apiiro

CASE STUDY

How Navan automated AppSec governance throughout the development lifecycle

NAVAN

apiiro

Background

The application security team at Navan is responsible for managing security throughout the development lifecycle, ensuring all security processes are correctly implemented, followed, and maintained. They were also tasked with expanding their application security automation and implementing a shift-left security approach. By detecting and resolving security issues earlier in the development lifecycle, Navan hoped to save time fixing them reactively.

Navan adopted Apiiro's Cloud Application Security Platform to automate its application security visibility, risk assessment, remediation, and prevention.

NAVAN

Navan is a corporate travel, card and expense management platform that empowers its customers to seamlessly manage business travel, corporate cards and expenses using AI-driven technologies.

Industry: Corporate Travel Management

Employees: 2K+

Developers: 250+

Highlights

Navan gained nearly instant visibility into all its components, risks, and material changes across repositories and applications.

Navan replaced manual security reviews and alert triage with automated risk assessments and prioritization across hundreds of weekly pull requests.

Navan shifted application security earlier in the development lifecycle with actionable, risk-based developer guardrails.

The Challenge: Automating security early in the development lifecycle at scale

Like many AppSec teams, Navan's didn't have nearly enough cycles or resources to manually keep up with the hundreds of pull requests created each week. Even with multiple AppSec tools in place, they couldn't guarantee that new changes were risk-free. Inundated with alerts, they also struggled to understand how constant code changes would actually impact their application attack surface.

Without a consolidated and automated way to prioritize noisy alerts, the Navan AppSec team needed a solution to reduce noise, ensure accuracy, and determine the most critical risks that needed to be remediated.

apiiro

The Solution: Continuous visibility and governance

Shortly after integrating Apiiro into their source control manager (SCM), Navan started getting continuous visibility into risky areas and behavior. By consolidating findings from native and third-party tools into a single pane of glass, Apiiro was able to correlate, deduplicate, and prioritize alerts to focus on what matters. By knowing what was and wasn't a real risk, the Navan AppSec team freed up triage cycles and dramatically cut down the alert backlog.

After assessing and understanding their risk, Navan implemented automated workflows to alert their AppSec team when a risky commit or pull request was introduced. That proactive approach and Apiiro's ability to tie risks to code owners decreased the time it took them to remediate issues.

Apiiro recognizes and classifies risks in a way I have not seen any other company do.

Tarik Ghbeish,
Manager of Application Security

NAVAN

The Impact: Reducing overall application risk

By automating Navan's application security visibility, risk assessment, remediation, and prevention, Apiiro helped optimize its team resources while reducing its overall application risk.

01 **Apiiro enables Navan to continuously and automatically maintain visibility across their applications and identify material changes that may create risk.**

02 **Apiiro's risk-based alerts allow the AppSec team to ensure that out of hundreds of pull requests each week, risky changes are identified automatically.**

03 **With Apiiro's built-in code security solutions, Navan can gain visibility into risks such as exposed API keys and credentials in code, sensitive data, and more at scale.**

Prioritize and remediate application risk with deep code analysis and runtime context.

Learn more | Get an Apiiro demo