Checklist para la corrección de vulnerabilidades

Tus endpoints se multiplican: portátiles, servidores, máquinas virtuales, dispositivos móviles... y los usuarios trabajan desde muchos lugares distintos. Se trata de una superficie de riesgo considerable que hay que cubrir. Aunque la gestión de parches mantiene actualizados los endpoints y ayuda a reforzar su seguridad, acelerar la aplicación de parches, especialmente de aquellos críticos, debería ser una prioridad. Al dotar a los equipos de gestión de parches de un acceso dinámico a los datos sobre vulnerabilidades, los equipos de TI pueden identificar, priorizar y resolver las vulnerabilidades de forma proactiva, acelerar la respuesta, mejorar la resistencia y mantener el cumplimiento.

34 %
más de vulnerabilidades explotadas

60 %
de las infracciones se deben a vulnerabilidades con parches disponibles que no se aplicaron

24 días
es el tiempo medio que se tarda en descubrir una infracción

Fuente: 2025 Verizon Data Breach Report

Importación automatizada de datos sobre vulnerabilidades
Acceso dinámico y continuo a los datos sobre vulnerabilidades, mayor visibilidad para priorizar los parches en función de los datos y una aplicación de parches más rápida, especialmente en el caso de vulnerabilidades críticas.

Aplicación de parches basada en el riesgo
Prioriza basándote en el CVE y la puntuación CVSS y aplica primero los parches críticos.

Evaluación de parches impulsada por IA
Utiliza la IA para evaluar la estabilidad de las actualizaciones KB de Windows y asegúrate de desplegar solo los parches efectivos.

Un panel de gestión de parches intuitivo
Permite a los técnicos identificar vulnerabilidades y desplegar parches a gran escala en todos los endpoints para reducir la superficie de ataque.

Alertas y notificaciones instantáneas
Recibe al instante notificaciones por correo electrónico, Slack, SMS y otros canales sobre vulnerabilidades de alta prioridad y parches fallidos para garantizar su corrección.

Visibilidad centralizada en una única consola
Mejora la precisión y la eficacia gracias a una mayor visibilidad sobre los endpoints, los parches y su estado. Asegúrate de corregir rápidamente los parches fallidos o rechazados, especialmente cuando se trata de vulnerabilidades críticas.

Un cumplimiento de la normativa más sencillo
Garantiza el cumplimiento de la HIPAA, RGPD, NIST, PCI DSS y otras normas de seguridad.

Herramientas de corrección integradas
Herramientas integradas como el terminal remoto, el editor de registro y el acceso remoto permiten una aplicación de parches más eficaz.

Más información en https://www.ninjaone.com/es/gestion-de-vulnerabilidades/

Prueba gratuita