



NETPROTECT

Telco & ISP

Diverzifikace příjmů díky službám kybernetické bezpečnosti nad rámec hlavní nabídky

Progress. Protected.

Aktuální situace

Mobilní i virtuální operátoři a poskytovatelé internetových služeb čelí v současné době mnoha výzvám. Hodnota trhů, které jsou pro telekomunikační firmy a poskytovatele internetu významné, se postupem času snižuje a zákazníci očekávají neustálé inovace. V rámci mobilních a pevných tarifů, které tvoří součást produktových portfolií těchto společností, zákazníci požadují stále více – rychlejší internet, větší objem dat, lepší stabilitu a další benefity. Tyto aspekty pak ovlivňují průměrnou hodnotu na uživatele (označovanou také jako ARPU).

Na trhu panuje s každou novou firmou, která na něj vstoupí s agresivní cenovou politikou a prostřednictvím telefonického prodeje a nabídkou různých výhod pro zákazníky, stále větší konkurence.

Firmám, které se v této oblasti pohybují, se navíc v postcovidové éře zvyšují neočekávané náklady a v důsledku nejistoty, změn ovlivňujících místní i mezinárodní mobilitu odběratelů služeb a skutečnosti, že klienti místo fyzických návštěv prodejních míst rychle přecházejí na on-line nakupování, je dnes ještě obtížnější získat koncové zákazníky pro portfolio špičkových produktů a služeb. Vše dále umocňuje fakt, že kapitáloví účastníci působících v oblasti telekomunikací a poskytování internetových služeb od firem očekávají meziroční růst finanční a transakční výkonnosti.

Jaký nový produkt zvolit?

Co se týče produktů, které mohou telekomunikačním společnostem/ poskytovatelům internetových služeb pomoci v růstu – ve smyslu tržeb a ukazatelů EBITDA a ARPU, mají produktoví manažeři obvykle na výběr z mnoha různých možností.

Mobilní i virtuální operátoři v současnosti nejčastěji přechází na prodej telekomunikačních produktů domácnostem namísto jednotlivců, na tarifní služby místo předplacených, neomezené hlasové tarify místo těch mobilních, nabídky mobilních dat místo datových balíčků pro posílání zpráv a na optické a místní bezdrátové sítě místo DSL.

Zajištění růstu příjmů ze základních produktů a služeb mobilních a pevných tarifů s sebou ovšem nese mnoho obtíží, a proto se nejvhodnější volbou, která může firmám pomoci v růstu, stávají doplňkové služby s přidanou hodnotou. Na základě každoročního výzkumu GSMA z roku 2021 o diverzifikaci příjmů operátorů se zdá, že mezi dvě oblasti s největším potenciálem růstu patří řešení kybernetické bezpečnosti. Produktoví manažeři se obvykle musí soustředit nejen na atraktivní nabídku produktů s vysokým růstovým potenciálem, ale také na porozumění dalším aspektům úspěšnosti produktů, jako je jednoduchost jejich prodeje koncovým zákazníkům, snadnost používání a jejich potenciál stát se novým a udržitelným

zdrojem příjmů. Hlavní prioritou pro společnosti, které se zaměřují na poskytování telekomunikačních a internetových služeb, jsou sice komplexnější základní služby, ale při úvahách o nových produktech je potřeba zohlednit také další parametry, jako jsou provize pro obchodníky, průměrná doba trvání obchodní prezentace a její průměrná míra úspěšnosti a potřeba poprodejní podpory.

Z každoročního výzkumu GSMA z roku 2021 o diverzifikaci příjmů operátorů vyplývá, že významný nárůst zaznamenávají příjmy z řešení kybernetického zabezpečení a cloudových služeb různého druhu. Slibnou novinkou jsou také hry, zejména s tím, jak se jejich hraní přesouvá na mobilní zařízení. Znovu roste i zájem o finanční služby.

Technické podrobnosti

Objem investic do zavádění nových sítí, ať těch mobilních 5G a LTE, pevných bezdrátových 5G, či optických, setrvale roste. Proto je také důležité neustále monitorovat výkonnost sítě a kvalitu služeb a mít připravené plány pro případ neočekávaných událostí.

Shromažďování a ukládání dat a jejich sdílení s třetími stranami je regulováno předpisy o ochraně osobních údajů (např. GDPR). Firmy se musí nejprve rozhodnout, zda z pohledu zabezpečení citlivých dat upřednostnit řešení založené na cloudu, nebo zvolit lokální řešení. V případě kybernetické bezpečnosti jsou na trhu k dispozici nejen různá řešení, ale ta se dále liší i v nabídce specifických funkcí v konkrétních produktech (např. možnost vytváření a správy vlastních seznamů důvěryhodných adres a seznamů blokováných adres).

Je proto velmi důležité hledat takového dodavatele, který má v nabídce cloudová i on-premise řešení, umožňuje snadno upravovat bezpečnostní funkce i koncovým zákazníkům, a zároveň by řešením mělo mít minimální dopad na výkonnost mobilní nebo pevné sítě.

Strategie uvádění produktů na trh

Nový produkt společně se specializovanou aplikací pro chytré telefony lze nabízet mnoha způsoby, ale problematickým aspektem tohoto procesu může být pomoc s instalací nebo aktivací. S ohledem na potenciál růstu by společnosti měly zvážit nabízení produktů jinými než standardními prodejními kanály – například prostřednictvím kampaní přímého prodeje, kdy produkty kybernetické bezpečnosti společností umožňují, aby je integrovaly do své architektury a systémů CRM.

Vedení kampaně prostřednictvím marketingových kanálů jako SMS, MMS, Viber, WhatsApp nebo e-mail může vést k vysoké míře přijetí služeb a nebývale vysokému růstu příjmů z nově nabízených produktů. Na druhé straně nevyžaduje od firem nijak velké úsilí – s výjimkou vytvoření cílových skupin ze zákaznické základny a vylepšení reklamních sdělení pro vyšší konverzi zákazníků.

Je zásadní, aby firmy byli připraveni spolupracovat se zavedenými dodavateli, kteří dokáží zajistit podporu pro požadavky druhé a třetí úrovně, a to i pro miliony aktivních odběratelů. Produkty kybernetické bezpečnosti sice obvykle chrání koncového uživatele před hrozbami, když jsou chytrá zařízení připojena k internetu prostřednictvím mobilního širokopásmového připojení, je ovšem nutné uvědomit si, že 70–90 procent datového provozu ve vyspělých zemích je tvořeno výhradně přenosy přes Wi-Fi.

Při přípravě sdělení o řešení kybernetické bezpečnosti pro koncového uživatele je tedy důležité pamatovat na možnost jeho ochrany nejen v případě používání mobilních dat, ale také kdykoli je připojen k bezdrátovým sítím.

Klíčovým rozlišovacím prvkem, který společnostem pomůže nabídnout přidanou hodnotu a přilákat nové zákazníky využívající služeb konkurence, může být implementace DNS proxy serverů. Vzhledem k tomu, že se v éře po covidu-19 stává standardem digitální a distanční vzdělávání, tráví hodně času on-line i děti. Proto je důležité hledat řešení, která jednak zajišťují standardní ochranu a kybernetickou bezpečnost, ale zároveň rodičům umožňují využívat filtry chránící jejich potomky před nevhodným obsahem.

Finanční modelování

Ve velkých firmách mobilních i virtuálních operátorů a poskytovatelů internetových služeb prochází marketingoví, generální a finanční ředitelé náročným obdobím. Musí totiž naplňovat očekávání ohledně neustálého růstu tržeb a ukazatelů EBITDAAL a ARPU u konvergentních a mobilních služeb, zrychlení růstu počtu zákazníků využívajících optické sítě typu FTTH a další typy připojení (xDSL, kabelové či pevné bezdrátové připojení), požadavků na zvýšení pokrytí sítí 5G, meziročního růstu maloobchodních služeb a dalších výnosů.

S novými službami nad rámec základní nabídky se otevírají nové možnosti diverzifikace příjmů a vytváření zcela nových a udržitelných zdrojů zisku. Nedávný průzkum ukazuje, že zatímco základní služby na většině trhů v oblasti telekomunikací a poskytování internetových služeb téměř

nerostou, nové služby nad rámec těch základních mohou zajistit růst příjmů a v roce 2020 dosáhly u analyzovaných operátorů 24 % z jejich celkového objemu, přičemž na nejnávýspějších trzích to bylo dokonce až 41 %.

Zároveň se ukázalo, že ke dvěma nejnávýznamnějším oblastem, které mohou zajistit dosažitelný růst, patří služby zaměřené na kybernetickou bezpečnost a cloudové služby.

Síťové služby kybernetické bezpečnosti mohou také dosáhnout vysoké míry přijetí (dvouciferný procentuální růst celkového počtu zákazníků). Důležitým zdrojem velkého, nového a udržitelného toku příjmů se stávají možnosti měsíčních plateb a vysoká retence zákazníků. Zákazníci, kteří využívají služby mobilního a pevného širokopásmového připojení, již za své základní telekomunikační služby platí měsíčně a očekává se, že za služby s přidanou hodnotou, které budou vyhovovat jejich potřebám, budou ochotni platit až o 33 % více.



NETPROTECT



Telcos a ISP přímo na míru

Zajistěte svým zákazníkům špičkovou ochranu před rostoucími webovými hrozbami. **ESET NetProtect** chrání všechny chytré telefony, domácí a IoT zařízení, na všech hlavních operačních systémech a lze jej použít v pevných (Fiber, FWA, DSL, kabelové, jiné) i mobilních síťových technologiích (5G, 4G, 3G, 2G).

Společnost ESET už více než 30 let vyvíjí bezpečnostní technologie ochrany proti hrozbám v kyberprostoru. ESET NetProtect není výjimkou, integruje v sobě dlouhodobé technologické know-how a odborné znalosti s využitím nejnovějších technologií v oblasti pokročilého strojového učení a umělé inteligence.

NAŠI ZÁKAZNÍCI



O jeden krok před hrozbami

Pokročilá online ochrana vašich zákazníků před webovými hrozbami - zejména před škodlivými doménami a phishingovými weby, které by mohly způsobit únik soukromých dat nebo útoky na jejich osobní zařízení.

ESET poskytuje uživatelům oceňovanou ochranu v reálném čase doma i na cestách, takže se mohou naplno věnovat svému digitálnímu životu. ESET NetProtect umožňuje zákazníkům nechat si zobrazit nebo rovnou zakázat různé kategorie obsahu na internetu podle jejich preferencí a chrání je tak před nevhodným obsahem.

Jeden poskytovatel bezpečnostních produktů



AKTIVACE JEDNÍM KLIKUTÍM

Snadné ovládání a integrace díky pozitivní adopci technologií ve společnosti a aktivaci jedním kliknutím.



DALŠÍ PŘÍJEM

Generujte další příjmy s vysokými maržemi.



PŘIDANÁ HODNOTA

Získejte konkurenční výhodu se zcela novou službou kybernetické bezpečnosti.



MINIMÁLNÍ NÁROKY

Nevyžaduje žádnou instalaci na straně zákazníka.



RYCHLÉ NASAZENÍ

Hladká implementace během pár týdnů.

Produkty ESET NetProtect

MOBILNÍ OPERÁTOŘI

ESET NetProtect for Mobile

- ✓ Anti-malware filtr, anti-phishing filtr, ochrana před potenciálně nechtěným obsahem
- ✓ Vlastní blacklist a whitelist
- ✓ 5G, IoT a starší **mobilní sítě**

MOBILE NETWORK OPERATORS

ESET NetProtect for Mobile Advanced

- ✓ Anti-malware filtr, anti-phishing filtr, ochrana před potenciálně nechtěným obsahem
- ✓ Vlastní blacklist a whitelist
- ✓ 5G, IoT a starší **mobilní sítě**
- ✓ Filtr webového obsahu

PEVNÍ OPERÁTOŘI

ESET NetProtect for Home Advanced

- ✓ Anti-malware filtr, anti-phishing filtr, ochrana před potenciálně nechtěným obsahem
- ✓ Vlastní blacklist a whitelist
- ✓ Kabel, 5G FWA a starší **pevné sítě**
- ✓ Web Content Filter

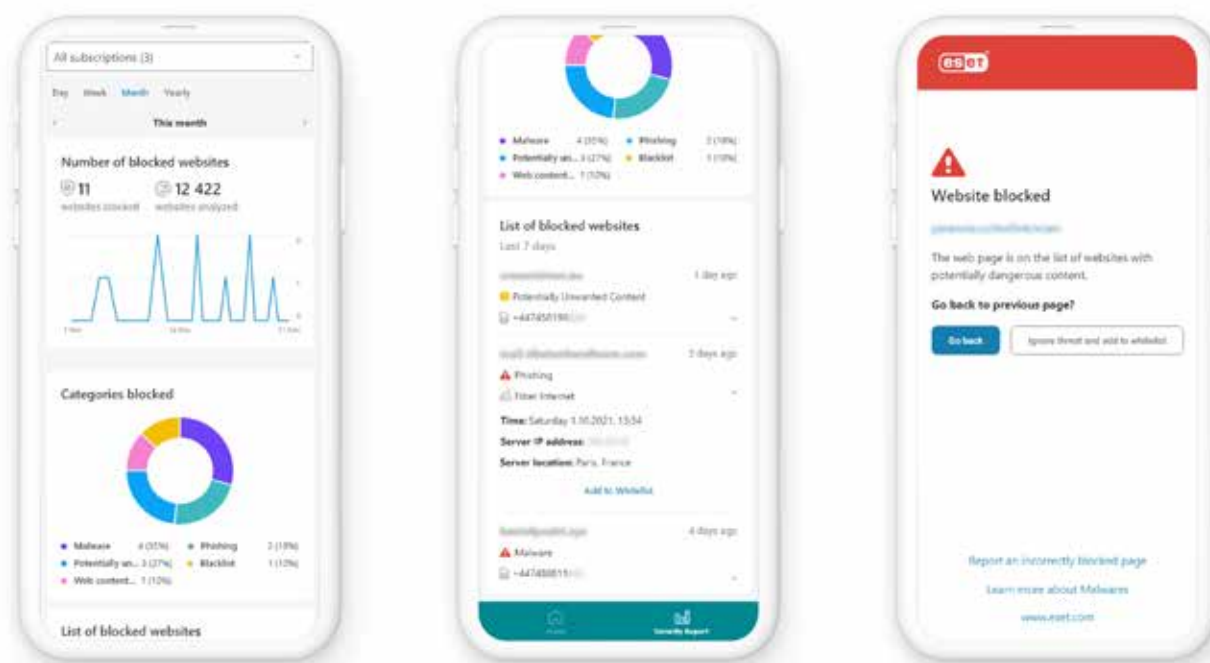


VÍCE INFORMACÍ
netprotect.eset.com

Jak to funguje

Po aktivaci "služby" jsou všechny navštívené webové stránky odeslány ke kontrole do **ESET NetProtect** DNS serveru. Pokud je doména identifikována jedním z pěti filtrů jako škodlivá nebo zakázaná, zobrazí se obrazovka blokování s uvedením důvodu, proč byla doména zablokována. Koncový zákazník má možnost změnit defaultně aktivované doménové filtry přes zákaznický portál.

POHLED KONCOVÉHO UŽIVATELE



JEDNODUCHÝ PROCES



Uživatel zadá stránku



Požadavek se oskenuje na ESET NetProtect DNS serveru



V případě detekce škodlivého obsahu je uživatel přesměrován na blokovací stránku.

NASTAVENÍ FILTRŮ

Anti-Malware

Chrání zákazníka před přístupem k doménám obsahujícím malware, který po instalaci může poskytnout vzdálený přístup k infikovanému zařízení, ukrást citlivá data, poškodit zařízení nebo způsobit jinou škodu majiteli.

Anti-Phishing

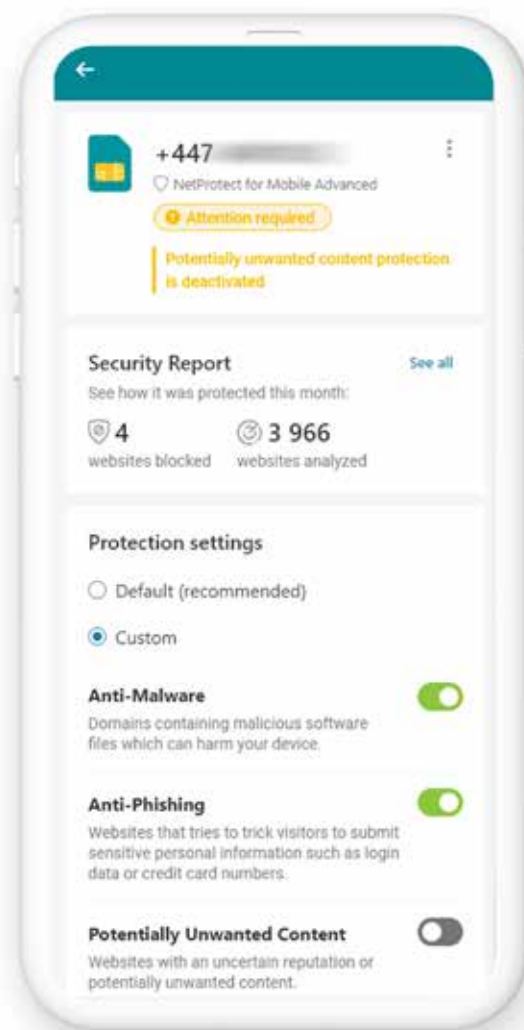
Chrání před podvodnými webovými stránkami, na kterých se útočník snaží získat citlivé informace, jako jsou uživatelská jména, hesla nebo přihlašovací údaje ke kreditním kartám.

Potenciálně nechtěný obsah

Chrání zákazníka před podezřelými doménami nebo webovými stránkami, na kterých je umístěn nežádoucí obsah.

Filtr webového obsahu

Zákazník si může vybrat z předdefinovaných skupin filtrů na základě věkového rozmezí nebo ručně vybrat libovolnou kategorii (35 filtrů, např. pro dospělé, násilí, náboženství atd.).



BLACKLIST A WHITELIST DOMÉN

Whitelist

Zákazník může ručně nebo přímo z obrazovky blokování vytvořit seznam povolených domén.

Blacklist

Zákazník může ručně vytvořit seznam zakázaných domén. Při příští návštěvě zakázané domény se zobrazí obrazovka blokování. Takovou doménu nelze zařadit na whitelist z blokovací obrazovky (pouze z portálu pro správu). Blacklist má vyšší prioritu než whitelist (v případě duplicity).

BEZPEČNOSTNÍ ZPRÁVY

Zákazník má přístup k měsíční bezpečnostní zprávě o filtrovaných doménách a může dostávat pravidelné e-maily s přehledy.

INTUITIVNÍ SPRÁVA

Portál správy

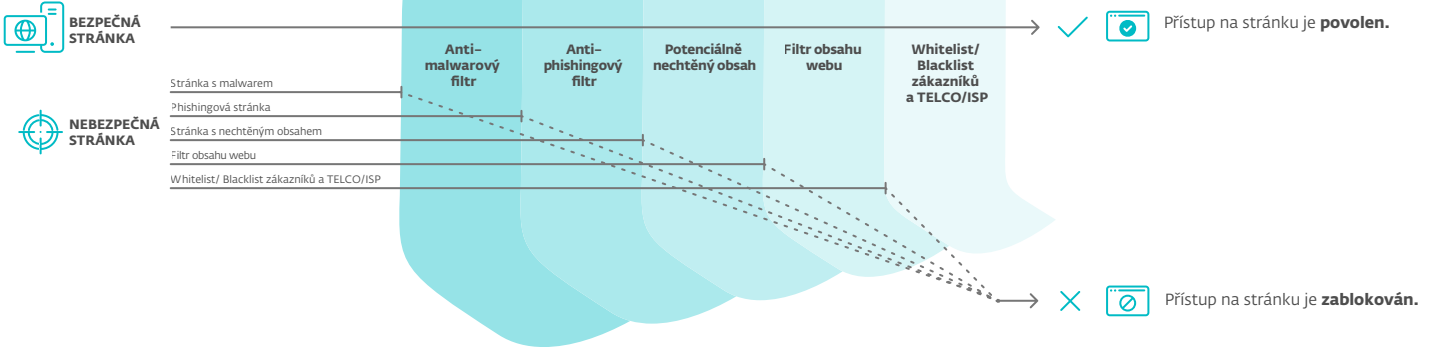
Na portálu mohou zákazníci snadno spravovat pravidla pro připojená zařízení, spravovat whitelisty a blacklisty, a zobrazovat bezpečnostní zprávy.

Portál pro správu (telco/ISP)

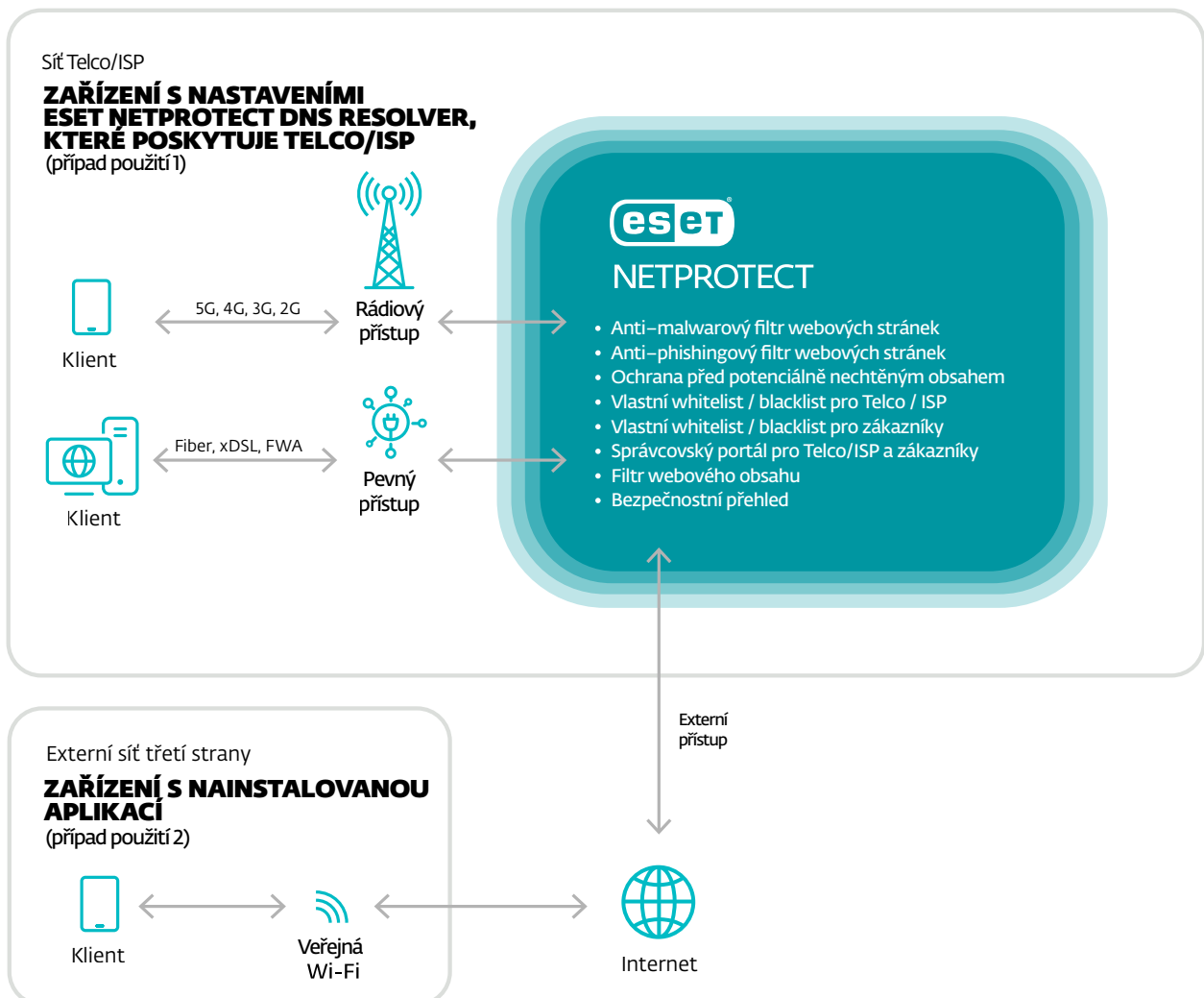
Jako partner Telco/ISP máte k dispozici speciální portál pro správu řešení a analýzu dat nebo reportování. Můžete také přistupovat k profilům zákazníků a upravovat nastavení podle jejich požadavků.

FILTRY ESET NETPROTECT

ZÁKAZNÍK HLEDÁ STRÁNKU



TELCO / ISP



O ESETu

Proč vám ESET pomůže zvýšit příjmy

ESET je soukromá společnost zabývající se digitální bezpečností s centrálou v EU a více než 30 lety zkušeností.

11+ Let

integrace TELCO a ISP
s jejich fakturačními systémy

#1

cybersecurity
partner v EU

13

výzkumných
a vývojových center

400K+

firrných zákazníků

200+

zemí



Společnost ESET je zakládajícím členem App Defense Alliance, která zajišťuje bezpečnost obchodu Google Play

"Spolupráce s uznávaným členem kyber bezpečnostního průmyslu, jako je společnost ESET, posílí ochranu Google Play"

Dave Kleidenmacher, vedoucí oddělení zabezpečení systému Android a ochrany soukromí ve společnosti Google



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.

www.eset.cz

OCENĚNÍ A TESTY

