vicarius

VS

BigFix

Modern, automated patching without limits

Ditch outdated, script-heavy patching. Vicarius delivers context-aware, no-code automation, real-time threat intelligence, and coverage for 10K+ 3rd party applications, empowering faster, smarter, and more secure remediation than legacy platforms like BigFix.

Vicarius key differentiators

No more script overhead

BigFix relies on complex fixlets and manual scripting. Vicarius delivers no-code, context-aware automation that eliminates delays, reduces human error, and accelerates remediation without sacrificing flexibility.

True security-first approach

Built for security teams, not legacy IT ops. Vicarius integrates exploit intel, CVEs, and KEVs into prioritization, enabling faster, more targeted risk reduction than BigFix's reactive, operations-driven patching philosophy.

Faster time-to-value

BigFix deployments can take weeks or months. Vicarius is lightweight, cloud-native, and operational within hours, delivering immediate impact without relay servers, complex infrastructure, or endless approvals.

10K+ apps out-of-the-box

BigFix's third-party patching needs custom scripts for ~400 apps. Vicarius supports over 10,000 3rd party applications natively, without extra cost or manual work.

Lower Infrastructure burden

BigFix demands relays, databases, and on-prem servers. Vicarius removes that overhead with a scalable cloud-native platform, reducing cost, complexity, and maintenance headaches.

Always ahead of threats

BigFix offers little exploit intelligence beyond CVE level. Vicarius bakes in real-time KEV awareness, exploit context, and zero-day intelligence for proactive, risk-based patching that BigFix simply can't match.

How Vicarius compares to BigFix

Capabilities	vicarius	BigFix
Remediation built-in	✅ Native, no-code remediation with automated patching, exploit-aware workflows, and immediate execution.	❌ Manual patching via fixlets and scripts; approvals slow down remediation.
Virtual Patching	✅ Enables virtual patching for zero-days and unsupported software	❌ No virtual patching; relies solely on vendor updates and scripts.
Cross-platform support	✅ Full patching for Windows, Linux, macOS, and over 10,000 third-party applications	🌓 Supports major OSes, but ~400 third-party apps require custom scripting.
Agent-based & agentless modes	✅ Offers both agent-based and agentless scanning for flexible deployment across asset types	❌ Primarily agent-based with heavy relay server dependency.
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.	❌ CVE-level intel only; lacks exploit context and real-time prioritization.
Multi-tenancy for MSSPs	✅ MSSP-friendly architecture with tenant isolation, delegated roles, and centralized control	❌ No true multi-tenancy; siloed deployments per customer.
Workflow Automation	✅ Unified platform for detection, prioritization, and remediation, minimizing tool sprawl	❌ Heavy scripting required; manual workflows dominate.
Ease of deployment	✅ Modern, cloud-native UI with fast onboarding and centralized console	❌ Long deployment cycles (weeks to months) with heavy infrastructure needs.
Coverage depth	✅ Covers vulnerabilities across system, apps, network, and even patchless or legacy systems	❌ Limited third-party coverage; extra cost and scripts for more apps.
Customer satisfaction	✅ G2: 4.9 / Gartner: 4.8 praised for ease of use, performance, and support	❌ G2: 4.4 / Gartner: 4.4 – feedback notes very expensive over time, complex UI, heavy reporting complexity, limited integrations, and steep learning curve.