Ivanti Neurons for Patch Management

Priorizar y remediar las vulnerabilidades de manera eficiente

Ivanti Neurons for Patch Management es una solución de gestión de Patch en la nube con inteligencia procesable sobre la exposición al riesgo activo, la fiabilidad de los Patch y el cumplimiento de los dispositivos, la salud y el riesgo que ayuda a las empresas a protegerse mejor contra las amenazas, incluido el ransomware.

Gestión de Patch basada en el riesgo

Los ataques de ransomware son cada año más frecuentes y graves. El impacto en las empresas es devastador. Las investigaciones sitúan el coste total medio de una brecha de ransomware en 4,62 millones de dólares - sin tener en cuenta el coste del rescate.[1]

Por desgracia, es probable que la situación empeore antes de que mejore. El Ransomware como servicio (RaaS) permite a casi cualquier persona lanzar un ataque - sin conocimientos de seguridad o experiencia en codificación. Además, el número de Vulnerabilidades y Exposiciones Comunes (CVEs) en las redes casi se cuadruplicó en 2020.[2] Peor aún, los atacantes de ransomware se dirigen cada vez más a las empresas medianas para evitar la atención mediática que supone atacar a las grandes empresas.[3]

La aplicación de Patch para corregir los CVE es una de las mejores cosas que puede hacer una empresa para hacer frente a los ataques de ransomware.

Lamentablemente, el 71 % de los profesionales de TI y seguridad consideran que la aplicación de Patch es demasiado compleja y requiere mucho tiempo.[4] Es posible que esto se deba al abrumador volumen de vulnerabilidades que existen. En la base de datos nacional de vulnerabilidades (NVD) de Estados Unidos figuran más de 100.000 vulnerabilidades. Mientras que solo un pequeño porcentaje está relacionado con el

ransomware, y un porcentaje aún menor son ataques activos, identificar cuáles representan el mayor riesgo para su empresa puede ser complicado. Entre 2018 y 2020, utilizando la puntuación CVSS v3, si se parchean solo las vulnerabilidades críticas, la cobertura contra el ransomware sería solo de un 35 %.[2]

Ivanti Neurons for Patch Management ofrece información sobre amenazas, fiabilidad de los Patch y visibilidad del riesgo de los dispositivos que permite a los equipos de TI priorizar y corregir las vulnerabilidades que suponen un mayor peligro para su empresa. Al aprovechar Ivanti Neurons for Patch Management para aumentar la eficiencia y la eficacia de sus esfuerzos de aplicación de Patch, las empresas pueden protegerse mejor de las filtraciones de datos, el ransomware y otras amenazas derivadas de las vulnerabilidades del software.

Características y capacidades principales

Patch proactivos contra las amenazas activas

Dar prioridad a la corrección en función del riesgo de los atacantes, con información sobre los riesgos conocidos y el contexto de las amenazas para las vulnerabilidades, incluidos los vínculos con el ransomware. La Calificación de Riesgo de Vulnerabilidad (VRR) de Ivanti le permite adoptar medidas prioritarias basadas en el riesgo en lugar de la calificación CVSS, ya que tiene en cuenta los datos de vulnerabilidad y amenaza de mayor fidelidad, además de la validación humana de los ataques por parte de los equipos de pruebas de penetración.

Consigue unos acuerdos de nivel de servicio más rápidos gracias a la fiabilidad de los Patch y a la información sobre tendencias

Ahorre tiempo y evite el fracaso en la instalación de Patch gracias a la información sobre la fiabilidad de los Patch obtenida de los datos sobre el sentimiento social y la telemetría anónima de la instalación de Patch. Esta información le permite evaluar los Patch en función de su fiabilidad en aplicaciones del mundo real antes de desplegarlos. Además, el seguimiento de los acuerdos de nivel de servicio (SLA), que proporciona visibilidad sobre los dispositivos que se acercan a los SLA, le permite tomar medidas sobre los dispositivos antes de que se incumplan.

Transición de la gestión de Patch en las instalaciones a la nube

Inicie su paso de la gestión de Patch en la nube con la fuerza de la tecnología de Patch de Ivanti. Ivanti Neurons for Patch Management es una solución nativa de la nube que permite la transición de la gestión de Patch en la nube a su propio ritmo en lugar de verse obligado a “extraer y sustituir”. Estas transiciones graduales son posibles gracias a la experiencia de panel único de la solución, que ofrece visibilidad de los dispositivos que gestiona en la nube junto con los gestionados a través de las soluciones de gestión de Patch de Ivanti.

Agilizar los procesos de gestión de Patch

Mejora la eficiencia operativa eliminando la necesidad de saltar entre soluciones de gestión de Patch aisladas. Ivanti Neurons for Patch Management ofrece visibilidad de todos los puntos finales de su entorno a través de un único panel. La información avanzada sobre vulnerabilidades y la inteligencia de Patch mejoran aún más la eficiencia operativa al permitirte priorizar de manera efectiva los esfuerzos de parcheo para que puedas concentrarte únicamente en lo que realmente importa. Además, cuando llega el momento de aplicar un parche, las configuraciones de Patch autónomas desplegadas en el agente Ivanti Neurons en los dispositivos distribuyen Patch minuciosamente probados a miles de máquinas en cuestión de minutos.

Sobre Ivanti

Ivanti hace que sea posible trabajar desde “cualquier parte”. En el teletrabajo, los empleados utilizan un sinfín de dispositivos para acceder a las redes y aplicaciones de TI, y a los datos a través de varias redes para seguir siendo productivos mientras trabajan desde cualquier lugar. La plataforma de automatización Ivanti conecta las soluciones líderes del sector de gestión unificada de puntos finales, seguridad de confianza cero y gestión de servicios empresariales, proporcionando un panel único para que las empresas puedan autocurar y autoproteger los dispositivos, y autoservir a los usuarios finales. Más de 40.000 clientes, entre los que se encuentran 96 de las 100 empresas de la lista Fortune, han optado por Ivanti para descubrir, gestionar, proteger y dar servicio a sus activos de TI desde la nube hasta el extremo, y ofrecer excelentes experiencias de usuario final a los empleados, dondequiera y comoquiera que trabajen. Para más información, visita 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 de julio de 2021. https://www.ibm.com/downloads/cas/OJDVQGRY
2. RiskSense, Cyber Security Works, “Ransomware Through the Lens of Threat and Vulnerability Management”, 9 de noviembre de 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 de octubre de 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
4. Ivanti, “Desafíos de la gestión de Patch: Resultados de la encuesta y perspectivas a medida que las empresas pasan al lugar de trabajo en todas partes”, 7 de octubre de 2021. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges