

Autonomous Patch Management

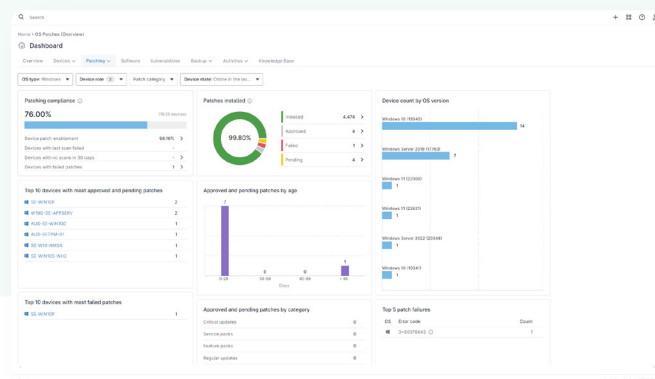
Improve patch compliance with intelligent automation.

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.

Vulnerability Management

Turn vulnerability intelligence into prioritized, automated remediation.

CVE ID	Severity	Managed devices	Unmanaged devices	Organizations	OS	Description
CVE-2022-3094	Critical	1	1	1	Windows	ActiveX code was discovered in the common version of .NET, starting with version 5.0.0. Through a series of complex calls...
CVE-2022-2793	Critical	1	1	1	Windows	The Zoom Client for Meetings (for Android, iOS, Linux, Mac OS, and Windows) before version 5.0.0 failed to properly control...
CVE-2022-29201	Critical	1	1	1	Windows	An attacker could have caused an out of bounds memory access using WebGL API, leading to memory corruption and a po...
CVE-2022-24343	Critical	1	1	1	Windows	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability
CVE-2022-32265	Critical	1	1	1	Windows	Memory safety bugs present in Firefox VTC. Some of these bugs allowed evidence of memory corruption and we presume t...
CVE-2022-29542	Critical	1	1	1	Windows	A newline in a filename could have been used to bypass the file extension security mechanisms that replace malicious file n...
CVE-2022-33944	Critical	1	1	1	Windows	Microsoft SQL Server Remote Code Execution Vulnerability
CVE-2022-34049	Critical	1	1	1	Windows	Windows Graphics Component Execution of Privilege Vulnerability
CVE-2022-34805	Critical	1	1	1	Windows	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2022-27754	Critical	1	1	1	Windows	The Zoom Client for Meetings (for Android, iOS, Linux, Mac OS, and Windows) before version 5.0.0 failed to properly parse...
CVE-2022-27765	Critical	1	1	1	Windows	The Zoom Client for Meetings (for Windows before version 5.0.0 and Zoom Rooms for Conference Room for Windows before...
CVE-2022-28428	Critical	1	1	1	Windows	Windows Photo Import API Elevation of Privilege Vulnerability
CVE-2022-32964	Critical	1	1	1	Windows	NetopSystem versions 6.4.1 and before are vulnerable to DLL hijacking where an attacker can replace the vulnerable dll (LanT...
CVE-2022-3999	Critical	1	1	1	Windows	There exists a use after free/buffer overflow in libpng. An attacker can use the Applet/Stream(Encoded) function and keep the...
CVE-2022-29442	Critical	1	1	1	Windows	Remote Procedure Call Runtime Error of Service Vulnerability
CVE-2022-28446	Critical	1	1	1	Windows	Windows Backup Service Elevation of Privilege Vulnerability
CVE-2022-28447	Critical	1	1	1	Windows	Windows Bluetooth Device Remote Code Execution Vulnerability

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.