vicarius

VS

ninjaOne

Beyond Patching: built for real Remediation

Unlike some vendors that deliver traditional patching and alerting, Vicarius drives real-world security action, automating asset discovery, context and risk-aware prioritization, automated remediation (including patchless protection), all within a unified, no-delay platform.

Vicarius key differentiators

Patchless Protection when needed most

Vicarius deploys in-memory mitigation around vulnerable applications, even when patches aren't available, immediately reducing exposure risk.

Unified scan to fix in one tool

Vicarius delivers discovery, context and risk-based prioritization, several remediation options, all in a single user-friendly platform, streamlining end-to-end vulnerability management.

Risk-smart Prioritization, not just severity

Vicarius enhances prioritization by blending environment and business context, exploit intelligence, and threat relevance, ensuring focus on what really matters.

Always-on exposure monitoring

Vicarius maintains continuous visibility and remediation across changing environments, unlike static, periodic scans.

Deep visibility into legacy & custom apps

Vicarius identifies vulnerabilities in legacy, third-party, and niche applications often missed by standard tools, ensuring no blind spots.

Automated fixes that slash manual load

Vicarius can cut remediation efforts by up to 80%, thanks to automation, including patching, scripting, and virtual mitigation, freeing teams to work on strategy.

How Vicarius compares to NinjaOne

Capabilities	vicarius	ninjaOne
Remediation built-in	Automated, in-platform remediation with scheduling, scripting, and guided patching	Offers agent-driven patch deployment workflows, but lacks integrated remediation, needs external tools to close the loop
Virtual Patching	Enables virtual patching for zero-days and unsupported software	Not supported
Cross-platform Support	Full patching for Windows, Linux, macOS, and over 10,000 third-party applications	Supports Windows, macOS, Linux, and ~120 third-party apps, coverage exists but is narrower
Agent-based & agentless modes	Offers both agent-based and agentless scanning for flexible deployment across asset types	Fully agent-based, cloud-native; no agentless scanning option reported
Real-time risk validation	Validates exploitability in live environments using telemetry, not simulated exploits	Identifies missing patches and CVEs (via ad-hoc scans) but does not validate real exploitability in real-time
Multi-tenancy for MSSPs	MSSP-friendly architecture with tenant isolation, delegated roles, and centralized control	Designed for MSPs, but reviews note challenges with organizational management complexity, multi-tenant usability is moderate
Workflow Automation	Unified platform for detection, prioritization, and remediation, minimizing tool sprawl	Automates patching with CVE/CVSS scoring, however, lacks unified detection-to-remediation workflow, separate tools or scripts still needed
Ease of deployment	Modern, cloud-native UI with fast onboarding and centralized console	Praised for intuitive UI and quick deployment with excellent support, however, scripting and policy setup may be non-trivial
Coverage depth	Covers vulnerabilities across system, app, network, and even patchless or legacy systems	Provides patch-centric coverage, but lacks deep exposure analytics and fails to address misconfigurations and legacy systems
Customer satisfaction	G2: 4.9 / Gartner: 4.8 praised for ease of use, performance, and support	G2: 4.7 / Gartner: 4.9 complaints around limited vulnerability scanning, reporting, and macOS support persist