vicarius

vs

Microsoft Intune

Security that doesn't stop at Patching

Many endpoint tools struggle with third-party and non-Windows patching, lack real-time risk clarity, and offer no protection before fixes arrive. Vicarius bridges these gaps with in-memory shielding, intelligent remediation, full OS/app coverage, and risk-prioritized automation, all from a single, unified platform.

Vicarius key differentiators

Protected beyond patches

When zero-day threats emerge, there's no time to wait for vendor patches. Vicarius instantly shields vulnerable apps, securing memory and executables, so you're protected even before a fix is available.

Coverage that leaves no gaps

Whether your environment includes Linux servers, macOS laptops, or legacy third-party apps, Vicarius deploys automated, broad-spectrum patching. Intune manages only a narrow OS subset and lacks native third-party app support.

Fix what matters most

Not every vulnerability poses the same danger. Vicarius prioritizes flaws based on real-world exploitability and business impact, ensuring your team acts on risks that actually matter, not just noisy CVEs.

One platform, seamless action

From discovery to risk analysis to remediation verification, everything happens in one unified interface. No context-switching, no manual handoffs, just faster, smarter vulnerability resolution.

Tailor-made fixes, effortlessly

Need to apply bespoke scripts? Vicarius empowers your team with a scripting engine that automates complex fixes, whether registry tweaks, config changes, or custom workflows, without the headache.

Reclaim teams' time

No more firefighting or repetitive patch cycles. Customers report slashing remediation time by up to 80%, with automation that lets security teams focus on strategic work, not mundane tasks.

How Vicarius compares to Microsoft Intune

Capabilities	vicarius	Microsoft Intune
Remediation built-in	✓ Automated, in-platform remediation with scheduling, scripting, and guided patching	✗ Provides security tasks via Defender, remediation is manual and limited to supported tasks only
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	◐ Able to natively patch Windows and Microsoft apps, Linux, macOS, and third-party apps need external tools for patching
Agent-based & agentless modes	✓ Offers both agent-based and agentless scanning for flexible deployment across asset types	✗ Agent-based only, no built-in agentless scanning mode, not detecting network devices
Real-time risk validation	✓ Validates exploitability in live environments using telemetry, not simulated exploits	✗ Uses Defender integration, lacks live exploit validation and immediate remediation paths
Multi-tenancy for MSSPs	✓ MSSP-friendly architecture with tenant isolation, delegated roles, and centralized control	✗ Intune is single-tenant per organization, complex for multi-tenant MSP workflows
Workflow Automation	✓ Unified platform for detection, prioritization, and remediation, minimizing tool sprawl	✗ Patch management and threat tasks are separate, no integrated end-to-end remediation
Ease of deployment	✓ Modern, cloud-native UI with fast onboarding and centralized console	◐ Cloud-native and easy to access, but native patching, especially for third-party applications, remains manual and complex
Coverage depth	✓ Covers vulnerabilities across system, app, network, and even patchless or legacy systems	✗ Limited to known CVEs, tasks, poor visibility for legacy or shadow IT, manual scripting needed
Customer satisfaction	✓ G2: 4.9 / Gartner: 4.8 praised for ease of use, performance, and support	✗ G2: 4.5 / Gartner: 4.3 criticized for management complexity and limited patching tools