BOOST SECURITY ASPM

The Fastest Path from Legacy Scanners to Modern ASPM

Stop managing pipelines. Start managing risk. Deploy in minutes.

Boost Security delivers full coverage without touching your existing DevOps automation.

While traditional tools require manual “plumbing” into every individual pipeline, Boost Security uses Zero-Touch Provisioning (ZTP) to provide instant coverage across your entire repository footprint without touching a single line of CI/CD code.

WHY IT’S TIME TO SWITCH

Deployment Without the Drama

Zero-Touch Provisioning

The biggest hurdle to security coverage is developer coordination. Boost Security eliminates this bottleneck by connecting at the SCM level (GitLab, GitHub, etc.). We automatically discover and secure every repository in your organization in minutes. No individual commands to insert, no pipelines to edit, and no developer tickets required.

Instant ASPM Intelligence

Deployment is fast, but the results are smart. Once deployed, Boost Security acts as a central brain, consolidating data into a unified risk view. Boost uses environmental context instead of rigid rules to prioritize what’s actually reachable and high-risk, so you can turn off the “noise” of legacy tools immediately.

No Code Exfiltration

Unlike other “easy” cloud scanners that require you to send your source code to their servers, Boost Security performs its analysis locally. Your code never leaves your environment. You get the speed of a SaaS platform with the privacy of an on-prem solution.

Easy to Own

Boost is designed so a small security team (or even a single AppSec owner) can run it confidently at scale. Policies are clear, workflows are predictable, and reporting is built for real operational use beyond audits.

Boost: A True ASPM Platform

Gartner recently distinguished between stand-alone ASPM (which only orchestrates third-party tools) and the ASPM Platform (which includes native, built-in scanners). **Boost's true ASPM Platform** combines the "Brain" (correlation and context) with the "Sensors" (native high-fidelity scanners).

Boost's Built-In Baseline Scanning

- Static & Dynamic Analysis (SAST/DAST)
- Software Composition Analysis (SCA)
- Secrets & Container Scanning
- IaC & Kubernetes Security
- CI/CD Guardrails
- SBOM Generation & Enrichment

How Boost Evaluates Risk

Boost evaluates application risk the same way experienced AppSec teams do: **by combining policy, context, and exposure.**

Each finding is assessed against your defined policies, then interpreted in light of where that software actually runs and how it is used. Issues that represent meaningful exposure—such as reachable vulnerabilities or unsafe supply-chain conditions—rise to the top because they create real downstream consequences.

This approach gives teams a defensible basis for action and reporting, grounded in how risk manifests in their own environment.

Proven at Real Scale

Boost is used by companies managing thousands of repositories, often with a single AppSec owner responsible for the entire program.

It's built to scale without becoming brittle or expensive to operate.

boost®
security.io

Built for Security Teams and Developers

Security teams get control and visibility. Developers get focused, actionable feedback, but only when it's warranted, in the tools they already use.

Boost supports:

Incremental analysis tied to real code changes

Direct feedback in pull requests or existing ticketing systems

Flexible enforcement, from passive visibility ("silent mode") to merge blocking

Teams stay aligned without constant back-and-forth.

BOOST SECURITY

Sophisticated protection. Simple deployment. Instant results.