CASE STUDY

How Paddle created a force multiplier for AppSec with Apiiro

paddle

© 2024 Apiiro

The challenge: Delayed releases due to reactive security

As a small application security team building out its AppSec program, Paddle knew they needed a way to multiply their efforts and foster better collaboration with development teams. Vulnerabilities from their existing tools were being surfaced too late in the SDLC, leading to delayed code releases and internal friction. But collaborating with the developers or engineering teams to address risks was also challenging because they didn't have insight into who owned what.

Paddle sought a solution to help them adopt a proactive, developer-centric approach to application security and optimize their existing tooling and manual risk assessment processes such as pen tests, security code reviews, and threat modeling.

Paddle is a payments infrastructure provider, enabling software companies to respond faster and more precisely to every growth opportunity.

Industry: B2B Software

Employees: 300+

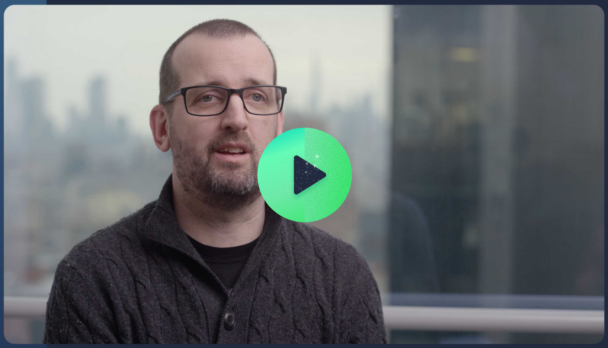
Developers: 80+

Highlights

As Paddle built out its application security program, they sought a partner to enable them to act as a force multiplier to boost their proactive security efforts and focus on the most business-critical risks.

With Apiiro's deep ASPM platform, Paddle was able to get an aggregated view of their application inventory and a single hub for enforcing security policies earlier in the development lifecycle.

Apiiro not only ingested and enriched Paddle's existing security testing but also consolidated and expanded their security coverage with next-gen open source security, secrets security, and software supply chain security.



> "Apiiro has allowed us to get much higher engagement from our development teams because the data we receive from Apiiro is timely, is contextual, and is actionable."

Jonny Herd
VP of InfoSec & Enterprise Technology

Watch the video →

© 2024 Apiiro

The solution: Developer-centric and risk-based AppSec

Paddle rolled out Apiiro in a staged approach to gain visibility across its application estate, use that context to build risk-based policies and developer workflows, and then measure and optimize their program success over time.

Through Apiiro's easy-to-install GitHub integration, Paddle quickly got a complete inventory across their nearly 500 repositories, including technologies, open source usage, exposed secrets, sensitive data, and development behavior. That visibility, coupled with the ingestion of vulnerability findings from existing tools, gave them an aggregated view of risks. It also enabled them to prioritize based on business impact and risk likelihood and connect risks to their root cause in code and developer owner.

Apiiro also provides a single hub for implementing policy-as-code, helping automate developer guardrails and enforce application security best practices on every pull request. This allows Paddle's application security team to meet the developers where they're comfortable with a common taxonomy.

Bonus use case: Deepening security coverage with Apiiro SCA + SSCS

In addition to leveraging Apiiro's ASPM to solve their core challenge of enabling a developer-centric approach to security, Paddle saw Apiiro as an opportunity to consolidate and deepen their application security testing coverage.

Paddle now leverages Apiiro's open source and software supply chain security solutions, giving them fully integrated visibility and risk detection across open source packages, repositories, and pipelines.

apiiro

Open platform augmented by native solutions

In addition to ingesting security findings from any and all security tools, Apiiro provides native visibility and risk detection for open source packages, pipelines, source control managers, exposed secrets in code, and more.

> "Since introducing Apiiro's Software Supply Chain Security (SSCS) at Paddle, we have been able to ensure pipelines are set up securely and have improved insights into the configuration of our source control repositories—a capability not provided by traditional AppSec tools. This heightened visibility, coupled with Apiiro's risk-based prioritisation and policy engine, instills confidence in our capability to continually measure supply chain risk and assess against best practice moving forward."

paddle

Colin Barr
Senior Engineering Manager - Application Security

The impact: Minimizing and optimizing security reviews

Apiiro’s continuous application inventory, policy-as-code engine, and application risk control plane have acted as a force multiplier for the Paddle application security team.

01 Apiiro monitors 100+ pull requests per week, blocking high-risk changes that need additional assessments, and giving developers the remediation context they need right then and there.

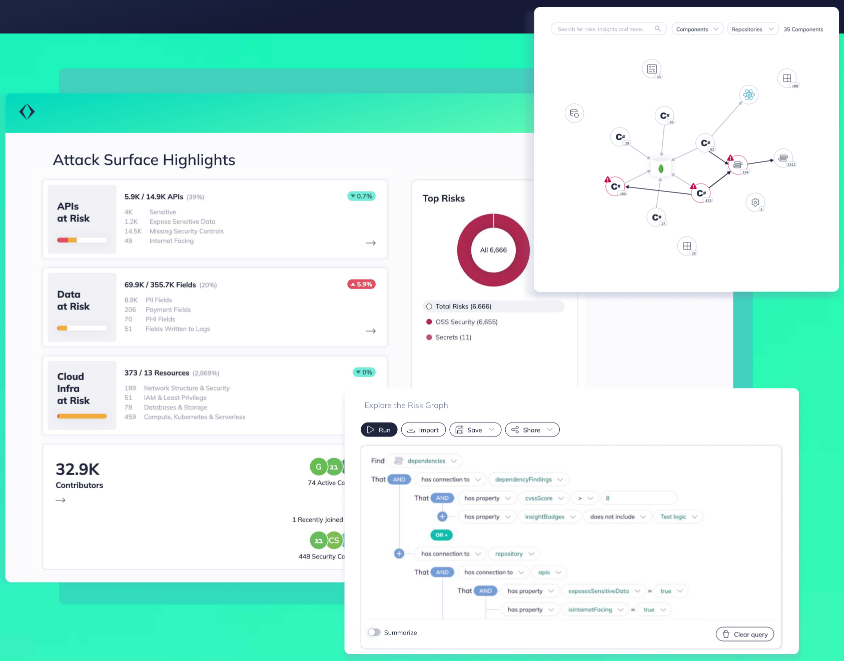
02 By saving them time combing through all code changes to identify only relevant, risky ones, Apiiro acts as a force multiplier for the Paddle application security team, giving them back 2 days' worth of work per week.

03 Apiiro's reports and dashboards allow everyone—from executives to security champions—to measure risk and understand security's impact on engineering productivity metrics such as those outlined in DORA.

> “The unique value that Apiiro provides Paddle is as a force multiplier we can do more with less, we can meet the developers where they’re comfortable, we can provide them the information that they need to fix or to mitigate issues in a single unified view.”

paddle

Jonny Herd
VP of InfoSec & Enterprise Technology


Search for risks, insights and more...
Components
Repositories
35 Components
Attack Surface Highlights
APIs at Risk
5.9K / 14.9K APIs (39%)
▼ 0.7%
4K Sensitive
1.2K Expose Sensitive Data
14.5K Missing Security Controls
49 Internet Facing
Data at Risk
69.9K / 355.7K Fields (20%)
▲ 5.9%
8.9K PII Fields
206 Payment Fields
70 PHI Fields
51 Fields Written to Logs
Cloud Infra at Risk
373 / 13 Resources (2,869%)
▼ 0%
189 Network Structure & Security
51 IAM & Least Privilege
78 Databases & Storage
459 Compute, Kubernetes & Serverless
32.9K
Contributors
74 Active Co
1 Recently Joined
448 Security Co
Top Risks
All 6,666
Total Risks (6,666)
OSS Security (6,655)
Secrets (11)
Explore the Risk Graph
Run
Import
Save
Share
Find dependencies
That AND has connection to dependencyFindings
That AND has property cvssScore > 8
has property insightBadges does not include Test logic
OR +
has connection to repository
That AND has connection to apis
That AND has property exposesSensitiveData = true
has property isInternetFacing = true
Summarize
Clear query

Apiiro Deep ASPM

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

Get an Apiiro demo