DATENBLATT

WATCHGUARD PATCH MANAGEMENT

Weniger Risiko und Komplexität beim Management von Sicherheitslücken in Betriebssystem und Drittanbieteranwendungen

Dem Ponemon Institute zufolge[1] geben 57 % der Opfer von Cyberangriffen an, dass ein Patch den Angriff verhindert hätte, und 34 % der Betroffenen sagen, sie hätten die Sicherheitslücke gekannt, bevor der Angriff erfolgte.

Ransomware wie Wanny Cry oder Petya sind ein ideales Verfahren, um Unternehmen mit mangelhaften Richtlinien für die Betriebssystemverwaltung anzugreifen – aber Cyberangriffe beschränken sich nicht darauf. 86 % der Sicherheitslücken sind auf Drittanbieteranwendungen ohne Patches wie Java, Adobe, Firefox, Chrome, Flash und OpenOffice zurückzuführen.

SICHERHEITSLÜCKEN: EIN VERKAPPTES RISIKO

Die Ausnutzung von Sicherheitslücken ist nach wie vor die häufigste Ursache für Sicherheitsverletzungen. Bekannte Fälle wie Wanna Cry, Petya und BlueKeep, die weltweit für Chaos sorgten, sind noch in aller Munde.

Nur wenige Angriffe erfolgen aufgrund tatsächlich unbekannter Sicherheitslücken (Zero-Day-Angriffe) – die Mehrzahl ist auf bekannte Sicherheitslücken zurückzuführen.

Mit der digitalen Transformation wird es angesichts der wachsenden Zahl an Nutzern, Geräten, Systemen und Drittanbieteranwendungen, die aktualisiert werden müssen, zunehmend schwerer, die Angriffsfläche zu reduzieren.

Programme für das Sicherheitslücken-Management (Vulnerability Management, VM) werden mindestens durch diese drei häufigen betrieblichen Probleme gehemmt:

- Die Identifizierung von Sicherheitslücken ist ein langwieriger Vorgang. Bei Vorfällen muss jedoch sofort reagiert werden.
- Unternehmen sind dezentral strukturiert und Mitarbeiter nicht durchgängig mit dem Unternehmensnetzwerk verbunden. On-Premises-VM-Tools decken diese Szenarien nicht ab.
- Andere Sicherheitslösungen mit Funktionen für das Patch-Management verknüpfen die Erkennung nicht mit gefährdeten Endpoints, um so die Reaktion auf Angriffe und ihre Eindämmung zu beschleunigen.

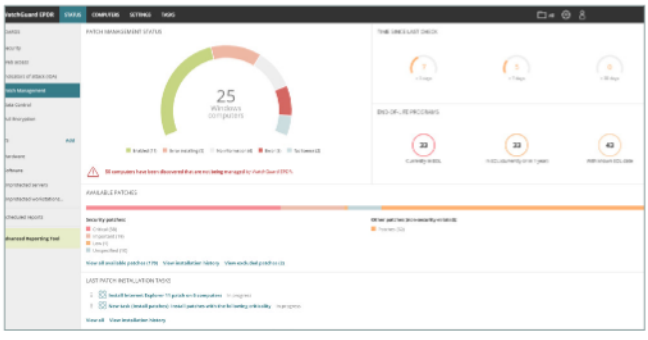


Abbildung 1: *Organisationsstatus für Patch-Management – Haupt-Dashboard*

WATCHGUARD PATCH MANAGEMENT

WatchGuard Patch Management ist eine anwenderfreundliche Lösung zur Verwaltung von Sicherheitslücken in Betriebssystemen und Drittanbieteranwendungen auf Windows-/macOS-/Linux-Workstations und -Servern. Sie reduziert die Angriffsfläche und verbessert zugleich die Präventions- und Abschirmungskapazität Ihrer Organisation.

Die Lösung ist vollständig in alle Endpoint-Lösungen von WatchGuard integriert setzt damit keinerlei neue Endpoint-Agenten oder Verwaltungskonsolen voraus.

Darüber hinaus bietet sie zentralisierte Echtzeit-Einblicke in den Sicherheitsstatus von Software-Sicherheitslücken, fehlende Patches, Updates und nicht mehr unterstützte Software (EOL)[2] und stellt Tools für den gesamten Patch-Management-Zyklus von der Identifizierung und Planung bis zu Installation und Monitoring bereit.

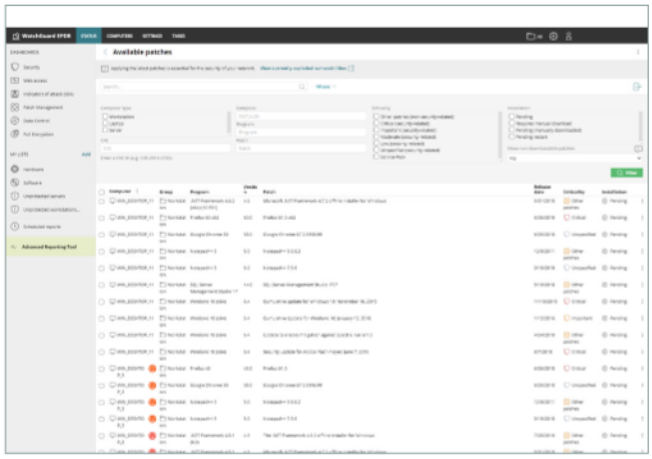


Abbildung 2: *Verfügbare Patches – Patch-Management*

[1] „Cost and Consequences of Gaps in Vulnerability Response", Ponemon.

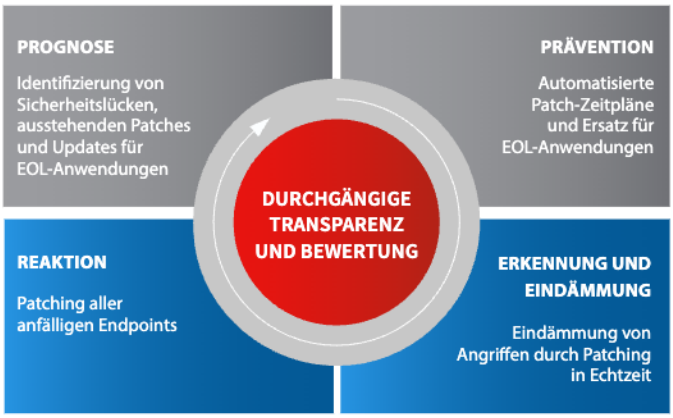
[2] EOL, End-of-Life: Produkte am Ende ihrer Nutzungsdauer, für die es keine Sicherheitsupdates mehr gibt.

VORTEILE

WatchGuard Patch Management eröffnet Ihnen als anwenderfreundliche zentrale Lösung folgende Möglichkeiten:

- Prüfung, Überwachung und Priorisierung von Betriebssystemen und Anwendungsupdates. Die Ein-Panel-Ansicht gibt einen zentralen, aktuellen, aggregierten Überblick über den Sicherheitsstatus des Unternehmens bei Sicherheitslücken, Patches und ausstehenden Updates für Systeme und Hunderte von Anwendungen.
- Verhinderung von Vorfällen durch systematische Reduzierung der durch Software-Sicherheitslücken geschaffenen Angriffsfläche. Handhabung von Patches und Updates mit anwenderfreundlichen Echtzeit-Management-Tools, mit denen Unternehmen Angriffen zur Ausnutzung von Sicherheitslücken zuvorzukommen können.
- Eindämmung und Behebung von Angriffen über Sicherheitslücken durch die sofortige Verteilung von Updates oder Patches über die Web-Konsole. Betroffene Computer können vom restlichen Netzwerk isoliert werden, um der Ausbreitung von Angriffen zuvorzukommen.
- Reduzierung der Betriebskosten:
  - Vereinfacht die Verwaltung, da Sie keine neuen Endpoint-Agenten bereitstellen und bestehende Agenten nicht aktualisieren müssen.
  - Minimiert den Patching-Aufwand, da Updates von der cloudbasierten Konsole aus gestartet werden.
  - Bietet unmittelbar nach der Aktivierung vollständigen, direkten Einblick in alle Sicherheitslücken, ausstehenden Updates und EOL-Anwendungen.
- Entspricht dem Rechenschaftsprinzip, das viele Vorschriften voraussetzen. Zwingt Unternehmen, die geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um sensible Daten unter ihrer Kontrolle ausreichend zu schützen.

WATCHGUARD PATCH MANAGEMENT
ADAPTIVE SICHERHEITSARCHITEKTUR



„Designing an Adaptive Security Architecture for Protection from Advanced Attacks", Gartner

WICHTIGE FUNKTIONEN

Identifizierung

- Ein-Panel-Ansicht mit Echtzeit-Informationen zu allen gefährdeten Computern, ausstehenden Patches und nicht mehr unterstützten Anwendungen (EOL) mit Korrekturstatus.
- Detaillierte Informationen zu ausstehenden Patches und Updates, Details zu relevanten Sicherheitsbulletins (CVE).
- Automatische Suche nach verfügbaren Patches in Echtzeit oder in regelmäßigen Abständen (alle 3, 6, 12 oder 24 Stunden).
- Benachrichtigungen zu ausstehenden Patches bei Exploit-Erkennung.
- Möglichkeit zu Isolierung, Patching und Entisolierung von Computern und Servern.

Planungs- und Installationsaufgaben für Patches und Updates:

- Konfiguration von Schweregrad und zu patchender Software.
- Planung der direkten einmaligen Ausführung oder wiederholten Ausführung in regelmäßigen Abständen (Tag/Zeit).
- Kontrolle von Computer-Neustarts und Festlegung von Ausnahmen.
- Zurücksetzung zur Deinstallation von Patches, die unerwartete Konflikte mit bestehenden Konfigurationen verursachen.

Monitoring von Endpoint- und Updatestatus über:

- Dashboard und Aufgabenlisten. Allgemeine und ausführliche Berichte.
- Listen mit aktualisierten Computern, Computern mit ausstehenden Updates/mit Fehlern.

Detaillierte gruppen- und rollenbasierte Verwaltung mit unterschiedlichen Berechtigungen:

- Rollenbasierte Anzeige von gefährdeten Computern, Patches und Service Packs.

Zentralle Kontrolle von Updates, Patches und Software:

- Möglichkeit zur Deaktivierung von Windows Update und zur zentralen Verwaltung von Betriebssystemupdates.
- Möglichkeit, bestimmte Patches und Software nach Version und Typ auszuschließen.
- Möglichkeit zum Ausschluss von Software (z. B. Java).
- Zwischenspeicherung heruntergeladener Patches.

Unterstützte Plattformen und Systemanforderungen für WatchGuard Patch Management

Kompatibel mit WatchGuard EPDR, WatchGuard Advanced EPDR, WatchGuard EDR und WatchGuard EPP

Unterstützte Betriebssysteme: Windows, macOS (Catalina oder höher) und Linux (RedHat, CentOS und SUSE).

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Microsoft Edge und Safari.

Patch-Management für Sicherheitslücken:
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

Unterstützte Drittanbieteranwendungen:
https://www.watchguard.com/wgrd-resource-center/patch-management

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.