

Check-list pour la remédiation des vulnérabilités



ninjaOne®

Qu'il s'agisse d'ordinateurs portables, de serveurs, de machines virtuelles ou d'appareils mobiles, vos terminaux se multiplient et vos utilisateurs sont répartis dans le monde entier. La surface de risque à couvrir est immense. Si la gestion des correctifs permet certes de maintenir les terminaux à jour et de renforcer leur sécurité, priorité devrait être donnée à en accélérer le rythme d'application, en particulier quand il s'agit de correctifs critiques. En dotant les équipes en charge de la gestion des correctifs d'un accès dynamique aux données sur les vulnérabilités, vous leur permettez d'identifier, de hiérarchiser et de résoudre les vulnérabilités de manière proactive, d'accélérer le rythme des réponses aux vulnérabilités, de renforcer la résilience et de maintenir la conformité.

34 %

d'augmentation
des vulnérabilités
exploitées

60 %

des failles de sécurité impliquent
des vulnérabilités pour lesquels
des correctifs étaient disponibles
mais non appliqués

24 jours

c'est le délai moyen
pour découvrir une
faille de sécurité

Source : [2025 Verizon Data Breach Report](#)

Importation automatisée de données sur les vulnérabilités

Accès dynamique et continu aux données sur les vulnérabilités, meilleure visibilité pour une priorisation des correctifs basée sur des données, et des correctifs accélérés, en particulier pour les vulnérabilités critiques.

Application de correctifs basée sur les risques

Donnez la priorité aux informations liées aux CVE et aux CVSS afin de traiter en premier lieu les correctifs les plus critiques.

Ressenti par rapport au correctif, généré par l'IA

Tirez parti de l'intelligence artificielle pour évaluer la stabilité des mises à jour de la base de connaissances Windows. Cela permet de déployer les correctifs en toute connaissance de cause et de s'assurer que les mauvais correctifs connus ne sont pas déployés.

Tableau de bord intuitif pour l'application des correctifs

Donnez la possibilité aux techniciens d'identifier les vulnérabilités et de déployer des correctifs à grande échelle sur tous les terminaux afin de réduire votre surface d'attaque.

Alertes et notifications instantanées

Recevez instantanément des notifications par e-mail, Slack, SMS et autres canaux sur les vulnérabilités hautement prioritaires et sur les correctifs qui n'ont pas été appliqués, pour une remédiation assurée.

Visibilité centralisée via une console unique

Améliorez la précision et gagnez en efficacité grâce à la visibilité sur les terminaux, les correctifs et l'état de ces derniers. Veillez à ce que les correctifs qui ont échoué ou qui ont été rejetés soient rapidement corrigés, en particulier pour les vulnérabilités critiques.

Mise en conformité avec la réglementation

Assurez la conformité aux normes HIPAA, RGPD, NIST, PCI DSS et autres normes de sécurité.

Outils de remédiation intégrés

Des outils intégrés tels que le terminal à distance, l'éditeur de registre et l'accès à distance facilitent l'efficacité des flux de travail en matière d'application des correctifs.

Pour en savoir plus : <https://www.ninjaone.com/fr/gestion-des-vulnerabilites/>

Essai gratuit