SOLUTION SHEET

JFROG SECURE SOFTWARE SUPPLY CHAIN:

Enabling the Federal Government to Fulfill its Trusted Mission

THE CHALLENGE

U.S. military branches and civilian agencies require trusted software in order to accomplish mission objectives and serve citizens. Whether this be on-premises in an "air gap" deployment, connected to the internet or hosted at a cloud service provider, the Federal government needs the confidence that the applications they deploy can be distributed securely from a trusted source and are composed of known, safe binary code components.

> Iron Bank: Trusted Software Repository

To be assured that compiled applications can be delivered from a validated source, the U.S. Department of Defense (DoD) has created a repository of digitally signed, binary container images called Iron Bank, also known as the DoD Centralized Artifacts Repository (DCAR). This repository of containers includes both Free and Open-Source software (FOSS), and Commercial off-the-shelf (COTS) software components. All artifacts are hardened according to the DoD Container Hardening Documents. The container images in Iron Bank have been accredited for use throughout the DoD and are currently published to the Iron Bank container registry.

Iron Bank is an initiative of the DoD's Platform One DevSecOps Enterprise Services team. This team manages software factories for DoD-related development teams so they can focus on building mission applications.

> Federal Government Security Guidance and Regulation

Furthermore, per the U.S. President's Executive Order on Improving the Nation's Cybersecurity, guidelines have been issued recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition analysis tools, and penetration testing.) The focus will be on not only performance testing, but also on how software is built and compiled, and the testing and manufacturing process. The results are known as the software manifest or software bill of materials (SBOM.)

This Executive Order will apply to all Federal Acquisition Regulation (FAR) contracts. In other words, any organization doing business with the Federal government will be required to understand the ability of their underlying data governance frameworks to classify, manage and protect sensitive data (i.e., controlled unclassified information [CUI].)

In addition, businesses will be expected to collect information related to threats, vulnerabilities and incidents and share it with relevant Federal agencies.

THE SOLUTION

To deliver on these challenges, the JFrog DevOps Platform provides enterprise-grade binary artifact management and software composition analysis solutions that meet the security standards defined by the US government. JFrog Artifactory is your "DevOps Database" for binaries, dependencies, and build artifacts for release management. Xray provides open source binary vulnerability and license compliance scanning, and allows you to see into all of the underlying layers and dependencies of binaries and container images. Both are available for use on-premises and in the public cloud. Both Artifactory certification and Xray certification are active on the Iron Bank registry.

Furthermore, in order to help organizations comply with the Executive Order on Improving the Nation's Cybersecurity, Artifactory provides an SBOM showing in detail the components that make up the software you build. Xray runs a deep recursive scan on the build down to the deepest level dependency, and if any vulnerabilities or license compliance issues are found, Xray can be configured to return an alert, fail a build, send a webhook or prevent a download. Xray scanning alerts are an effective way to address vulnerabilities and licence compliance issues, and prevent any infected builds from being delivered to and by the Federal government.

THE BENEFITS

Through compliance with Iron Bank and the Executive Order on Improving the Nation's Cybersecurity, the DoD and other Federal agencies gain confidence with JFrog Artifactory and Xray that the applications they deploy are of known good components and will help assure the Federal government that there is a secure chain of custody from packaging through deployment.

This helps ensure that mission objectives can be met confidently and quickly, and that citizens are securely served. Applying JFrog Artifactory and Xray to the software deployment needs of the DoD and Federal agencies aims to:

- Improve confidence in the security of on-premises and cloud-based applications
- Accelerate the adoption of secure applications
- Achieve consistent security authorizations using a baseline set of agreed-upon standards for Federal government deployments
- Ensure consistent application of best known security practices
- Increase automation and reduce manual effort

The JFrog Platform solutions provide a cohesive, seamless way to build integrity into your software development process to minimize risk and ensure compliance, create operational efficiencies, reduce time to deployment and minimize costs.

Please contact us at Federal@jfrog.com