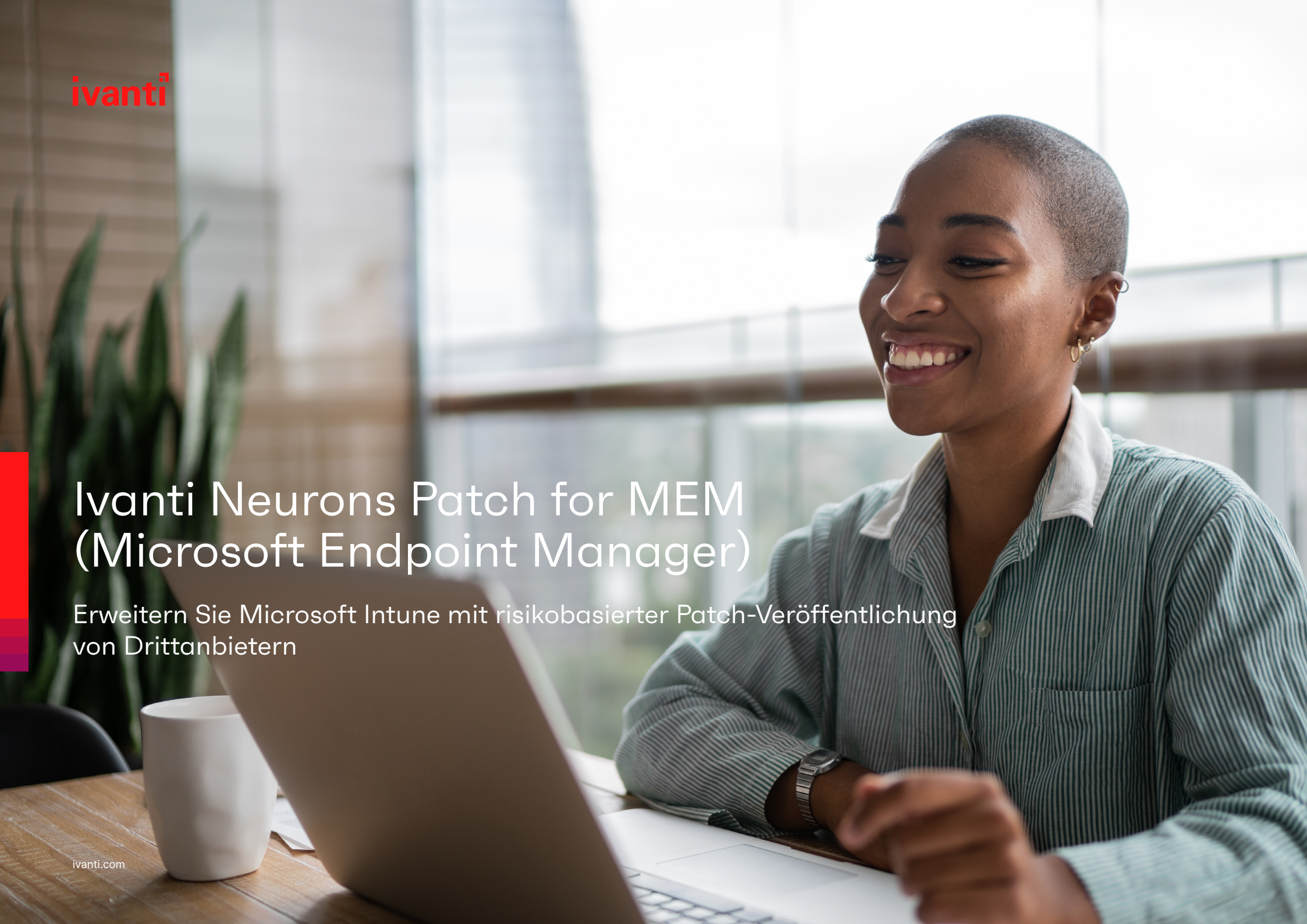


Ivanti Neurons Patch for MEM (Microsoft Endpoint Manager)

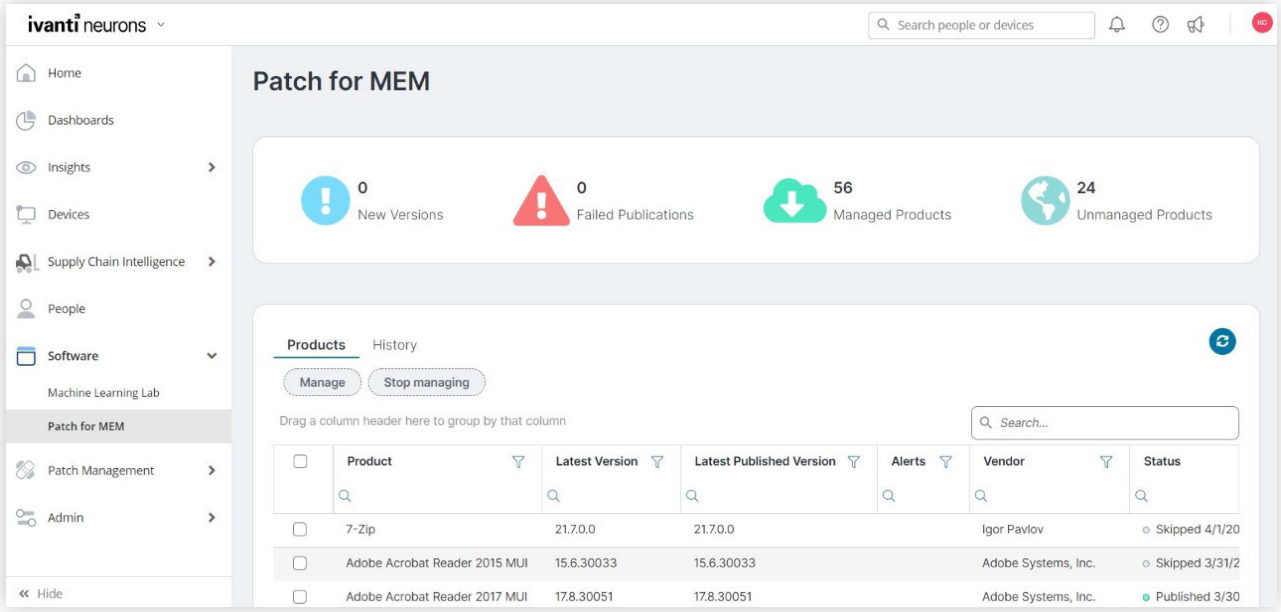
Erweitern Sie Microsoft Intune mit risikobasierter Patch-Veröffentlichung von Drittanbietern

Ivanti Neurons Patch for MEM erweitert bestehende Microsoft Intune-Implementierungen, um Anwendungsupdates von Drittanbietern einzubeziehen. Die Informationen zu Bedrohungen und Patches helfen Unternehmen, bei der Behebung von Schwachstellen in der Software von Drittanbietern die richtigen Prioritäten zu setzen.

Updates von Drittanbietern in Intune

Datenschutzverletzungen und Ransomware-Angriffe nehmen jedes Jahr zu. Auch die Anzahl der von Unternehmen eingesetzten Anwendungen nimmt zu, seit 2016 um 24 %.[1] Es sollte daher nicht überraschen, dass Anwendungen von Drittanbietern zu einem der attraktivsten Angriffsvektoren für Cyberangreifer geworden sind. Leider gehören Datenschutzverletzungen, die auf Schwachstellen in Anwendungen von Drittanbietern zurückzuführen sind, auch zu den teuersten: Sie kosten Unternehmen durchschnittlich 4,33 Millionen Dollar.[2]

Unternehmen müssen daher die Anwendungen von Drittanbietern sorgfältig aktualisieren, was bei der ständig wachsenden Zahl von Anwendungen, die sie berücksichtigen müssen, eine Herausforderung darstellen kann. Erschwerend kommt hinzu, dass die Zahl der Schwachstellen, die sie verfolgen müssen, immer weiter zunimmt – im Durchschnitt werden täglich 61 Schwachstellen in der National Vulnerability Database (NVD) veröffentlicht.[3]



Die gute Nachricht ist, dass nur 4 % aller CVEs (Common Vulnerabilities and Exposures – Gemeinsame Schwachstellen und Gefährdungen) öffentlich ausgenutzt wurden.[4] Die schlechte Nachricht ist, dass es schwierig sein kann, diese 4 % aus den insgesamt über 130.000 Schwachstellen in der NVD zu identifizieren. Wenn ein Unternehmen beispielsweise alle kritischen Schwachstellen auf der Grundlage des Common Vulnerability Scoring System (CVSS) v3 patchen würde, würden 73,61 % der Ransomware-Schwachstellen nicht gepatcht werden.[3]

Diese Situation kann für Unternehmen, die Microsoft Intune für die Bereitstellung von Anwendungen und Updates auf ihren Geräten nutzen, sogar noch problematischer sein. Intune bietet zwar umfassende Patch-Management-Funktionen für Microsoft-Anwendungen, aber keine nativen Funktionen für die Aktualisierung von Drittanbieter-Anwendungen.

Wir stellen vor: Ivanti Neurons Patch for MEM

Ivanti Neurons Patch for MEM erweitert bestehende Microsoft Intune-Implementierungen um die Möglichkeit, Anwendungen von Drittanbietern zu aktualisieren, ohne dass dafür eine zusätzliche Infrastruktur erforderlich ist. Außerdem bietet es IT-Teams verwertbare Erkenntnisse über Bedrohungen und Patch-Zuverlässigkeit, damit sie die Schwachstellen, die das größte Risiko für ihr Unternehmen darstellen, priorisieren und beheben können. Mit Ivanti Neurons Patch for MEM können sich Unternehmen besser vor Datenschutzverletzungen, Ransomware und anderen Bedrohungen schützen, die von Schwachstellen in Drittanbieteranwendungen ausgehen.

Wichtigste Merkmale und Fähigkeiten

Microsoft Intune um die Veröffentlichung von Patches von Drittanbieter-Apps erweitern

Maximieren Sie die Rendite Ihrer Intune-Investition und schützen Sie sich gleichzeitig vor Bedrohungen, die von Sicherheitslücken in Anwendungen von Drittanbietern herrühren. Ivanti Neurons Patch for MEM veröffentlicht vorab getestete Anwendungsupdates von Drittanbietern von Ivantis Neurons Cloud-Plattform direkt in Intune. So können IT-Teams Anwendungsupdates von Drittanbietern zusammen mit Betriebssystem- und Anwendungsupdates von Microsoft innerhalb von Intune als Teil ihrer bestehenden Workflows für das Application Lifecycle Management bereitstellen.

Als Cloud-native Lösung ermöglicht Ivanti Neurons Patch for MEM den Intune-Kunden außerdem, ihre Patching-Workloads vollständig in die Cloud zu verlagern und Microsofts Vision eines modernen Managements zu verwirklichen, ohne dass eine zusätzliche Infrastruktur benötigt wird.

Proaktiver Schutz vor aktiven Exploits

Priorisierung der Problembehebung auf der Grundlage des Angriffsrisikos, mit Informationen über bekannte Exploits und den Bedrohungskontext für Schwachstellen – einschließlich Verbindungen zu Ransomware. Das Vulnerability Risk Rating (VRR) von Ivanti gibt dir bessere Möglichkeiten, risikobasierte und priorisierte Maßnahmen zu ergreifen als die einfache CVSS-Bewertung, indem es die genauesten Daten über Schwachstellen und Bedrohungen sowie die menschliche Validierung von Exploits durch Penetrationstest-Teams berücksichtigt.

Vermeiden Sie fehlgeschlagene Patch-Implementierungen

Sparen Sie Zeit und vermeiden Sie fehlgeschlagene Patch-Implementierungen mit vorab getesteten Anwendungsupdates und Einblicken in die Patch-Zuverlässigkeit. Ivanti testet jedes von uns erstellte Patch-Inhaltspaket gründlich. Die Tests werden in einer umfangreichen virtuellen Umgebung durchgeführt, um sicherzustellen, dass die Pakete in einer breiten Palette von Anwendungsversionen und Betriebssystemen funktionieren, bevor sie für das Produkt freigegeben werden.

Um Ihr Vertrauen weiter zu stärken, können Sie die Patch-Zuverlässigkeit anhand von sozialen Stimmungsdaten und anonymisierten Telemetriedaten zur Patch-Bereitstellung auf der Grundlage der Zuverlässigkeit von Anwendungsupdates in realen Umgebungen bewerten, bevor Sie diese bereitstellen.

Optimierung der Patch-Management-Prozesse

Erzielen Sie mit der hilfreichen Funktion von Ivanti Neurons Patch for MEM eine Reihe von betrieblichen Effizienzsteigerungen:

- Veröffentlichen Sie Anwendungsupdates von Drittanbietern automatisch in Intune, sobald sie verfügbar sind (automatische Veröffentlichung optional).
- Erzielen Sie ein zuverlässigeres Patching mit weniger Fehlern, indem Sie vorab getestete Anwendungsupdates in Verbindung mit Erkenntnissen über die Patch-Zuverlässigkeit nutzen.
- Setzen Sie mithilfe von Bedrohungsdaten effektiv Prioritäten bei den Patch-Maßnahmen, damit Sie sich nur auf das Wesentliche konzentrieren.
- Vereinfachen Sie Daten- und Risikodialoge zwischen Sicherheits- und IT-Betriebsteams mit Einblicken in Exploits und Malware, um die operative Zusammenarbeit zu verbessern.

Über Ivanti

Ivanti macht den Everywhere Workplace möglich. Im Everywhere Workplace nutzen Mitarbeiter unzählige Geräte, um über verschiedene Netzwerke auf IT-Netzwerke, Anwendungen und Daten zuzugreifen und so von überall aus produktiv arbeiten zu können. Die Ivanti-Automatisierungsplattform verbindet die branchenführenden Unified-Endpoint-Management-, Zero-Trust-Sicherheits- und Enterprise-Service-Management-Lösungen des Unternehmens und bietet Unternehmen eine zentrale Plattform für die Selbstheilung und Selbstsicherung von Geräten sowie für den Self-Service von Endanwendern. Mehr als 40.000 Kunden, darunter 96 der Fortune 100, haben sich für Ivanti entschieden, um ihre IT-Assets von der Cloud bis zum Edge zu erkennen, zu verwalten, zu sichern und zu warten und ihren Mitarbeitern ein hervorragendes Endbenutzererlebnis zu bieten, egal wo und wie sie arbeiten. Weitere Informationen finden Sie unter https://www.ivanti.de.

ivanti

ivanti.de
+49 (0)69 66 77 80 134
contact@ivanti.de

1. Okta, „Business at Work 2022 Report“, 2022. https://www.okta.com/report/businesses-at-work-2022/
2. IBM Security, „2021 Cost of a Data Breach Report“, 28. Juli 2021. https://www.ibm.com/security/data-breach
3. Cyber Security Works, Cyware, Ivanti, „2022 Ransomware Spotlight Report“, 26. Januar 2022. https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
4. Agentur für Cybersicherheit und Infrastruktursicherheit (CISA), „Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities“, 3. November 2021. https://cyber.dhs.gov/bod/22-01/