boost security.io

2026

DEMANDBASE

DEMANDBASE CASE STUDY

Scaling Security with Context at Demandbase

Boost takes Demandbase from “Compliance Noise” to a 10x Improvement in Security Posture

---

“Our security posture meaningfully increased by 10x because developers actually fix things with Boost. I can guarantee that wouldn’t happen with other tools”

— DAPHNE YANG, STAFF TECHNICAL PRODUCT MANAGER, DEMANDBASE

THE PROBLEM

Compliance-Based Scanning & The Never-Ending Backlog

For the security team at DemandBase, legacy scanning looked more like a box-ticking exercise than a proactive defense. While they used Veracode to meet **SOC2** and **ISO** requirements, the platform suffered from a 95-99% false positive rate.

Noisy tools led to inaction. The security team lacked confidence in the results, so they couldn't justify blocking builds. Developers didn't trust results either, making them unlikely to understand or improve the security of their own coding practices.

With trust lacking in security findings, the backlog grew over time instead of shrinking. **"We had a scanner, but we weren't doing enough about it. Our CSO realized that if we didn't stop the bleeding, we simply couldn't catch up,"** said Daphne Yang, leader of the AppSec team.

"We had a scanner, but we weren't doing enough about it. Our CSO realized that if we didn't stop the bleeding, we simply couldn't catch up."

THE BOOST SOLUTION

ASPM-Driven Prioritization & Policy Control

Demandbase needed a way to move beyond AppSec scanning tools and toward a proactive, defensible **ASPM** strategy. To make the leap, they evaluated several options, including GitLab Ultimate, but found that the bundled tools and policies lacked the granularity required for their security program. They chose the Boost Security **ASPM** Platform because it provided the "intelligence layer" needed to prioritize risk in a smart, tailored way.

Key Boost capabilities that made the decision easy:

1 Custom Guardrails

Demandbase used Boost to build a custom "tag checker" guardrail that enforced repository ownership tags, solving a fundamental hurdle legacy scanners struggle with: How can you fix something if you don't know who owns it?

2 Granular Policy Engine

Boost allowed the team to define specific policies that distinguished between theoretical flaws and material risks, to a degree that Yang says simply didn't exist in other tools the team auditioned.

3 Confidence to Block

By eliminating the vast majority of false positives, the security team gained the confidence to move from "notification mode" to "blocking mode," ensuring that no unhealthy resources reached production.

HOW IT WORKS

The “Living Rollout” & Developer Experience

Transitioning security at Demandbase involved scaling across **2,000 repositories and 500 developers.** Yang implemented a “living rollout” strategy designed to minimize friction while maximizing impact.

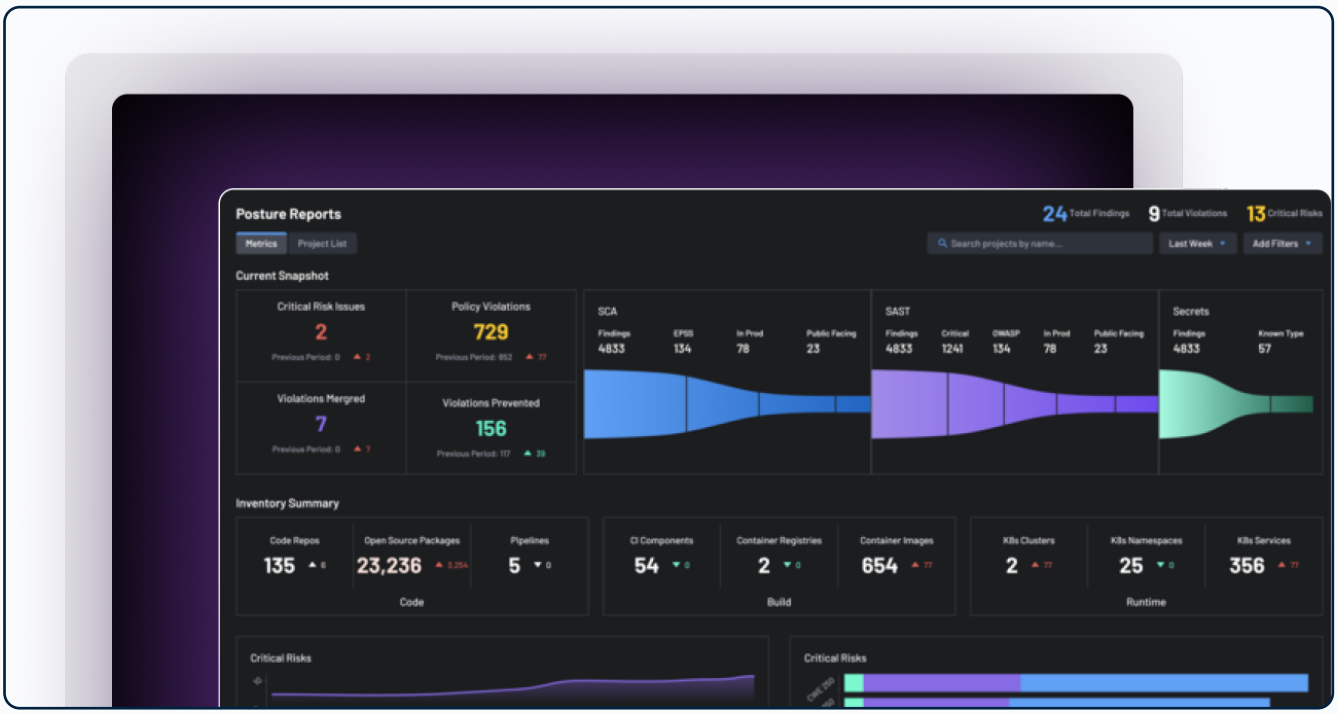
The PR-First Workflow

The “defining factor” for success, in Yang’s estimation, was Boost’s inline PR comments. By delivering straightforward, actionable feedback directly in GitLab, security became part of the developer’s existing discussion instead of an external hurdle imposed in a separate workflow. **“The comments don’t have a lot of fluff,”** Yang noted. **“The content itself is actionable and easy to find.”**

Phased Migration

Yang’s team ran Boost in “silent mode” for several weeks to gather data and tune policies. This allowed them to understand (and educate developers about) what would have been blocked before actually enforcing the guardrail. This transparency transformed the relationship between security and engineering, allowing devs to stop feeling like security was “breaking things” and instead building loops that improved quality and security.

> “The comments don’t have a lot of fluff. **The content itself is actionable and easy to find.”**



THE RESULT

10x Posture Improvement & “Healthy Repos”

One year after migrating to Boost, the security program at Demandbase has shifted from reactive compliance-based maintenance to automated security oversight.

Key results include:

Massive Remediation Velocity

In a single two-week period, the team recorded **530 verified fixes**, a volume of activity that was impossible under the old legacy model.

Drastic MTTR Reduction

For high-end, critical vulnerabilities, the Mean Time to Response dropped to **under 48 hours.**

Defensible Security Spending

When budget reviews occurred, Yang successfully defended the platform to the organization’s General Counsel by proving that their security posture had improved **10x** relative to legacy scanning tools.

Healthy Repos

Demandbase has now been able to move to a strategic **“Healthy Repo”** metric, identifying repositories that have zero high-risk vulnerabilities unaddressed for **more than 30 days.**

ASPM: Strategy Beyond the Scan

Scanners can find bugs. **ASPM** Platforms can govern development. For Demandbase, shifting to an **ASPM** meant being able to implement security controls at scale.

Why Switch to an ASPM?

Noise Suppression

The Boost Security **ASPM** Platform uses environmental context and multiple native-built scanners to prioritize reachable, material threats while suppressing false positives

Centralized Control

Boost enables a single security owner to enforce global guardrails across thousands of repositories without manual pipeline edits or developer intervention.

Shift Further Left

Most tools “shift left” by moving scan results to the PR. The Boost **ASPM** Platform moves shift left even further by leveraging Model Context Protocol (MCP) to funnel security standards directly into the IDE to prevent vulnerabilities at the moment of inception.

boost® security.io

Get in Touch

info@boostsecurity.io
3 Place Ville Marie, Montreal
H3B-2E3, QC, Canada
boostsecurity.io