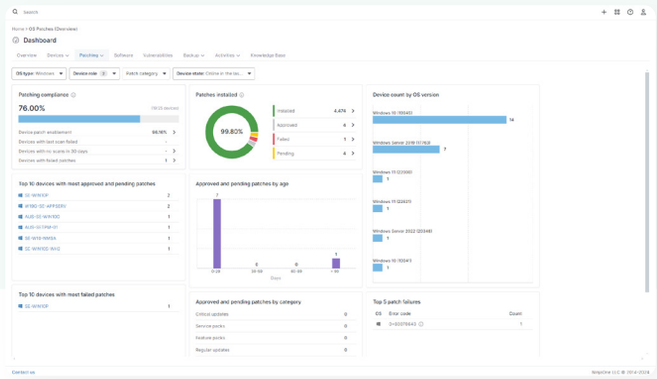
NinjaOne®

Autonomous Patch Management

Improve patch compliance with intelligent automation.



Protect any endpoint, anywhere

NinjaOne Autonomous Patch Management uses cloud-based, policy-driven automation and Patch Intelligence AI to continuously patch on-premises, remote, and hybrid endpoints — no VPN, domain, or network dependency required.

Reduce zero-day risk and avoid unstable patches

Patch Intelligence AI prioritizes vulnerabilities and automatically blocks high-risk or unstable updates, while granular controls enable rapid manual approvals for zero-day response — preventing outages without slowing remediation.

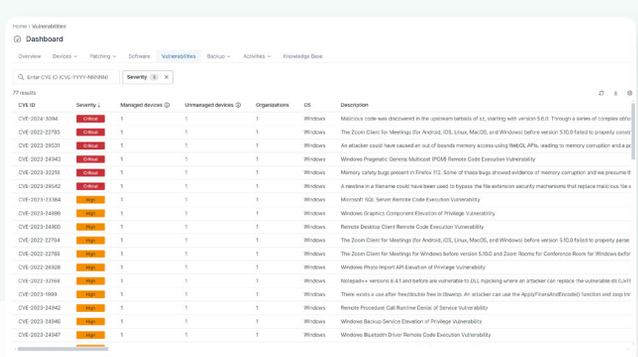
Autonomously patch OS and third-party applications

Automatically identify, evaluate, and deploy trusted patches across Windows, macOS, and Linux endpoints anywhere. Patch 8800+ third-party applications with zero-touch automation, accelerating remediation while maintaining consistent, reliable patching.

NinjaOne®

Vulnerability Management

Turn vulnerability intelligence into prioritized, automated remediation.



Accelerate remediation with intelligence

Accelerate vulnerability remediation using NinjaOne Vulnerability Importing and Patch Intelligence AI to deliver real-time risk insight, automated prioritization, and faster resolution.

Strengthen security posture with risk-based action

Improve security posture by prioritizing exploitable vulnerabilities, guiding remediation with intelligence-driven insights, and validating patch effectiveness through a unified, risk-based remediation approach.

Unify visibility and remediation workflows

Give IT and security teams centralized, real-time visibility into vulnerabilities and remediation status across your environment. Eliminate silos between detection and patching, enabling faster decisions and confident, coordinated response.