AVERLON + snyk

Secure What Matters: From Code to Cloud with Real-World Risk Context

Transform Alerts into (Insightful) Action

Snyk and Averlon help security teams and developers cut through vulnerability overload—shrinking false positives by 95%, improving security efficacy 10x, and resolving critical vulnerabilities 90% faster.

By combining Snyk's deep application-layer visibility with Averlon's environment-aware context, the integration identifies which vulnerabilities are truly exploitable in your environment, traces them back to code, and enables fast, targeted remediation. Where possible, Averlon also applies automated mitigations —such as WAF rules or entitlement management—to reduce exposure even before a fix is deployed.

The result: *smarter prioritization, faster response, tighter DevSecOps alignment, and dramatically reduced breach exposure.*

95%↓
false positives

10x ↑
efficiency

90%↑
time to resolution

Why Snyk and Averlon?

A simple truth: if you're chasing a thousand issues, you're not fixing what matters. Security teams are buried in vulnerabilities across code and cloud—without knowing which ones affect their environment or expose critical assets. It's not just noise. It's wasted cycles, misaligned teams, and risks left open longer than they should be. That's what Snyk & Averlon address together.

Prioritize What's Exploitable

Focus only on vulnerabilities that are exploitable in your specific environment

Trace Risk to the Source

Map infrastructure and application issues back to the exact code or config responsible

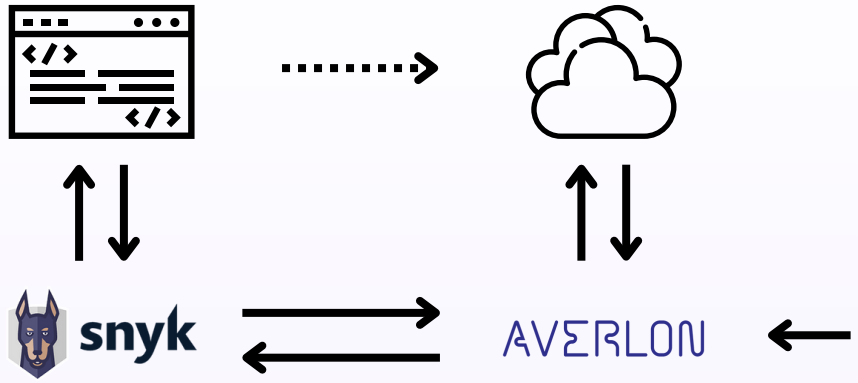
Respond with Speed

Accelerate remediation with targeted fixes or automated mitigations that break attack chains early

Contact us - info@averlon.io

AVERLON

How it Works



1

Detect issues across stack

- Snyk identifies vulnerabilities in code, containers, IaC, and dependencies using SCA, SAST, and other scanners

2

Map to attack chains

- Averlon ingests cloud misconfigs, vulnerabilities, and identity risks across the environment
- Averlon maps app and infra issues into attack chains—prioritizing vulnerabilities that pose highest risk

3

Prioritize and respond

- Issues are traced to their source in code, enabling swift and targeted remediation
- Averlon automates resolution—e.g., WAF rules, entitlement management—to break the attack chain while remediation is in progress

Key Use Cases

Reduce Vulnerability Overload

Focus on the small set of issues that are truly exploitable in your environment. Eliminate noise and false positives, prioritizing issues based on real-world impact

Trace Issues to the Origin

Trace misconfigurations and cloud risks back to specific code or IaC files, enabling root-cause remediation and accelerating engineering response

Speed Up DevSecOps Workflows

Give security and dev teams shared visibility into what's exploitable, not just what's severe. Integrate risk context into CI/CD and improve collaboration and handoffs

Break Attack Chains with Minimal Fixes

Identify the smallest set of nodes that, if fixed or mitigated, will break multiple attack pathways with source-level details to implement those fixes quickly

Reduce Exposure Before Fixes Deploy

Apply automated resolutions (e.g. WAF-based mitigations, entitlement updates) to reduce exposure before fixes deploy. Contain risk in production and buy time without slowing teams down

ABOUT AVERLON

Averlon brings agentic AI to cloud vulnerability management—eliminating manual triage, surfacing what matters, and both accelerating and automating remediation. Built for fast-moving cloud environments, Averlon delivers contextual workflows that boost analyst productivity and eliminate wasted engineering effort.

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