



Close the Remediation Gap: From Vulnerability Detection to Risk Reduction

Turning Alerts into Action

Tenable provides deep, continuous visibility across your entire attack surface—from cloud workloads to identity and on-premises infrastructure. Averlon augments Tenable's detection with contextual agentic AI triage and remediation. Enriching Tenable findings with runtime signals, exploit intelligence, and environment-specific context, Averlon's AI agents identify which issues are exploitable in your environment, map them into likely attack pathways, and trigger targeted resolution. Whether it's developer PRs, cloud-native mitigations, or compensating controls like WAF rules, Averlon AI agents help security teams prioritize risks that drive business exposure and resolve them without delay or friction.

The result: dramatically reduced alert fatigue, faster remediation, and tighter alignment across security, DevOps, and cloud teams.

95% ↓
false positives

90% ↑
time to resolution

10x ↑
team efficiency

Why Tenable and Averlon?

Timely detection of vulnerabilities is crucial, but it's only the first step. The scale, speed, and complexity of the cloud often leads to thousands of ever-evolving vulnerabilities, with little focus on what's truly critical and how to act on it. That's the gap Tenable + Averlon close, by combining comprehensive detection with intelligent triage and remediation.

Cut Analyst Overload

Eliminate the noise and focus on what's actually exploitable, reducing burnout and speeding up triage

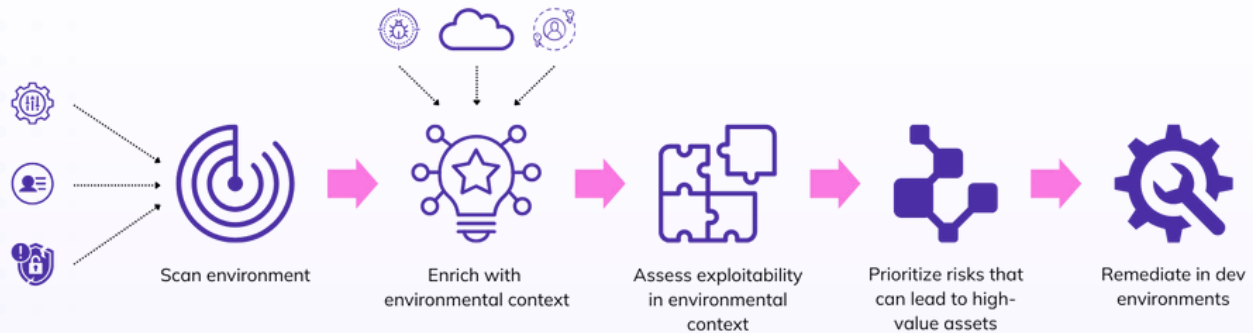
Connect Risk to Business Impact

Map findings into attack pathways and prioritize vulnerabilities leading to critical assets

Reduce Exposure, Fast

Trigger fixes directly in developer workflows and automate mitigations to shrink window of risk

How it Works



1

Discover and Detect

- Tenable identifies vulnerabilities across the enterprise—spanning multi-cloud, containers, and on-premises environments.
- It also uncovers misconfigs and exposures that increase the attack surface.

2

Enrich and Triage

- Averlon ingests Tenable findings and enriches them with exploitability signals (EPSS, KEV), runtime context, identity risk, and more.
- AI agents evaluate each issue for contextual applicability and reachability to filter out noise and surface real risks.

3

Prioritize and respond

- Averlon maps vulnerabilities into attack chains—adversary pathways to high-value assets—to prioritize risks.
- AI agents trigger automated resolution in developer IDEs or cloud consoles, always with human oversight.

Key Use Cases

Prioritizing What to Fix First

Security teams are buried in CVEs without knowing what's exploitable or relevant. Averlon helps cut through noise and focus on issues that are exploitable and high-risk in your environment.

Meet Your Patching SLAs

Critical risks remain open while teams wait on fixes. Averlon's AI agents provide fixes within IDEs and mitigate via compensating controls like WAF rules or IAM updates to reduce exposure.

Address Cloud Misconfigs and Identity Gaps

Cloud policy drift, asset exposure, and excessive access are often as critical as CVEs. Averlon's AI agents map these risks into attack chains so teams can understand and address these critical gaps.

Overcome Analyst Overwhelm

Analysts waste countless hours chasing issues and tickets that don't lead to risk. Averlon filters out non-exploitable findings, so teams can focus on risks that matter.

ABOUT AVERLON

Averlon is pioneering agentic vulnerability remediation, using AI agents to automate and scale response. It helps teams cut noise, eliminate manual triage, and accelerate remediation in modern cloud environments. Trusted by enterprises of all sizes, Averlon boosts analyst and developer productivity with contextual workflows and automation built for real-world scale and complexity.

 info@averlon.io

 <https://averlon.ai>