Ivanti Neurons for Patch Management

Effiziente Priorisierung und Behebung von Schwachstellen

Ivanti Neurons for Patch Management ist eine Cloud-native Patch Management-Lösung mit verwertbaren Informationen zu Risikostatus, Patch-Zuverlässigkeit, Geräte-Compliance, -Zustand und -Risiko. Organisationen schützen sich damit besser vor Bedrohungen, einschließlich Ransomware.

Risikobasierte Patch-Verwaltung

Ransomware-Angriffe nehmen jedes Jahr an Häufigkeit und Schwere zu. Die Auswirkungen auf die Unternehmen sind verheerend. Untersuchungen zufolge belaufen sich die durchschnittlichen Gesamtkosten eines Verlustes durch Ransomware auf 4,62 Millionen Dollar – ohne die Kosten für das Lösegeld.[1]

Leider wird sich die Situation eher verschlechtern, bevor sie besser wird. Ransomware as a Service (RaaS) ermöglicht es so gut wie jedem, einen Angriff zu starten – ohne irgendwelche Security- oder Programmierkenntnisse. Darüber hinaus hat sich die Zahl der CVEs (Common Vulnerabilities and Exposures) in Netzwerken im Jahr 2020 fast vervierfacht.[2] Schlimmer noch: Ransomware-Angreifer haben es zunehmend auf mittelständische Unternehmen abgesehen, um die mediale Aufmerksamkeit zu vermeiden, die Angriffe auf Großunternehmen mit sich bringen.[3]

Zur Behebung von CVEs ist Patchen das Beste, was eine Organisation tun kann, um Ransomware-Angriffe abzuwehren. Leider finden 71% der IT- und Security-Experten, dass Patchen zu komplex und zeitaufwändig ist.[4] Das mag an der überwältigenden Anzahl der vorhandenen Schwachstellen liegen. In der US National Vulnerability Database (NVD) sind weit über 100.000 Schwachstellen aufgelistet. Obwohl nur

ein kleiner Prozentsatz mit Ransomware in Verbindung steht und ein noch kleinerer Prozentsatz aktive Exploits sind, kann es schwierig sein, herauszufinden, welche davon das größte Risiko für Ihr Unternehmen darstellen. Wenn Sie im Zeitraum 2018-2020 nur kritische Schwachstellen patchen würden, läge Ihr Schutz vor Ransomware unter Verwendung der CVSS v3-Bewertung nur bei etwa 35 %.[2]

Ivanti Neurons for Patch Management bietet verwertbare Informationen über Bedrohungen, Einblicke in die Patch-Zuverlässigkeit und einen Überblick über das Geräterisiko. So können Sie die Schwachstellen priorisieren, die für Ihr Unternehmen am gefährlichsten sind und diese beheben.
Durch den Einsatz von Ivanti Neurons for Patch Management können Sie Ihre Organisation besser vor Datenschutzverletzungen, Ransomware und anderen Bedrohungen schützen, die von Software-Schwachstellen ausgehen.

Die wichtigsten Merkmale und Funktionalitäten

Proaktive Patches gegen aktive Exploits

Priorisieren Sie die 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 Ihnen bessere Möglichkeiten, risikobasierte, priorisierte Maßnahmen zu ergreifen als die CVSS-Bewertung, da es die genauesten Daten über Schwachstellen und Bedrohungen sowie die menschliche Validierung von Exploits durch Penetrationstests berücksichtigt.

Erreichen Sie schnellere SLAs mit zuverlässigen Patches und Einblicken in die Trendentwicklung

Sparen Sie Zeit und vermeiden Sie fehlgeschlagene Patch-Implementierungen mit Erkenntnissen zur Patch-Zuverlässigkeit aus sozialen Stimmungsdaten und anonymisierten Telemetriedaten zur Patch-Implementierung. Diese Informationen ermöglichen es Ihnen, Patches auf der Grundlage ihrer Zuverlässigkeit in realen Anwendungen zu bewerten, bevor Sie sie einsetzen. Die Verfolgung von Service-Level-Agreements (SLAs), die einen Einblick in Geräte bieten, die sich dem SLA nähern, ermöglicht es Ihnen, Maßnahmen zu ergreifen, bevor die Geräte nicht mehr compliant sind.

Umstellung von lokalem auf Cloud-Patch Management

Beginnen Sie Ihren Weg vom On-Premise-Patch Management in die Cloud mit der starken Patch-Technologie von Ivanti. Ivanti Neurons for Patch Management ist eine Cloud-native Lösung, die es Ihnen ermöglicht, in Ihrem eigenen Tempo von der On-Premise-Patch-Verwaltung in die Cloud zu wechseln, anstatt zu einem kompletten Neustart gezwungen zu sein. Solche schrittweisen Übergänge werden durch den Single Pane of Glass-Ansatz realisiert, der einen Überblick über die Geräte bietet, die in der Cloud verwaltet werden, sowie über die Geräte, die über die On-Premise-Patch-Management-Lösung verwaltet werden.

Optimierung der Patch Management-Prozesse

Verbessern Sie die betriebliche Effizienz, indem Sie nicht mehr zwischen verschiedenen, isolierten Patch Management-Lösungen wechseln müssen. Ivanti Neurons for Patch Management bietet Transparenz in alle Endpunkte in Ihrer Umgebung. Erweiterte Einblicke in Schwachstellen und Patch-Intelligenz verbessern die betriebliche Effizienz weiter, indem sie es Ihnen ermöglichen, Patches effektiv zu priorisieren, damit Sie sich nur auf das Wesentliche konzentrieren.
Und wenn es an der Zeit ist, Patches aufzuspielen, verteilen autonome Patch-Konfigurationen, die auf den Ivanti Neurons Agent auf den Geräten aufgespielt werden, gründlich getestete Patches innerhalb von Minuten auf Tausende von Rechnern.

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 zu arbeiten. Die Ivanti-Automatisierungsplattform verbindet die branchenführenden Unified-Endpoint-Management-, Zero-Trust-Security- und Enterprise-Service-Management-Lösungen und bietet Organisationen eine zentrale Plattform für Self-Heal und Self-Secure 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 ivanti.com

ivanti neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com

1. IBM Security, „2021 Cost of a Data Breach Report", 28. Juli 2021 https://www.ibm.com/downloads/cas/OJDVQGRY
2. RiskSense, Cyber Security Works, „Ransomware Through the Lens of Threat and Vulnerability Management", 9. November 2021. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw
3. Coveware, „Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021", 21. Oktober 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
4. Ivanti, „Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace", 7. Oktober 2021. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges