PREHĽAD

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 aplikácií 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 nasadiť.

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 priorizácie a nástroje na automatizáciu práce, ktoré najlepšie pokryjú potreby vašej infraštruktúry.

Je súčasťou platformy ESET PROTECT, a preto zaisťuje nielen priebežné vyhodnocovanie zraniteľností s priorizáciou 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

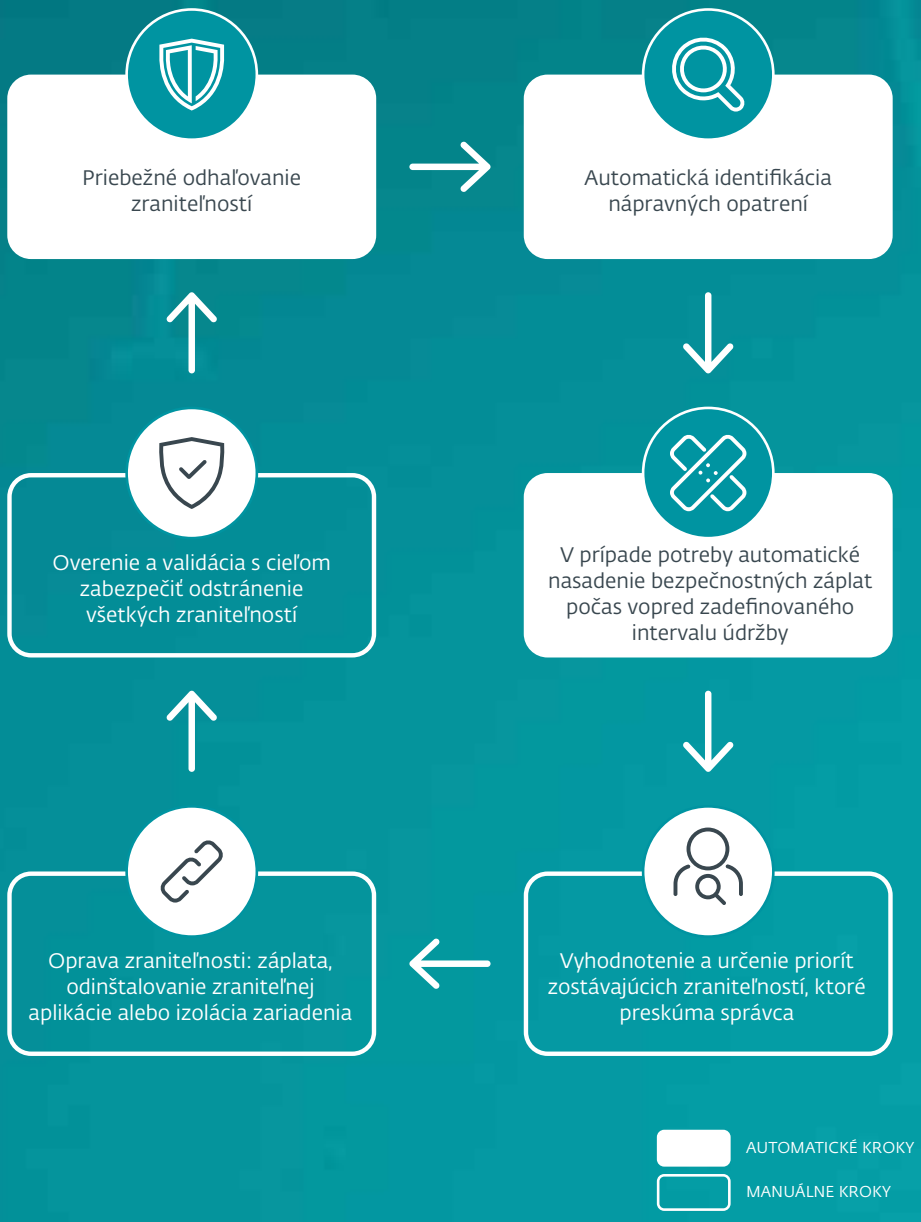
Vyhodnotenie zraniteľností

- 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
- Konzola ESET PROTECT Cloud zaisťuje jednotný prehľad s podporou viacerých jazykov a nízkymi nárokmi na vašu IT infraštruktúru

Správa záplat

- Spustite okamžité aktualizácie a nasadenie záplat prostredníctvom prispôsobiteľných možností alebo manuálne
- Zjednodušte proces nasadzovania záplat: uprednostnite kritické aktíva a zvyšné 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 priorít 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.
- ✓ Prispôsobte 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, koordinačné 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 politík správy zraniteľností a záplat.

NÁKUP:

Modul ESET Vulnerability and Patch Management je k dispozícii v rámci týchto úrovní ochrany:

ESET PROTECT COMPLETE

ESET PROTECT ELITE

Toto je ESET

Proaktívna ochrana. Minimalizujte riziká vďaka prevencii.

Buďte o krok vpred pred známymi aj novými kybernetickými hrozbami vďaka nášmu prístupu, ktorý je založený na umelej inteligencii a zameraný na prevenciu. Kombinovaním sily umelej inteligencie a odborných znalostí našich pracovníkov dokážeme poskytovať jednoduchú a efektívnu ochranu.

ESET PROTECT, naša cloudová platforma kybernetickej bezpečnosti s podporou XDR, kombinuje next-gen schopnosti prevencie, detekcie a proaktívneho vyhľadávania hrozieb so širokou škálou bezpečnostných služieb vrátane riadenej detekcie a reakcie (MDR). Naše vysoko prispôsobiteľné riešenia zahŕňajú podporu v lokálnom jazyku, majú minimálny vplyv na výkon zariadenia, identifikujú a zneškodnia známe aj nové hrozby ešte v zárodku, podporujú plynulý chod prevádzky a znižujú náklady na implementáciu a správu.

ESET chráni vašu firmu, aby ste mohli naplno využívať potenciál technológií.

ESET V ČÍSLACH

1 mld.+
chránených používateľov internetu

400-tis.+
firemných zákazníkov

200
krajín a teritórií

13
globálnych centier výskumu a vývoja

NIEKTORÍ Z NAŠICH ZÁKAZNÍKOV

MITSUBISHI MOTORS
Drive your Ambition

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

Allianz Suisse

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

Canon
Canon Marketing Japan Group

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

AV comparatives APPROVED Business Security DEC 2023

V nezávislých testoch AV-Comparatives dosahuje ESET stabilne najlepšie výsledky a najlepšiu mieru detekcie bez falošných poplachov alebo len s minimálnym počtom nesprávne detegovaných položiek.

G2 Leader WINTER 2024

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

kuppingercole ANALYSTS

ESET je podľa spoločnosti KuppingerCole celkovým a trhovým lídrom v hodnotení MDR Leadership Compass 2023.