Elenco di controllo per la correzione delle vulnerabilità

I tuoi endpoint si moltiplicano: laptop, server, virtual machine, dispositivi mobili... e gli utenti lavorano da molti luoghi diversi. È una superficie di rischio molto ampia da coprire. Sebbene il patch management mantenga aggiornati gli endpoint e contribuisca a rafforzarne la sicurezza, rendere il patching il più veloce possibile, soprattutto per le patch critiche, dovrebbe essere una priorità. Dotando i team di patch management di un accesso dinamico ai dati sulle vulnerabilità, i team IT possono identificare, organizzare per priorità e risolvere le vulnerabilità in modo proattivo, accelerare la risposta, migliorare la resilienza e mantenere la conformità.

34%
di aumento delle vulnerabilità sfruttate

60%
delle violazioni riguardano vulnerabilità per le quali erano disponibili patch che non erano state applicate

24 giorni
tempo medio di scoperta di una violazione

Fonte: 2025 Verizon Data Breach Report

Importazione automatica dei dati sulle vulnerabilità
Accesso dinamico e continuo ai dati sulle vulnerabilità, maggiore visibilità per definire la priorità delle patch in base ai dati, oltre a un patching più rapido soprattutto per le vulnerabilità critiche.

Patching basato sul rischio
Organizza le priorità basandoti sulle informazioni CVE e CVSS, in modo da occuparti prima delle patch più critiche.

Sentiment delle patch guidato dall'AI
Sfrutta il sentiment delle patch guidato dall'AI per valutare la stabilità degli aggiornamenti KB di Windows. Questo assicura una distribuzione consapevole delle patch e che le patch note come non funzionanti non vengano distribuite.

Dashboard del patching intuitiva
Consenti ai tecnici di identificare le vulnerabilità e di distribuire le patch anche su larga scala a tutti gli endpoint, per ridurre la superficie di attacco.

Avvisi e notifiche istantanei
Ricevi istantaneamente notifiche via e-mail, Slack, SMS e altri canali, sulle vulnerabilità ad alta priorità e sulle patch non riuscite, che ti permetteranno di agire e di correggere i problemi.

Visibilità centralizzata attraverso un'unica console
Migliora l'accuratezza dei dati e guadagna efficienza con una visibilità completa su endpoint, patch e stato delle patch. Assicurati che le patch non riuscite o rifiutate vengano rapidamente corrette, soprattutto per le vulnerabilità critiche.

Raggiungimento e mantenimento della conformità normativa
Garantisci la conformità a HIPAA, GDPR, NIST, PCI DSS e ad altri standard di sicurezza.

Strumenti di correzione integrati
Strumenti integrati come il terminale remoto, l'editor del registro di sistema e l'accesso remoto facilitano flussi di lavoro di patching più efficaci.

Per saperne di più: https://www.ninjaone.com/it/gestione-delle-vulnerabilita/

Prova gratuita