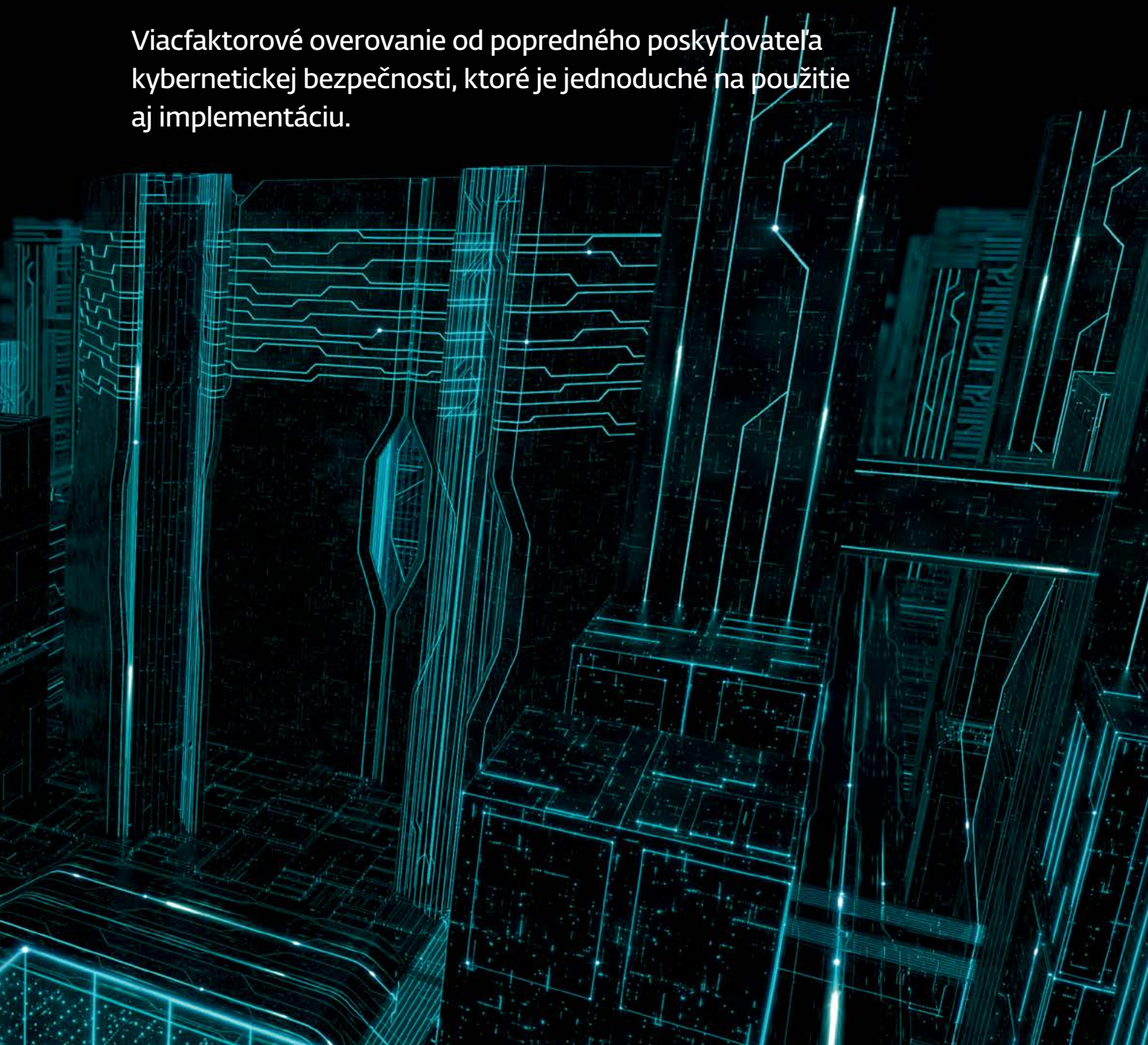
PREHĽAD RIEŠENIA

SECURE AUTHENTICATION

Viacfaktorové overovanie od popredného poskytovateľa kybernetickej bezpečnosti, ktoré je jednoduché na použitie aj implementáciu.



Čo je **viacfaktorové overovanie?**

Viacfaktorové overovanie (MFA), známe aj ako dvojfaktorové overovanie (2FA), je spôsob autentifikácie, ktorý na overenie identity používateľa vyžaduje dve nezávislé množiny informácií. Viacfaktorové overovanie je oveľa účinnejšie než tradičná autentifikácia pomocou statického hesla alebo PINu. Doplnením tradičného overovania o dynamický druhý faktor sa účinne znižuje riziko únikov údajov spôsobených slabými alebo prezradenými heslami.

Riešenie ESET Secure Authentication poskytuje firmám všetkých veľkostí ľahký spôsob implementácie viacfaktorového overenia naprieč bežne používanými systémami, ako sú siete VPN, služby Remote Desktop Protocol, Office 365, Outlook Web Access, prihlasovanie do operačného systému a ďalšie.

Prečo používať **viacfaktorovú autentifikáciu?**

Nielenže zamestnanci používajú rovnaké heslo na viacerých webových stránkach a vo viacerých aplikáciách, ale niekedy aj voľne zdieľajú svoje heslá s priateľmi, rodinou a kolegami.

SLABÁ KULTÚRA ZAOBCHÁDZANIA S HESLAMI

Vraví sa, že „zamestnanci sú váš najslabší článok", keďže zamestnanci zvyčajne vystavujú vašu firmu riziku rôznymi spôsobmi. Jedným z najväčších rizík je slabé povedomie o správnom zaobchádzaní s heslami. Nielenže zamestnanci používajú rovnaké heslo na viacerých webových stránkach a vo viacerých aplikáciách, ale niekedy aj voľne zdieľajú svoje heslá s priateľmi, rodinou a kolegami. A akoby už toto nebol dosť veľký problém, zavedenie politiky tvorby hesiel má vo firmách zvyčajne za následok, že zamestnanci používajú variácie svojho predošlého hesla alebo si zapisujú heslá na lepiace papieriky.

Viacfaktorová autentifikácia chráni firmu pred slabou kultúrou zaobchádzania s heslami tým, že okrem štandardného hesla implementuje aj doplnkové heslo, napríklad tak, že ho vygeneruje v telefóne zamestnanca. Uplatňovanie tohto riešenia zabraňuje útočníkom získať prístup do vašich systémov jednoducho iba uhádnutím slabého hesla.

ÚNIKY ÚDAJOV

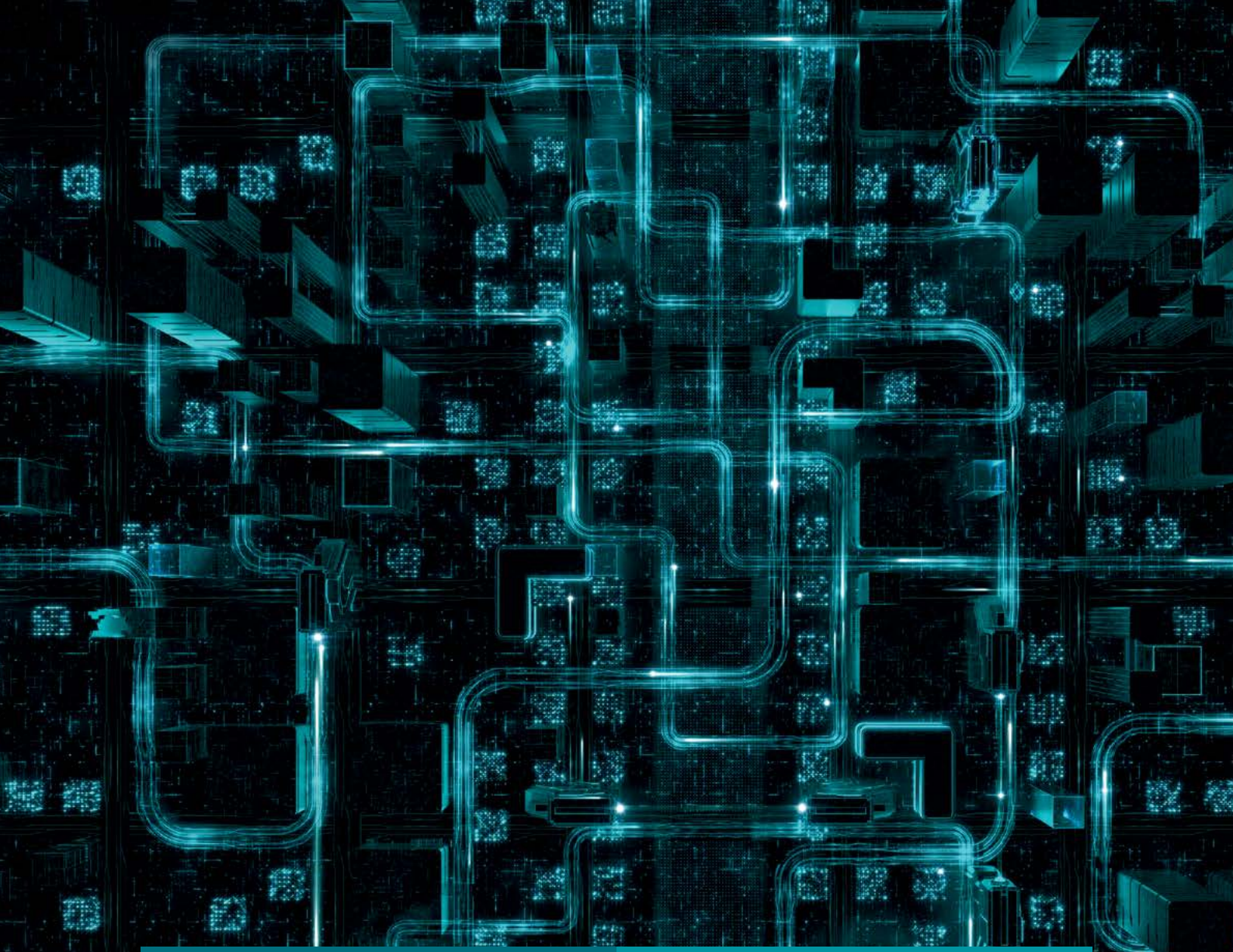
V súčasnom prostredí IT bezpečnosti každým dňom narastá počet únikov údajov. Jedným z najbežnejších spôsobov, akými hackeri môžu získať prístup k dátam vašej firmy, sú slabé alebo odcudzené heslá. Okrem ochrany normálnych prihlásení používateľov do kritických služieb môžu firmy implementovať viacfaktorovú autentifikáciu pre všetky elevácie oprávnení, aby sa tak zabránilo neoprávnenému správcovskému prístupu.

Pridaním viacfaktorového overovania firmy značne sťažia hackerom možnosť získať prístup k systémom a narušiť ich. Hlavnými odvetviami, ktorých sa týkajú úniky údajov, sú tradične odvetvia s cennými údajmi, ako sektor financií, maloobchodu, zdravotnej starostlivosti či verejný sektor. Neznamená to však, že ostatné odvetvia sú v bezpečí. Hackeri totiž zvyčajne chcú, aby sa im vynaložené úsilie vyplatilo.

POTREBA SÚLADU S PRAVIDLAMI

Pokiaľ ide o súlad s legislatívou, väčšina firiem musí najskôr zistiť, či musia zabezpečiť súlad alebo nie. Potom musia skontrolovať požiadavky, ktorých implementáciu táto legislatíva odporúča a vyžaduje. Pokiaľ ide o viacfaktorovú autentifikáciu, jeho implementáciu už vyžadujú mnohé normy, ako sú PCI-DSS a GLBA, a väčšina zákonov vrátane GDPR a HIPAA vo všeobecnosti zdôrazňuje potrebu silnejšieho overovania.

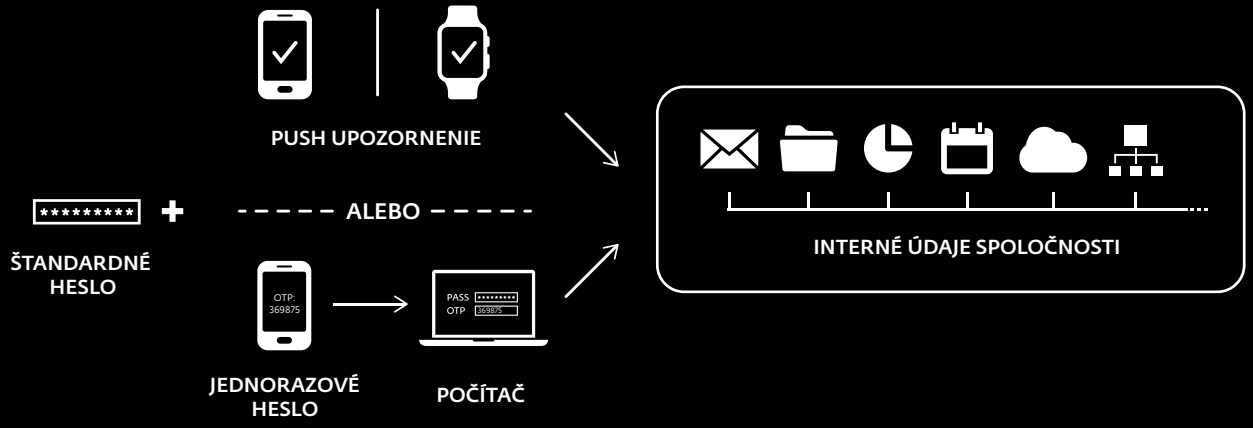
Viacfaktorová autentifikácia už pre väčšinu firiem, ktoré pracujú s kreditnými kartami alebo v oblasti finančných transakcií, nie je iba dobrovoľným riešením, ale skôr povinnosťou. Každá firma by mala uskutočniť prieskum a vyhodnotiť, ktorými pravidlami sa musí riadiť.



Jedným z najbežnejších spôsobov, akým hackeri môžu získať prístup k dátam vašej spoločnosti, sú slabé alebo odcudzené heslá.

Uplatňovanie tohto riešenia zabraňuje útočníkom získať prístup do vašich systémov jednoducho iba uhádnutím slabého hesla.

Jednoduché overenie pomocou jedného ťuknutia – nebudete musieť zadávať manuálne jednorazové heslo.



V čom je ESET iný

JEDNODUCHO SI VYBERTE SPÔSOB INTEGRÁCIE

Nástroj ESET Secure Authentication ponúka dva spôsoby integrácie – so službou Active Directory pre organizácie používajúce doménové prostredie v systéme Windows, alebo standalone integráciu, ktorá je vhodná pre organizácie bez Windows domény. Nech už si vyberiete ktorýkoľvek spôsob, nastavenie a konfigurácia je rýchla a jednoduchá, riešenie je spravovateľné cez webovú konzolu..

NEVYŽADUJE SA ŽIADNY ŠPECIALIZOVANÝ HARDVÉR

Všetky náklady na riešenie ESET Secure Authentication sú v ňom už obsiahnuté, pretože nevyžaduje žiadny špecializovaný hardvér. Stačí len nainštalovať aplikáciu na ľubovoľný server.

SPOLUPRACUJE S EXISTUJÚCIMI SMARTFÓNMI

Zamestnancom nie je potrebné poskytnúť žiadne špeciálne tokeny alebo zariadenia. ESET Secure Authentication funguje hladko so všetkými iOS a Android zariadeniami, pre zvýšenie zabezpečenia a pohodlnejšie používanie dokáže byť integrovaný s biometriou na zariadení (Touch ID, Face ID, Android fingerprint).

NASTAVENIE ZABERIE 10 MINÚT

Do tvorby riešenia ESET Secure Authentication bolo investovaných mnoho hodín v záujme toho, aby bolo celé nastavenie čo najľahšie. Naším zámerom bolo vytvoriť aplikáciu, ktorú by si mohla nainštalovať a nastaviť malá firma bez pomoci IT personálu. Či už má vaša firma päť používateľov alebo tisíce používateľov, nastavenie riešenia ESET Secure Authentication – vďaka jeho schopnosti obsluhovať viacerých používateľov naraz – zaberie iba minimálny čas.

SÚČASŤOU JE SDK A ROZHRANIE API

Pre podniky alebo spoločnosti, ktoré chcú riešenie ESET Secure Authentication využívať ešte pokročilejším spôsobom, poskytujeme plnohodnotné API a SDK s plným vybavením, ktoré môžu používatelia využiť na rozšírenie multifaktorovej autentifikácie pre aplikácie a platformy aj bez nutnosti využitia dedikovaného pluginu.

PUSH UPOZORNENIE

Umožňuje overovanie jedným ťuknutím, bez nutnosti zadávať jednorazové heslo. Spolupracuje s telefónmi so systémom iOS a Android.

„Inštalácia na jedinom serveri, ľahké nastavenie, integrácia s Active Directory a jeden z významných plusov: aplikácia, ktorú sme mohli dať členom nášho personálu, takže nebolo potrebné neustále posielať SMS. K tomu všetkému nás ešte veľmi potešil fakt, že to bezproblémovo funguje s otvorenou VPN, takže sme nemuseli meniť nastavenie svojej VPN na prispôsobenie sa softvéru.“

— Tom Wright, vedúci IT služieb, Gardners Books

Príklady použitia

Predchádzanie únikom údajov

Firmy každý deň informujú cez médiá svojich zákazníkov, že došlo k úniku údajov.

RIEŠENIE

- ✓ Chráňte citlivé pripojenia, napríklad k vzdialenej pracovnej ploche, pridaním protokolu viacfaktorovej autentifikácie.
- ✓ Pridajte viacfaktorovú autentifikáciu pre všetky siete VPN, ktoré sú využívané.
- ✓ Požadujte viacfaktorovú autentifikáciu pri prihlásení do zariadení s citlivými údajmi.
- ✓ Chráňte citlivé údaje pomocou riešenia ESET Endpoint Encryption.

ESET PRODUKTY

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Proces overenia prihlásenia používateľa

Firmy používajú zdieľané počítače v zdieľaných pracovných priestoroch a vyžadujú overenie všetkých používateľov, ktorí sa prihlasujú počas pracovného dňa.

RIEŠENIE

- ✓ Implementujte viacfaktorovú autentifikáciu pre desktopové prihlásenia na všetkých zariadeniach v zdieľaných pracovných priestoroch.

ESET PRODUKTY

- ✓ ESET Secure Authentication

Posilnite ochranu hesiel

Používatelia používajú rovnaké heslá vo viacerých aplikáciách a webových službách a vystavujú tak firmy riziku.

RIEŠENIE

- ✓ Obmedzte prístup k firemným prostriedkom pomocou viacfaktorovej autentifikácie.
- ✓ Vyžadovanie viacfaktorovej autentifikácie zníži obavy a nebezpečenstvo spojené so zdieľanými alebo odcudzenými heslami tým, že sa okrem hesla bude vyžadovať aj ďalšie overenie, napríklad schválenie push správ.

ESET PRODUKTY

- ✓ ESET Secure Authentication

Technické informácie a chránené platformy

PUSH UPOZORNENIE

Overenie jedným ťuknutím na všetkých smartfónoch so systémom iOS a Android.

INÉ SPÔSOBY OVERENIA

ESET Secure Authentication podporuje na doručovanie jednorazových hesiel mobilné aplikácie, push upozornenia, hard tokeny, SMS, FIDO kľúče ako aj vlastné metódy.

VZDIALENÁ SPRÁVA

Realizuje sa cez webovú konzolu riešenia ESET Secure Authentication alebo konzolu MMC (Microsoft Management Console). Integruje sa so službou Active Directory v záujme ľahkej správy alebo funguje samostatne v prípade organizácií bez domény Windows.

PODPORA OCHRANY

ESET Secure Authentication natívne podporuje siete VPN (Virtual Private Networks), protokol RDP (Remote Desktop Protocol), Outlook Web Access (OWA), VMware Horizon View aj služby založené na protokole RADIUS.

DOPLNKOVÁ OCHRANA OPERAČNÉHO SYSTÉMU

Doplnkové overenie na desktopové prihlásenia a eleváciu oprávnení je tiež chránené prostredníctvom viacfaktorového overovania. Podporuje systém Windows, ako aj systémy macOS a Linux.

PODPORA CLOUDU

Pridajte viacfaktorovú autentifikáciu na posilnenie prístupu do služieb ako Google Apps, Office 365, Dropbox a mnohých iných. ESET podporuje integráciu cez autentifikačný protokol SAML-2, ktorý používa väčšina poskytovateľov overovania identity.

PODPORA HARD TOKENOV

Hoci sa hard tokeny nevyžadujú, podporované sú všetky eventbased HOTP tokeny, ktoré spĺňajú štandard OATH, ako aj hardvérové kľúče FIDO2 a FIDO U2F.

PODPOROVANÉ VDI A VPN

VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

Podpora pre integrácie s rôznymi RADIUS VPN riešeniami.

O spoločnosti ESET

ESET, globálny hráč v oblasti informačnej bezpečnosti, bol zaradený do kvadrantu vyzývateľov (Challengers) v správe Magic Quadrant for Endpoint Protection Platforms na rok 2019, ktorú pravidelne vypracúva analytická spoločnosť Gartner.* Ako jediný bol do kvadrantu vyzývateľov zaradený dvakrát po sebe.

Už viac ako 30 rokov ESET® vyvíja popredný softvér a služby zamerané na IT bezpečnosť, ktoré poskytujú okamžitú a komplexnú ochranu pred vyvíjajúcimi sa hrozbami pre firmy a spotrebiteľov na celom svete. ESET je v súkromnom vlastníctve. Vďaka tomu, že nemáme dlhy ani pôžičky, môžeme slobodne robiť všetko, čo si špičková ochrana všetkých našich zákazníkov vyžaduje.

ESET V ČÍSLACH

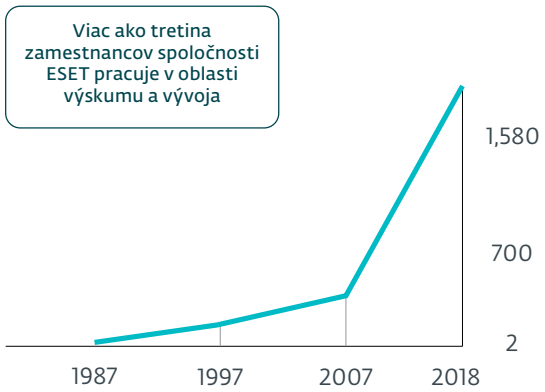
Vyše 110 miliónov
používateľov po celom svete

Vyše 400-tisíc
firemných zákazníkov

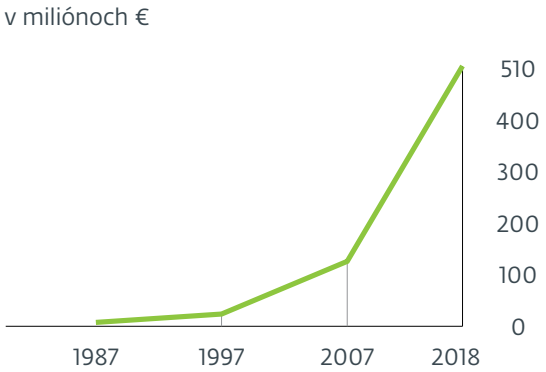
Vyše 200
krajín a teritórií

13
globálnych R&D centier

ZAMESTNANCI SPOLOČNOSTI ESET



VÝNOSY SPOLOČNOSTI ESET



* Spoločnosť Gartner nepodporuje ani nepropaguje žiadneho výrobcu, produkt ani službu, ktoré uvádza vo svojich výskumných publikáciách. Tieto výskumné publikácie pozostávajú z názorov výskumnej organizácie Gartner a nemali by byť interpretované ako fakty. Spoločnosť Gartner v súvislosti s týmto výskumom neposkytuje nijaké záruky, či už vyjadrené alebo predpokladané, vrátane záruky obchodovateľnosti či vhodnosti na konkrétny účel.

NIEKTORÍ Z NAŠICH ZÁKAZNÍKOV

MITSUBISHI MOTORS
Drive your Ambition

s ochranou od spoločnosti ESET už od roku 2017
viac ako 14-tisíc koncových zariadení

Canon
Canon Marketing Japan Group

s ochranou od spoločnosti ESET už od roku 2016
viac ako 9-tisíc koncových zariadení

Allianz Suisse

s ochranou od spoločnosti ESET už od roku 2016
viac ako 4 000 e-mailových adries

T

ISP bezpečnostný partner od roku 2008
2 milióny zákazníkov

NIEKTORÉ Z NAŠICH NAJVÝZNAMNEJŠÍCH OCENENÍ

„Vzhľadom na skvelé funkcie ochrany pred malvérom, ako aj spravovateľnosť či široký globálny dosah zákazníkov a podpory, by mal byť ESET zaradený na shortlist kandidátov, ktorí poskytujú firemné antimalvérové riešenia.“

Analýza spoločnosti KuppingerCole pod názvom Leadership Compass: Enterprise Endpoint Security: Anti-Malware Solutions, 2018