vicarius

VS

ManageEngine

All-in-one Vulnerability Remediation

Vicarius combines scanning, contextual risk prioritization, and in-platform remediation to address vulnerabilities across all systems and applications. Unlike ManageEngine, which offers limited remediation options and lacks virtual patching, Vicarius provides zero-day shielding, broader application coverage, and streamlined workflows that cut tool sprawl and accelerate time to fix.

Vicarius key differentiators

Integrated Remediation workflows

Vicarius delivers automated, in-platform remediation with scheduling, scripting, and guided patching, eliminating the need for external tools or manual processes.

Virtual Patching capability

Protects against zero-days and unsupported software through virtual patching, securing systems before vendor fixes are available.

Broader application coverage

Supports Windows, Linux, macOS, and over 10,000 third-party applications, far exceeding ManageEngine's ~1,350 application coverage.

Risk-driven remediation decisions

Focuses resources on the vulnerabilities most likely to be exploited, using live telemetry to validate real-world exploitability.

Faster time-to-fix

Streamlines the remediation process from detection to remediation, drastically reducing the window of exposure compared to multi-tool workflows.

Patchless and legacy system coverage

Extends protection to unpatchable and legacy systems, ensuring security even when vendor patches are unavailable.

How Vicarius compares to ManageEngine

Capabilities	vicarius	ManageEngine
Remediation built-in	Automated, in-platform remediation with scheduling, scripting, and guided patching	Limited remediation; options outside of applying vendor patches are restricted
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 ~1,350 third-party applications
Agent-based & agentless modes	Offers both agent-based and agentless scanning for flexible deployment across asset types	Requires agents or VPN connected devices for remote patching
Real-time risk prioritization and validation	Prioritizes vulnerabilities using contextual, risk-based analysis that goes beyond CVSS, and validates exploitability in live environments using telemetry, not simulated exploits.	Provides only basic prioritization and relies on admins to manually adjust beyond CVSS severity; no exploit-likelihood or real-time validation features mentioned.
Multi-tenancy for MSSPs	MSSP-friendly architecture with tenant isolation, delegated roles, and centralized control	Supports multi-tenant architecture for MSPs, with tenant isolation, role-based access, and centralized client management
Workflow Automation	Unified platform for detection, prioritization, and remediation, minimizing tool sprawl	Lacks integrated scripting engine for vulnerability remediation
Ease of deployment	Modern, cloud-native UI with fast onboarding and centralized console	Agent installation can be manual; some configuration complexity reported
Coverage depth	Covers vulnerabilities across system, apps, network, and even patchless or legacy systems	Primarily focused on patchable systems; limited remediation options
Customer satisfaction	G2: 4.9 / Gartner: 4.8 praised for ease of use, performance, and support	G2: 4.4 / Gartner: 4.6 – feedback notes complex setup and patch management piece being cumbersome