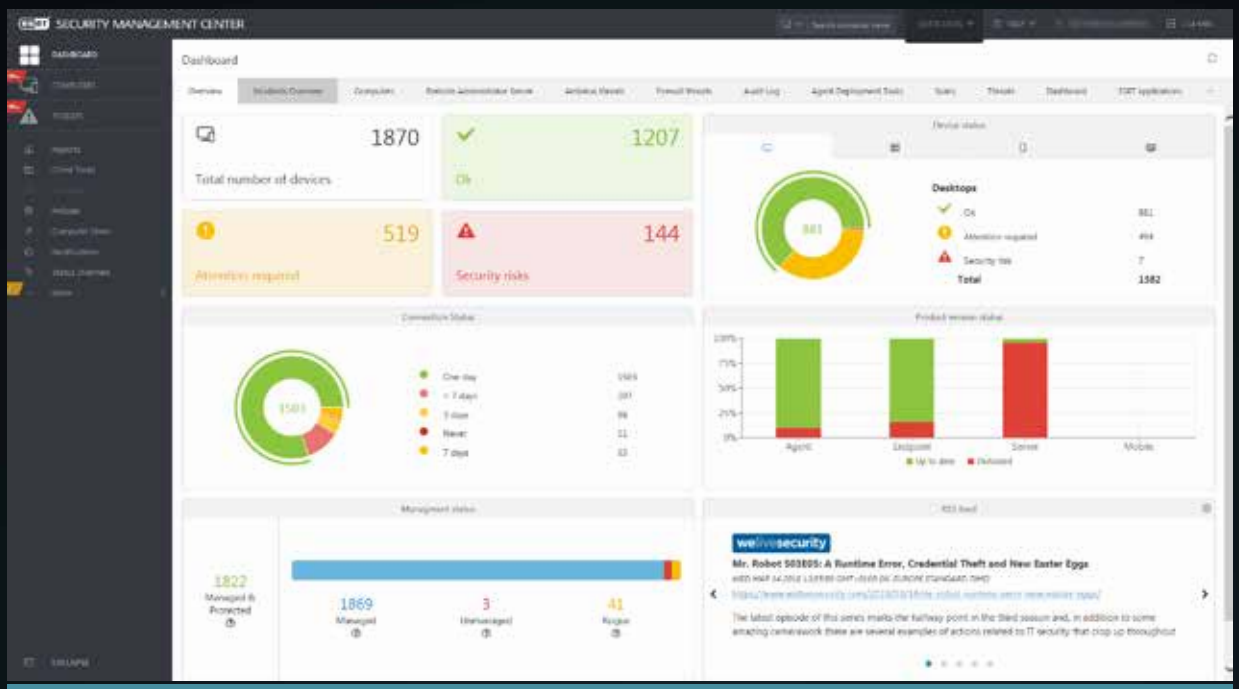
Chrání počítač před útoky již před startem Windows – na systémech s rozhraním UEFI. Uživatel je informován o případné změně firmwaru.

OCHRANA PROTI BRUTE FORCE ÚTOKU

Funkce chrání zařízení před malwarem, který se snaží uhádnout přihlašovací údaje a neoprávněně navázat vzdálené připojení. Parametry lze snadno nakonfigurovat prostřednictvím politik přímo z konzole, a vytvořit výjimky, když dojde k blokaci legitimního procesu.

„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



ESET PROTECT

Všechna řešení ESET lze spravovat z jediné konzole vzdálené správy ESET PROTECT. Ta může být cloudová nebo on-premises, a zajišťuje správci kompletní přehled o stavu bezpečnosti ve firemní síti.

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.

Ukradené přihlašovací údaje

Počet phishingových útoků a falešných webových stránek, které napodobují skutečné organizace a primárně slouží ke krádeži přihlašovacích údajů a finančních dat, roste.

ŘEŠENÍ

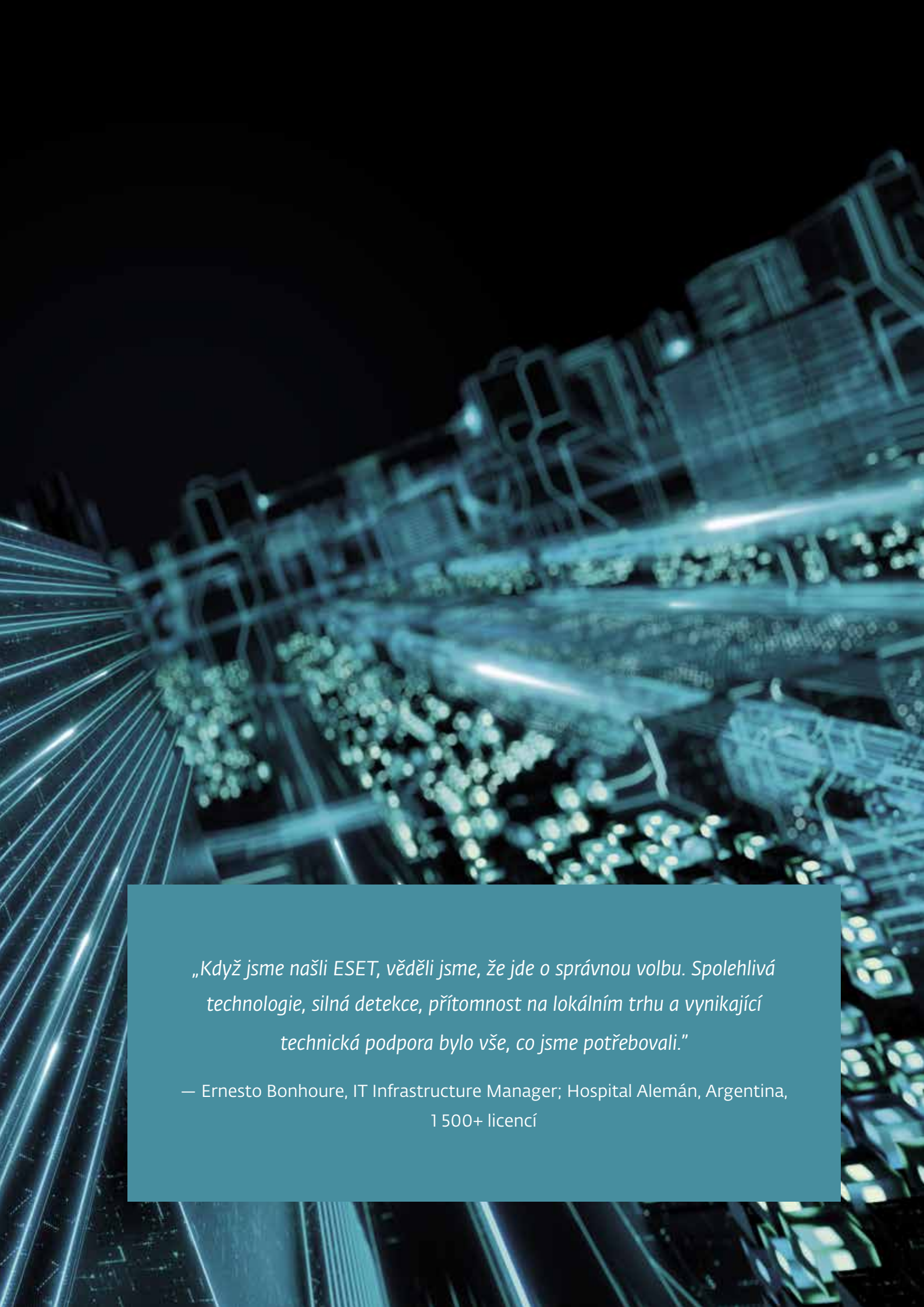
- ✓ ESET Endpoint Security obsahuje vestavěný předdefinovaný seznam známých stránek internetového bankovnictví, které automaticky otevírá v zabezpečeném prohlížeči. Tento seznam můžete kdykoli rozšířit o internetový portál své banky.
- ✓ Zabezpečený prohlížeč představuje další vrstvu ochrany, která má chránit vaše citlivá data při prohlížení webu (například finanční údaje během online transakcí).

Útok na hesla

Ochrana proti útokům hrubou silou blokuje pokusy o uhádnutí hesel pro RDP a SMB služby, které mohou útočníkovi umožnit získat plnou vzdálenou kontrolu nad systémem.

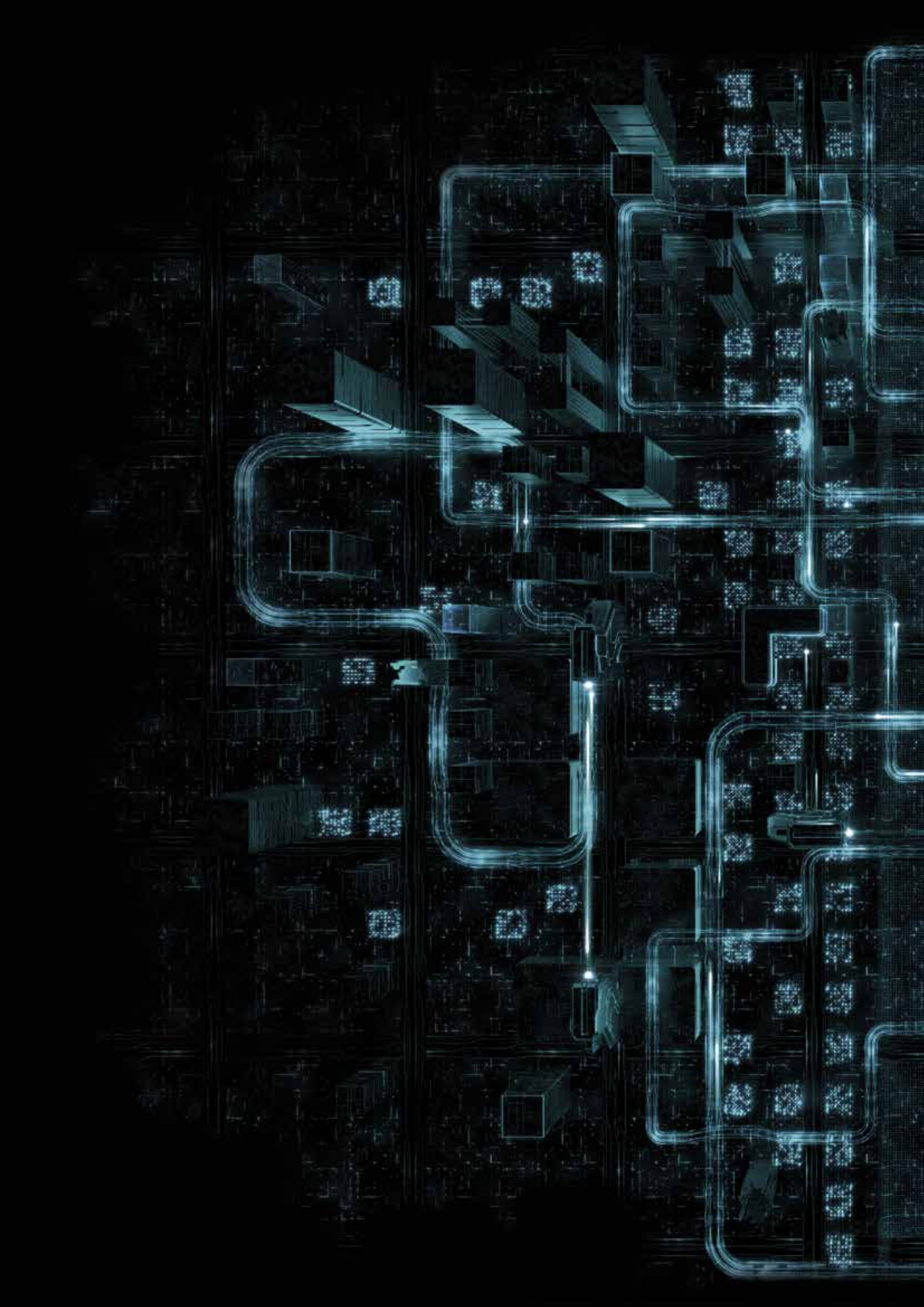
ŘEŠENÍ

- ✓ Chrání zařízení před potenciálním uhodnutím přihlašovacích údajů a neoprávněným navázáním vzdáleného připojení.
- ✓ Lze snadno konfigurovat prostřednictvím politik přímo z konzole a vytvářet výjimky.
- ✓ Uživatelé mohou přidávat vlastní pravidla nebo upravovat stávající.



„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 již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností, která díky vysoké úrovni ochrany získala více než 100 ocenění prestižního magazínu Virus Bulletin VB100.

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

1mld+
uživatelů po celém světě

400k+
firemních zákazníků

200+
zemí a teritorií

13
vývojových center

NAŠI ZÁKAZNÍCI

MITSUBISHI MOTORS
Drive your Ambition

Zákazníkem od roku 2017, více než 9 000 licencí

Allianz Suisse

Zákazníkem od roku 2016, více než 4 000 mailboxů

Canon
Canon Marketing Japan Group

Zákazníkem od roku 2016, více než 32 000 licencí

ISP partnerem od roku 2008, 2 miliony zákazníků

VYBRANÁ OCENĚNÍ

AV comparatives APPROVED Business Security DEC 2021

ESET získal v prosinci 2021 ocenění „APPROVED" za ochranu koncových řešení v business security testu společnosti AV-Comparatives.

G2 Leader WINTER 2022

ESET trvale dosahuje špičkových výsledků na celosvětové platformě hodnocení uživatelů G2 a jeho řešení jsou oceňována zákazníky po celém světě.

FORRESTER®

Řešení ESET jsou pravidelně oceňována předními analytickými firmami, včetně „The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021".

eset® Digital Security
Progress. Protected.


Progress. Protected.