Vulnerability Remediation Checklist

Your endpoints are multiplying - laptops, servers, VMs, mobile devices – and your users are everywhere. That's a lot of risk surface to cover. While patch management keeps endpoints up-to-date and helps harden endpoint security, accelerating patching, especially for critical patches, should be a priority. Equipping patch management teams with dynamic access to vulnerability data helps IT teams proactively identify, prioritize, and resolve vulnerabilities, accelerate response, enhance resilience, and maintain compliance.

34%
increase in vulnerabilities exploited

60%
of breaches involve vulnerabilities for which patches were available but not applied

24 days
average time to discover a breach

Source: 2025 Verizon Data Breach Report

Automated vulnerability data imports
Dynamic and continuous access to vulnerability data, enhanced visibility for data-informed patch prioritization, and expedited patching, especially for critical vulnerabilities.

Risk-based patching
Prioritize CVEs and CVSS information to address the most critical patches first.

AI-driven patch sentiment
Leverage AI-driven patch sentiment to assess the stability of Windows KB updates. This ensures informed patch deployment and that known bad patches are not deployed.

Intuitive patching dashboard
Enable technicians to identify vulnerabilities and deploy patches at scale across all endpoints to reduce your attack surface.

Instant alerts and notifications
Instantly receive notifications via email, Slack, SMS and other channels of high priority vulnerabilities and failed patches for assured remediation.

Centralized visibility through a single console
Improve accuracy and gain efficiency with visibility into endpoints, patches, and patch status. Ensure failed or rejected patches are quickly remediated, especially for critical vulnerabilities.

Regulatory compliance enablement
Ensure compliance with HIPAA, GDPR, NIST, PCI DSS, and other security standards.

Integrated remediation tools
Integrated tools such as remote terminal, registry editor, and remote access facilitate more effective patching workflows.

Learn more at www.ninjaone.com/vulnerability-management/

Free trial