Industry:
Financial Services

Full Speed, Full Coverage: How Adyen Secured Millions of Lines of Code Without Friction

Hundreds
Daily merges secured without pipeline disruption

MM+
Lines of code under automated, policy-enforced protection

0
Malicious packages reaching production since deployment

How one of the world's leading payment platforms embedded security into a monolith without adding friction to the people building it.

ABOUT THE CUSTOMER

Adyen is one of the world's leading financial technology platforms, providing end-to-end payment infrastructure, data insights, and embedded financial products in a single unified solution. Trusted by some of the world's largest brands, **Adyen processes billions in transactions annually across dozens of markets, where milliseconds of latency and absolute reliability aren't ambitions, but requirements.**

ABOUT THE CUSTOMER
Amsterdam, Netherlands

Industry
Financial Technology

Scale
Hundreds of developers, MM+ lines of code

JFrog products
JFrog Artifactory · Xray · Curation

Challenge

Adyen's DevSecOps team was faced with a common current compounding issue: as the dependency footprint grows across multiple languages and hundreds of open-source packages, so does the blast radius of any security intervention. For Adyen, hundreds of developers push several hundred merge requests every day into a multi-language monolith exceeding tens of millions of lines of code. A single broken dependency doesn't just affect one team; it can stop the entire development environment.

> When you're dealing with a monolith at this scale, so many languages, so many teams, a day, imagine if a vulnerability or a pipeline issue hits. It scales instantly. All pipelines break. Nobody can move forward, nobody can merge, nobody can ship.
> *– Supun Vidana Pathiranage, DevSecOps Specialist, Adyen*

The team needed security that was invisible when things went right, and decisive when they didn't.

Solution

Rather than layering security onto existing pipelines, Adyen built a centralized "Security Gateway," a managed architecture that lets the security team evolve policies in the background while developers keep shipping at full velocity. JFrog Curation and Xray form the twin pillars of this gateway, creating a layered defense from the moment an open-source package is requested to the moment a container is deployed to Kubernetes.

> Frog Curation is a firewall for open-source packages. You instill policies that defend the organization, but the goal isn't to say no. It's about how we can help developers continue their work without disrupting their workflow. We enable development, we don't block it.
> *– Supun Vidana Pathiranage, DevSecOps Specialist, Adyen*

JFrog Curation

The Front-Line Firewall

Curation acts as a transparent proxy for every open-source package request. Adyen enforces two non-negotiable policies: an immediate build break on any malicious package detection, and a 21-day maturity rule that prevents bleeding-edge dependencies from entering the ecosystem before they've been vetted by the community. JFrog's Compliant Version Selection (CVS) automatically resolves dependencies to the most policy-compliant available version; eliminating developer toil without requiring a single manual intervention.

JFrog Xray

Deep Scanning at the Merge

While Curation controls the front door, Xray delivers granular SCA scanning at the merge request level – the highest-leverage point in Adyen's pipeline. Combined with Secret Scanning, SAST (via Semgrep and SonarQube), and container image scanning, Xray gives the security team a unified view across build artifacts, golden container images, and Kubernetes-destined releases. As Adyen consolidates all package storage in JFrog, Xray becomes the single source of truth for compliance posture across the entire estate.

Battlestar Integration

Signal, not Noise

By combining Terraform-managed infrastructure and OIDC (OpenID Connect) keyless authentication in GitHub Actions, pipeline interactions with JFrog are now identity-based and ephemeral – no more long-lived tokens, no credential sprawl and no single key that can unlock the supply chain.

Unified Visibility

Single-Pane Security Posture

Adyen's DevSecOps team operates a centralized dashboard tracking repository coverage (reaching 100% in production), active policy watches, and gap analysis across staging and production environments. This single-pane view allows the team to enforce PCI compliance and internal security standards across the full 35-million-line estate without touching individual developer pipelines.

> Compliant Version Selection is a big helper for our immature package policy. It's one flag in Curation and JFrog automatically falls back to the most compliant version of that dependency. It's frictionless and fully transparent for the developer, and everything has an audit trace so you can see the context behind it.
> *– Supun Vidana Pathiranage, DevSecOps Specialist, Adyen*

Results

By integrating JFrog into their core architecture, Adyen has achieved a state where security is a seamless part of the developer experience.

- **Zero malicious packages in production**
  Curation's non-negotiable block policy eliminates the threat at the source, before it can cascade into a platform-wide incident.
- **Zero security-induced halts**
  The Security Gateway operates transparently. Developers ship at the same velocity as before, with security enforced in the background.
- **Automated dependency remediation at scale**
  CVS resolves compliance issues before they surface as developer blockers, turning a manual security task into a silent background process.
- **100% production repository coverage**
  Full coverage is tracked continuously, not periodically, meeting PCI compliance as a matter of course.
- **Actionable security feedback, not alert noise**
  Battlestar turns JFrog findings into triaged, developer-ready tasks, preserving focus without sacrificing security visibility.

WHAT'S NEXT?

As Adyen completes its migration of all package storage to JFrog, the team is expanding Xray's merge-request-level policy enforcement across every language and repository. The Security Gateway architecture, built to evolve without developer disruption, positions Adyen to adopt new JFrog capabilities, including advanced container runtime security, without reengineering the pipelines that run one of the world's most critical payment platforms.

> Before touching any tool, think about the problem it's going to solve. Address the business needs, not the tool. Think about the potency of what you're bringing in, the value it delivers, and whether it's going to help things run smoothly. Work gradually. Don't try to boil the ocean.
> – *Supun Vidana Pathiranage, DevSecOps Specialist, Adyen*

v1.0251217

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd