

Vulnerability detection & management with UEM-driven remediation



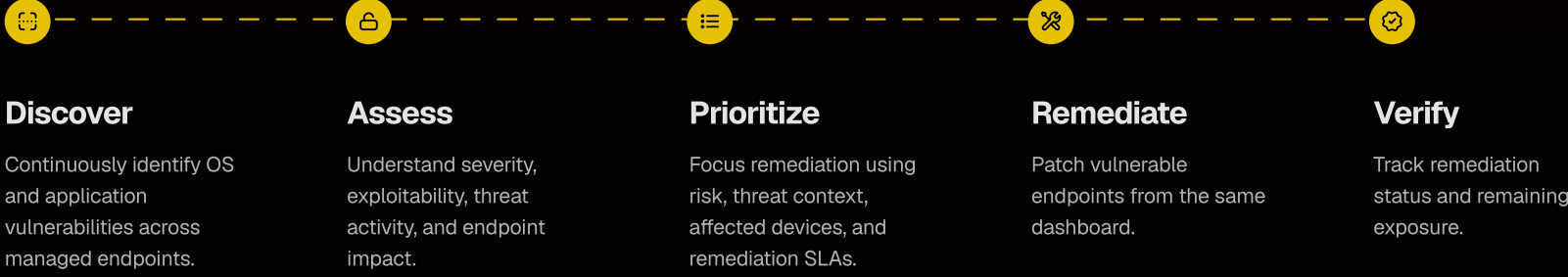
Discover, prioritize, and remediate software vulnerabilities across Windows and macOS without additional security agents. Give IT and SecOps teams one actionable view to move endpoints from exposure to patch resolution.

Eliminate tool switching with Veltar's continuous vulnerability detection, risk prioritization, and simplified remediation, powered by the Scalefusion UEM platform.

Complete Vulnerability Loop

From exposure to remediation, in one continuous workflow.

Veltar keeps vulnerability discovery, risk assessment, endpoint context, remediation, and verification connected, so your team can move from exposure to resolution without losing the thread.



Key Capabilities

Unified, multi-OS endpoint coverage & zero agent overhead.

Achieve complete software vulnerability detection across all your devices without complex setups or secondary agent maintenance.

- **Cross-platform vulnerability visibility**

Out-of-the-box vulnerability discovery and patching across supported versions of Windows and macOS, endpoints.
- **Comprehensive application coverage**

Scans and reports CVEs for OS components and third-party software applications.
- **Seamless remediation workflows**

Native remediation for Windows and macOS, all in one view/from a single dashboard.
- **Lightweight where it counts**

Get vulnerability detection and remediation without putting unnecessary load on endpoint resources.

Separate the noise from the real risk.

- **Spot what's likely to be exploited next.**

Use EPSS-based exploitability predictions to find vulnerabilities that could become tomorrow's problem.
- **Act on what's already being exploited.**

Let us identify vulnerabilities with confirmed exploitation and keep them at the top of the priority list with continuous sync to CISA KEV.
- **Put the threat in context.**

Factor in affected devices, ransomware relevance, vulnerability age, and remediation deadlines to determine what needs attention first.

Dynamic device risk scoring.

Legacy CVSS ratings generate constant noise, treating threats on paper with the same urgency as active exploits. Scalefusion Veltar replaces raw CVSS scores with a dynamic Device Risk Score to prioritize what matters most.



Proactive compliance enforcement with resolution deadlines.

Transition from reactive patching routines to policy-driven compliance

- **Automated group rules**

Trigger custom compliance rules to quarantine devices in device and user groups based on Vulnerability Risk Status, Risk Score, or active priority status.
- **SLA-driven resolution windows**

Enforce strict compliance deadlines by establishing maximum resolution windows based on severity to fulfill regulatory compliance requirements.

Why Veltar vulnerability management?

- **Single platform economy**

Ensure safe, encrypted access to sensitive company assets from anywhere, on any device.
- **Zero implementation friction**

Eliminate agent fatigue and other delays between SecOps and IT Admins with direct, closed-loop patching.
- **Real-world prioritization**

Stop chasing low-risk CVEs; let EPSS modeling and CISA KEV intelligence focus your team on actively exploitable vulnerabilities.

Vulnerability management software to detect, prioritize, and patch every endpoint.

Start your free trial

Book a Demo