vicarius

VS

Qualys.

Built for speed, depth & control

Vicarius delivers a unified platform for vulnerability management, real-time risk mitigation, and automated remediation without the cost, complexity, or patching delays of Qualys. From broader app coverage to faster deployment and intuitive workflows, Vicarius gives teams the tools they need to act, not just react.

Vicarius key differentiators

All-in-One, no add-ons

Vicarius includes vulnerability management, risk prioritization, and patch automation in one unified platform without needing extra modules or hidden costs like Qualys' modular setup.

Real-time risk mitigation

Vicarius predicts, prioritizes, and remediates vulnerabilities in real time, no waiting on signature updates or manual triggers like in traditional Qualys workflows.

Broader OS and app coverage

Supports ~60 OS versions and over 10,000 third-party applications for comprehensive, cross-platform protection.

Faster, easier deployment

Vicarius offers rapid deployment with minimal setup, often live in hours. Qualys' modular system can take weeks or months to configure.

Simplified, modern experience

Vicarius delivers an intuitive UI and streamlined workflows. Qualys users cite a steep learning curve and outdated interface, especially for patching tasks.

Lower total cost of ownership

Vicarius is more cost-efficient, delivering full functionality out-of-the-box. Qualys requires multiple modules, often doubling the total cost for equivalent capabilities.

How Vicarius compares to Qualys

Capabilities	vicarius	Qualys.
Remediation capabilities	Built-in remediation with scheduling, scripting, and automation, no add-ons needed	Requires separate patch management module for remediation
Virtual patching	Supports virtual patching for zero-day threats and unpatchable systems	Not supported
Third-party app coverage	Supports 10,000+ third-party applications natively	Limited to ~420 apps
Platform consolidation	All-in-one platform: scanning, risk prioritization, and patching in a single console	Requires multiple modules for full functionality (e.g., VMDR + PM + TP)
Deployment speed	Cloud-native and deploys in hours with minimal configuration	Deployment can take weeks to months depending on module complexity
Cross-platform patching	Patches Windows, Linux, macOS, and many third-party applications	Limited OS and app coverage; gaps in patch support
Predictive risk reduction	Prioritizes and remediates risks in real time using telemetry and threat modeling	Reactive approach relying on scheduled scanning and manual analysis
Total cost of ownership	Full functionality included out-of-the-box, reducing overhead and cost	Highly modular pricing; TCO is 1.5x–2x higher on average
Usability & UI	Intuitive, modern UI with easy workflow navigation and automation	Steep learning curve, outdated UI, especially for patching workflows
Customer ratings	G2: 4.9 / Gartner: 4.8 Praised for usability, depth, and automation	G2: 4.4 / Gartner: 4.5 Users cite poor support, false positives, high cost