AVERLON

Agentic Remediation Operations

Findings Don't Reduce Exposure. Fixing Does.

Most security tools find vulnerabilities. They don't fix them. The gap between finding and fixing is where real risk lives. Attackers exploit in days. Remediation takes months.

That gap is the Exposure Window. Closing it is what matters.
Averlon is built around that gap.

5 days
Median time to exploit

80%
Still unpatched at 30 days

200+ days
Average remediation time

The Shift: From Visibility to Action

Traditional Approach	Averlon
Findings	Fixes
Severity scores	Environment-specific exploitability
Backlogs	Closed Exposure
Manual triage	Automated attack-chain clarity
Ticket driven workflows	Remediation within developer workflows
Reactive response	Prevent new backlog

How Averlon Delivers Remediation Operations

1

Identify what's actually exploitable

Determine applicability and reachability in your environment, not just CVSS severity. Most findings are eliminated here before they enter your backlog.

2

Break attack chains to high-value assets

Model how exposures combine to reach critical systems and data. Focus on what matters. Eliminate pathways for attackers.

3

Remediate safely at speed

Deliver context-aware fixes directly in developer workflows, accounting for breaking changes.

4

Prevent new exposure before production

Apply the same exploitability and attack-chain reasoning pre-merge to stop risky changes before they become backlog.

Contact us - info@averlon.io

AVERLON

From Thousands of Findings to Handful That Need Fixing

In one global production environment spanning 140,000 assets. Months of work reduced to hours.



255,000
vulnerabilities

500
exploitable exposures

102
assets at risk

a few hours
time to break attack chains

90%
faster remediation

95%
noise reduction

100x
remediation velocity

Trusted by Security Teams Fixing Real Risk

"Averlon has saved my team over 13,000 hours by cutting through the noise and helping us fix the issues that actually matter!"

Scott Roberts, CISO, UiPath

"Averlon shows what is exploitable in our environment and helps us remediate risk quickly."

Vaseem MV, SVP IT, Ziply Fiber

"Averlon cut through the noise and made risk understandable at the board level."

Head of Security, SaaS Unicorn

UiPath · OLERIA · ZYLO · ziply fiber · ITERABLE

How Security Teams Use Averlon

CISO

Demonstrate real risk reduction, not just findings. Focus teams on what actually matters and show outcomes to the board.

Vulnerability Management

Eliminate backlog, not just manage it. Remove noise, focus on exploitable risk, and defend prioritization with clear reasoning.

Security Operations

Know what matters during an incident. Understand blast radius and prioritize response based on real exposure, not alert volume.

Cloud Security

Move beyond visibility into your cloud. Identify what is exploitable in your environment and how attackers can chain issues to reach critical assets.

ABOUT AVERLON

Averlon is a Remediation Operations platform that helps security teams move from managing vulnerability backlogs to reducing real risk and closing the Exposure Window. Trusted by security teams at enterprises and fast-growing companies to efficiently scale their security programs.

info@averlon.io
https://averlon.ai