boost security.io

MATTEL CASE STUDY

Permissionless Visibility: How Mattel Scaled AppSec with Zero-Touch Provisioning

2026

THE PROBLEM

The High Cost of Manual Integration

At one of the world's largest toy manufacturers, the Head of AppSec found himself in an impossible position with a Snyk deployment that proved impossible to scale. He was solely responsible for managing **700+ repositories from over 200+ developers,** but kept finding his rollout stalled by the developers whose code he was trying to keep secure.

Snyk required a unique, manual command for every CI/CD pipeline in order for the AppSec lead to have the visibility he needed to do his job. With each developer maintaining his or her own pipelines, the security lead found himself responsible for coordinating **700 individual manual updates.**

Unsurprisingly, this deployment requirement created a permanent bottleneck. **"We needed to create and insert an individual command into their CI/CD pipeline, but we never finished,"** the Head of AppSec said. **"Some developers did it right away. But others ignored the instructions, so we had to call them again and again to move forward, and no progress was being made."** The rollout hit a wall, because security depended entirely on developer favors.

"If I need to individually roll out that scanning command and add it to 700 CI/CD pipelines, that is a real pain," the lead explained. The security program needed full coverage, but the "YAML tax" on developers was too high.

THE BOOST SOLUTION

Permissionless Visibility

Boost broke the deadlock by removing the requirement for developer intervention with Zero-Touch Provisioning (ZTP). Using ZTP, the Head of AppSec gained the ability to integrate scanning directly at the source control management level, removing the requirement for developer intervention and allowing him to act unilaterally to secure the organization.

The lead connected the entire 700-repo footprint using only a GitLab service account and an API key. Boost's unique approach provided total visibility while leaving existing CI/CD code untouched—and without spending political capital with developers. **"Boost is integrated into the production directly,"** the lead explained. **"It's much easier for me to provision the scanning."**

The Boost platform also consolidated various scanners into a single view. **"Boost comes with all those kinds of scanners natively, built into a single dashboard to show them in a central location,"** the lead said. This centralization allowed the solo practitioner to prioritize risks independently, even for a large organization with hundreds of developers.

This setup changed the relationship between the security lead and the engineering teams. Instead of asking for favors, the lead became an informed auditor who could pinpoint issues and raise awareness.

"Zero-touch provisioning makes Boost really stand out," he said. "It never changes in security: some teams follow instructions, other teams may not. But at Boost, we don't need them. We can do it by ourselves."

HOW IT WORKS

The Two-Hour Rollout

The technical rollout of 700 repositories, which had previously stalled for years, was completed in a single afternoon. To begin the rollout, the Head of AppSec simply created a service account in GitLab and gathered an API key, then followed a similar process for Google Cloud and container image scanning.

Boost's unique **Zero-Touch Provisioning** (ZTP) enables the platform to secure code without manual pipeline edits. **"When I use Boost, the only thing I need to collaborate on with developers is GitLab management,"** the lead said. **"I don't need developer permission to roll out the product or understand our biggest risks."**

The organization also used a integrated the platform with Microsoft Teams, providing management with automated notifications for new or resolved vulnerabilities.

Boost's platform maintains coverage as the engineering team grows, detecting and scanning new organizations and projects in GitLab as they are created. **"Boost can automatically identify new organizations and new projects,"** he explained. **"When developers create new repositories, the platform detects it and begins scanning right away."**

The ZTP Advantage

1 CONTINUOUS VS. SCHEDULED

Traditional scanning tools often limit the number of scans to control costs, leading to "scheduled" security that only runs once a week. Boost Zero-Touch Provisioning (ZTP) integrates at the SCM level, allowing for continuous scanning of every Pull Request (PR) and every merge.

2 PRIVACY-FIRST ARCHITECTURE

Unlike cloud scanners that require your code to be ingested by the vendor, ZTP ensures your code never leaves your environment. You get the ease of a "connected" tool with the security of a localized scanner.

3 ZERO BOTTLENECKS

ZTP removes the "security tax" on developers and puts security back in control of the security teams that know it best. With no individual commands to insert and no pipelines to edit, security teams get total visibility from day one.

RESULTS

Continuous Coverage and Executive Visibility

Transitioning from Snyk's manual deployment to Boost's permissionless ZTP model helped this enterprise to reclaim hundreds of hours of manual labor, transforming the Head of AppSec from a coordinator needing developer favors into an orchestrator capable of unilateral action and a fully-scaled rollout.

When Boost removed AppSec's dependency on developers, a program that had stalled for years became a persistent feature of the environment in a single afternoon. Boost's coverage scales autonomously and visibility is evergreen, with the Boost platform automatically ingesting and analyzing new code the moment a developer creates it.

Thanks to Boost, the solo AppSec lead now manages the entire **700-repo enterprise with 100% visibility** while dedicating only half of his time to the program. The operational drag of Snyk's legacy tooling has been fully replaced by Boost's automated system that requires zero manual maintenance to scale.

Automating infrastructure with Boost Security provided the AppSec lead with a new level of professional confidence when reporting up to senior leadership. Instead of anecdotal progress and limited visibility, he can now provide management with weekly, data-driven reports that justify security investments, thanks to Boost's native reporting capabilities.

> **Senior management spends the money, and that means they need to know whether our tools have been used, who is using them, and the progress we made," the lead explained. "Now they can see exactly what is being resolved each week. Boost makes my life much, much easier.**

boost® security.io

Get in Touch

info@boostsecurity.io

3 Place Ville Marie, Montreal

H3B-2E3, QC, Canada

boostsecurity.io