apiiro

CASE STUDY

How Rakuten Rewards saves hundreds of hours triaging application security alerts monthly

Rakuten

Background

The Rakuten Rewards security team is responsible for security design practices, security operations, privacy, and compliance. Their goal is to maintain a strong security and risk posture across applications and infrastructure to ensure the highest level of security for internal systems and customer data—with the most efficient tools and processes possible.

With thousands of projects and repositories, Rakuten Rewards needed a solution to help them effectively understand their risk posture at scale and give them a framework to quickly make risk-based security decisions for their existing backlog of alerts and proactively for new code changes.

Rakuten

Formerly eBates, Rakuten Rewards provides cash-back and shopping rewards. It has 12 million members who have earned over $1 billion in cash back at their favorite stores.

Industry: Technology, Information and Internet

Employees: 400+

Developers: 100+

Highlights

Rakuten Rewards saved hundreds of hours each week manually triaging alerts and reviewing code for application risks with Apiiro's code-to-runtime context.

Rakuten Rewards was able to efficiently shift security left to surface risks proactively with Apiiro's risk-based developer guardrails.

Rakuten Rewards leveraged Apiiro's automated workflows and consolidated AppSec platform to improve DevSecOps efficiency and make risk-based decisions.

The Challenge: Understanding application risk continuously and at scale

Despite having several existing automated application security tools to identify vulnerabilities and misconfigurations, the biggest challenges the Rakuten Rewards team faced were being able to truly understand their application risk posture—from design to production and address security alerts based on risk. Without visibility and control over their application risks throughout the development lifecycle, they found it challenging to ensure effective and efficient security across their thousands of projects and repositories.

The Solution: A continuous, risk-based approach to improving application security

To give Rakuten Rewards a solid understanding of their risk, Apiiro first provided visibility into all their technologies, frameworks, infrastructure, languages, data, and more. That code-based inventory provided them with deep visibility into their repositories and continuous, real-time monitoring for changes.

Now the Rakuten Rewards security team can understand their application security posture in real time—including on every new commit—and has the context needed to triage risks effectively. In addition to prioritizing and surfacing the critical risks to the application security team and developers at the right time, Apiiro also provides bird's-eye view dashboards so Rakuten Rewards can understand their overall application security posture and drill down to the details as needed.

> "With Apiiro, our security team is **saving hundreds of hours every month.**"
>
> Cloud Security Architect
> **Rakuten**

The Impact: Improving AppSec efficiency

With its deep code-based inventory as a foundation, Apiiro contextualizes new risks based on Rakuten Rewards' application and business to help them make risk-based security decisions.

01 Apiiro enables Rakuten Rewards with context to save hours triaging and prioritizing alerts in a single platform and make risk-based application security decisions.

02 Apiiro's shift-left approach improves their development and security team's efficiency by embedding risk-based guardrails earlier in the development lifecycle.

03 With Apiiro's workflows, Rakuten Rewards automates previously manual tasks, such as triggering security code reviews and vulnerability remediation cycles.

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

Learn more   Get an Apiiro demo