# VULNERABILITY & PATCH MANAGEMENT

Aktivní posuzování a opravy zranitelností
na všech vašich koncových zařízeních

Progress. Protected.

# Co je služba **ESET Vulnerability and Patch Management?**

**ESET Vulnerability & Patch Management aktivně sleduje zranitelnosti v operačních systémech a běžných aplikacích a umožňuje instalovat automatizované záplaty na všech koncových zařízeních, která se spravují na naší sjednocené platformě.**

Automaticky skenuje software a aplikace třetích stran na vašich koncových zařízeních a díky okamžitým hlášením odesílaným na konzoli poskytuje pohotový přehled o zranitelnostech. K zajištění nepřetržité ochrany si můžete nakonfigurovat automatické záplatování, zvolit pro něj strategii (všechny položky, pouze povolené položky nebo všechny položky kromě vyloučených) a určit konkrétní intervaly, kdy se má záplatování provádět.

eset® Digital Security
Progress. Protected.

# Včasné záplatování operačních systémů a aplikací

Záplatování chyb v zabezpečení operačních systémů a aplikací je zcela zásadní a zároveň je stále jednou z časově nejnáročnějších úloh v IT. Řešení ESET Vulnerability & Patch Management poskytuje další vrstvu zabezpečení organizacím, které potřebují mít aplikace stále aktuální, ale chybí jim lidské zdroje v oblasti IT. Detekuje zranitelnosti a odstraňuje je nebo zmírňuje riziko jejich zneužití tím, že na všech koncových zařízeních instaluje nejnovější záplaty pro aplikace a operační systémy.

Řešení využívá pokročilé metody určení priorit a nástroje pro automatizované pracovní postupy tak, aby co nejlépe naplnilo vaše potřeby v oblasti infrastruktury.

Je součástí platformy ESET PROTECT, a tak zajišťuje nejen průběžné vyhodnocování zranitelností s určováním priorit a nápravy podle rizika, ale také chrání proti hrozbám přesahujícím pouhé softwarové zranitelnosti. Poskytne vám v jednom sjednoceném řešení ochranu proti škodlivému kódu všech typů, včetně ransomwaru, a prevenci hrozeb nultého dne na všech koncových zařízeních, serverech a v poště.

# Klíčové funkce

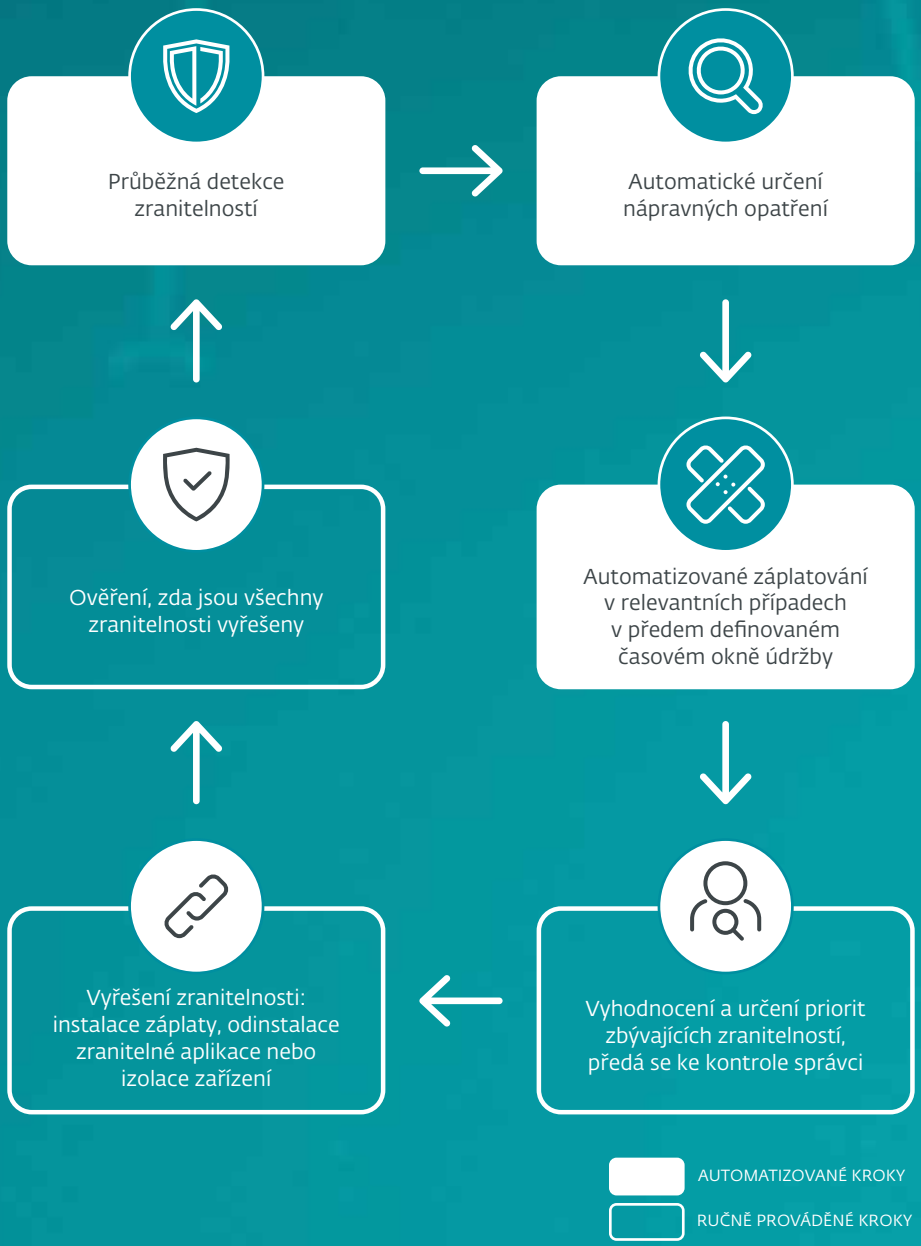
## Vyhodnocování zranitelnosti

- Skenuje tisíce aplikací, jako je Adobe Acrobat, Mozilla Firefox nebo klient Zoom, a podporuje několik verzí systému Windows (a brzy také macOS).
- Rozpozná přes 35 000 běžných zranitelností a bezpečnostních děr, jejichž seznam se stále rozšiřuje.
- Provádí automatizované skenování s možností nastavit si plán podle vlastních potřeb.
- Určuje priority zranitelností a filtruje je podle skóre rizika a závažnosti.
- Poskytuje přehledy zranitelností shrnující nejzranitelnější software a zařízení.
- V komplexních síťových prostředích podporuje víceklientskou architekturu; umožňuje přehled o zranitelnostech v konkrétních částech organizace.
- Sjednocený přehled na cloudové konzoli ESET PROTECT s podporou více jazyků a bez velké zátěže pro vaši IT infrastrukturu.

## Správa záplat

- Umožňuje spouštět okamžité aktualizace a záplaty s využitím přizpůsobitelných možností nebo ručně.
- Zjednodušuje proces záplatování: upřednostňuje kritická aktiva a zbytek plánuje na časy mimo špičku, aby se předešlo přerušování provozu.
- Dovoluje registrovat a sledovat výjimky pro záplaty u vybraných aplikací.
- Poskytuje aktualizovaný katalog záplat zahrnující název záplaty, novou verzi aplikace, známé zranitelnosti, závažnost/důležitost záplaty, dotčené aplikace.
- Všechny záplaty jsou dostupné prostřednictvím konzole ESET PROTECT Cloud.

# Jak to funguje?




eset Digital Security
Progress. Protected.

# Případy použití

Vzhledem k rostoucímu počtu zaměstnanců pracujících na dálku a stále častějšímu využívání cloudových služeb se dnes hrozby rozšiřují nad rámec softwarových zranitelností. I přesto je ale včasné záplatování aplikací a operačních systémů v prevenci narušení bezpečnosti naprosto zásadní.

Každý správce vám zároveň potvrdí, že tato úloha patří v IT k časově nejnáročnějším. Když se tedy nedostává zdrojů, právě záplatování se často odkládá a zranitelnost může vznikat téměř nepozorovatelně. Rostoucí složitost IT systémů také může vést k horší koordinaci mezi týmy z různých oddělení, vzniku mezer v přehledech o inventáři a omezení přehlednosti v otázce aktuálních hrozeb.

.

## Nestíháme záplatování

### PROBLÉM

Náš IT tým je přetížený, a tak je pozadu s instalací záplat.

### ŘEŠENÍ

Využijte pokročilé metody určování priorit a automatizace

- ✓ Nastavte si optimální frekvenci skenování a synchronizujte ho s nastavením záplat tak, abyste mohli řešit relevantní, zneužitelné zranitelnosti bez přetížení IT specialistů.
- ✓ Filtrujte zranitelnosti podle závažnosti a prioritně řešte ty, s kterými jsou spojena významná obchodní rizika.
- ✓ Přizpůsobte si firemní politiky pro instalaci záplat. Upřednostněte nejdůležitější aktiva a ručně řešte závažné zranitelnosti. Záplatování dalších aktiv automatizujte tak, aby probíhalo mimo špičku a předešlo se tak přerušením provozu.
- ✓ Registrujte a sledujte výjimky pro záplaty tak, abyste nemuseli sledovat každou jednotlivou záplatu.

## Nedostatek zdrojů v IT

### PROBLÉM

Potřebujeme udržovat aplikace v aktuálním stavu, ale chybí nám IT zdroje.

### ŘEŠENÍ

Využijte plně automatizované vyhodnocování zranitelností a správu záplat spolu s podporou odborníků společnosti ESET:

- ✓ Automatické skenování softwaru a aplikací třetích stran na vašich koncových zařízeních s okamžitým odesíláním hlášení do konzole, která poskytuje pohotový přehled o zranitelnostech.
- ✓ K zajištění nepřetržité ochrany vaší organizace si nakonfigurujte automatické záplatování, zvolte strategii (všechny položky, pouze povolené položky nebo všechny položky kromě vyloučených) a určete konkrétní intervaly, kdy se má záplatování provádět.

# Rostoucí složitost a náročná koordinace

## PROBLÉM

Naše IT systémy jsou pořád složitější, což komplikuje koordinaci mezi týmy z různých oddělení.

## ŘEŠENÍ

Využijte výhod naší platformy ESET PROTECT, která vám umožní spravovat řešení ESET Vulnerability & Patch Management a širší kontext zabezpečení vašich digitálních aktiv a zařízení.

- ✓ Centralizujte a automatizujte řadu úloh z oblasti zabezpečení a správy IT s platformou ESET PROTECT, která zahrnuje řešení ESET Vulnerability & Patch Management*. Snížíte tak složitost správy IT.
- ✓ Využijte možnosti víceklientského nastavení ve službě ESET Vulnerability & Patch Management: můžete tak mít úplný přehled o celé síti a přitom se soustředit na oblast, kterou máte na starost.
- ✓ Udržujte si aktuální přehled o zařízeních a zbavte se slepých míst v infrastruktuře.
- ✓ Využijte strategie prevence, detekce hrozeb a reakcí na ně na platformě ESET PROTECT a snižte na minimum vystavení hrozbám, které překračují rámec softwarových zranitelností.
- ✓ Řešení ESET Vulnerability & Patch Management vám zjednoduší dodržování předpisů jako GDPR, HIPAA, PCI DSS a dalších, které stanoví oborové, vládní a regulační autority.

# Omezený přehled o IT systémech

## PROBLÉM

Nemáme přesný přehled o zabezpečení našeho IT ekosystému.

## ŘEŠENÍ

Využijte možnosti sjednoceného pohledu z centrální konzole ESET PROTECT Cloud.

- ✓ Získejte úplný a vždy aktuální přehled o koncových zařízeních a licencích ve vaší organizaci a o stavu zranitelností a záplat ve vašem inventáři aktiv.
- ✓ Stav zabezpečení IT zobrazíte v reálném čase prostřednictvím konzole ESET PROTECT Cloud.
- ✓ Připojit se můžete kdykoli a odkudkoli ze svého oblíbeného webového prohlížeče a v případě potřeby tak okamžitě reagovat.
- ✓ Vytvářejte relevantní přehledy, které měří efektivitu a pokroky v zásadách pro správu zranitelností a záplat.

## JAK ZAKOUPIT:

ESET Vulnerability & Patch Management je součástí následujících úrovní řešení:

ESET PROTECT COMPLETE

ESET PROTECT ELITE

# O ESETu

## Digitální zabezpečení nové generace

### MALWAROVÉ HROZBY UMÍME ZASTAVIT, ALE PŘEDEVŠÍM JIM PŘEDCHÁZÍME.

Na rozdíl od běžných řešení, která se zaměřují na reakci na již aktivní hrozby, nabízí společnost ESET bezkonkurenční preventivní přístup využívající umělou inteligenci, lidské znalosti, renomovanou globální službu Threat Intelligence a rozsáhlou síť výzkumných a vývojových center.

Využijte jedinečnou ochranu proti ransomwaru, phishingu, hrozbám nultého dne a cíleným útokům s oceňovanou cloudovou platformou kybernetické bezpečnosti XDR, která kombinuje prevenci nové generace, detekci a proaktivní vyhledávání hrozeb. Naše bezpečnostní řešení mají minimální dopad na výkon koncových zařízení, identifikují a neutralizují vznikající hrozby dřív, než vás mohou ohrozit, zajišťují kontinuitu provozu a snižují náklady na implementaci a správu. Samozřejmostí je obchodní i technická podpora v českém jazyce.

## ESET V ČÍSLECH

**1mld+**
chráněných uživatelů na internetu

**400k+**
firemních zákazníků

**200**
zemí a teritorií

**13**
vývojových center

## NAŠI ZÁKAZNÍCI

MITSUBISHI MOTORS
Drive your Ambition

Zákazníkem od roku 2017, více než 9 000 licencí

Allianz Suisse

Zákazníkem od roku 2016, více než 4 000 mailboxů

Canon
Canon Marketing Japan Group

Zákazníkem od roku 2016, více než 32 000 licencí

T

ISP partnerem od roku 2008, 2 miliony zákazníků

## VYBRANÁ OCENĚNÍ

AV comparatives APPROVED Business Security JUL 2023

V červenci 2023 ESET získal ocenění „APPROVED" za ochranu koncových řešení v business security testu společnosti AV-Comparatives.

G2 Leader WINTER 2024

ESET trvale dosahuje špičkových výsledků na celosvětové platformě hodnocení uživatelů G2 a jeho řešení jsou oceňována zákazníky po celém světě.

kuppingercole ANALYSTS

Podle KuppingerCole Leadership Compass 2023 je ESET uznáván jako lídr trhu a celkový lídr v oblasti MDR.