vicarius

VS

tenable

Built for Remediation, not just Reporting

Vicarius was purpose-built to help security teams take action, not just generate alerts. While Tenable stops at discovery, Vicarius delivers real-time, in-platform remediation that actually fixes vulnerabilities, no external tools or delays required.

Vicarius key differentiators

Built-In Remediation

Vicarius goes beyond detection, offering real-time, automated remediation in-platform, eliminating the operational gap Tenable leaves between scanning and patching.

Proactive threat mitigation

Vicarius uses AI-driven, cloud-native protection to proactively reduce risk, unlike Tenable's reactive, scheduled scans and signature-based updates.

Low operational overhead

Vicarius provides a streamlined, modern interface with seamless deployment and centralized workflows, in contrast to Tenable's high complexity and deployment burden.

MSSP-ready architecture

Vicarius is built for multi-tenancy and flexible pricing, while Tenable faces challenges with MSSP support and scaling across clients.

Superior Automation & coverage

Vicarius automates patching and supports over 10,000 apps with virtual patching and scripting, Tenable lacks integrated remediation and requires third-party tools.

Higher user satisfaction

Vicarius scores higher across G2 and Gartner reviews, with customers praising ease of use, patchless protection, and immediate remediation, unlike Tenable's issues with false positives and slow scans.

How Vicarius compares to Tenable

Capabilities	vicarius	tenable
Remediation built-In	Automated, in-platform remediation with scheduling, scripting, and guided patching	No native remediation relies on external integrations
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 patch coverage; relies on third-party tools like Adaptiva that supports ~2,500 3rd-party applications
Agent-based & agentless modes	Offers both agent-based and agentless scanning for flexible deployment across asset types	Primarily agent-based or requires additional setup
Real-time risk validation	Validates exploitability in live environments using telemetry, not simulated exploits	Relies on traditional scanning without exploit validation
Multi-tenancy for MSSPs	MSSP-friendly architecture with tenant isolation, delegated roles, and centralized control	Lacks mature multi-tenant and MSP-specific capabilities
Workflow Automation	Unified platform for detection, prioritization, and remediation, minimizing tool sprawl	Requires manual effort and multiple tool handoffs
Ease of deployment	Modern, cloud-native UI with fast onboarding and centralized console	High deployment and operational overhead
Coverage depth	Covers vulnerabilities across system, app, network, and even patchless or legacy systems	Lacks complete coverage for unpatchable/unsupported assets
Customer satisfaction	G2: 4.9 / Gartner: 4.8 praised for ease of use, performance, and support	G2: 4.5 / Gartner: 4.6 common UI, reporting, and performance complaints