

Ivanti Neurons for Patch Management

Verringern der Angriffsfläche und des Risikos durch Priorisierung und gezielte Behebung von Schwachstellen

Ivanti Neurons for Patch Management ist eine Cloud-native Lösung, die einen Überblick über die Risiken auf Endgeräten bietet und sofort um verwertbare Informationen anreichert. Dabei ist es egal ob die Geräte unter Windows, macOS oder Linux betrieben werden, ob Risiken vom Betriebssystem oder von Anwendungen von Drittanbietern ausgehen. Priorisieren und beheben Sie Schwachstellen mit Hilfe von Informationen über aktuell ausgenutzte Exploits, die Zuverlässigkeit von Patches und Gerätekonformität. Schützen Sie sich vor einer Vielzahl von Bedrohungen, einschließlich Ransomware.

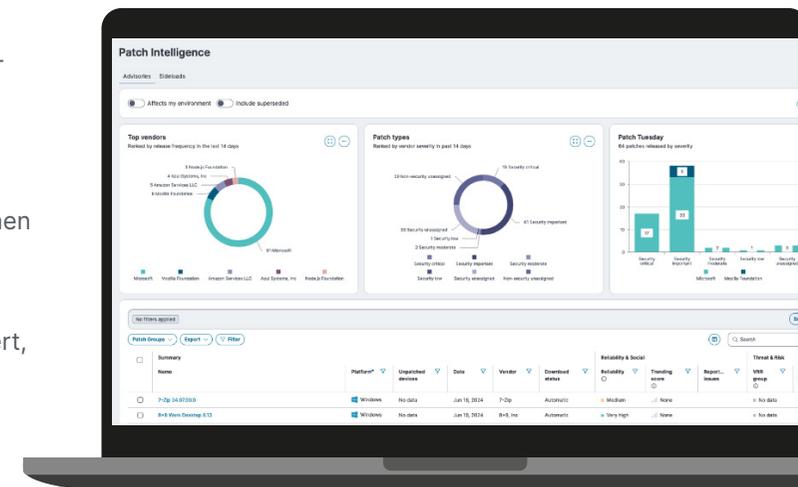
Risikobasiertes Patch-Management

Ransomware-Angriffe werden von Jahr zu Jahr häufiger und schwerwiegender, was für Unternehmen verheerende Folgen hat. Untersuchungen zufolge belaufen sich die durchschnittlichen Gesamtkosten einer Datenschutzverletzung auf 4,88 Millionen US-Dollar – ein Anstieg von 10 % gegenüber 2023 und der größte Anstieg seit der Pandemie.¹

Angriffe werden durch technologische Fortschritte sowie durch KI weiter zunehmen. Ransomware as a Service (RaaS) ermöglicht es nahezu jedem, einen Angriff zu starten – ohne nennenswerte Sicherheits- oder Programmierkenntnisse. Das Ausnutzen von Schwachstellen ist im Vergleich zum Vorjahr um 180 % gestiegen.² Untersuchungen von Google zeigen, dass Zero-Day-Exploits um 50 % zugenommen haben.³ Noch besorgniserregender: Das Zeitalter des KI-Hackings hat begonnen. Forscher an der University of Illinois haben KI-Agenten darauf trainiert,

selbstständig Websites zu hacken, um Zero-Day-Schwachstellen zu entdecken und auszunutzen.⁴

Patches zur Behebung gängiger Schwachstellen und Gefährdungen zählen zu den wirksamsten Maßnahmen, die ein Unternehmen zum Schutz vor Ransomware-Angriffen ergreifen kann. Leider halten 71 % der IT- und Sicherheitsfachleute das Patchen für zu komplex und zeitaufwendig.⁵ Dies könnte an der überwältigenden Anzahl von Sicherheitslücken liegen. In der US-amerikanischen National



Vulnerability Database (NVD) sind weit über 230.000 Schwachstellen verzeichnet.⁶ Obwohl nur ein kleiner Prozentsatz dieser Schwachstellen mit Ransomware in Verbindung steht und nur für einen noch kleineren Prozentsatz aktive Exploits existieren, kann es dennoch schwierig sein, zu erkennen, welche davon das größte Risiko für Ihr Unternehmen darstellen.

Ivanti Neurons for Patch Management bietet verwertbare Bedrohungsdaten, Einblicke in die Zuverlässigkeit von Patches und Sichtbarkeit des Geräterisikos für Geräte unter Windows, macOS und Linux. Dank dieser wichtigen Erkenntnisse können IT-Teams die Schwachstellen priorisieren und beheben, die das größte Risiko für ihr Unternehmen darstellen. Durch den Einsatz von Ivanti Neurons for Patch Management zur Steigerung der Effizienz und Effektivität ihrer Patching-Maßnahmen können Unternehmen sich besser vor Datenschutzverletzungen, Ransomware und anderen Bedrohungen schützen, die aus Softwareschwachstellen resultieren.

Wichtige Features und Funktionen

Risikobasierte Priorisierung

Ivanti Neurons for Patch Management nutzt eine risikobasierte Priorisierungsstrategie, um Patches, die kritische Schwachstellen beheben, bevorzugt zu installieren – insbesondere jene, die mit Ransomware in Verbindung stehen. Durch die Fokussierung auf Patches, die die größten Risiken beseitigen, können

IT-Teams ihre Ressourcen zielgerichtet einsetzen, den Patch-Management-Prozess optimieren und die Sicherheitseffektivität insgesamt steigern. Mit diesem Ansatz werden schwerwiegende Schwachstellen sofort behoben, was das Risiko von Ransomware und anderen Sicherheitsverletzungen erheblich verringert – und somit eine robuste Verteidigung gegen eine komplexe Bedrohungslage sicherstellt.

Aktiver Bedrohungskontext

Verbessern Sie Ihre IT-Sicherheit, indem Sie kritische Schwachstellen mit einem fortschrittlichen Vulnerability Risk Rating (VRR)-System priorisieren. Diese Beurteilung geht über die traditionellen CVSS-Scores hinaus, da sie auch reale Risikobewertungen enthält. Unser VRR-System priorisiert Patches basierend auf detaillierten Erkenntnissen über die Risiken durch Angreifer, einschließlich Informationen über Exploits und Ransomware-bezogene Schwachstellen. Gestützt auf qualitativ hochwertige Daten und die fachkundige Validierung durch Penetrationstest-Teams steuert das VRR-System die Abhilfemaßnahmen effektiv und verstärkt Ihren Schutz vor aktiven und potenziellen Bedrohungen erheblich.

Risikobasierte Bereitstellung

Mit zunehmender Anzahl von Schwachstellen veröffentlichen Hersteller häufiger spontane Updates, um diese zu beheben. Dies ist entscheidend für die Minimierung von Risiken, insbesondere bei Zero-Day-Exploits oder öffentlicher Bekanntgabe von Exploits. Die Abstimmung dieser außerplanmäßigen Updates

mit den üblichen monatlichen Wartungsintervallen der Unternehmen gestaltet sich schwierig, was dazu führen kann, dass Sicherheitslücken trotz verfügbarem Patch über Wochen hinweg bestehen bleiben.

Die Funktion „Risikobasierte Bereitstellung“ unterstützt mehrere parallele Bereitstellungsaufgaben: regelmäßige monatliche Wartungszyklen, wöchentliche Prioritäts-Updates und sofortige Verteilung von Zero-Day-Patches. Dies ermöglicht ein automatisiertes Update-Management, das die Systeme stets mit den neuesten Patches versorgt – unabhängig vom Zeitpunkt der Veröffentlichung.

„63 % der IT- und Sicherheitsexperten geben an, dass isolierte Daten die Reaktionszeiten im Sicherheitsbereich verlangsamen.“⁷

Überwinden der Hürden zwischen IT und Sicherheit

Schaffen Sie Gleichberechtigung zwischen IT- und Sicherheitsteams, indem Sie beiden Teams den gleichen Zugang zu wichtigen Informationen wie SLA-Tracking und risikobasierten Informationen ermöglichen. Dies fördert eine ganzheitliche Sichtweise und eine gemeinsame Sprache, die

schnelle und effektive funktionsübergreifende Maßnahmen erleichtert. Der Austausch von Erkenntnissen zur Zuverlässigkeit von Patches, die aus Crowdsourcing- und Telemetriedaten gewonnen werden, ermöglicht proaktive Bewertungen und verhindert die Verteilung fehlerhafter Patches. Diese Strategie verbessert die Koordination und stärkt die Sicherheitslage des Unternehmens.

Von On-Premises-Lösungen zur Cloud

Starten Sie Ihre Umstellung vom On-Premise-Patch-Management in die Cloud mit Ivanti Neurons for Patch Management. Mit unserer Cloud-nativen Lösung können Sie die Umstellung in die Cloud in Ihrem eigenen Tempo vornehmen, ohne dass Sie bestehende Systeme vollständig ersetzen müssen. Die Migrationserfahrung von Ivanti bietet einen umfassenden Überblick sowohl über die bereits in der Cloud verwalteten Geräte als auch über die Geräte, die weiterhin mit den On-Premise-Patch-Management-Lösungen von Ivanti verwaltet werden.

Zuverlässigkeit von Patches

Die Zuverlässigkeit von Patches ist entscheidend für die Integrität und Sicherheit des Systems. Ivanti nutzt Meinungsumfragen, anonymisierte Implementierungsdaten und fortschrittliche Tests, um die Wirksamkeit und Sicherheit von Patches vor deren Implementierung zu bewerten. Der Ivanti Neurons Agent konfiguriert und verteilt eigenständig getestete Patches auf Tausende von Geräten und erkennt dabei frühzeitig potenzielle Probleme. IT-Teams können

fundierte Patching-Entscheidungen treffen, die das Risiko von Fehlern minimieren und gleichzeitig die Stabilität und Leistung der IT-Umgebung verbessern. Diese Methode reduziert Ausfallzeiten und sorgt für einen kontinuierlichen Schutz vor Schwachstellen.

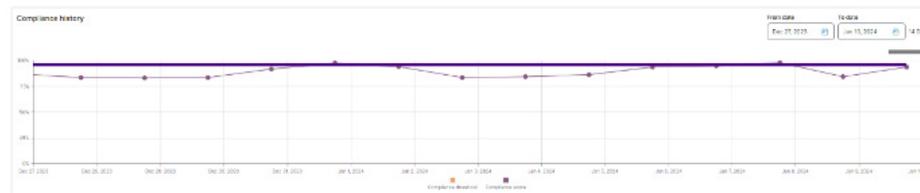
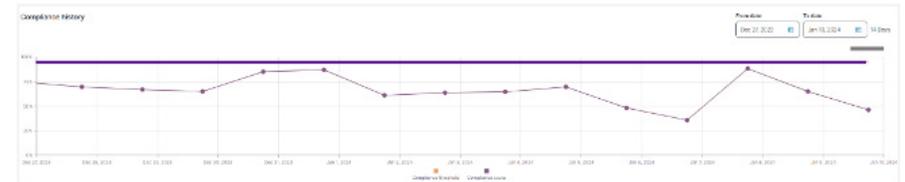
Plattformübergreifendes Patch-Management

Plattformübergreifendes Patch-Management ist essentiell, um Sicherheitsstandards in heterogenen IT-Umgebungen aufrechtzuerhalten, und effizientes und proaktives IT-Sicherheitsrisikomanagement zu ermöglichen. Ivanti Neurons for Patch-Management unterstützt Windows, macOS und Linux und ermöglicht das Management von Patches für Betriebssysteme sowie Anwendungen von Drittanbietern aus einer einheitlichen Oberfläche.

Ändern der Art und Weise, wie wir messen: „Expositionszeit“

Auf der Jagd nach SLAs:

Es werden fast täglich Updates veröffentlicht. SLAs zu erfüllen ist so nahezu unmöglich.



Die Verwendung einer zentralen Management-Plattform sorgt für einheitliche Sicherheitsrichtlinien und steigert die betriebliche Effizienz, ohne dass zwischen verschiedenen Patch-Management-Systemen gewechselt werden muss. Die Lösung reduziert die Komplexität und das Risiko von Fehlern und bietet umfassenden Schutz sowie volle Transparenz für alle Endgeräte. Durch die schnelle Identifizierung von Schwachstellen und Inkonsistenzen verhindert dieser umfassende Ansatz Sicherheitsverletzungen, reduziert Ausfallzeiten und Wiederherstellungskosten und schützt die Assets des Unternehmens.

Messen der tatsächlichen Risiken:

Risikobasierte KPIs ermöglichen es den Teams, sich auf das tatsächliche Risiko zu konzentrieren und gleichzeitig die Einhaltung von SLAs sicherzustellen.

Compliance-Reporting

Das automatisierte System von Ivanti konzentriert sich auf risikobasierte KPIs, die reale Risiken widerspiegeln. Es stellt sicher, dass alle Patches dokumentiert sind und gesetzlichen Standards entsprechen, wodurch das Risiko einer Nichteinhaltung von Vorschriften erheblich reduziert wird. Das System passt das Patch-Management an die Sicherheitsanforderungen an, indem es die SLAs auf das Release-Datum des Updates und nicht auf die üblichen IT-Betriebszeitpläne bezieht. IT-Abteilungen erhalten so auf einen Blick ein realistisches Bild davon wie lange die Beseitigung bekannter Sicherheitslücken tatsächlich dauert ohne die Einhaltung von SLAs mühselig für einzelne Patches ermitteln zu müssen.



Über Ivanti

Ivanti steigert und sichert Everywhere Work, damit Menschen und Unternehmen erfolgreich sein können. Wir sorgen dafür, dass die Technologie für die Menschen arbeitet, und nicht umgekehrt. Die Mitarbeitenden von heute nutzen eine breite Palette von Firmen- und Privatgeräten, um über mehrere Netzwerke auf IT-Anwendungen und Daten zuzugreifen und so produktiv zu bleiben, egal wo und wie sie arbeiten. Ivanti ist das einzige Technologieunternehmen, das alle IT-Assets und Endgeräte in einem Unternehmen findet, verwaltet und schützt. Mehr als 40.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um ihren Mitarbeitenden ein hervorragendes digitales Erlebnis zu bieten und die Produktivität und Effizienz ihrer IT- und Sicherheitsteams zu verbessern. Bei Ivanti sind wir bestrebt, ein Umfeld zu schaffen, in dem alle Perspektiven gehört, respektiert und geschätzt werden, und wir engagieren uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten. Weitere Informationen finden auf [ivanti.com](https://www.ivanti.com)

ivanti neurons

Für weitere Informationen oder um Ivanti zu kontaktieren, besuchen Sie bitte [ivanti.de](https://www.ivanti.de).

1. IBM, „Cost of a Data Breach Report 2024,“ 2024. <https://www.ibm.com/reports/data-breach>
2. Verizon, „2024 Data Breach Investigations Report“, 2024. <https://www.verizon.com/business/resources/reports/dbir/>
3. Google, „A Year in Review of Zero-Days Exploited In-the-Wild in 2023,“ März 2024. <https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends>
4. Richard Fang, Rohan Bindu, Akul Gupta, Qiusi Zhan, Daniel Kang, „Teams of LLM Agents can Exploit Zero-Day Vulnerabilities,“ 2. Juni 2024. <https://arxiv.org/abs/2406.01637>.
5. Ivanti, „Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace,“ 7. Oktober 2021. <https://www.ivanti.com/resources/v/doc/ivi/2634/712cff539c8a>
6. Securin, „Ransomware Report 2023 Year in Review,“ 2024. <https://www.securin.io/ransomware-report-2023-year-in-review-download/>
7. Ivanti, „Report zum Stand der Cybersicherheit 2024“, 2024. <https://www.ivanti.com/de/resources/research-reports/state-of-cybersecurity-report>