

AI-Powered Vulnerability Management and Autonomous Patching

ninjaOne®

Continuous vulnerability assessment with autonomous remediation

Together, Real-Time Assessment and Autonomous Patch Management eliminate the delay between vulnerability discovery and remediation. Continuous exposure intelligence, including Known Exploited Vulnerability (KEV) data, flows directly into risk-aware patch execution, reducing security risk while maintaining operational control.

KEY FEATURES

Continuous, scan-free vulnerability assessment

Eliminate periodic scans by continuously correlating live and last-known endpoint software state with real-time CVE and KEV intelligence. Identify newly disclosed vulnerabilities within minutes, even when devices are offline, without endpoint disruption or performance impact.

Risk-aware autonomous patch execution

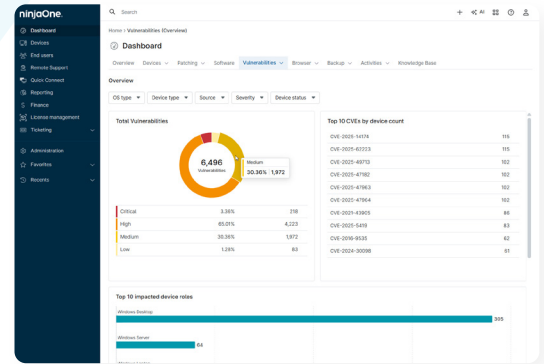
Patch Intelligence AI evaluates vendor advisories, community telemetry, and real-world deployment outcomes to identify unstable updates. Stable patches deploy automatically. Risky patches are paused before they create operational disruption.

Closed-loop remediation workflows

Leverage continuous vulnerability intelligence, including KEV indicators, and AI-powered patch management to prioritize and remediate the most urgent vulnerabilities first.

Compress exposure windows from weeks to minutes

By removing scan cycles and manual process delays, accelerate the time between vulnerability disclosure and effective remediation.



Better together

Pair Real-Time Assessment with NinjaOne Autonomous Patch Management to create a closed-loop remediation system. Vulnerability intelligence flows directly into AI-driven patch workflows accelerating remediation while reducing operational risk.

Closed-loop remediation

Eliminate handoffs between detection and execution. Identify risk and initiate remediation within the same operational system.

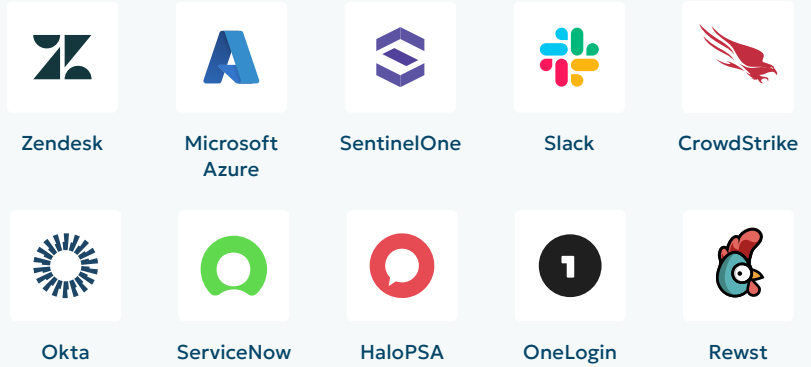
Risk-aware patch execution

Patch Intelligence AI evaluates real-world patch outcomes before deployment. Stable updates deploy automatically. Risky updates are paused accelerating remediation while protecting operational stability.

Real-time exposure tracking

Continuously monitor what has been remediated, what remains exposed, and which vulnerabilities are actively exploited in the wild using KEV intelligence.

NinjaOne Integrations



Manage

Monitor and manage every endpoint

Protect

Patch and back up endpoints

Support

Support every employee



SERVICES | WORKSTATIONS | LAPTOPS | TABLETS | SMARTPHONES | HOSTS | NETWORKS

NinjaOne Unified IT Operations Platform

Policy-Based Automation

Unified Reporting & Analytics

Multi-Tenant Architecture

API & Integrations

HUMAN-CENTERED AI

10-15

TOOLS REPLACED

“Before, I needed 10-15 different tools to execute what NinjaOne does in its centralized, single pane of glass.”

Vetcor

98%

CSAT SCORE

“I have never experienced the speed or knowledge of support the NinjaOne team exhibited with any other RMM vendor.”

InHouse Support

30%

LESS TIME FOR PATCHING

“We observed a 30% reduction in the time taken for patch deployments compared to our previous solution.”

Alabbar Group