boost security.io

TRAVELPORT

TRAVELPORT CASE STUDY

Scaling Application Security at Travelport

Centralizing Security Visibility for 6,000 Repos

“I would tell any peer that Boost is a great tool. It’s an all-in-one style solution and it is a good buy.”

— JILLIAN RODRIGUEZ, APPSEC TEAM LEAD, TRAVELPORT

2026

THE PROBLEM

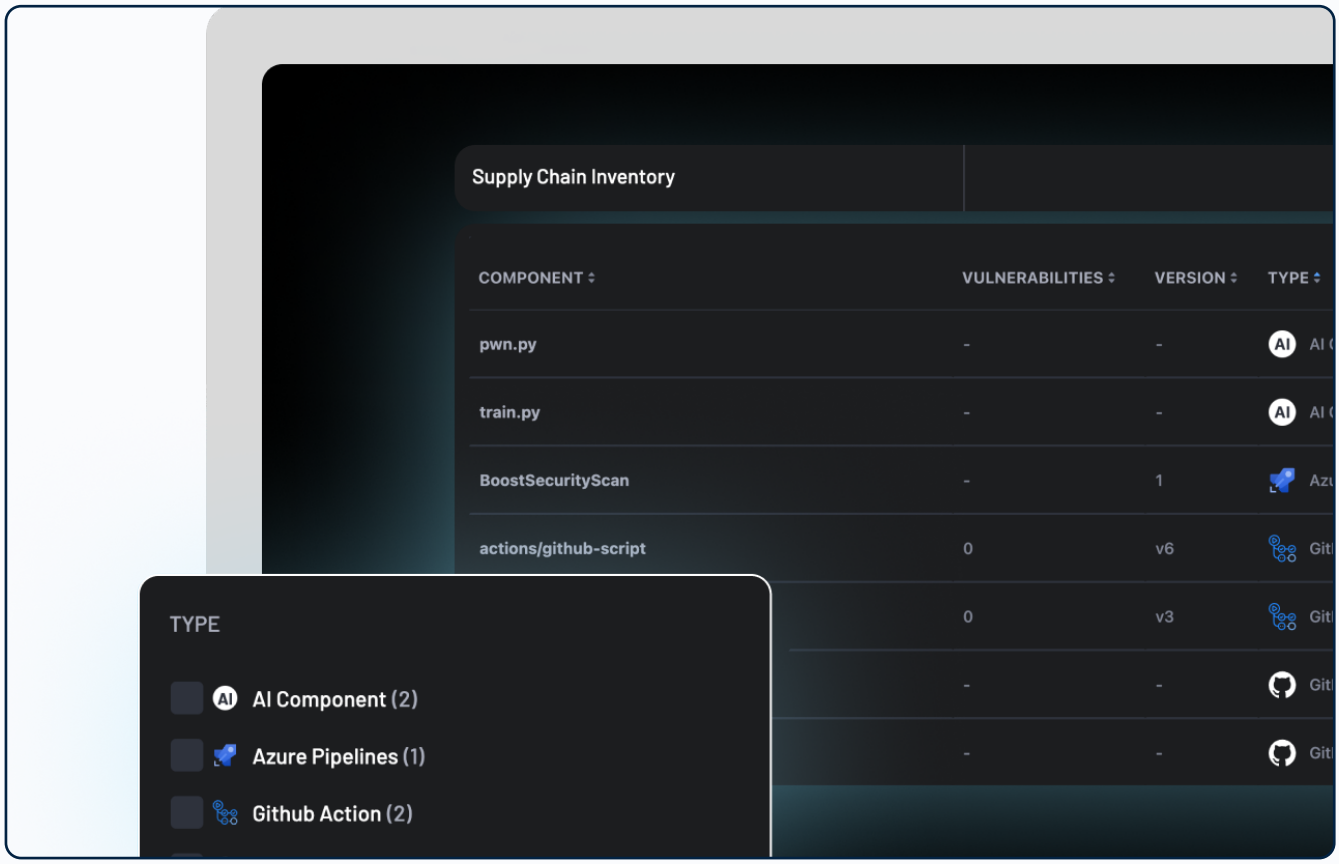
Fragmented Tooling & Limited Repository Visibility

For the AppSec team at Travelport, a lack of environmental data created a massive obstacle to scaling security efforts. Jillian Rodriguez oversaw a footprint of 6,000 repositories and 500 developers as Travelport's AppSec Team Lead, managing a lean team of two other security engineers. When she arrived at Travelport, Rodriguez found a fragmented, legacy stack of AppSec tools: Fortify On Demand and Sonatype Nexus, both of which required constant manual intervention.

Legacy tools created scaling pain in two ways. First, some legacy infrastructure was on-prem, forcing Rodriguez into a dual role as system administrator. **"I had to manage that on-prem solution,"** she said. **"Any time there was a problem with the VM certificates, scanning would go down. We were maintaining infrastructure where we should have been addressing risk."**

Second, the team lacked a comprehensive view of their own attack surface. Without an automated way to pull repository data, "shadow repos" and archived projects remained invisible. "I had no visibility. That's the easiest way to say it," Rodriguez explained. **"[Sonatype] Nexus doesn't pull items in the way Boost does. I couldn't see what was active."**

When these legacy tools identified vulnerabilities, informing developers and checking on their work was completely manual. Findings were trapped in multiple UIs, requiring AppSec team members to send individual emails to developers to request fixes. This created a permanent bottleneck that led to increasing security debt across the organization. Something needed to change.



THE BOOST SOLUTION

Tool Consolidation + Automation = Value

In the summer of 2024, Rodriguez began evaluating a shift to a cloud-native, unified platform. Her objective was to consolidate the functions of her existing legacy scanners into a single dashboard. While the team reviewed major incumbents including Snyk, the final decision was driven by a comparison of functionality versus cost.

"From what I could see, functionality-wise it was 1:1 between Boost and Snyk," she said, but noted that Boost's price point was significantly better.

"If I can cut costs in scanners, I'd rather do that than cut people. The best thing for us was finding a way to consolidate that actually saved us money."

Boost offered three major Security Boosts that Travelport knew could accelerate and scale their AppSec program:

Tool Consolidation

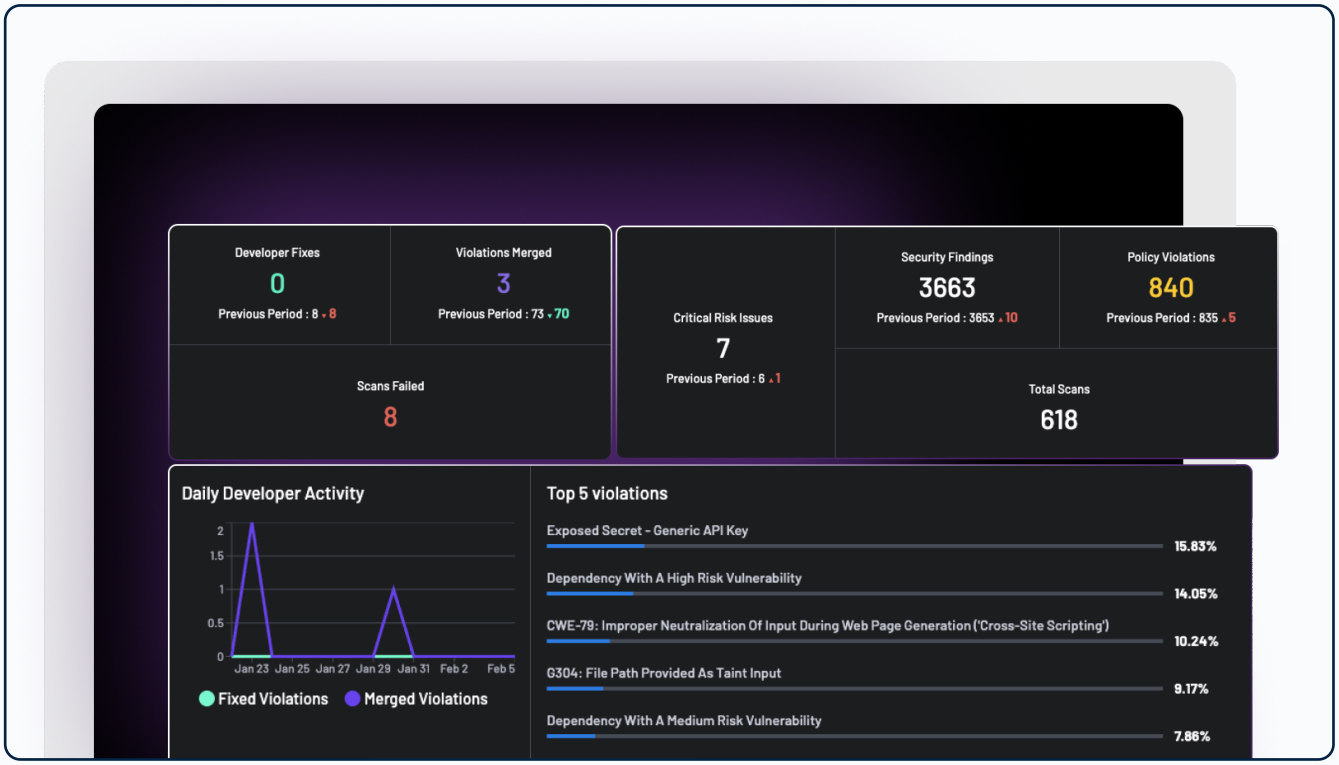
Replacing Fortify and Sonatype with a single platform that offered multiple scan types in a single interface.

Workflow Automation

Moving vulnerabilities out of email threads and into an automated Jira integration so important findings could be attached to tickets automatically.

Infrastructure Offloading

Shifting to a cloud-native model to eliminate the management of VMs and certificates.



HOW IT WORKS

Deployment Strategy & Engineering Onboarding

Boost's rollout happened fast, with Rodriguez and her team implementing a fully change-managed migration of their **6,000-repository footprint in just under 90 days**, including developer training.

This accelerated process was made possible by Boost's capability to hook directly into GitHub, instantly mapping Travelport's true scanning footprint. **"That's the best part of Boost,"** Rodriguez said. "**Actually seeing what your scanning footprint should be, knowing what's active and what's archived instead of relying on guesswork."**

Deployment success also hinged on Rodriguez's communication strategy, initiated months before the first scan. Bypassing the common Boost "silent mode" deployment where developers are brought in at a later stage, Rodriguez saw her devs as partners and opted for radical transparency within the engineering organization. She attended executive-level calls months in advance to set expectations for the tool consolidation, and held training sessions in advance of the January 2025 launch.

"It just works better for us to be hooked in with engineering, so we can let them know in advance what changes are coming," she explained. To drive adoption among 500 developers, she augmented live developer training sessions with video-based training modules, which Rodriguez found more effective than static documentation for accelerating onboarding.

"That's the best part of Boost," Rodriguez said. "Actually seeing what your scanning footprint should be, knowing what's active and what's archived instead of relying on guesswork."

THE RESULT

Defensible Security Spending & Automated Visibility

One year after migrating to Boost, the AppSec program at Travelport has moved from a reactive maintenance model to an automated oversight model. Rodriguez has been able to centralize AppSec findings and see risks in a single tool that automatically detects new repositories, giving her team of three a level of visibility that was previously impossible.

Key results for the Travelport team include:

Visibility Gains

Rodriguez estimates a **minimum 80% increase in visibility** of the application surface across the enterprise.

Lower Developer Friction

By automating security checks and removing them from manual pipeline management, Rodriguez streamlined the developer experience. **“I’ve made developers happier because they no longer have to manage these pipelines,”** she said.

Budget Defensibility

The consolidation of Travelport’s AppSec stack gave Rodriguez a strong position in budget negotiations. **“If my boss asks to cut costs now, I can say we’ve already consolidated enough. Boost gives us everything we need,”** she explained. **“I’ve had these conversations before, and I’ve won them all.”**

boost® security.io

Get in Touch

info@boostsecurity.io

3 Place Ville Marie, Montreal

H3B-2E3, QC, Canada

boostsecurity.io