vicarius

VS

AUTOMOX

Beyond patching, complete risk Remediation

Vicarius unifies vulnerability scanning, risk-based prioritization, and remediation into one platform. Unlike Automox, which relies on third parties and focuses mainly on patching, Vicarius delivers advanced protection, compliance readiness, and zero-day shielding, reducing tool sprawl, admin effort, and time to remediation across all applications and environments.

Vicarius key differentiators

Unified scanning and Remediation

Vicarius combines vulnerability scanning, contextual prioritization, and remediation in one platform, eliminating the need for separate tools and reducing operational complexity and cost.

Broad application coverage

Supports patching for both mainstream and over 10,000 applications, going beyond Automox's 580 third-party limit, ensuring coverage across diverse IT environments.

Compliance and Reporting built-In

Delivers robust compliance audits and detailed reporting to meet regulatory requirements, no reliance on external compliance tools.

Advanced zero-day protection

Includes zero-day shielding and runtime protection, (patchless protection) safeguarding systems before vendor patches are released.

Risk-based Prioritization

Prioritizes vulnerabilities based on contextual risk, not just CVSS severity, enabling teams to focus on the threats most likely to be exploited.

Lower total cost of ownership

By consolidating scanning, patching, and compliance into one platform, Vicarius reduces tool sprawl, licensing fees, and the overhead of managing multiple vendors.

How Vicarius compares to Automox

Capabilities	vicarius	AUTOMOX
Remediation built-in	Automated, in-platform remediation with scheduling, scripting, and guided patching	Relies mostly on patching; lacks advanced remediation workflows
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	Limited to ~580 third-party applications
Agent-based & agentless modes	Offers both agent-based and agentless scanning for flexible deployment across asset types	Primarily agent-based with cloud-native agent (no agentless mode)
Real-time risk validation	Validates exploitability in live environments using telemetry, not simulated exploits	Prioritization based solely on CVSS severity; no exploit-likelihood or contextual risk scoring=
Multi-tenancy for MSSPs	MSSP-friendly architecture with tenant isolation, delegated roles, and centralized control	Supports multi-tenant administration, flexible billing, centralized control for MSPs
Workflow Automation	Unified platform for detection, prioritization, and remediation, minimizing tool sprawl	Supports vulnerability sync; integrates with scanners like Tenable, Rapid7 for coordinated remediation
Ease of deployment	Modern, cloud-native UI with fast onboarding and centralized console	Lightweight cloud-native agent; no VPN or infrastructure needed (fast deployment)
Coverage depth	Covers vulnerabilities across system, apps, network, and even patchless or legacy systems	Focuses on patchable assets with limited compliance audits; lacks patchless coverage
Customer Satisfaction	G2: 4.9 / Gartner: 4.8 praised for ease of use, performance, and support	G2: 4.5 / Gartner: 4.6 – feedback cites delays, limited app coverage, and reliance on scripting