

GravityZone Patch Management

Halten Sie Systeme mit automatischer Aktualisierung durch Patches sicher und auf dem neuesten Stand.

Nicht gepatchte Sicherheitslücken in gängigen Anwendungen stellen eine erhebliche Bedrohung für die IT-Sicherheit dar. Doch das Verwalten und Einspielen von Softwareupdates kann für IT-Abteilungen mühsam und zeitaufwändig sein. Mit GravityZone Patch Management können Sie das Patchen von Betriebssystemen und Anwendungen automatisieren, bis ins Detail steuern und entsprechende Berichte erstellen. Dabei wird die gesamte Windows-Umgebung Ihrer Kunden berücksichtigt: vom Arbeitsplatzrechner bis hin zu physischen und virtuellen Server.

Dank blitzschneller Patch-Scans, Unterstützung für die breiteste Palette an Drittanwendungen, zahlreicher Feineinstellungen und höchster Zuverlässigkeit ist GravityZone Patch Management anderen Lösungen weit überlegen. Durch Konsolidierung des Patchings und der IT-Sicherheit werden außerdem Betriebskosten gesenkt und Verwaltung und Berichterstattung verschlankt. Mit dem vollständig in die GravityZone-Plattform integrierten Add-On-Modul Patch Management können Unternehmen ihre Betriebssysteme und Softwareanwendungen stets auf dem neuesten Stand halten. Ferner erhalten sie einen umfassenden Überblick über den Patch-Status auf allen Windows-Systemen.

Das GravityZone-Modul Patch Management beinhaltet verschiedene Funktionen, darunter manuelle/geplante Suche nach Patches, automatisches/manuelles Einspielen der Patches sowie Meldung fehlender Patches. Unternehmen, die ihre Endpoints sorgfältig durch Installation der neuesten Patches schützen, festigen ihre Sicherheitslage und halten gleichzeitig alle maßgeblichen Vorschriften ein. Zur gleichen Zeit steigern sie ihre betriebliche Effizienz.

Hauptfunktionen

Schnellste Patch-Scans und -Installationen:

GravityZone Patch Management kann Systeme sekundenschnell auf fehlende Patches überprüfen. Wurden Sicherheitslücken gefunden, können die entsprechenden Patches mit automatischen oder manuellen Optionen schnell eingespielt werden.

Zusammengefasst

Das GravityZone-Patch-Management-Modul unterstützt sowohl automatisches als auch manuelles Patchen. Unternehmen profitieren von mehr Flexibilität und Effizienz in Ihrem Patch Management. Sie können ein Patch-Inventar anlegen, Patch-Scans einplanen, das automatische Patchen auf vom Admin bevorzugte Anwendungen einschränken, unterschiedliche Zeitpläne für sicherheitsrelevante und nicht sicherheitsrelevante Patches festlegen und Neustarts für Patches, die einen Neustart erfordern, verschieben.

Hauptvorteile

- Sicherheitsrisiken durch kritische Schwachstellen minimieren durch drastisch beschleunigtes Patch-Verfahren
- Bessere Cyber-Hygiene und Produktivität der IT-Abteilung durch automatisierte Patch-Scans, Installation und Berichterstattung
- Compliance- und Patch-Reporting vereinfachen, Risiko-Management-Anforderungen erfüllen
- Kosten senken durch Patch-Managements und Endpointsicherheit aus einer Hand.
- Produktivität bei den Kunden steigern durch zuverlässig aktuelle Anwendungen und weniger Probleme und Verzögerungen.

„Bitdefender Patch Management ist fantastisch. Wenn ein Zero-Day-Fix veröffentlicht wird, kann Bitdefender im Handumdrehen über die gesamte Organisation den neuesten Sicherheitspatch aufspielen. Die Patch-Compliance ist von 75 auf fast 99 % gestiegen. Vorher kam es nicht selten vor, dass Computer in entlegeneren Gemeinden jahrelang kein Update bekamen.“

US Archdiocese, IT-Direktor

Unterstützung für größte Palette an Drittanwendungen sowie Windows und Linux:

Unkomplizierte Patch-Installation nicht nur fürs Betriebssystem, sondern auch für eine umfangreiche Liste an Anwendungen, die bei Ihren Kunden im Einsatz sind. Patching-Vorgänge werden über mehrere Standorte, physische und virtuelle Computer und Server hinweg zentralisiert gesteuert.

Verbesserte Abläufe mit flexiblen automatischen und manuellen Patching-Optionen:

Patch-Inventare erstellen, Patch-Scans planen, manuell zu patchende Anwendungen festlegen, getrennte Patch-Zeitpläne für sicherheitskritische und andere Patches definieren, Systemneustarts verschieben und mehr.

RISK ANALYTICS AND HARDENING	PREVENTION	DETECTION AND RESPONSE	REPORTING AND INTEGRATION
 ENDPOINT RISK ANALYTICS	 PATCH MANAGEMENT*	 SIGNATURE AND CLOUD LOCKUP	 LOCAL & CLOUD MACHINE LEARNING
 FULL-DISK ENCRYPTION*	 THREAT PROTECTION	 MALICIOUS PROCESS MONITORING	 ACCESS BLOCKING
 APPLICATION CONTROL	 EXPLOIT DEFENSE	 QUARANTINE	 AUTOMATIC DISINFECTION & REMOVAL
 DEVICE CONTROL	 NETWORK ATTACK DEFENSE	 SIEM INTEGRATION	 API SUPPORT
	 EMAIL SECURITY*	 PROCESS TERMINATION	
	 FIREWALL	 ROLLBACK	
	 FILELESS ATTACK DEFENSE		

* ADD-ON