



National Energy Operator's Journey to DevSecOps Excellence with JFrog



Single System of Record
for Secure, Automated
Software Releases



Integrated Security at
Every Stage of
Development



End-to-end Auditability &
Traceability

\$4M

Annual savings through
automation and process
improvements

1,000+

Proactive blocking of
potential vulnerabilities
by JFrog Curation

3000

Pipelines under
management



"For us, it's about visibility, traceability but it's also really about auditability and being able to monitor in real time what people are doing – as a lot of them are in small self-contained siloes. By pushing everything through the JFrog Platform, we're achieving the capability of really understanding what's happening internally with our technology at any time."

DevSecOps Team Lead, National Energy Operator

Company Overview

This energy operator and facilitator is responsible for ensuring the efficient and secure delivery of energy to millions of consumers. It manages the national electricity markets, providing energy and gas grid operations across the country. This includes monitoring supply, demand, voltage and frequency, as well as managing planned outages and emergencies.

They are also responsible for the national electricity and gas exchange, where energy-related services are bought and sold according to supply and demand. This allows electricity generators to sell their electricity to retailers, or gas suppliers and distributors to schedule their deliveries for the day. Their goal is to provide the lowest available prices, settle trades, and ensure that accurate data and information flows between stakeholders.

With 400 unique applications in production and over 100 developers working across its systems, they operate at the intersection of technology, energy trading, and critical infrastructure. The increased demand for applications has led to challenges related to scaling software development operations while adhering to the highest standards of security and quality that are required for critical infrastructure operators.

Challenges

The company was faced with a number of challenges regarding their software development operations mainly due to continued dependence on manual processes, legacy systems, unaddressed security gaps and limitations regarding scalability.

Before deploying the **JFrog Platform**, their development environment included manual processes to build and deploy applications, which led to inefficiencies and potential security risks. The human error associated with these processes opened the door for security issues that could potentially ripple across their critical systems. As a result, each deployment was essentially an ad-hoc plan that could not be translated into a repeatable motion. Therefore, when vulnerabilities or other issues were discovered further down the SDLC, they would have to roll back the entire development process, resulting in missed deadlines and financial loss due to inefficient use of resources.

These challenges made it difficult to react to discovered vulnerabilities and hindered the DevOps team's ability to scale their development program. For an organisation responsible for powering a national grid, these vulnerabilities posed unacceptable risks and had to be dealt with immediately.

Adding to the complexity was the issue of knowledge silos. Key deployment information was stored with individual team members, making the system susceptible and prone to disruptions because there was no direct access to important information about the software components and dependencies that were part of a specific build. This lack of shared knowledge not only created bottlenecks but also exposed the organisation to continuity risks.

With no automated scanning mechanisms in place, the process of identifying and addressing critical vulnerabilities was time-consuming and unreliable. The DevSecOps Team Lead expressed the seriousness of the situation when he remarked that: **"Manual processes made scaling a nightmare. We knew we needed a comprehensive transformation to automate, secure, and streamline our pipelines, and that's how we found JFrog."**

Solution

After a rigorous evaluation process, the DevOps and Security teams selected the JFrog Platform to provide a solution for their requirements. It answered their need for a single source of truth covering software builds, artifacts, and releases, that was accessible by all stakeholders anywhere and anytime, which was key in their decision to partner with JFrog.

By adopting the JFrog Platform — including JFrog Artifactory, JFrog Xray, JFrog Advanced Security, and JFrog Curation — they transformed their DevSecOps practices, achieving significant operational efficiencies, enhanced security, and millions in cost savings.

With JFrog Artifactory storing and managing the software components used and generated throughout the software supply chain, the team no longer needed to rely on manual processes for deploying individual applications. They also benefitted from guaranteed repeatability, as opposed to the ad-hoc process that had previously been part of their deployment process.

With over 400 unique applications in production and releases involving over 25 different versions of over 25 unique applications, the JFrog Platform provided them with a single source of truth to deliver scalability, reliability, and stability, along with automation of crucial security and operational tasks, while eliminating performance bottlenecks.

Their implementation began with JFrog Artifactory and JFrog Xray and later expanded to include JFrog Advanced Security and JFrog Curation.

The key benefits for each module include:

JFrog Advanced Security

- ✔ **Contextual Analysis:** Automates the prioritization of vulnerabilities based on JFrog's proprietary research, enabling the security team to focus on high-risk issues.
- ✔ **Secrets Detection:** Identifies and mitigates the use of hardcoded secrets in real-time, fostering better security practices across teams.
- ✔ **Behavior Monitoring:** Provides visibility into developer activities, ensuring compliance and addressing misconfigurations without disrupting workflows.



With JFrog Advanced Security, we saw value on day one. It's a game-changer for contextualizing vulnerabilities and protecting our systems.

JFrog Curation

- ✔ **Trusted Repositories:** Enforces the use of vetted packages, blocking unapproved dependencies and enhancing overall system integrity.
- ✔ **Proactive Blocking:** Prevents hundreds of risky downloads. Within weeks of implementation, it already blocked thousands of potentially dangerous packages, resulting in immediate safety improvements.

- ✔ **Auditability and Traceability:** Offers comprehensive reporting on package usage, enabling DevOps tracking and optimization for its software supply chain operations.
- ✔ **Integration with SIEM:** Facilitates the ingestion of logs into centralized security systems, allowing for real-time monitoring and actionable alerts.



Curation has given us unprecedented traceability. It's not just about blocking unsafe packages; it's about educating our developers and improving our overall code quality.

Results

The DevSecOps team significantly improved scalability and now supports thousands of pipelines, repositories, and developers on a single platform, ensuring seamless operations as opposed to previously siloed teams and processes.

Their adoption of the JFrog Platform has delivered transformative results, and the team is anticipating even more forward-moving traction as they begin to see the results of the recent JFrog Curation deployment. The ability to implement automated scans and contextual analysis with JFrog Advanced Security has significantly improved code quality as well as enhanced their security posture.

Other key benefits include:

- ✔ **Immutable releases:** JFrog Artifactory ensured reliability with a single source of truth, enhancing deployment repeatability and rollback capabilities.
- ✔ **Improved governance:** Centralized control over artifact storage and developer behavior, enhancing compliance and reducing risks. The team is now able to prevent hundreds of unsafe downloads, ensuring safer local environments.
- ✔ **Cost savings:** Achieved approximately \$4M in annual savings through automation and process improvements.
- ✔ **Operational efficiency:** Scaled from managing five pipelines to over 3,000 pipelines and 4,000 repositories, supporting 100+ developers.
- ✔ **Contextual analysis:** The DevSecOps team gained deeper insight into CVE findings with vulnerability data from JFrog's Security Research team, allowing them to reduce noise and focus on actionable threats.
- ✔ **Secrets detection:** The ability to identify secrets exposed in source code and binaries helps the team improve team behaviors by uncovering and addressing potential vulnerabilities.
- ✔ **Traceability:** Gained real-time insights into the behavior of siloed teams, enhancing visibility and auditability. The team is now able to see what is actually being downloaded, which machines have specific packages on them and if vulnerabilities are being ignored and by whom. This level of traceability is unprecedented and allows them to proactively identify and manage vulnerabilities.

In three words, the DevSecOps Team Lead describes JFrog as “forthcoming, proactive, and reliable.” The company's partnership with JFrog underscores the power of innovation and collaboration in driving meaningful transformation in the energy sector.

The JFrog Software Supply Chain Platform

The ability to provide access to all software artifacts, remediate potential vulnerabilities, and increase operational efficiency at scale is what the JFrog Platform is all about. Whether it's operations, security, MLOps, or IoT, our EveryOps solution means a single end-to-end development platform covering all your software development requirements..

We invite DevOps and Security professionals from the energy sector who are managing software updates to edge devices to schedule a [one-on-one demo](#) or take an [online guided tour](#) and see how the JFrog Platform changes the way IoT software is developed and delivered to the edge.



Implementing JFrog has fundamentally changed how we operate. It's not just about cost savings but about creating a resilient, scalable system for the future. Any software that goes through the approved JFrog build and release pipeline helps us achieve our quality and security goals that enable us to serve our customers more effectively and efficiently.

DevSecOps Team Lead, National Energy Operator

Products

[The JFrog Platform](#), [JFrog Artifactory](#), [JFrog Xray](#), [JFrog Advanced Security](#), [JFrog Curation](#)

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.



Start for free at <https://jfrog.com/start-free>

LEGAL STATEMENT

Copyright © 2024 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.



www.jfrog.com



www.twitter.com/jfrog



www.facebook.com/artifrog/



www.linkedin.com/company/jfrog-ltd