

GravityZone Patch Management

Aktualizujte a zabezpečujte systémy pomocí automatického záplatování.

Neopravené bezpečnostní chyby v oblíbených aplikacích představují významnou hrozbu pro bezpečnost IT. Avšak správa a administrace aktualizací softwaru může být pro IT oddělení zdoluhavá a časově náročná. GravityZone Patch Management umožňuje automatizovat záplatování operačních systémů a aplikací pomocí přesných kontrolních mechanismů a robustního reportování. Pokrývá celou instalační základnu systému Windows: pracovní stanice, fyzické servery i virtuální servery.

GravityZone Patch Management překonává ostatní řešení díky velmi rychlému skenování záplat, podpoře nejširší základny aplikací třetích stran, detailním možnostem a vysoké spolehlivosti. Konsolidací záplatování a zabezpečení dále snížíte náklady a zefektivníte správu a reportování. Přídavný modul Patch Management, plně integrovaný do platformy GravityZone, umožňuje organizacím udržovat operační systémy a softwarové aplikace aktuální, a poskytuje komplexní přehled o stavu záplat v celé instalační základně systému Windows.

Modul GravityZone Patch Management zahrnuje několik funkcí, například skenování záplat na vyžádání / plánované skenování záplat, automatické / ruční záplatování, nebo hlášení chybějících záplat. Podniky, které záplatují své koncové body, posilují svou bezpečnostní pozici a kompatibilitu s požadavky právních nařízení, a současně zvyšují provozní efektivitu.

Hlavní výhody:

- **Minimalizace bezpečnostních rizik** - výrazné zkrácení doby potřebné k opravě kritických zranitelností.
- **Zlepšení kybernetické hygieny a produktivity vašeho IT týmu** - automatizujte skenování záplat, jejich nasazení a reportování.
- **Zjednodušení reportování o záplatách a o souladu s právními předpisy** - splnění požadavků na řízení rizik
- **Snížení nákladů** - konsolidace správy záplat a zabezpečení koncových bodů u jediného dodavatele a na jediné platformě.
- **Zvýšení produktivity zákazníků** - s aktuálními aplikacemi a menším počtem problémů ,nebo se zpomalením systémů.

Přehledně

Modul GravityZone Patch Management podporuje automatické i ruční záplatování. Poskytuje organizaci větší flexibilitu a efektivitu při správě záplat, díky možnosti vytvářet inventář záplat, plánovat skenování záplat, omezit automatické záplatování na aplikace preferované správcem, měnit plánování bezpečnostních a jiných záplat, a odložit restartování u záplat vyžadujících restart.

Hlavní výhody

- Zajišťuje soulad s legislativními požadavky na zabezpečení informací, jako jsou GDPR, HIPAA a PCI DSS.
- Podporuje automatické i manuální záplatování, což organizacím poskytuje větší flexibilitu a efektivitu celého procesu, a to jak na pracovišti, tak vzdáleně.
- Udržuje operační systémy a softwarové aplikace v aktuálním stavu, a poskytuje komplexní přehled o stavu záplat v celé instalační základně systému Windows, čímž snižuje riziko pokročilých útoků.

"Bitdefender Patch Management je fantastický. Pokud se objeví oprava zero-day, Bitdefender dokáže rychle aktualizovat celou organizaci nejnovější bezpečnostní záplatou. Dodržování záplat se zvýšilo ze 75 na téměř 99 procent. Dříve bylo obvyklé, že pracovní stanice ve vzdálených lokalitách zůstávaly roky bez aktualizace."

Arcidieceze USA,
IT Director

Funkce a vlastnosti

Nejrychlejší skenování a nasazení záplat

GravityZone Patch Management dokáže během několika sekund prohledat systémy a najít chybějící záplaty. Po identifikaci lze tyto záplaty rychle nasadit pomocí automatických nebo ručních postupů.

Podpora největší množiny aplikací třetích stran, operačních systémů Windows a Linux.

Snadno záplatujete nejen operační systémy Windows a Linux, ale také nejrozsáhlejší seznam aplikací, které vaši zákazníci s největší pravděpodobností používají. Centralizujte záplatování napříč lokalitami, fyzickými i virtuálními pracovními stanicemi a servery.

Vylepšené pracovní postupy s flexibilním automatizovaným a řízeným záplatováním

Můžete vytvářet inventář záplat, plánovat skenování záplat, vybírat aplikace, které mají být automaticky záplatovány, měnit plánování bezpečnostních a jiných záplat, a odkládat restarty po instalacích záplat.

ANALÝZA RIZIK A HARDENING	PREVENCE	DETEKCE A REAKCE	REPORTING A INTEGRACE
ANALÝZA RIZIK KONCOVÉHO BODU PATCH MANAGEMENT*	SIGNATURY A ZABLOKOVÁNÍ CLOUDU LOKÁLNÍ & CLOUDOVÉ STROJOVÉ UČENÍ	SLEDOVÁNÍ ŠKODLIVÝCH PROCESŮ BLOKOVÁNÍ PŘÍSTUPŮ	DASHBOARDY & REPORTY NOTIFIKACE
FULL-DISK ENCRYPTION* OCHRANA PŘED HROZBAMI	OCHRANA PROTI EXPLOITŮM NETWORK ATTACK DEFENSE	KARANTÉNA AUTOMATICKÁ DEZINFEKCE & ODSTRANĚNÍ	SIEM INTEGRACE PODPORA API
KONTROLA APLIKACE KONTROLA ZAŘÍZENÍ	EMAIL SECURITY* FIREWALL OCHRANA PROTI BEZ SOUBOROVÝM ÚTOKŮM	UKONČOVÁNÍ PROCESU OBNOVENÍ	

* ADD-ON