



PREHLAD

# VULNERABILITY & PATCH MANAGEMENT

Aktívne sledovanie a oprava  
zraniteľností vo všetkých koncových  
zariadeniach

Progress. Protected.

# Čo je nástroj ESET Vulnerability and Patch Management?

Nástroj ESET Vulnerability and Patch Management aktívne sleduje zraniteľnosti v operačných systémoch a bežných aplikáciách a umožňuje automatizované opravy na všetkých koncových zariadeniach spravovaných prostredníctvom našej jednotnej platformy.

Zautomatizujte kontroly softvéru na koncových zariadeniach a aplikáciách tretích strán s výhodou okamžitého prehľadu o zraniteľnostiach a ich nahlasovania do konzoly. Ak chcete zabezpečiť nepretržitú ochranu svojej firmy, môžete nakonfigurovať automatické nasadenie bezpečnostných záplat, a to tak, že si vyberiete stratégiu (všetky záplaty, len povolené alebo všetky okrem vylúčených) a nastavíte konkrétne časové intervaly, keď sa má záplata nasaďiť.



# Včasné nasadenie záplat pre operačné systémy a aplikácie

Oprava bezpečnostných dier v operačných systémoch a aplikáciách je veľmi dôležitá, ale zároveň patrí medzi časovo najnáročnejšie úlohy v oblasti IT. Nástroj ESET Vulnerability and Patch Management poskytuje ďalšiu úroveň ochrany organizáciám, ktoré potrebujú, aby boli ich aplikácie aktuálne, ale chýbajú im potrebné IT zdroje. Zisťuje zraniteľnosti a eliminuje alebo zmierňuje ich zneužitie inštaláciou najnovších záplat pre aplikácie a operačné systémy na všetkých koncových zariadeniach.

Nástroj ESET Vulnerability and Patch Management využíva pokročilé techniky prioritizácie a nástroje

na automatizáciu práce, ktoré najlepšie pokrývajú potreby vašej infraštruktúry.

Je súčasťou platformy ESET PROTECT, a preto zaisťuje nielen priebežné vyhodnocovanie zraniteľností s prioritizáciou a nápravou na základe ich závažnosti, ale poskytuje tiež ochranu pred hrozbami, ktoré ďaleko presahujú rámec zraniteľností softvéru. Na firemnej úrovni vás chráni pred všetkými typmi malvéru vrátane ransomvéru a poskytuje prevenciu zero-day hrozieb na všetkých koncových zariadeniach, serveroch a e-mailoch prostredníctvom jednotného a univerzálneho riešenia na správu.

## Hlavné funkcie

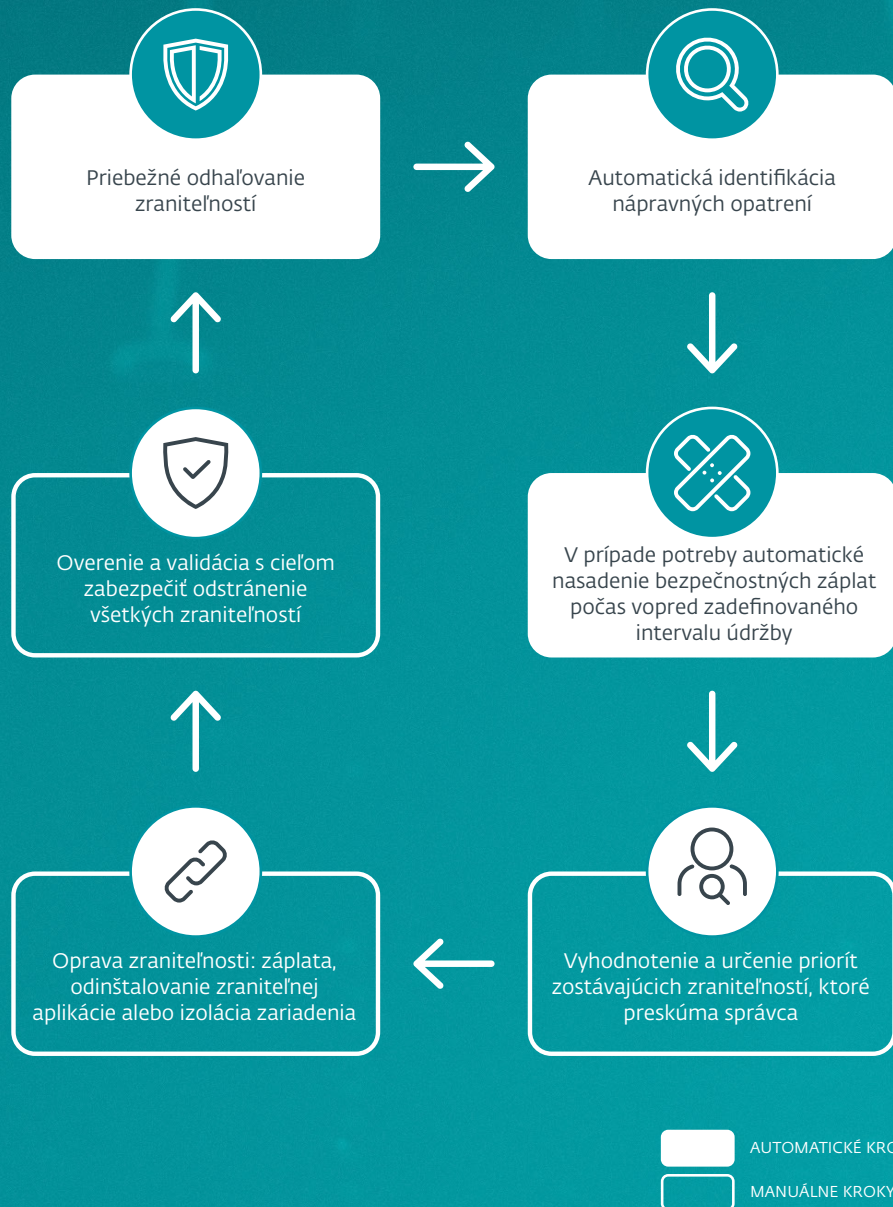
### Vyhodnotenie zraniteľností

- Kontroluje tisíce aplikácií, napríklad Adobe Acrobat, Mozilla Firefox a Zoom Client, a podporuje viacero verzií systému Windows (a čoskoro aj macOS)
- Deteguje cez 35 000 bežných zraniteľností a rizík (CVE) a tento počet neustále narastá
- Poskytuje automatizované kontroly podľa vlastného harmonogramu na základe prispôsobiteľných pravidiel
- Uprednostňuje a filtruje zraniteľnosti podľa ukazovateľa vystavenia rizikám a závažnosti
- Prináša správy o zraniteľnostiach najzraniteľnejšieho softvéru a zariadení
- Podporuje multitenantnosť v komplexných sieťových prostrediach; umožňuje prehľad zraniteľností v konkrétnych častiach organizácie
- Databáza zraniteľností, CVSS 2.0 a CVSS 3.1
- Konzola ESET PROTECT Cloud zaisťuje jednotný prehľad s podporou viacerých jazykov a nízkymi nárokmi na vašu IT infraštruktúru

### Správa záplat

- Spustíte okamžité aktualizácie a nasadenie záplat prostredníctvom prispôsobiteľných možností alebo manuálne
- Zjednodušte proces nasadzovania záplat: uprednostnite kritické aktíva a zvýšené opravy naplánujte na čas mimo špičky, aby ste sa vyhli prerušeniam
- Registrujte a sledujte výnimky pre záplaty vybraných aplikácií
- Poskytuje aktualizovaný inventár záplat s názvom záplaty, novou verziou aplikácie, údajmi o CVE, úrovňou závažnosti/dôležitosti záplaty, ovplyvnenými aplikáciami
- Všetky záplaty sú dostupné prostredníctvom konzoly ESET PROTECT Cloud

# Ako to funguje?



# Príklady použitia

Hoci rastúci počet zamestnancov pracujúcich z domu a čoraz častejšie využívanie cloudových služieb signalizuje, že kybernetické hrozby sa rozšírili aj nad rámec zraniteľností softvéru, včasné nasadenie bezpečnostných záplat pre aplikácie a operačné systémy zostáva aj naďalej kľúčové na predchádzanie narušeniam bezpečnosti.

Každý správca vám potvrdí, že oprava zraniteľností je jednou z časovo najnáročnejších úloh v oblasti IT. Keď sú IT zdroje preťažené, nasadzovanie záplat sa odsúva na druhú koľaj a zraniteľnosti sa tak môžu takmer nepozorovane vyvíjať. Čoraz zložitejšia IT infraštruktúra môže zapríčiniť aj horšiu koordináciu medzifunkčných tímov, nedostatočný inventár a obmedzený prehľad o hrozbách.

## Sme pozadu s nasadzovaním záplat

### PROBLÉM

Náš IT tím je preťažený, a preto nestíha nasadzovať bezpečnostné záplaty.

### RIEŠENIE

Využite pokročilé techniky určovania priorit a automatizácie.

- ✓ Nastavte optimálnu frekvenciu kontrol a zosynchronizujte ich s nastaveniami nasadzovania záplat s cieľom riešiť relevantné a zneužiteľné zraniteľnosti bez preťažovania svojich IT tímov.
- ✓ Filtrujte zraniteľnosti na základe ich závažnosti; uprednostnite zraniteľnosti, ktoré predstavujú významné obchodné riziká.
- ✓ Prispôbte si politiky zásad. Uprednostňujte kritické aktíva manuálnou opravou závažných zraniteľností a zautomatizujte nasadzovanie záplat pre ostatné aktíva mimo špičku s cieľom vyhnúť sa prerušeniam.
- ✓ Registrujte a sledujte výnimky pre záplaty; vyhnite sa nutnosti sledovať každú jednu záplatu.

## Nedostatok IT zdrojov

### PROBLÉM

Potrebujem, aby boli naše aplikácie aktuálne, ale chýbajú nám potrebné IT zdroje.

### RIEŠENIE

Využite výhody plne automatizovaného vyhodnocovania zraniteľností a správy záplat, ako aj podporu ESET:

- ✓ Zautomatizujte kontroly softvéru na koncových zariadeniach a aplikácií tretích strán s výhodou okamžitého prehľadu o zraniteľnostiach a ich nahlasovania do konzoly.
- ✓ Ak chcete zabezpečiť nepretržitú ochranu svojej organizácie, môžete nakonfigurovať automatické nasadenie bezpečnostných záplat, a to tak, že si vyberiete stratégiu (všetky záplaty, len povolené alebo všetky okrem vylúčených) a nastavíte konkrétne časové intervaly, keď sa má záplata nasadiť.

# Rastúca zložitosť, koordináčn é výzvy

## PROBLÉM

Zložitosť našich IT systémov narastá, čo sťažuje koordináciu medzifunkčných tímov.

## RIEŠENIE

Využite výhody našej platformy ESET PROTECT, cez ktorú môžete používať správu zraniteľností a záplat ESET a spravovať širšie potreby zabezpečenia všetkých vašich digitálnych aktív a inventára.

- ✓ Centralizujte a automatizujte viaceré úlohy súvisiace s IT bezpečnosťou a správou pomocou platformy ESET PROTECT, ktorá zahŕňa správu zraniteľností a záplat ESET.\* Zjednodušte si vlastnú IT správu.
- ✓ Využite multitenantnosť správy zraniteľností a záplat ESET: môžete mať úplný prehľad o celej sieti, ale zároveň sa zamerať iba na vyhradenú oblasť.
- ✓ Udržujte si aktuálny inventár a odstráňte všetky prípadné slepé miesta v infraštruktúre.
- ✓ Využite výhody stratégií prevencie, detekcie a reakcie platformy ESET PROTECT a minimalizujte svoje vystavenie hrozbám, ktoré presahujú rámec zraniteľností softvéru.
- ✓ Nástroj ESET Vulnerability and Patch Management zjednodušuje dodržiavanie nariadení GDPR, HIPAA, PCI DSS a ďalších požiadaviek na bezpečnosť údajov od vládnych a regulačných orgánov, ako aj orgánov odvetvia.

# Obmedzený prehľad o IT zabezpečení

## PROBLÉM

Nemám úplný prehľad o svojom IT zabezpečení.

## RIEŠENIE

Využite výhody jednotného prehľadu, ktorý poskytuje konzola ESET PROTECT Cloud.

- ✓ Získajte komplexný a aktuálny prehľad o koncových zariadeniach, licenciách a stavoch zraniteľností a opráv naprieč celým inventárom aktív.
- ✓ Prezrite si stav svojho zabezpečenia v reálnom čase prostredníctvom konzoly ESET PROTECT Cloud.
- ✓ Pripojte sa kedykoľvek a kdekoľvek zo svojho obľúbeného webového prehliadača a v prípade potreby okamžite zareagujte.
- ✓ Vytvárajte relevantné reporty na meranie účinnosti a progresu politik správy zraniteľností a záplat.

\* K dispozícii len v rámci úrovni riešenia ESET PROTECT Complete a ESET PROTECT Elite.

### NÁKUP:

Nástroj ESET Vulnerability and Patch Management je k dispozícii v rámci týchto úrovní riešenia:

 PROTECT COMPLETE

 PROTECT ELITE

# O spoločnosti ESET

## Firemná digitálna bezpečnosť novej generácie

### NARUŠENIAM BEZPEČNOSTI NIELEN ZABRAŇUJEME, ALE IM AJ PREDCHÁDZAME

Na rozdiel od bežných riešení, ktoré sa zameriavajú na reakciu na hrozby po ich spustení, ESET ponúka bezkonkurenčné produkty zamerané na prevenciu s využitím umelej inteligencie, ktoré sú podporené odbornými znalosťami, renomovanými informáciami o hrozbách v globálnom meradle a rozsiahlou sieťou výskumu a vývoja vedenou uznávanými výskumníkmi – to všetko pre neustálu inováciu našej viacvrstvovej bezpečnostnej technológie.

Vyskúšajte si bezkonkurenčnú ochranu pred ransomvérom, phishingom, zero-day hrozbami a cieľenými útokmi s našou oceňovanou cloudovou platformou kybernetickej bezpečnosti s podporou XDR, ktorá kombinuje schopnosti prevencie, detekcie a proaktívneho vyhľadávania hrozieb novej generácie. Naše vysoko prispôsobiteľné riešenia zahŕňajú hyperlokálnu podporu. Majú minimálny vplyv na výkon koncových zariadení, identifikujú a neutralizujú vznikajúce hrozby skôr, ako k nim dôjde, zabezpečujú plynulý chod prevádzky a znižujú náklady na implementáciu a správu.

Vo svete, kde technológie pomáhajú meniť svet k lepšiemu, ochráňte svoju firmu s riešeniami ESET.

### ESET V ČÍSLACH

**1 mld.+**

chránených  
používateľov internetu

**400-tisíc+**

firemných  
zákazníkov

**200**

krajín  
a teritórií

**13**

globálnych centier  
výskumu a vývoja

### NIEKTORÍ Z NAŠICH ZÁKAZNÍKOV



Viac než 9 000 koncových zariadení chránených spoločnosťou ESET od roku 2017



Viac než 4 000 e-mailových schránok chránených spoločnosťou ESET od roku 2016



Viac než 32 000 koncových zariadení chránených spoločnosťou ESET od roku 2016



Bezpečnostný partner v oblasti poskytovania internetových služieb 2 miliónom zákazníkov od roku 2008

### UZNANIE



V júli 2023 získal ESET v teste Business Security spoločnosti AV-Comparatives ocenenie Business Security APPROVED (overený bezpečnostný produkt pre firmy).



Spoločnosť ESET neustále dosahuje najvyššie hodnotenia od používateľov na globálnej platforme G2 a jej riešenia oceňujú zákazníci po celom svete.



ESET už štvrtý rok po sebe získal titul Top hráča v hodnotení Advanced Persistent Threat Market Quadrant spoločnosti Radicati za rok 2023.