Industry:
Financial Services

LEDGER

Fortification Boost: How Ledger and JFrog Implemented a Security-First Software Supply Chain

Single Source of Truth

All software artifacts are unified across cloud, on-prem and firmware – globally

Zero-Trust OSS Ingestion

Open-source dependencies pass strict risk thresholds before entering the development environment

Keyless CI/CD Authentication

OIDC keyless authentication mitigates credential exposure across all GitHub Actions pipelines

How the world's leading digital asset security and self-custody company unified its infrastructure, automated open-source vetting, and eliminated static secrets from CI/CD – without compromising development velocity and application security.

About Ledger

Headquarters
Paris, France

Security Model
Two specialized teams: Product Security and Cybersecurity Engineering

Industry
Digital asset security / hardware

JFrog Products
JFrog Artifactory · JFrog Xray · JFrog Curation · JFrog Advanced Security

Ledger is the global leader in digital asset security for individuals and institutions, best known for the Ledger Signer – the gold standard for secure ownership of digital value. In addition to developing hardware, Ledger operates a vast and complex software ecosystem including:

- **The Ledger Wallet™ App**
- **Cloud-Native Web Services**
- **Firmware for Embedded Devices**
- **Manufacturing Systems for Hardware Production**

Across all of these products, services and processes, a single security failure doesn't just compromise a specific product, but can potentially threaten the financial holdings of millions of customers.

Challenge

Established more than a decade ago, Ledger's global operations have scaled significantly, with its software artifacts expanding across multiple systems – GitHub, Harbor, local FTP servers, and various package registries spanning Cargo, Conan, and npm. For a fintech company with stringent security requirements this dispersed structure could be improved.

The security team needed a single, audited source of truth, to check that the artifact in staging was the same artifact that reached production, as well as a mechanism for scanning open source packages used by developers for potential vulnerabilities prior to usage.

In an important strategic shift, the Security Engineering team took an increasingly proactive approach to help secure their software supply chain without impeding developer speed. This means identifying and stopping potentially malicious code before it even has the opportunity to enter the development environment. All this must be done in a way that doesn't create friction between engineers working across multiple environments.

> As Ledger scaled, maintaining consistent visibility and control across multiple artifact ecosystems became increasingly complex. The objective was to consolidate this into a stronger, auditable, and security-first model.
>
> **— Enguerrand Allamel, Staff Cloud Security Engineer, Ledger**

Solution

Ledger selected the JFrog Platform as the core of its software supply chain – deploying a hybrid architecture spanning Kubernetes on AWS, and on-prem data centers to serve the full range of Ledger's business units.

To ensure the success of their security-first approach, JFrog Artifactory became the mandatory repository for every type of software artifact. This includes everything from open-source dependencies entering the environment, to packages published to public registries for Ledger's partners and ecosystem.

JFrog Curation

A firewall for open-source dependencies

Before any open-source package can enter Ledger's development environment, it is designed to pass through JFrog Curation. Ledger enforces strict, custom risk thresholds - blocking all dependencies with a threshold CVE score, as well as proactive detection of malicious packages and typosquatting attempts. The result is an intelligent gatekeeper that gives developers freedom to pull pre-scanned, secure OSS packages as they need them.

JFrog Advanced Security & JFrog Xray

Continuous compliance for all binaries

JFrog Xray and JFrog Advanced Security provide deep scanning across Ledger's full artifact ecosystem supporting Rust (Cargo), Python, npm, Docker, and more. The resulting vulnerability detection, secrets scanning, and metadata verification give Ledger's security team the ability to audit any artifact, at any point in the lifecycle, with the intention of confirming it is exactly what it claims to be. Kubernetes cluster visibility means every image running in production can be traced back to a verified, JFrog-managed origin.

GitHub Actions + OIDC

Zero static secrets in the pipeline

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.

Hybrid Deployment

1 platform, 3 distinct environments

Ledger's product surface spans hardware firmware (extreme lockdown), backend services (strict), and web applications (agile). JFrog's hybrid deployment – AWS plus on-premises – allows each environment to operate under its own security policy while feeding into a single, unified artifact registry. This enables the security team to enforce compliance globally without requiring valuable enineering team hours to manage infrastructure.

> With JFrog Curation and Xray, we have a genuine firewall for our dependencies. Developers can pull what they need – packages are already audited, verified, and cleared before they touch it. Security becomes a property of the environment, not a step they have to remember.
>
> **— Enguerrand Allamel, Staff Cloud Security Engineer, Ledger**

Results

The JFrog Platform has boosted Ledger's software development operations, providing a secure foundation for the company's ongoing growth and innovation.

Business value realized with JFrog:

- **Single Source of Truth Achieved:** Artifacts, including web, backend and containers, are now managed through JFrog across cloud and on-prem environments, eliminating the fragmented registry sprawl that can create blind spots.
- **Zero Static Credentials in CI/CD:** OIDC-based keyless authentication has eliminated long-lived tokens from all GitHub Actions pipelines, removing the attack vector that defined the industry's most damaging recent supply chain attack.
- **Hybrid Compliance at Scale:** Three distinct security environments – from locked-down firmware to open web services – are now managed under a single unified platform with environment-specific policies enforced automatically.
- **Proactive Dependency Defense:** JFrog Curation automatically blocks malicious packages, typosquatting attempts, and any dependency exceeding Ledger's CVE risk threshold – before developers ever encounter them.
- **Prevention of Software Supply Chain Security Incidents:** Consolidating with JFrog helps Ledger prevent software supply chain security incidents linked to their packages.
- **Full Production Kubernetes Visibility:** Every container image running in Ledger's production clusters can now be traced to a verified, JFrog-managed origin, turning runtime provenance from an audit exercise into a continuous guarantee.

> The best impact we've seen from JFrog is unification. We no longer have artifacts scattered across different systems. Everything is in one place, with the visibility and control that our security team requires and the simplicity that our developers deserve.
>
> **— Enguerrand Allamel, Staff Cloud Security Engineer, Ledger**

What's Next?

JFrog is now the mission-critical infrastructure for Ledger. Not a point tool for the security team, but a platform the entire software supply chain is built upon. As Ledger continues to scale its operations, the team is deepening its use of JFrog Advanced Security for runtime artifact analysis and extending policy enforcement further left into the development lifecycle. For a company whose essence is trust, the ability to check the provenance, integrity, and security of every artifact, from commit to customer, is not a feature - it's a foundation.

> Frog is a core component for our environment; all of our software supply chain management is based on it. It is mission-critical for us, which is why we are continuing to expand our use of the platform as we keep moving forward.
>
> — Enguerrand Allamel, Staff Cloud Security Engineer, Ledger

v1.0240129

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.

LEGAL STATEMENT

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd