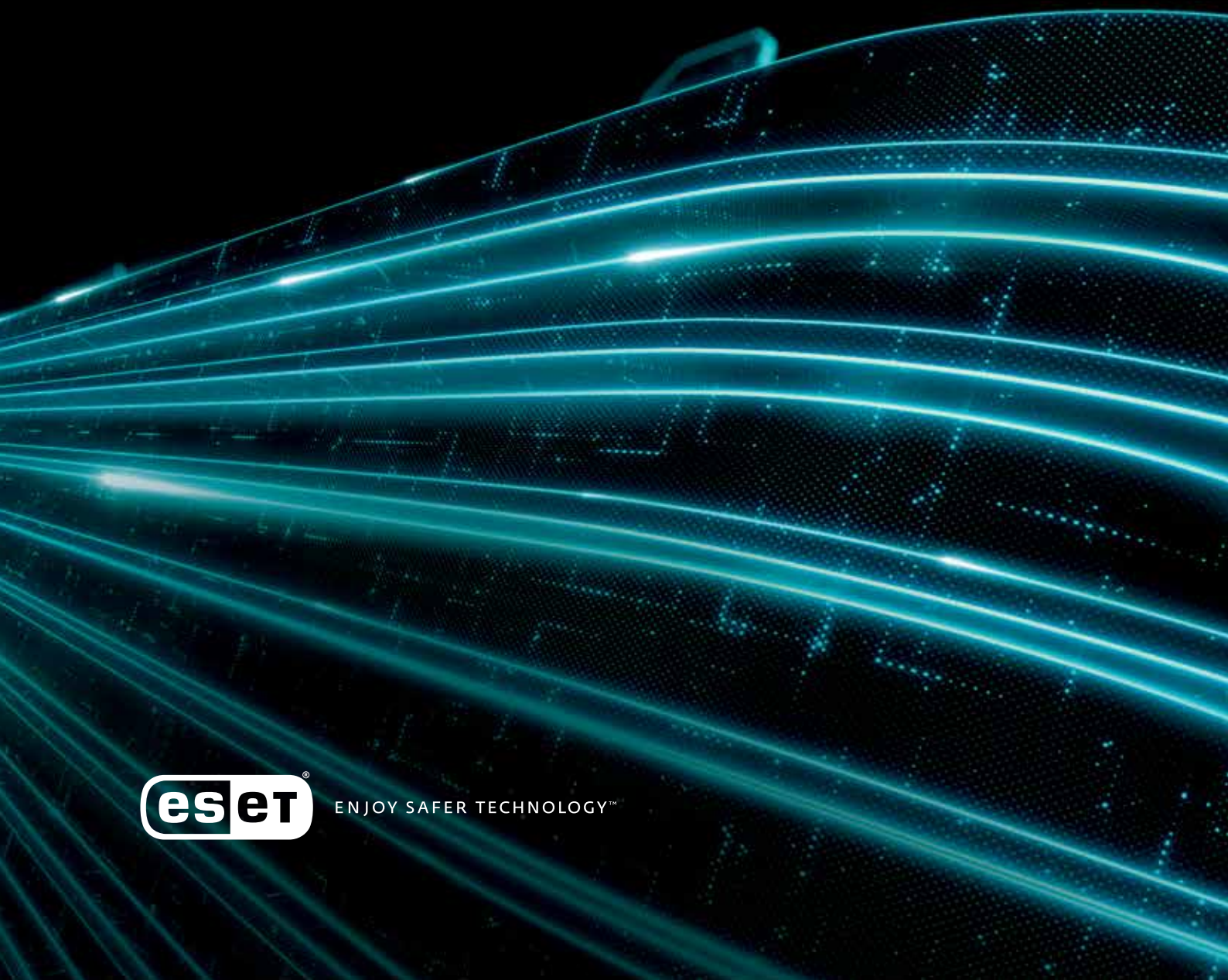
ENDPOINT ENCRYPTION

Jednoduché a silné šifrování pro firmy všech velikostí



ENJOY SAFER TECHNOLOGY™

Co je **ESET Endpoint Encryption?**

ESET Endpoint Encryption je nástroj na ochranu dat. Poskytuje šifrování souborů, složek a disků na firemních zařízeních. Firmám umožňuje preventivně chránit citlivá data pro případ, že by skončila v nechtěných rukou.

ESET Endpoint Encryption je snadno implementovatelné šifrování pro firmy všech velikostí, které podporuje plné šifrování disku (FDE), šifrování souborů a složek, e-mailu a USB zařízení.

Proč **šifrování?**

ÚNIKY DAT

S úniky citlivých dat se v poslední době setkáváme stále častěji. Pokud k úniku dojde v prostředí, kde se nepoužívá šifrování, pak pro útočníka není problém následně firmu vydírat, případně získaná data prodat na černém trhu. Odcizení citlivých dat může vést nejen k přímým finančním ztrátám, ale poškozena je i pověst firmy, což v dlouhodobém horizontu může být mnohem větší problém.

Implementací silného šifrování citlivých dat firma zajistí, že jsou data pro útočníka nečitelná, nepoužitelná, a tedy i nezajímavá. Nejohroženější jsou tradičně finanční instituce, banky, pojišťovny a veřejný sektor. Ale ani menší firmy nejsou úplně v bezpečí. Útočníci vždy poměřují riziko útoku s možným výdělkem. Pokud tedy usoudí, že je pro ně lukrativní zaútočit na malý podnik, pak to udělají.

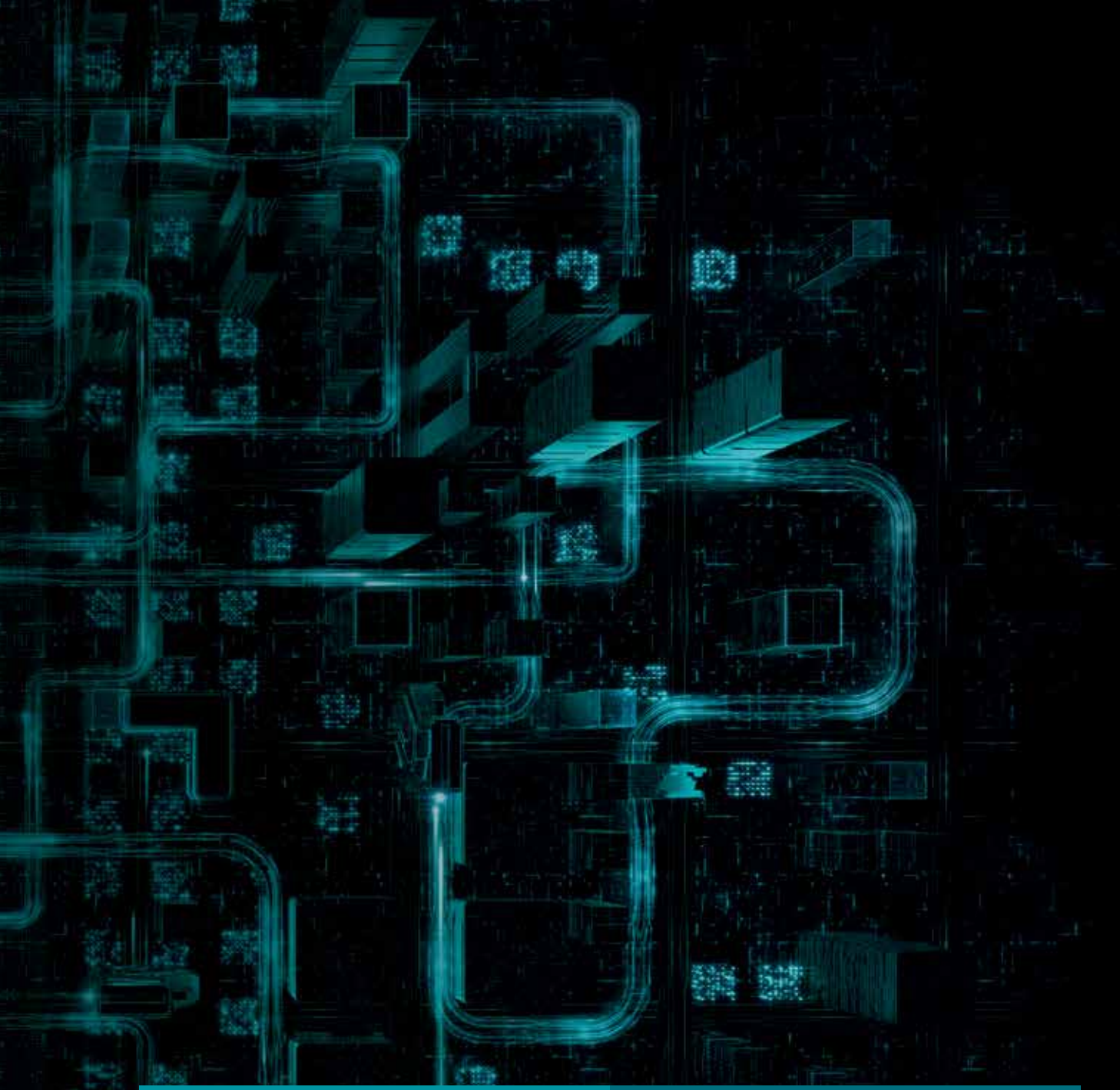
MOBILNÍ ZAMĚSTNANCI

Dalším rizikem, které roste v závislosti na oblibě práce z domova a mimo firmu, jsou mobilní zaměstnanci. U těch hrozí, že dojde k úniku dat nejen v důsledku malwarového útoku, ale také v případech, kdy dojde k fyzické ztrátě nebo odcizení zařízení. I tady je proto velmi důležité chránit citlivá data, v nejlepším případě silným šifrováním. Kvalitní šifrovací řešení většinou umožňuje i zcela „vypnout" ukradené zařízení vzdáleně a zabránit tak nechtěnému zneužití uložených dat.

SOULAD

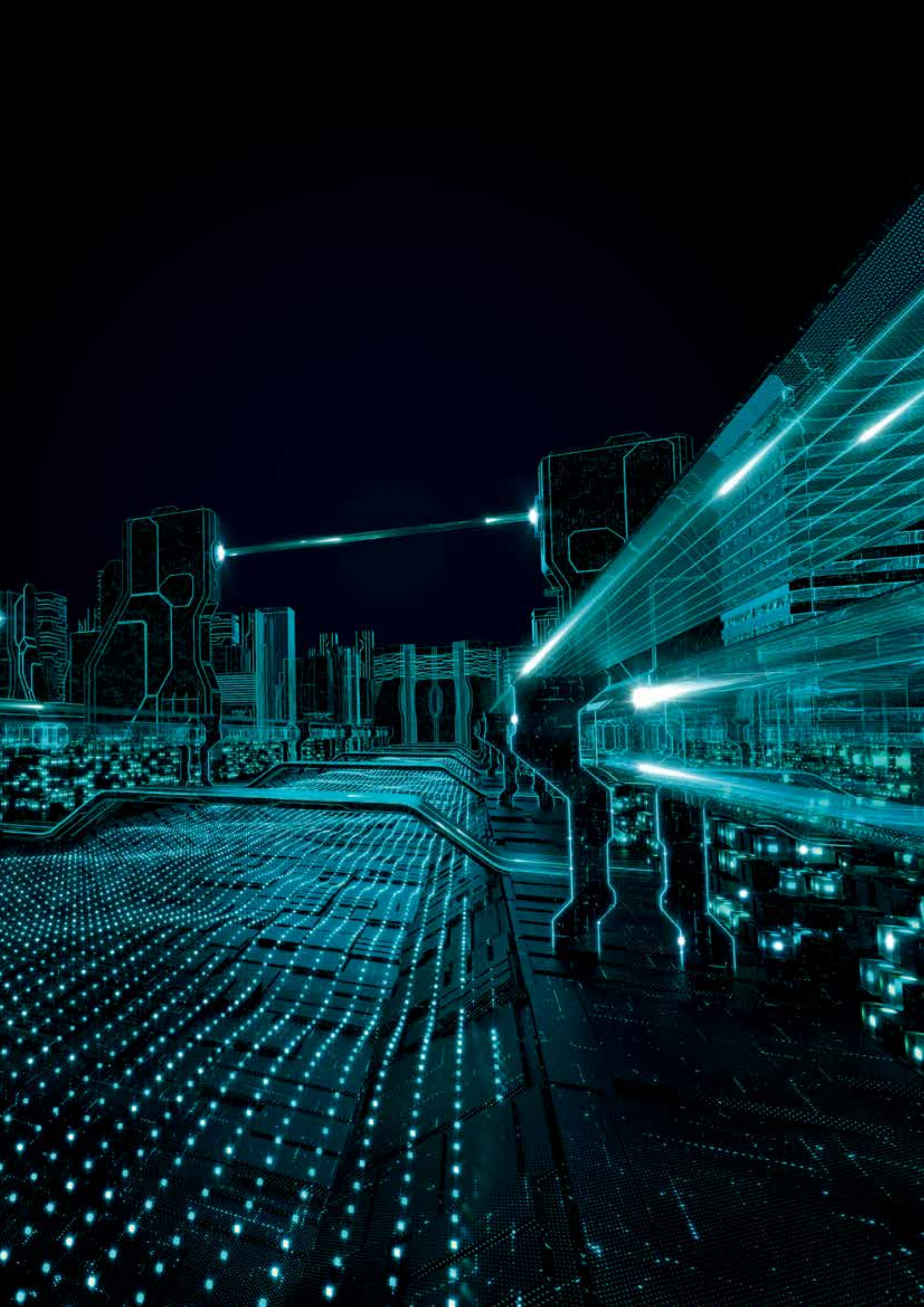
Firmy si musejí nejprve ověřit, zda jsou povinny vyhovět nějaké zákonné normě, či nikoli. Dalším krokem je zjistit, jaké požadavky daná norma doporučuje a nařizuje zavést.

Vlivem mnoha nařízení a zákonů, jako je GDPR, PCI-DSS, HIPAA, SOX a GLBA, se šifrování stalo doporučenou či přímo vyžadovanou metodou ochrany citlivých dat. Šifrování se tak může týkat nejen finančních institucí či zdravotních pojišťoven, ale také všech firem, které zpracovávají a ukládají data zákazníků.



Čím větší je počet mobilních zaměstnanců, tím vyšší je riziko ukradení nebo ztráty zařízení.

Šifrování dat vlivem regulací a zákonů není jen volitelnou metodou ochrany dat. V mnohých případech jde o vyžadované řešení ochrany citlivých dat zákazníků.



Výhody ESETu

SPRÁVA ZAŘÍZENÍ ODKUDKOLI

ESET Endpoint Encryption umožňuje spravovat zařízení odkudkoli na světě bez nutnosti VPN či výjimek ve firewallu. Správa probíhá přes internetové připojení využívající protokol HTTPS k připojení na proxy server. Tím se eliminuje nutnost potenciálně nebezpečného příchozího připojení. Všechny komunikace jsou šifrované pomocí SSL a všechny příkazy a data pomocí AES nebo RSA.

NULOVÝ VLIV NA PRODUKTIVITU

Implementace šifrování je z pohledu uživatele kompletně transparentní a nevyžaduje z jeho strany žádnou akci. Nedochází k zatěžování IT pracovníků ani uživatelů a není potřeba provádět speciální školení.

UNIKÁTNÍ SYSTÉM ŠIFROVÁNÍ KLÍČŮ

Díky použití centrálně spravovaných sdílených klíčů nedochází k problémům, jež se vyskytují u šifrovacích řešení, která typicky používají buď sdílená hesla, nebo veřejné klíče. Systém, který používá ESET Endpoint Encryption, je v zásadě velmi podobný používání fyzických klíčů, například při zamykání domu nebo auta. Zaměstnanci mají tento koncept zažitý, a proto se po implementaci šifrování nemusí učit nic nového. V kombinaci se vzdálenou správou jsou sdílené klíče velmi bezpečnou a praktickou záležitostí.

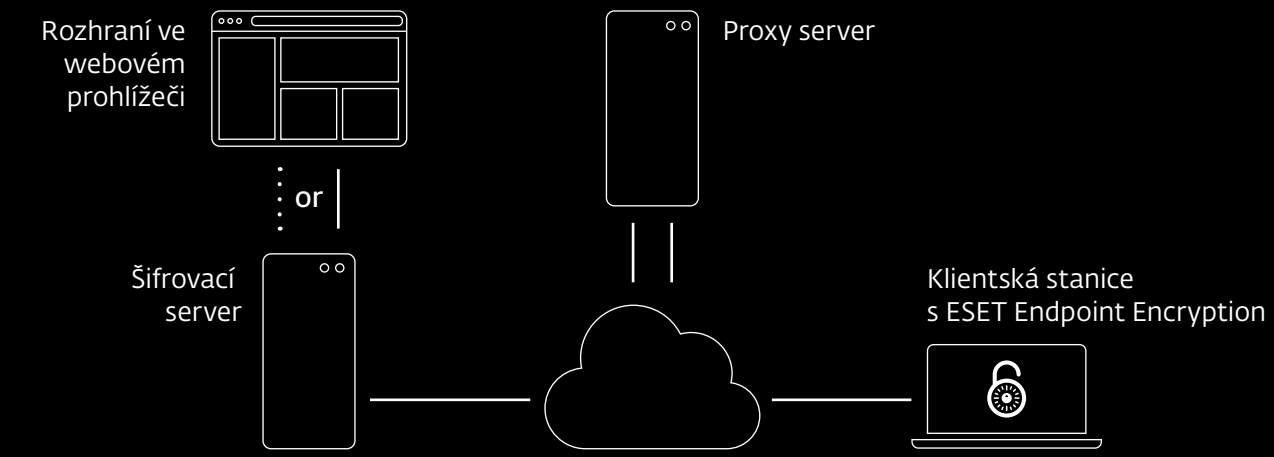
BEZPEČNÁ USB MÉDIA

Správa výměnných médií je někdy ve větších firmách problémem. ESET Endpoint Encryption automaticky vytvoří na USB médiu šifrovaný oddíl, který je přístupný pouze při znalosti daného šifrovacího klíče. Po vložení do neautorizovaného počítače se zobrazí pouze nešifrovaná část disku. Pro koncového uživatele je po krátkém zaškolení celý proces snadno pochopitelný a firmě zaručuje, že uložená citlivá data jsou zcela v bezpečí.

VZDÁLENÉ ZAMKNUTÍ ZAŘÍZENÍ

Práce mimo standardní pracoviště je poměrně běžná a mezi zaměstnanci populární. Z hlediska bezpečnosti to však už ideální řešení není. Může dojít ke ztrátě nebo odcizení zařízení a zneužití uložených dat. Při použití šifrování tato obava odpadá, ESET Endpoint Encryption navíc umožňuje ukradené zařízení vzdáleně vypnout nebo zamknout. Celý proces nevyžaduje VPN ani žádné výjimky pro firewall.

Systém, který používá ESET Endpoint Encryption, je v zásadě velmi podobný používání fyzických klíčů například při zamykání domu nebo aut. Zaměstnanci mají tento koncept zažitý, a proto se po implementaci šifrování nemusejí učit nic nového.



HTTPS, bezpečné připojení

HTTP, LAN

Správa koncových stanic pomocí proxy serveru nevyžaduje žádné příchozí komunikace. Nejsou vyžadovány výjimky ve firewallu ani otevřené porty. Šifrovací server podporuje jakékoli PC nebo server s Windows.

Instalace šifrovacího serveru obvykle trvá méně než 10 minut.

Kompletní nasazení řešení ESET Endpoint Encryption typicky trvá méně než hodinu, což výrazně urychlí dobu přijetí šifrování v celé organizaci.

Příklady použití

Prevence ochrany dat

Zprávy o únicích dat se ve sdělovacích prostředcích objevují každý den.

ŘEŠENÍ

- ✓ Ochrana citlivých dat s pomocí šifrování plného disku (FDE).
- ✓ Dvoufaktorová autentizace pro komunikace typu vzdálená plocha.
- ✓ Vynucení dvoufaktorového přihlášení k zařízení, které obsahuje citlivá data.

DOPORUČENÉ ŘEŠENÍ ESET

- ✓ **ESET Endpoint Encryption**
- ✓ **ESET Secure Authentication**

Vzdálená správa zaměstnanců

Firmy potřebují chránit citlivá data na zařízeních pro případ ukončení pracovního poměru zaměstnance nebo ztráty či odcizení zařízení.

ŘEŠENÍ

- ✓ Omezení přístupu k citlivým datům pomocí dvoufaktorové autentizace.
- ✓ Správce musí mít možnost zamknout/vymazat ztracený nebo ukradený notebook a telefon.
- ✓ Umožňuje odstranit uživatele ze vzdáleného zařízení pro zajištění bezpečnosti dat v případě ukončení pracovního poměru.

DOPORUČENÉ ŘEŠENÍ ESET

- ✓ **ESET Endpoint Encryption**
- ✓ **ESET Secure Authentication**

„Pro nás jako poskytovatele služeb je důležité, že můžeme doporučit, nasadit a podporovat šifrovací řešení, které pomáhá udržet kontinuitu ve vzdělávacích zařízeních Staffordshire a snižuje celkové náklady."

Andy Arnold, CS Team Leader of System Solutions,
Staffordshire Learning Technologies (SLT), UK

Prevence úniku dat

Používání přenosných médií ke kopírování ze zařízení na zařízení je ve firmách běžné. Málokdy se však sleduje, zda citlivá data zůstávají pouze na firemních zařízeních

ŘEŠENÍ

- ✓ Implementace zabezpečení pro výměnná média, které neumožní šíření citlivých dat mimo firmu.
- ✓ Omezení přístupu na výměnná média pro vybrané uživatele.

DOPORUČENÉ ŘEŠENÍ ESET

- ✓ **ESET Endpoint Encryption**

„Pilotní nasazení probíhalo v reálně používaném prostředí a zjistili jsme, že řešení je se svým webovým rozhraním velmi uživatelsky příjemné. Server je velmi dobrý, dokonce umožňuje kontrolu zařízení přes internet, je nezávislý na síti nebo adresářové struktuře."

Simon Goulding, Aster's Network Services Analyst, UK

ESET Endpoint Encryption technické funkce

ŠIFROVÁNÍ DLE POTŘEBY

Šifrování celého disku (FDE), virtuálních disků, souborů a složek, šifrování USB zařízení a e-mailů.

BEZPEČNÉ ŠIFROVÁNÍ

Transparentní (pre-boot) zabezpečení s použitím 256bitového šifrování AES a certifikací podle FIPS 140-2.

ALGORITMY A STANDARDY

AES 256 bit, AES 128 bit, SHA 256 bit, SHA1 160 bit, RSA 1024 bit, Triple DES 112 bit, Blowfish 128 bit.

PODPORA OPERAČNÍCH SYSTÉMŮ

Microsoft® Windows® 10, 8, 8.1 včetně UEFI a GPT, 7, Vista, XP SP 3; Microsoft Windows Server 2003–2012; Apple iOS.

BEZ NUTNOSTI SPECIÁLNÍHO HARDWARU

TP čipy jsou volitelné, ale pro šifrování celého disku nejsou podmínkou.

PROXY SERVER

Zprostředkovává komunikaci mezi klientem a enterprise serverem. Není nutné vlastnit certifikát SSL a další hardware, měnit nastavení sítě nebo firewallu.

ŠIFROVÁNÍ E-MAILŮ A PŘÍLOH

Transparentní šifrování zpráv pomocí dedikovaného pluginu v Outlooku.

ŠIFROVÁNÍ TEXTU A SCHRÁNKY

Umožňuje šifrovat celý text nebo jeho vybrané části.

VZDÁLENÁ SPRÁVA

Umožňuje plnou kontrolu nad licencováním a softwarovými funkcemi, bezpečnostními politikami a šifrovacími klíči.

SPRÁVA ŠIFROVACÍCH KLÍČŮ

Používá patentovanou technologii. Vzdálená a „tichá“ změna politiky bez nutnosti zásahu uživatele.

Všechny firmy na trhu pracují s citlivými daty, jako jsou informace o zákaznících a zaměstnancích, podrobnosti o prodejích, proprietární informace a podobně.

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

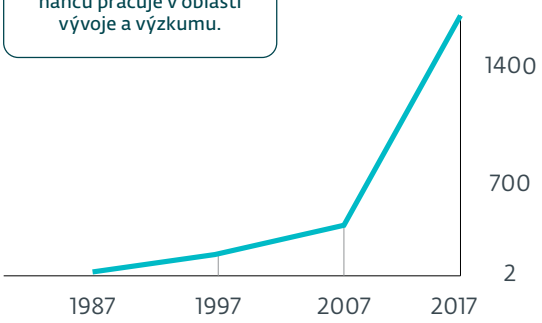
400k+
firemních zákazníků

200+
zemí a teritorií

13
vývojových center

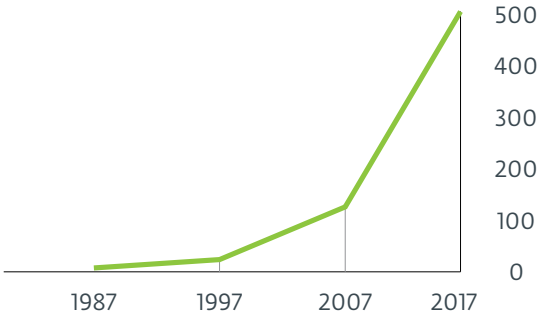
ZAMĚSTNANCI ESETU

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 zříká všech záruk, vyjádřených nebo předpokládaných s ohledem na výzkum, včetně záruky obchodovatelnosti nebo vhodnosti pro konkrétní účel.

NAŠI ZÁKAZNÍCI

HONDA

Zákazníkem od roku 2011

3x prodloužení licence, 2x rozšíření

KOMPAN®

Zákazníkem od roku 2010

více než 1 300 licencí

Canon

Zákazníkem od roku 2016

více než 14 000 licencí

T

ISP partnerem od roku 2008

2 miliony zákazníků

NĚKTERÁ OCENĚNÍ

SE Labs AAA ENTERPRISE ENDPOINT OCT-DEC 2016

THE CHANNEL CO. CRN ★★★★★ PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

„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

ENJOY SAFER TECHNOLOGY™

120918