




UŽÍVAJTE SI BEZPEČNEJŠIE  
TECHNOLÓGIE™

# Bezpečnostné riešenia pre domácich používateľov

pre zariadenia s operačným  
systémom Windows

*Praktické rady, ako sa chrániť pred  
digitálnymi hrozbami doma i na cestách.*





Spoločnosť ESET už viac ako 30 rokov vytvára bezpečnostné produkty a riešenia, ktoré spoľahlivo chránia vaše zariadenia v domácnosti. Pre majiteľov počítačov alebo laptopov s operačným systémom Windows poskytuje tri druhy ochrany – ESET NOD32 Antivirus, ESET Internet Security a ESET Smart Security Premium.

V tejto príručke nájdete rozdiely medzi funkcionalitou týchto produktov. Zároveň v nej opisujeme, prečo je dôležité používať bezpečnostné produkty, aké funkcie ponúkajú, čo dokážu a pred čím vás chránia. Nájdete tu zároveň praktické informácie, ako si svoje digitálne zariadenia ochránite nielen doma, ale aj na dovolenke alebo na cestách.

## Lahké použitie aj bez expertných znalostí

Na trhu existuje mnoho výrobcov bezpečnostného softvéru. Človek by si preto možno povedal, že vytvoriť program, ktorý bude odchytať škodlivý kód, je jednoduché. Opak je však pravdou. Bezpečnostní experti musia držať krok s útočníkmi, ktorým ide o to, aby na vašich dátach čo najviac zarobili. Prípadne si priamo poslali peniaze z vášho účtu.

Experti musia svoje poznatky o útokoch pretaviť do bezpečnostného riešenia, ktoré:

- Odchyta iba škodlivý kód a neblokuje užitočné programy. Takejto prípadnej chybe pri detekcii sa hovorí falošný poplach.
- Nezaťažuje operačný systém počítača.
- Je také jednoduché, že na jeho používanie nepotrebujete expertné IT znalosti.

V ESETe sa nám darí takéto riešenia vyvíjať niekoľko desaťročí. Sme známi tým, že naše riešenia nezaťažujú systém, vyvolávajú extrémne nízky počet falošných poplachov a sú jednoducho použiteľné. Toto všetko potvrdzuje množstvo ocenení, ktoré naše produkty získali.

## Tajomstvo silnej detekcie

Aj útočníci však stále vylepšujú svoje nástroje a počet vírusov. V závislosti od dňa v ESETe odchytaťame 200- až 400-tisíc vzoriek škodlivého kódu, ktorý sme nikdy predtým nevideli.

Takéto množstvo útokov nedokážu analyzovať ani stovky našich výskumno-vývojových zamestnancov. Už od roku 1998 preto v našich produktoch používame Machine Learning, respektíve strojové učenie. Odvtedy sa mnohé zmenilo a vylepšeniami prešla aj táto technológia.

## Ochrana pred doteraz neznámymi hrozbami

Strojové učenie sa považuje za jednu z technológií, ktoré môžu byť kľúčové na dosiahnutie skutočnej umelej inteligencie. Technológie založené na strojovom učení sa stále častejšie využívajú v boji proti veľkým podvodom, pomáhajú vyhodnocovať a optimalizovať obchodné procesy, zlepšovať testovacie postupy a vyvíjať nové riešenia existujúcich problémov.

ESET svoje strojové učenie používa na rýchlejšiu a efektívnejšiu analýzu vzoriek škodlivého kódu. ESET využil roky vlastného výskumu a vývoja v tejto oblasti a neustále vylepšuje svoje mimoriadne silné detekčné jadro využívajúce pokročilé strojové učenie.

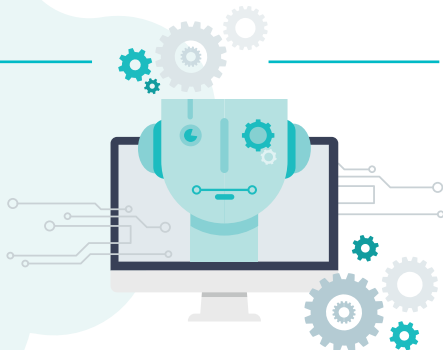
## Ako zvýšiť bezpečnosť svojho Windows počítača alebo laptopu

Používať spoľahlivé viacvrstvové bezpečnostné riešenie je pri ochrane zariadení len jednou časťou skladačky. Antivírus vás totiž niekedy neochráni pred vami samotnými, prípadne pred správaním ľudí, ktorým vaše zariadenie požičiate. Ak však budete dodržiavať tieto základné bezpečnostné pravidlá, výrazne znížite šance toho, že vám útočníci infikujú počítač:

- Pravidelne **aktualizujte všetky programy a aplikácie**, ktoré máte nainštalované. Aktualizácie obsahujú aj dôležité bezpečnostné záplaty. Ak už niektorý program vôbec nepoužívate, odinštalujte ho. Pri bežnej práci sa do Windowsu neprihlasujte pod admin účtom.
- Aktualizujte aj svoje bezpečnostné riešenie. Ak máte platnú licenciu na ESET, prechod na najnovšiu verziu je vždy bezplatný. Neignorujte upozornenia svojho bezpečnostného riešenia a nevypínajte jeho funkcie. Výnimočne sa stane, že útočníkom sa podarí infikovať aj legitímnu webstránku alebo program, ktorý si inštalujete.
- **Pravidelne zálohujte údaje**, ktoré máte v počítači uložené. Ak ich napadne útočník alebo dôjde k hardvérovej poruche, budete mať k dispozícii ich kópiu.
- Trikrát premýšľajte a raz klikajte. **Neotvárajte prílohy podozrivých e-mailov** a zbystrite pozornosť, ak sa vám niečo nepozdáva na sociálnych sieťach.
- Všade, kde sa to dá, si zapnite dvojfaktorovú autentifikáciu. Ide o dodatočné overenie prihlásenia, napríklad cez SMS. Ak aj niekto uhádne alebo ukradne vaše heslo, nedostane sa k vašim e-mailom alebo do vašich sociálnych sietí.
- Na každú stránku, ktorá požaduje prihlásenie, si **vytvorte unikátne heslo**. Prípadne používajte funkciu Password Manager v ESET Smart Security Premium.
- Rozmyslite si, komu budete posilať svoje heslá, osobné alebo finančné údaje. Žiadna seriózna inštitúcia od vás nebude žiadať heslá e-mailom. Niektorí útočníci sa však za ňu môžu vydávať.
- Ak sa stretnete s problémom a máte platnú licenciu na ESET riešenie, spojte sa s našou technickou podporou. Jej konzultácie sú súčasťou vašej licencie.

### bezpečne *na* nete.sk

Na Bezpečne na nete vás naučíme spoznať základné riziká digitálneho sveta a poskytneme vám praktické rady, ako sa pred nimi chrániť.



## S laptopom bezpečne aj na cestách

Pri cestovaní s laptopom by ste sa mali pripraviť na dve potenciálne hrozby. Prvou je nebezpečenstvo straty alebo krádeže zariadenia, v ktorom máte uložené rodinné fotky a množstvo údajov. Ak však používate ESET Internet Security alebo ESET Smart Security Premium, **nastavte si funkcionality Anti-Theft cez webstránku my.eset.com**. Cez tento web budete môcť svoje zariadenie označiť ako ukradnuté alebo stratené a sledovať tak jeho polohu. Funkcia vám môže zároveň posilať fotografie aktuálneho používateľa vášho laptopu.

Druhou hrozbou je všadeprítomná bezplatná Wi-Fi a jej lákanie. Môžete sa totiž omylom pripojiť k takej, ktorú vytvorili útočníci a poskytnúť im tak prehľad o svojich heslách a všetkom, čo na internete robíte. Pred pripojením na nezabezpečenú Wi-Fi sa preto v podniku alebo hoteli spýtajte, ako sa volá ich oficiálna Wi-Fi sieť. Nasledujte tiež upozornenia funkcionality Známe siete, ktorá vás vyzve na prepnutie do režimu zvýšenej ochrany. **Pre najvyššiu mieru zabezpečenia používajte na svojom laptopu VPN** – Virtual private network. Tá medzi vašim počítačom a webstránkami vytvára akoby zabezpečený tunel, ktorým budú tiecť vaše dáta.

*Chcete na cestách chrániť aj svoj Android mobil? Vyskúšajte bezpečnostnú aplikáciu ESET Mobile Security.*



## Online nakupovanie bez strachu

Obzvlášť pred Vianocami a počas výpredajových období nás webstránky bombardujú s ponukami výhodného nákupu online. Napriek neustálemu rastom online predaja sa niektorí ľudia stále boja kliknúť na tlačidlo kúpiť. Niet sa však čoho báť.

- Základom je **nakupovať v overených online obchodoch**. Ak vás zaujal tovar v neznámom e-shope, vyhľadajte si jeho recenzie a riaďte sa len tými negatívnymi. Pozitívne sa totiž dajú ľahko sfaľšovať. Preštudujte si tiež informácie o predajcovi.
- Nakupujte len **na bezpečnej Wi-Fi sieti a na chránenom počítači**.
- Osobné a platobné údaje zadávajte len do formulára, ktorý je na webstránke so SSL šifrovaním. Spoznáte ju tak, že jej adresa sa začína na HTTPS a nie len na HTTP.
- Pri podozrivom prevode peňazí z vášho účtu sa **ihneď spojte so svojou bankou**.

# Funkcie ESET bezpečnostných riešení pre počítače a laptopy

s operačným systémom Windows

## Antivírus a antispyware

Poskytuje proaktívnu ochranu pred digitálnymi hrozbami vrátane vírusov, rootkitov, červov a spyware, ktoré proaktívne odchyta a lieči. Týmto hrozbám sa hovorí malvér.

## Kontrola s podporou cloudu

Porovnáva správanie malvéru s naším cloudovým reputačným systémom ESET LiveGrid®, a tým pomáha proaktívne a rýchlo blokovať jeho neznáme formy.

## Ochrana proti skriptovým útokom

Zachytáva útoky vyvolané nebezpečnými skriptmi, ktoré sa snažia zneužiť Windows PowerShell. Zároveň chráni aj pred škodlivými JavaScriptmi, ktoré môžu útočiť cez prehliadač. Podporuje prehliadače Mozilla Firefox, Google Chrome, Microsoft Internet Explorer a Microsoft Edge.

## Host-based Intrusion Prevention System (HIPS)

Umožňuje podrobné nastavenie správania systému, čím umožňuje do detailov doladiť celkové zabezpečenie.



## Antispam

Chráni vašu e-mailovú schránku pred nevyžiadanými správami.

## Kontrola počas sťahovania súborov

Skracuje čas trvania kontroly tým, že niektoré typy súborov, napríklad archívy, kontroluje už počas sťahovania.

## Kontrola v nečinnosti

Vykonáva hĺbkové kontroly systému počas jeho nečinnosti. Pomáha detegovať neaktívne potenciálne hrozby predtým, než napáchajú škody.

## Anti-Phishing

Chráni vaše súkromie tak, že v internetovom prehliadači blokuje falošné webstránky, ktoré sa snažia získavať citlivé informácie ako prihlasovacie údaje, heslá alebo bankové údaje. Blokuje aj weby, ktoré podobnými znakmi vo svojej adrese napodobňujú legitímne stránky.

## Pokročilá kontrola pamäte

Odhaľuje sofistikovaný malvér, ktorý sa pred detekciou skrýva pod viacerými vrstvami šifrovania.

## Exploit Blocker

Blokuje útoky špeciálne navrhnuté tak, aby sa vyhli antivírusovej detekcii, a tiež chráni pred ransomvérom a útokmi, pri ktorých dochádza k uzamknutiu obrazovky. Okrem toho poskytuje ochranu pred útokmi mierenými na webové prehliadače, programy

na zobrazovanie PDF dokumentov a iné aplikácie vrátane softvéru založeného na Java.

## Ochrana pred botnetmi

Zabraňuje zneužitiu počítača na spamové aktivity a sieťové útoky. Vďaka sieťovým signatúram máte k dispozícii výhody nového typu detekcie pre ešte rýchlejšie blokovanie škodlivej komunikácie.

## Firewall

Zabraňuje neoprávnenému prístupu k počítaču a zneužitiu vašich osobných dát.

## Ochrana pred sieťovými útokmi

Spolu s firewallom automaticky chráni počítač pred škodlivou sieťovou aktivitou tým, že blokuje hrozby odhalené na základe nebezpečných prejavov na sieti.

## Kontrola WMI

Vyhľadáva odkazy na infikované súbory alebo malvér vložené ako dáta v službe Windows Management Instrumentation, súprave nástrojov na správu zariadení a aplikácií v prostredí Windows.

## Kontrola systémových registrov

Vyhľadáva odkazy na infikované súbory alebo malvér vložené ako dáta v hierarchickej databáze Registry systému Windows, ktorá uchováva nastavenia na nižšej úrovni pre operačný systém Microsoft Windows a aplikácie používajúce databázu Registry.

# Špeciálne funkcie, ktoré vám pomôžu užívať si bezpečnejšie technológie



## Ransomware Shield

Chrání pred ransomvérom, čo je druh škodlivého kódu, ktorý infikované zariadenie zablokuje alebo zašifruje a za odšifrovanie požaduje výkupné. Ide o veľmi nepríjemný škodlivý kód, pretože po úspešnej infekcii sa obeť reálne nevie dostať k rodinným fotografiám alebo k dôležitým dokumentom. Odborníci z ESETu zároveň neodporúčajú útočníkom za dešifrovanie platiť. Ani samotní tvorcovia ransomvéru totiž nevedia zaručiť, že sa dáta podarí dostať do pôvodného stavu. Aj napriek tomu sa však podvodníkom podarilo týmto spôsobom vylákať od ľudí miliardu eur.

## Kontrola UEFI

UEFI je štandard, teda súbor pravidiel, ktorými sa riadi firmvér – počítačový kód, ktorý sa spúšťa hneď po zapnutí počítača. Predchodcom UEFI bol BIOS. Kontrola UEFI chrání pred hrozbami, ktoré útočia na váš počítač ešte predtým, ako sa spustí jeho operačný systém Windows. ESET je prvý veľký výrobca bezpečnostných riešení, ktorého produkty majú takúto bezpečnostnú vrstvu určenú na detekciu škodlivých doplnkov vo firmvéri počítača.

## Známe siete

Ak sa pripájate do neznámej internetovej siete, program vás upozorní a vyzve na prepnutie do režimu zvýšenej ochrany. Ostatné počítače pripojené do tej istej siete vaše zariadenie neuvidia.

## Správa zariadení

Predchádza nepovolenému kopírovaniu vašich súkromných dát na neznáme

externé zariadenia. Poskytuje možnosť blokovať CD, DVD, USB a iné vymeniteľné médiá a úložné zariadenia. Umožňuje tiež zablokovať prístup zariadeniam, ktoré sa pripájajú cez Bluetooth, FireWire a sériový alebo paralelný port.

## Zariadenia v domácej sieti

Umožňuje otestovať váš domáci router a zariadenia k nemu pripojené na zraniteľnosť, akými sú napríklad slabé heslá alebo zastaraný firmvér, a zároveň ponúka možnosti nápravy prípadných problémov. Poskytuje tiež ľahko dostupný zoznam zariadení pripojených k vášmu routeru (smartfón, televízory a iné IoT zariadenia atď.), aby ste mali vždy prehľad o tom, kto je pripojený (názov zariadenia, IP adresa, MAC adresa atď.). Zistíte tak, či ste náhodou nezabudli zaheslovať domácu Wi-Fi a teraz vám dáta čerpajú iniciatívni susedia.

## Detekcia potenciálne nechcených aplikácií

Potenciálne nechcené a podozrivé aplikácie (PUA) sú programy, ktoré síce nemusia predstavovať bezpečnostné riziko, avšak môžu mať negatívny vplyv na výkon a spoľahlivosť operačného systému a môžu tiež odosielať informácie tretím stranám. Môže ísť napríklad o program sledujúci vaše internetové správanie pridružený k inému softvéru, ktorý ste si kúpili. Alebo o skript, ktorý po otvorení webstránky začne na vašom počítači ťažiť kryptomeny, čím môže spomaľovať vaše zariadenie. Nejde o hrozbu, ale o tomto správaní by ste mali vedieť a mali by ste mať možnosť ho blokovať. Táto funkcia vás na PUA

upozorní a vy sa následne môžete rozhodnúť, či chcete ich aktivitu povoliť alebo ju zablokujete.

## Ochrana webovej kamery

Monitoruje všetky procesy a aplikácie, ktoré sa snažia získať prístup k vašej webovej kamere a aktivovať ju. Na túto aktivitu vás aplikácia upozorní a vy môžete prístup ku kamere buď povoliť, alebo zablokovať. Predídete tak nechcenému sledovaniu, keďže táto funkcia je vo svete malvéru relatívne bežná.

## Ochrana online platieb so zabezpečeným internetovým prehliadačom

Zahŕňa špeciálny zabezpečený prehliadač, cez ktorý môžete bez obáv platiť online, ako aj možnosť predvolene spúšťať akýkoľvek podporovaný prehliadač v zabezpečenom režime (po nastavení). Predstavuje tak dodatočnú vrstvu ochrany, ktorej cieľom je chrániť pred zneužitím vaše online transakcie, kryptomenové peňaženky a finančné údaje, ako sú heslá alebo čísla platobných kariet. Funkcia zároveň chráni klávesnicu a myš pred keyloggerni. Sú to škodlivé programy, ktorých cieľom je odchyťovať vami stlačené klávesy tak, aby sa podvodníci dostali ku všetkým údajom, ktoré ste vyplnili do internetbankingu alebo do akýchkoľvek iných webstránok.

## Rodičovská kontrola

Ide o užitočnú funkciu, ak majú k počítaču prístup aj deti. Jej hlavnou úlohou je zamedziť im prístup na nebezpečné alebo nevhodné webové stránky. Blokovanie stránok je možné na základe preddefinovaných kategórií a veku dieťaťa. Na jej nastavenie je potrebné, aby malo každé dieťa samostatný používateľský Windows účet. Je dôležité chrániť nastavenia v produkte ESET heslom, inak môže šikovné dieťa nielen vypnúť blokovanie nevhodných stránok, ale aj stiahnuť do počítača niečo, čím by ohrozilo zabezpečenie celej rodiny.

*Chcete svoje deti chrániť pred nebezpečným obsahom aj na ich mobilných zariadeniach s OS Android?*

**Stiahnite im z Google Play aplikáciu ESET Parental Control, mesiac ju môžete testovať bezplatne.**



## Herný režim

Ak hráte vy alebo vaše deti na výkon náročnú hru, alebo sledujete video vo vysokom rozlíšení, potrebujete využiť maximum výkonu vášho počítača. Zároveň nechcete byť rušení žiadnymi vyskakovacími oknami, upgradmi či upozoreniami. Funkcia ich posunie na neskôr, hoci počítač je stále chránený. Viete ju zapnúť manuálne alebo nastaviť tak, aby sa automaticky zapla pri prepnutí zobrazenia na plnú obrazovku.

## Anti-Theft

Funkcia užitočná hlavne pre majiteľov laptopov. Ak je vaše zariadenie odcudzené alebo stratené, ESET Anti-Theft vám umožní sledovať, či zariadenie niekto používa. Na mape môžete sledovať, kde sa nachádza, a cez webkameru sa dozviete, kto ho práve používa. Tejto osobe môžete cez funkciu zaslať priamo správu a dohodnúť si s ňou vrátenie zariadenia alebo zozbierané údaje odovzdáte polícii. Plnohodnotnému použitiu predchádza vytvorenie konta na portáli my.eset.com, prostredníctvom ktorého budete môcť označiť zmiznuté zariadenie ako stratené, čím sa aktivuje jeho automatické sledovanie.

## Secure Data

Nástroj umožňuje šifrovať dáta na vašom počítači a pripojených vymeniteľných médiách, napríklad USB kľúčoch. Predídete tak tomu, že sa vaše fotky alebo dokumenty pri strate USB kľúča dostanú do nesprávnych rúk.

## Password Manager

Nástroj slúži ako správca hesiel, ktorý chráni a uchováva vaše heslá a osobné údaje. Ak si neviete vytvoriť silné heslá, generátor tohto nástroja ich vytvorí za vás. Pamätať si tak budete musieť už len jedno jediné heslo – to, ktoré budete používať na prihlásenie sa do Password Managera. Cez nástroj sa tiež môžete odhlásiť z každej webovej stránky a vzdialene zabezpečiť svoju históriu prehľadávania. Nástroj vás taktiež upozorní v prípade, že došlo k ohrozeniu vašich prihlasovacích údajov. Password Manager môžete pohodlne používať aj na svojich Mac, iOS a Android zariadeniach. V systéme iOS je integrovaná detekcia tváre a je tiež možná integrácia viacfaktorovej autentifikácie s aplikáciou Google Authenticator pre ešte lepšíu ochranu vašich hesiel.

### Ako si vytvoriť silné heslo?

*Vymyslite si konkrétne spojenie viacerých slov, číslíc a znakov, ktoré má pre vás význam. Nepoužívajte však slávne citáty alebo frázy. Útočníci ich totiž majú vo svojej databáze a takzvaným slovníkovým útokom by heslo uhádli.*



# Vyberte si produkt podľa svojich potrieb

ESET ponúka vo svojich riešeniach viaceré vrstvy ochrany, od účinného a rýchleho antivírusu a internetovej ochrany až po všestranne prémiové bezpečnostné riešenie.



## ESET NOD32 Antivirus

Predstavuje základnú bezpečnostnú ochranu.



## ESET Internet Security

Komplexný bezpečnostný softvér s mnohými vrstvami zabezpečenia. Ak zlyhá jedna, zastúpi ju ďalšie.



## ESET Smart Security Premium

Prémiové riešenie pre náročných používateľov, obsahuje navyše šifrovanie a Password Manager.



## ESET Family Security Pack

Vyberte si bezpečnostné produkty podľa svojich potrieb a ochráňte až 4 rôzne zariadenia.



### Počítače:

Windows:

- ESET Internet Security
- ESET NOD32 Antivirus

Mac:

- ESET Cyber Security Pro
- ESET Cyber Security



### Smartfóny a tablety so systémom Android:

- ESET Mobile Security pre Android
- ESET Parental Control pre Android

### Android TV:

- ESET Smart TV Security

Chráňte svoje deti v online svete. Aplikácia **ESET Parental Control pre Android** je súčasťou balíka ESET Family Security Pack. Umožňuje inštaláciu na viacerých zariadeniach detí, vďaka čomu doprajete svojim deťom možnosť bezpečne spoznávať online svet.

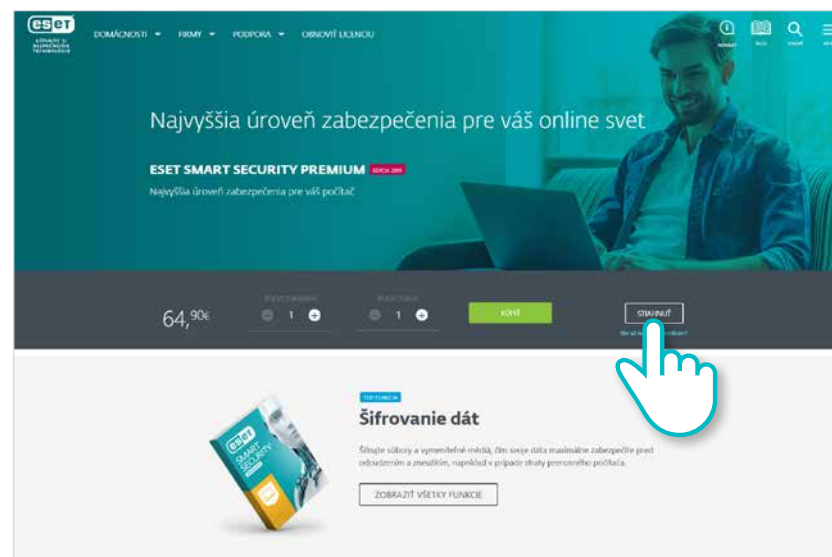
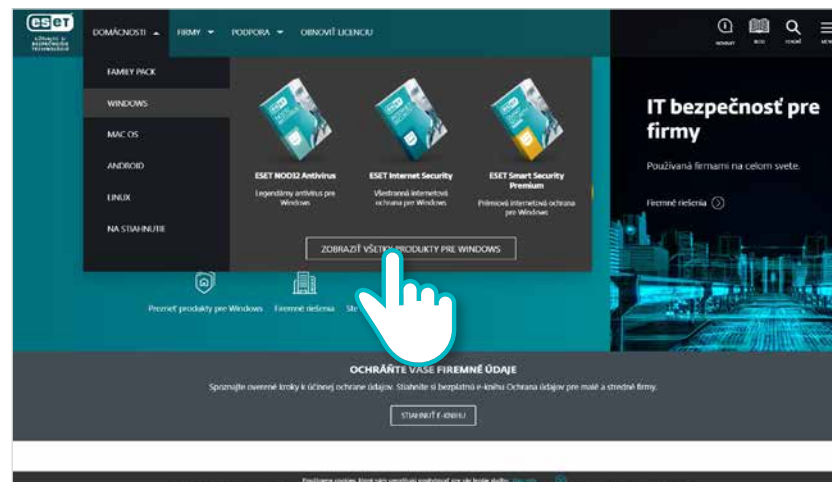
	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Multiplatformová ochrana*	•	•	•
Antivírus a antispypware	•	•	•
Kontrola s podporou cloudu	•	•	•
Pokročilé strojové učenie	•	•	•
Ochrana proti skriptovým útokom	•	•	•
HIPS	•	•	•
Kontrola počas sťahovania súborov	•	•	•
Kontrola v nečinnosti	•	•	•
Anti-Phishing	•	•	•
Exploit Blocker	•	•	•
Pokročilá kontrola pamäte	•	•	•
Ransomware Shield	•	•	•
Kontrola UEFI	•	•	•
Kontrola WMI	•	•	•
Kontrola systémových registrov	•	•	•
Správa zariadení	•	•	•
Detekcia potenciálne nechcených aplikácií	•	•	•
Herný režim	•	•	•
Antispam		•	•
Ochrana pred botnetmi		•	•
Firewall		•	•
Ochrana pred sieťovými útokmi		•	•
Známe siete		•	•
Zariadenia v domácej sieti		•	•
Ochrana webovej kamery		•	•
Ochrana online platieb		•	•
Rodičovská kontrola		•	•
Anti-Theft		•	•
Secure Data			•
Password Manager			•

\* Licenciu ESET NOD32 Antivirus je možné preniesť na operačný systém Mac. Licencie ESET Internet Security a ESET Smart Security Premium na operačný systém Mac a Android. Funkcionalita na týchto operačných systémoch je odlišná.

# Ako získať jeden z ESET produktov pre Windows zariadenia



ESET NOD32 Antivirus, ESET Internet Security alebo ESET Smart Security Premium môžete získať jednoducho online. Kliknite na [www.eset.sk](http://www.eset.sk). V hornom menu v záložke domácnosti pod položkou WINDOWS si vyberiete produkt, ktorý chcete kúpiť alebo ste ho už zakúpili a chcete si ho stiahnuť a nainštalovať.





## Inštalácia produktu

Inštalácia produktu je veľmi jednoduchá a intuitívna, stačí sa riadiť inštrukciami, ktoré vás inštaláciou prevedú v jednotlivých krokoch:

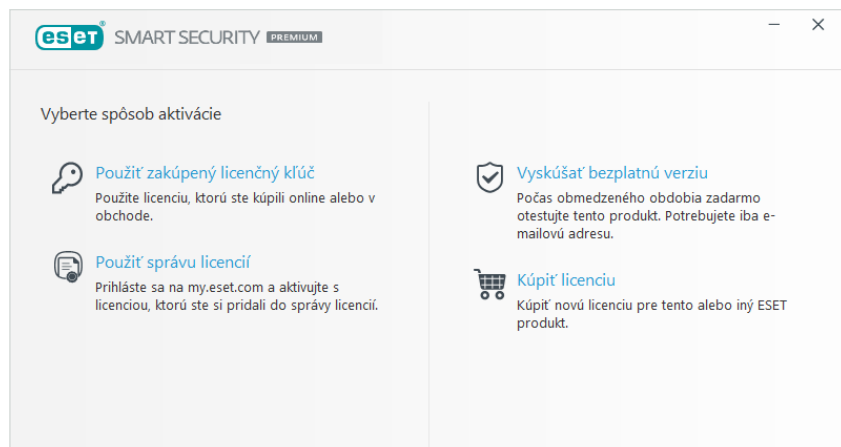
- 1** Po spustení stiahnutého inštaláčného súboru a povolení vykonania zmien v počítači (vyžaduje operačný systém Windows) vás sprievodca inštaláciou vyzve zvoliť si jazyk, v ktorom chcete so softvérom komunikovať.
- 2** Pre ďalšie pokračovanie je potrebné udeliť súhlas s licenčnými pravidlami.
- 3** V ďalšom kroku si zvolíte spôsob aktivácie produktu:

**Použiť zakúpený licenčný kľúč** – Kliknete v prípade ak už máte licenčný kľúč. Ak ste si túto príručku našli v zakúpenom produkte, súčasťou balenia je aj kartička s licenčným kľúčom.

**Použiť správu licencií** – Kliknete v prípade, že máte vytvorené konto na my.eset.com. Vytvorenie konta sa odporúča nielen z dôvodu jednoduchého spravovania vašich licencií, ale aj z dôvodu plnohodnotného používania niektorých funkcií, napríklad Anti-Theft.

**Vyskúšať bezplatnú verziu** – V prípade, že nemáte licenčný kľúč a ESET produkt chcete vyskúšať zadarmo po dobu 30 dní, kliknite na túto možnosť.

**Kúpiť licenčný kľúč** – Ak ešte nemáte zakúpený produkt, nemáte licenčný kľúč, môžete si ho zakúpiť kliknutím na túto možnosť.



- 4** Súčasťou inštalácie sú aj dve nastavenia, ktorým by ste mali venovať pozornosť:

**Zapnúť ESET LiveGrid systém spätnej väzby (odporúča sa)** – táto unikátna funkcia je jednou z najúčinnějších foriem ochrany proti stále sa meniacim a novovzniknutým hrozbám, napríklad aj proti ransomvéru – škodlivému kódu, ktorý dokáže zašifrovať dáta vo vašom počítači a následne od vás požadovať výkupné. Technológia ESET LiveGrid je cloudový systém ochrany, ktorý zbiera a porovnáva informácie o hrozbách od používateľov z celého sveta a zároveň sleduje správanie potenciálne škodlivého kódu, vďaka čomu dokáže rýchlo, efektívne a automaticky detegovať a blokovať aj ten najmodernejší malvér.

**Zapnúť detekciu potenciálne nechcených aplikácií** – nechajte sa upozorniť na to, ak sa niekto pokúša zneužiť váš počítač napríklad na ťažbu kryptomien. Táto funkcia vás rovnako upozorní aj na aplikáciu či softvér, ktorý sa vám nenápadne na pozadí sťahuje spolu s aplikáciou, ktorú si stiahnuť naozaj chcete.

Poznámka: Nech sa pri inštalácii rozhodnete akokoľvek, obe z týchto užitočných funkcií si budete môcť zapnúť aj dodatočne.

- 5** Prebehne samotná inštalácia.

Po inštalácii venujte pozornosť upozorneniam. Je možné, že vás produkt bude chcieť varovať pred niektorými aktivitami.

### ESET produkt vyžaduje vašu pozornosť:



Chce vás informovať alebo upozorniť na nové zistenia, ktoré bezprostredne neohrozujú bezpečnosť vášho počítača.



Červený výkričník znamená, že váš počítač je vystavený možnému riziku a mali by ste výstrahe čo najskôr venovať pozornosť.



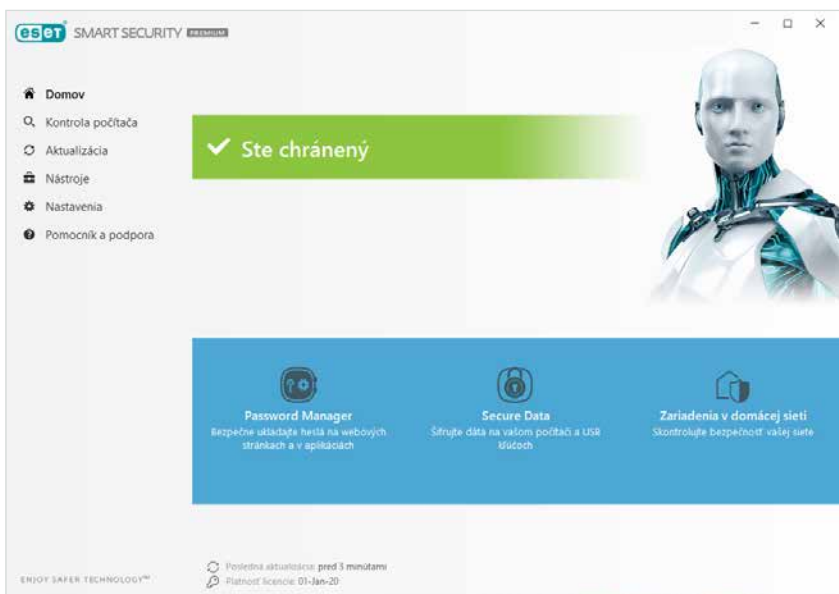
Zelené označenie znamená, že všetko vo vašom počítači je v poriadku a váš počítač je chránený.

## Nastavenia a sprievodca funkciami ESET produktu po inštalácii

Meniť a prispôbovať nastavenia ESET produktu môžete kedykoľvek, stačí kliknúť na ikonu produktu a zobrazí sa vám prehľadné menu.

**Domov** – Po otvorení tejto záložky uvidíte, v akom stave sa nachádza váš počítač, prípadne vás upozorní na nedostupnosť niektorej z dôležitých funkcií, napríklad LiveGrid.

Porovnanie funkcií jednotlivých produktov pre domácnosti nájdete na strane 13.



**Skontrolovať váš počítač** – Skontrolujete váš počítač na prítomnosť malvéru.

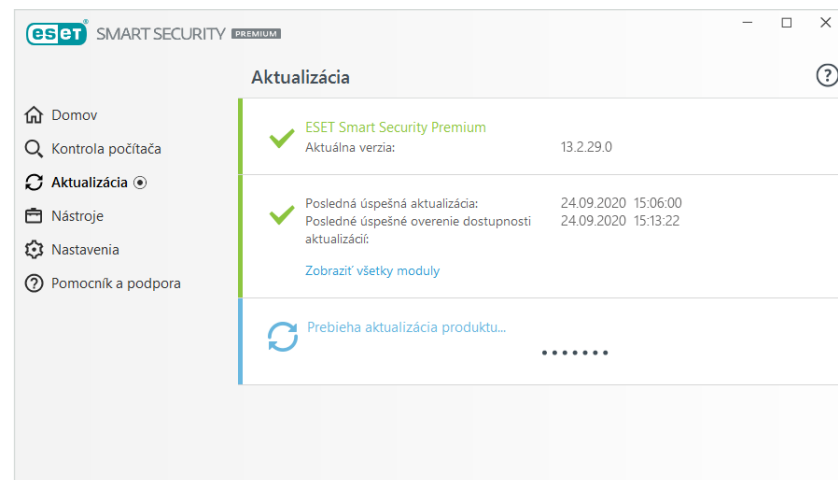
**Ochrana online platieb** – Otvorí sa špeciálny prehliadač, ktorý chráni vaše osobné údaje a iné dáta počas surfovania, online nakupovania alebo používania internet bankingu.

**Zariadenia v domácej sieti** – Skontroluje router a všetky zariadenia pripojené na domácu sieť a ponúkne tipy, ako zvýšiť ich zabezpečenie.

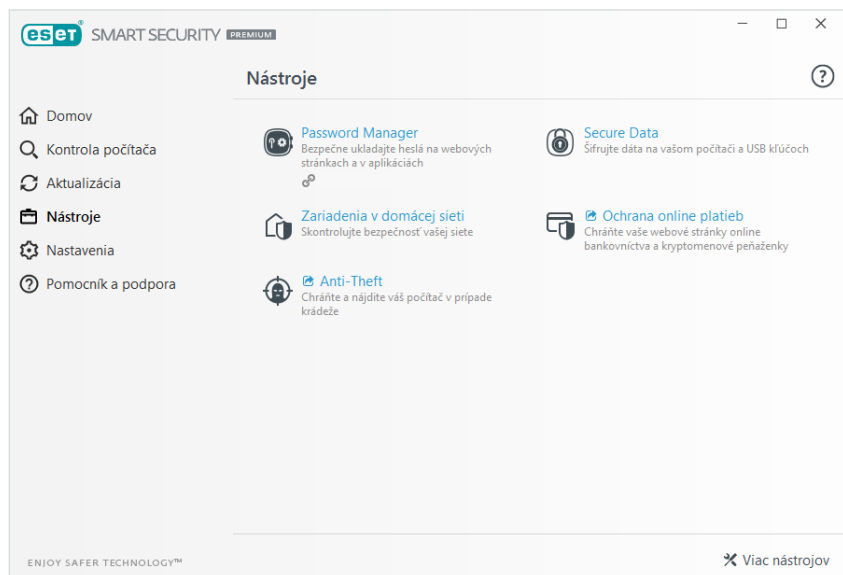
**Kontrola počítača** – Umožní okamžite skontrolovať váš počítač. V pokročilej kontrole môžete určiť vlastné ciele kontroly, prípadne skontrolovať vymeniteľné médiá ako napríklad USB alebo DVD a CD.



**Aktualizácia** – Prebieha automaticky, avšak kliknutím na túto záložku si môžete skontrolovať, či máte vždy najnovšiu verziu produktu. Pre úspešnú aktualizáciu je potrebné, aby bol počítač pripojený na internet. Ak ste offline, nie je možné aktualizovať niektoré moduly, na čo vás produkt upozorní. Zároveň ich aktualizuje ihneď po pripojení počítača na internet.



**Nástroje** – Zobrazí užitočné funkcie a aplikácie obsiahnuté v produkte ESET Internet Security alebo ESET Smart Security Premium.



**Password Manager** – Prémiová funkcia, pomocou ktorej si môžete vytvárať a spravovať heslá. Tie sa vám do príslušných prihlasovacích okien predvyplnia automaticky, ak to budete chcieť.

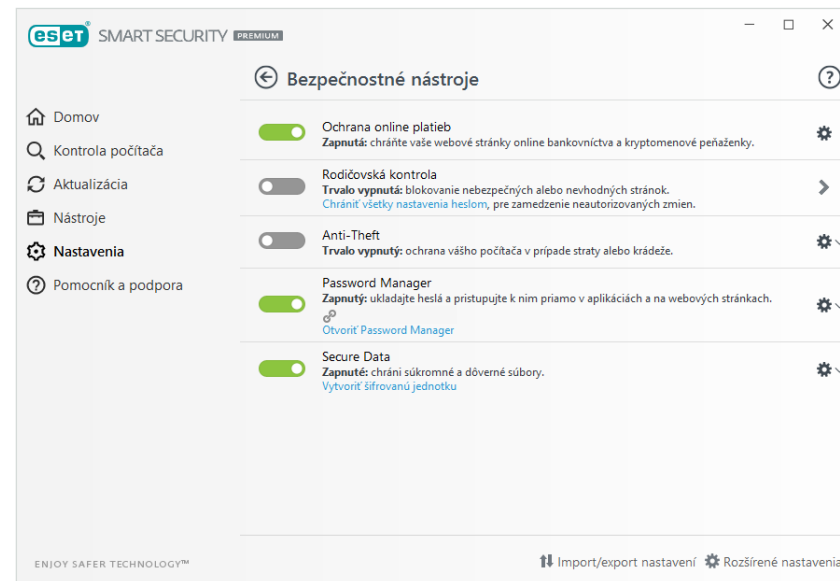
**Secure Data** – Umožňuje šifrovať dáta vo vašom počítači vytvorením virtuálnej jednotky – špeciálneho priečinka, v ktorom sa zašifrujú všetky súbory, ktoré doň vložíte. Zároveň umožňuje šifrovanie dát na vymeniteľnej jednotke (USB, DVD, CD...).

**Ochrana domácej siete** – Tu opäť nájdete funkciu, ktorá skontroluje všetky zariadenia pripojené na domácu sieť a ponúkne tipy, ako zvýšiť ich zabezpečenie.

**Ochrana online platieb** – Cez tento nástroj sa dostanete k špeciálnemu prehliadaču, ktorý šifruje komunikáciu medzi vaším počítačom a týmto prehliadačom. Vy tak môžete bezpečne zadávať citlivé prihlasovacie údaje napríklad do internetbankingu. Nie je potrebné toto okno otvárať manuálne, po kliknutí na tlačidlo „Internet banking“ vo vašom prehliadači sa otvorí automaticky.

**Anti-Theft** – Dôležitou súčasťou ochrany počítača a dát v ňom je možnosť sledovania zariadenia v prípade straty alebo krádeže. Preto odporúčame vytvoriť si konto na portáli my.eset.com.

**Nastavenia** – umožňujú nastaviť si, zapnúť alebo vypnúť jednotlivé funkcie obsiahnuté v tejto brožúrke.



Na **my.eset.com** budete môcť pridávať vaše zariadenia a v prípade straty alebo krádeže ich označiť ako „ukradnuté“. Hneď ako ktokolvek vaše zariadenie pripojí na internet, budete ho môcť lokalizovať, aktivovať na diaľku webovú kameru, odfoťiť osobu sediacu za vaším počítačom a poslať jej správu.

Okrem funkcie Anti-Theft má konto na portáli my.eset.com ešte ďalšie užitočné využitie. Práve prostredníctvom neho budete mať prehľad o všetkých zariadeniach, na ktorých používate svoju ESET licenciu. Tú môžete cez portál aj spravovať.

**Ochrana počítača** – Umožňuje nastavenie **Rezidentnej ochrany súborového systému**, ktorá permanentne kontroluje súbory, okamžite deteguje a lieči malvér vo vašom počítači. V záložke **Správa zariadení** si môžete nastaviť, určiť pravidlá a definovať skupiny pre povolenie alebo zakázanie prístupu k vymeniteľným médiám (CD, USB...). Funkcia **HIPS – Host Intrusion Prevention System** kontroluje činnosť aplikácií a procesov a zároveň zabráňuje ich nežiaducemu správaniu. Zapnutý **Herný režim** optimalizuje výkon pre hry, sledovanie filmov, videí alebo čohokoľvek zobrazeného na celú obrazovku. Automaticky deaktivuje vyskakovacie okná, naplánované úlohy, ktoré môžu ovplyvniť výkon počítača. **Ochrana webovej kamery** chráni vašu webovú kameru pred zneužitím a pokusmi o špehovanie.

**Ochrana internetu – Ochrana prístupu na web** – Deteguje a blokuje webové stránky, ktoré obsahujú škodlivý obsah (zapnutá funkcia chráni napríklad aj pred zneužitím vášho počítača na ťažbu kryptomien). **Ochrana poštových klientov** – kontroluje bezpečnosť odoslaných a prijatých e-mailov cez e-mailových klientov. Zapnutá **Antispamová ochrana** – deteguje a odstraňuje nevyžiadané e-maily. **Anti-Phishing ochrana** – deteguje a blokuje podvodné webové stránky, ktoré sa môžu pokúšať o krádež vašich prihlasovacích údajov napríklad aj do internetbankingu.

**Ochrana siete** – filtrovaná sieťová komunikácia **Firewall**, detekcia a **Ochrana pred sieťovými útokmi** a **Ochrana pred botnetmi** sú súčasťou ochrany siete, ku ktorej je pripojený váš počítač. V tejto sekcii viete zároveň zistiť, k akej sieti ste aktuálne pripojený a aké IP adresy sú aktuálne zablokované.

**Bezpečnostné nástroje** – Umožňujú nastavenia funkcií **Ochrana online platieb**, **Rodičovská kontrola** a **Anti-Theft**, ktorých úlohy sú špecifikované v úvode tejto brožúrky v opise jednotlivých funkcií.

**Pomocník a kontrola** – V tejto sekcii nájdete rýchlu pomoc a odpovede na časté otázky, ale získate aj informácie o aktuálnych i starších hrozbách. Nenašli ste odpovede na vaše otázky a ste naším zákazníkom? V prípade problémov s produktom alebo v otázkach bezpečnosti sa môžete obrátiť na technickú podporu.

*Kompletného online pomocníka k vášmu ESET produktu nájdete na produktových stránkach na [www.eset.sk](http://www.eset.sk)*



## Najviac oceňovaná antivírusová technológia

ESET technológia ako jediná na svete získala viac ako 100 prestížnych ocenení VB100 od renomovanej organizácie Virus Bulletin.

---

**Vyššie 30**

rokov technológiíe NOD32

**Vyššie 110 miliónov**

chránených používateľov  
na celom svete

**Vyššie 100**

prestížnych ocenení VB100

---

**ESET, spol. s r. o.**

Einsteinova 24, 851 01 Bratislava

Slovenská republika

[www.eset.sk](http://www.eset.sk)



Prídajte sa k nám na Facebooku.

<http://fb.eset.sk>

**Systemové požiadavky** • ESET Internet Security a ESET NOD32 Antivirus sú kompatibilné so systémom Microsoft Windows® 10, 8.1, 8, 7 s nainštalovaným balíkom SPI a najnovšími aktualizáciami KB; ESET Cyber Security a ESET Cyber Security Pro sú kompatibilné so systémom Mac OS 10.12 a novšími verziami; ESET Mobile Security a ESET Parental Control sú kompatibilné so systémom Android 4.1 a novšími verziami. Vyžaduje sa pripojenie na internet. ESET Smart TV Security je kompatibilný so systémom Android 7 a novšími verziami. Kompatibilitu s najnovšími verziami mobilných operačných systémov si overte na stránke [www.eset.sk](http://www.eset.sk).

Copyright © 1992 – 2021 ESET, spol. s r. o. ESET, ESET logo, postava ESET androida, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo alebo iné tu uvedené produkty spoločnosti ESET sú registrovanými ochrannými známkami spoločnosti ESET, spol. s r. o. Mac a Mac logo sú ochranné známky spoločnosti Apple Inc., registrované v USA a iných krajinách. Ostatné názvy tu uvedených spoločností alebo produktov môžu byť registrovanými ochrannými známkami ich príslušných vlastníkov. Vyrobené v súlade so štandardom ISO 9001:2008.