Ivanti Neurons for Patch Management

Reduce la exposición y el riesgo de amenazas priorizando y corrigiendo las vulnerabilidades.

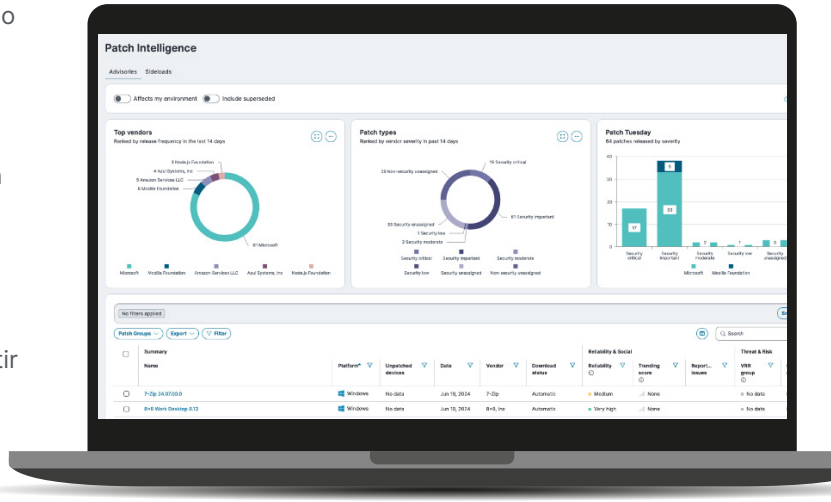
Ivanti Neurons for Patch Management es una solución nativa de la nube que proporciona inteligencia procesable y visibilidad de riesgos de dispositivos en Windows, macOS, Linux y aplicaciones de terceros. Prioriza y remedia las vulnerabilidades con información sobre la exposición al riesgo activo, la fiabilidad de los parches y la conformidad de los dispositivos. Protégete contra toda una amplia gama de amenazas, incluyendo el ransomware.

Gestión de parches basada en el riesgo

Los ataques de ransomware aumentan en frecuencia y gravedad cada año, con efectos devastadores sobre las empresas. Las investigaciones estiman que el coste medio total de una violación de datos es de 4,88 millones de dólares - un 10 % más que en 2023 y el mayor aumento desde la pandemia.[1]

Los ataques seguirán aumentando a medida que la tecnología y la inteligencia artificial avancen. El Ransomware como Servicio (RaaS) permite a casi cualquier persona lanzar un ataque - sin conocimientos de seguridad o experiencia en codificación. Un aumento en las vulnerabilidades conlleva un mayor riesgo; la explotación de estas ha crecido un 180 % año tras año.[2] Las investigaciones de Google revelan que los exploits de día cero han subido cada año un 50 %.[3] Aún más preocupante, la era de los ataques con IA ya está aquí. Investigadores de la Universidad de Illinois formaron a agentes de IA para que hackear sitios web de forma autónoma, con el fin de descubrir y explotar vulnerabilidades de día cero.[4]

Aplicar parches para corregir vulnerabilidades y exposiciones comunes es una de las medidas más efectivas que una empresa puede tomar para combatir los ataques de ransomware. Lamentablemente, el 71 % de los profesionales de TI y Seguridad considera la aplicación de parches excesivamente compleja y laboriosa. [5] Esto se debe, posiblemente, al abrumador volumen de vulnerabilidades. La Base de Datos Nacional de Vulnerabilidades (NVD) de Estados Unidos registra más de 230.000 vulnerabilidades. Aunque solo un pequeño porcentaje está relacionado con el ransomware, y aún menos son los exploits activos, identificar cuáles representan el mayor riesgo para tu organización puede resultar complicado.



Ivanti Neurons for Patch Management proporciona información procesable sobre amenazas y sobre la fiabilidad de los parches, así como visibilidad de los riesgos de los dispositivos en Windows, MacOS, Linux y aplicaciones de terceros. Esta información clave permite a los equipos de TI priorizar y corregir las vulnerabilidades que plantean un mayor riesgo para tu empresa. Al aprovechar Ivanti Neurons for Patch Management para aumentar la eficiencia y la eficacia de sus esfuerzos de aplicación de parches, las empresas pueden protegerse mejor contra filtraciones de datos, ransomware y otras amenazas derivadas de vulnerabilidades en el software.

Características y funciones clave

Priorización basada en los riesgos

Ivanti Neurons for Patch Management utiliza una estrategia de priorización basada en los riesgos, para dirigirse primero a los parches que abordan las vulnerabilidades críticas, especialmente aquellas relacionadas con el ransomware. Al centrarse en los parches que mitigan los principales riesgos, los equipos de TI pueden asignar eficientemente los recursos a otras prioridades estratégicas, agilizar el proceso de gestión de parches y mejorar la eficacia de la seguridad. Este enfoque aborda rápidamente las vulnerabilidades graves, reduciendo significativamente el riesgo de ransomware y otras brechas de seguridad, manteniendo así una defensa sólida en un entorno de amenazas complejo.

Contexto de amenazas activas

Mejore tu seguridad de TI priorizando las vulnerabilidades críticas con un sistema avanzado de Clasificación de Riesgos de Vulnerabilidad (VRR). Este sistema supera las puntuaciones CVSS tradicionales al incluir evaluaciones de riesgos en situaciones reales. Nuestro sistema VRR clasifica los parches utilizando información detallada sobre riesgos adversos, como inteligencia sobre exploits y vulnerabilidades relacionadas con el ransomware. Impulsado por datos de alta calidad y validación experta de los equipos de pruebas de penetración, el sistema VRR orienta eficazmente los esfuerzos de reparación, fortaleciendo de manera considerable sus defensas contra amenazas activas y potenciales.

Deploy by Risk - Despliega según el riesgo

A medida que aumentan las vulnerabilidades, los proveedores lanzan constantemente actualizaciones para solucionarlas. Esto es crucial para mitigar los riesgos, en particular con exploits de día cero o divulgaciones públicas. Sin embargo, alinear estas actualizaciones continuas con los calendarios de mantenimiento mensuales típicos de las empresas es desafiante, ya que deja brechas de seguridad durante semanas.

La función Deploy by Risk admite tareas de implementación múltiples y paralelas: mantenimiento periódico mensual, actualizaciones semanales prioritarias y parches inmediatos de día cero. Esto permite la gestión automática de las actualizaciones que mantiene los sistemas al día con los últimos parches, independientemente del momento de su lanzamiento.

«El 63 % de los profesionales de TI y Seguridad afirman que los datos en silos ralentizan los tiempos de respuesta de seguridad».[7]

Rompiendo las barreras entre TI y Seguridad

Crea paridad entre los equipos de TI y de seguridad ofreciendo el mismo acceso a información crucial como el seguimiento de SLA y la inteligencia basada en riesgos. Esto fomenta una visión global y un lenguaje común que promueve acciones interfuncionales rápidas y eficaces. Un enfoque unificado reduce las discrepancias y permite coordinar las respuestas a las partes interesadas. El intercambio de información sobre la fiabilidad de los parches, obtenida a partir de datos de fuentes colectivas y telemetría de despliegue, permite realizar evaluaciones proactivas y evitar implementaciones fallidas para garantizar el cumplimiento de los acuerdos de nivel de servicio. Esta estrategia mejora la coordinación y refuerza la postura de seguridad de la empresa.

Del on-premise a la nube

Inicia tu viaje desde la gestión on-prem de parches hacia la nube con Ivanti Neurons for Patch Management. Nuestra solución en la nube te permite realizar la transición a tu propio ritmo, en lugar de verte obligado a «extraer y reemplazar». La experiencia en migración de Ivanti proporciona visibilidad de los dispositivos gestionados en la nube junto a los gestionados con soluciones de gestión de parches Ivanti en tus instalaciones.

Fiabilidad de los parches

La fiabilidad de los parches es crucial para la integridad y seguridad del sistema. Ivanti utiliza las opiniones de los usuarios, los datos anonimizados de implementación y las pruebas avanzadas para evaluar la eficacia y la seguridad de los parches antes de su implantación. El Agente de Ivanti Neurons configura y distribuye de forma autónoma parches probados a miles de dispositivos con rapidez, identificando posibles problemas temprano. Los equipos de TI pueden tomar decisiones informadas sobre la aplicación de parches, minimizando el riesgo de fallos y mejorando la estabilidad y el rendimiento del entorno de TI. Este método reduce el tiempo de inactividad y garantiza una protección continua contra las vulnerabilidades.

Heterogéneo en una sola plataforma

Una plataforma heterogénea es crucial para mantener altos estándares de seguridad en diversos entornos de TI, favoreciendo una gestión eficaz y proactiva de los riesgos de seguridad. Ivanti Neurons for Patch Management es compatible con Windows, MacOS, Linux y aplicaciones de terceros, brindando una experiencia de gestión unificada que simplifica la supervisión de varios sistemas y mejora la productividad.

El uso de una única plataforma proporciona políticas de seguridad consistentes y mejora la eficiencia operativa, sin tener que cambiar entre distintos sistemas de gestión de parches. Esto reduce la complejidad y el riesgo de descuido, garantizando protección y visibilidad completas en todos los endpoints. Al identificar rápidamente las vulnerabilidades y las incoherencias, este enfoque integral previene las brechas, reduce el tiempo de inactividad y los costes de recuperación y salvaguarda los activos de la empresa.

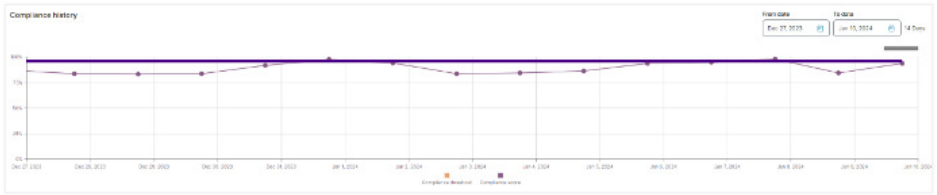
Informes de conformidad

Los informes de conformidad en la gestión de parches son cruciales. El sistema automatizado de Ivanti se centra en KPIs basados en riesgos que reflejan los riesgos del mundo real. Garantiza que todos los parches estén documentados y cumplan con las normativas, reduciendo en gran medida el incumplimiento. El sistema alinea la gestión de parches con las necesidades de seguridad, basando los acuerdos de nivel de servicio (SLA) en la fecha de lanzamiento de la actualización en lugar de en los plazos operativos típicos de TI. Esto es fundamental, ya que los equipos de seguridad enfrentan desafíos con ciclos continuos de parches. Al recalibrar los SLA desde el punto de vista de la exposición a vulnerabilidades, los departamentos de TI pueden cumplir mejor con los requisitos de seguridad mientras gestionan las demandas operativas, reforzando el marco de seguridad general de la empresa.

Cambiando la forma de medir: «Tiempo de exposición»

Persiguiendo los números:

Las actualizaciones se lanzan continuamente. Es casi imposible lograr el cumplimiento.



Mide lo que importa:

Un KPI basado en riesgos permite a los equipos centrarse en los riesgos reales y lograr el cumplimiento.

Acerca de Ivanti

Ivanti mejora y asegura el «Everywhere Work» para que las personas y las empresas puedan prosperar. Hacemos que la tecnología funcione para las personas, no al revés. Los empleados actuales utilizan una amplia gama de dispositivos corporativos y personales para acceder a aplicaciones y datos de TI a través de múltiples redes y seguir siendo productivos dondequiera y comoquiera trabajen. Ivanti es la única empresa tecnológica que encuentra, gestiona y protege cada activo y endpoint TI y de una empresa. Más de 40.000 clientes, incluidas 85 de las 100 empresas de Fortune, confían en Ivanti para que puedan ofrecer a sus empleados una excelente experiencia digital, mejorando la productividad y la eficiencia de los equipos de TI y Seguridad. En Ivanti, nos esforzamos por crear un entorno en el que se escuchen, respeten y valoren todas las perspectivas, y estamos comprometidos con un futuro más sostenible para nuestros clientes, socios, empleados y el planeta. Para más información, visita ivanti.com

ivanti neurons

Para más información o para contactar con Ivanti, visita ivanti.com.

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», marzo de 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 de junio de 2024. https://arxiv.org/abs/2406.01637.
5. Ivanti, «Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace», 7 de octubre de 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, «2024 State of Cybersecurity Report», 2024. https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report