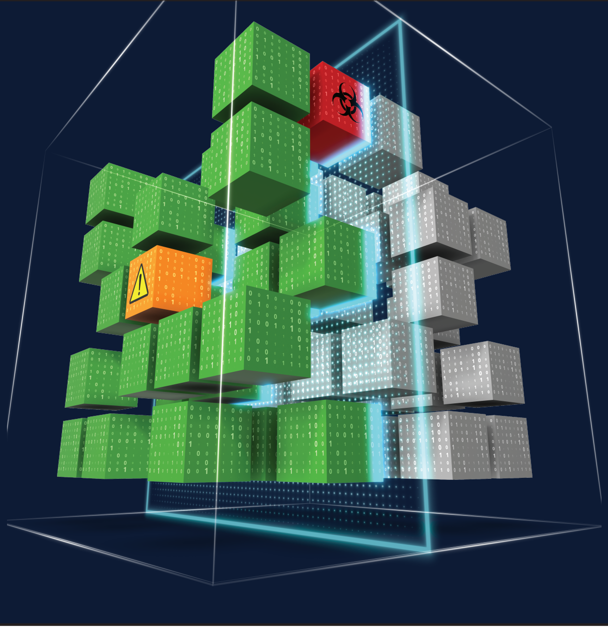
JFrog

SECURITY SOLUTION SHEET

JFrog RUNTIME

Fast Discovery and Remediation from Code to Production



The Challenge

Keeping your applications secure in runtime is a complex task. Organizations often struggle with maintaining real-time visibility into runtime vulnerabilities, effectively managing and prioritizing risks, and ensuring deployment integrity. The ultimate goal is to quickly identify and remediate vulnerabilities while minimizing business impact and accurately tracking all runtime components.

The Solution

JFrog Runtime enables Security, R&D and DevOps teams to effectively monitor Kubernetes clusters, quickly identify and remediate vulnerabilities, and ensure the integrity of images running in production. It tackles the critical challenge of securing applications in production by focusing on what matters most: real-time visibility into runtime vulnerabilities, and addressing risks that are critical, applicable, and running.

Reduce Risk by Instantly Closing Window of Exposure

Frictionless alignment between R&D, DevOps and Security: easily identify the source and owner of a vulnerable package to mitigate risks faster.

Gain Real-time Visibility into Runtime Vulnerabilities

Real-time visibility into your runtime environment, with rich data and comprehensive contextual analysis, help to accurately identify and respond to security incidents as they happen.

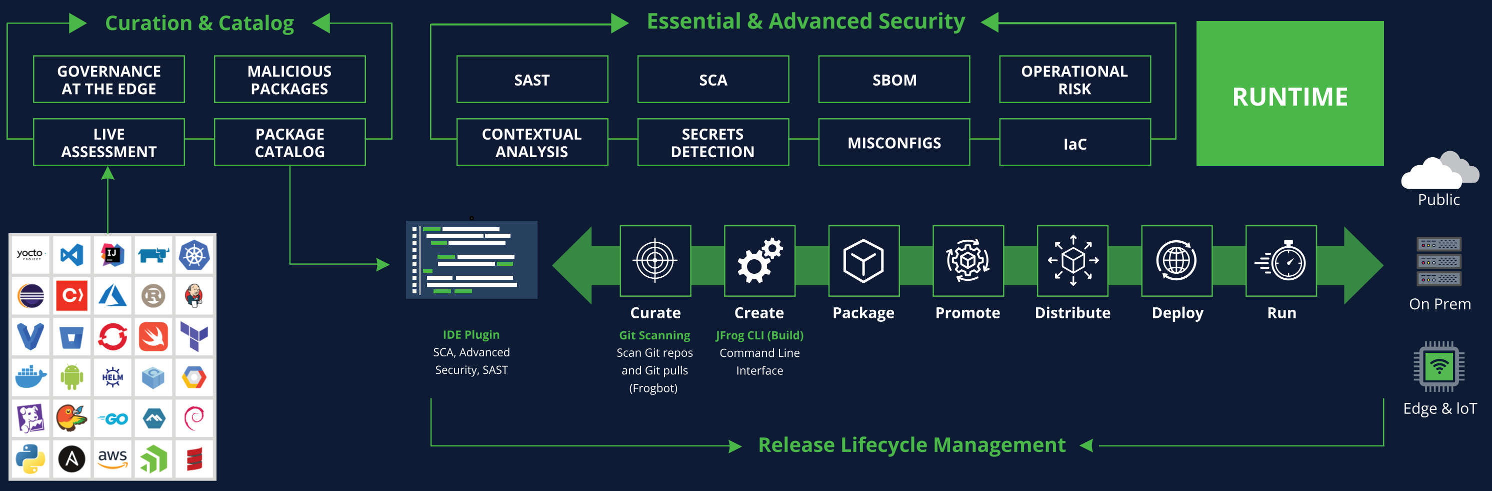
Accelerate Triage with Advanced Prioritization

Gain a deeper understanding of risk with contextual analysis, filter out irrelevant alerts, and prioritize security events based on potential business impact.

Verify Application Integrity in Production

Seamless integration between the software supply chain and production environment, automatically alerting on modifications and untrusted sources.

End-to-End Security from Left to Right



Key Features

Repository View

Full visibility into Artifactory repositories containing artifacts detected in the runtime environment.

Sensor Management

Easy installation and monitoring of sensors on clusters, tracking cluster health and node status.

Repository Image View

Rich information on images from the selected repository and their associated Kubernetes workloads.

Artifacts in Runtime

Identify artifacts running in production in Artifactory, highlighting vulnerabilities and their locations.

JFrog Artifactory

Serves as a universal repository manager and a single source of truth, securely storing and managing all artifacts and Docker images with metadata for traceability and verification.

Essential & Advanced Security

Scan images for vulnerabilities and license violations, prioritize risks based on potential business impact, and remediate faster with guided steps provided by JFrog Security Research.

Metadata Management

Enables attachment of metadata to artifacts and Docker images, storing integrity verification and compliance information.

How Enterprises Use JFrog

Easily discover and manage running packages across multiple cloud vendors through a single management console. With JFrog Runtime you can quickly find where each package is located in Artifactory and structure your repositories based on what's currently running. By organizing repositories according to environment type and activating Xray and JFrog Advanced Security policies, you can enhance your security posture from code to runtime.

Make sure that all images running in your production environment are from the trusted JFrog Platform, blocking any unauthorized code from being executed. JFrog Runtime enables you to quickly find and fix any discrepancies between stored and running images that could indicate a man-in-the-middle attack. Additionally, you can monitor and reconcile any unauthorized updates or accidental rollbacks in image versions to ensure consistency and reliability across all operational environments.

Gain complete visibility into runtime vulnerabilities at the software package level, helping you focus on the riskiest workloads that are currently running. You can easily prioritize vulnerabilities based on your release information, identifying the most vulnerable clusters, repositories, or namespaces. JFrog Runtime helps you filter out the noise by quickly finding and addressing high-impact vulnerabilities using CVE search, or by specific package and version.

With JFrog Runtime you can easily identify who uploaded a package to Artifactory, its owner, deployment status, and applicable risks. Quickly verify which workloads are affected across your environment and plan how to address each vulnerability. Identify the least vulnerable package and software version to replace critical packages with minimal business disruption. Get expert remediation recommendations from JFrog's Security Research team to guide your next steps.

JFrog Runtime is designed to help you navigate the complexities of securing applications in production. By offering real-time visibility into runtime vulnerabilities, prioritizing risks, verifying the integrity of your deployments, it empowers your teams to act with confidence and efficiency.

Want to hear more about how JFrog Runtime can streamline your security efforts and keep your business safe? Schedule a demo today

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 Software supply chain Platform.

LEGAL STATEMENT

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd

Request a personalized Trial or Demo at http://jfrog.com/start-free/