



vicarius

VS



**Microsoft
Defender**

Turning Visibility into Action

Vicarius delivers full-stack, cross-platform remediation with built-in automation, exploit-aware prioritization, and support for over 10,000 third-party applications, without the complexity of Intune, MEM, or PowerShell. Simplify your vulnerability management and reduce risk faster, with no hidden licensing or infrastructure dependencies.

Vicarius key differentiators

Built-in Remediation engine  Vicarius includes native, automated remediation with scheduling, scripting, and patchless protection, no Intune, MEM, WSUS, or additional licenses required.	Full OS and app coverage  Vicarius supports macOS, Linux, and Windows plus 10,000+ third-party apps, covering what Defender doesn't natively handle.	Exploit-aware Prioritization  Risk scoring in Vicarius goes beyond CVE with real-time telemetry, exploitability context, and KEV/EPSS alignment.
Cross-platform Patch Automation  Delivers full-stack remediation across platforms instantly, no PowerShell scripting or manual processes needed.	Flat cost, no add-ons  Vicarius includes all core functionality in one platform, avoiding complex Microsoft licensing structures and hidden admin overhead.	Faster time to value  Vicarius deploys instantly, reduces MTTR, and doesn't require deep Microsoft stack integration or onboarding delays.

How Vicarius compares to Microsoft Defender

Capabilities	 vicarius	 Microsoft Defender
Remediation capabilities	✓ Built-in remediation engine with automation, virtual patching, and rollback support	✗ Requires MEM/Intune/WSUS/SCCM; no native remediation engine
Platform & OS coverage	✓ Cross-platform support: Windows, Linux, macOS, +10,000 third-party apps	✗ Primarily focused on Microsoft stack; limited non-Windows compatibility
Exploit-aware Prioritization	✓ Combines CVSS, KEV, exploitability, telemetry and environmental context for accurate prioritization	✗ Based only on CVE scoring within Microsoft ecosystem
Patchless Protection	✓ Virtual patching available for high-risk or unpatchable vulnerabilities	✗ Not supported
Automated Remediation	✓ Scripting, scheduling, and guided patching workflows built in	✗ Requires manual configuration or external tools
Cost & licensing simplicity	✓ Flat pricing model with no extra tools or licenses	✗ Requires multiple licenses, modules, and admin rights
Deployment speed	✓ Instant deployment, no infrastructure or deep Microsoft integration needed	✗ Long onboarding time, especially for new devices
Role-based access control	✓ Supports RBAC and advanced user management across tenants	✗ RBAC and reporting require improvement
Real-time threat reduction	✓ Reduces dwell time and patch lag with exploit-aware, instant remediation	✗ Reactive: detection-focused, remediation is manual
Customer ratings	✓ G2: 4.9 / Gartner: 4.8, praised for automation, patching ease, visibility	✗ G2: 4.4 / Gartner: 4.5, noted complexity, false positives, and poor onboarding