IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

JFrog Announces New Software Supply Chain Security Capabilities

October 27, 2022

By: Katie Norton, Jim Mercer

IDC's Quick Take

On October 18, 2022, JFrog announced the availability of advanced security features bolstering the capabilities of Xray, its software composition analysis (SCA) tool. The features announced are the latest fruits of JFrog's acquisition of Vdoo and offer the company's customers a unified, integrated, and DevOps-centric approach to securing their software supply chain.

Product Announcement Highlights

The advanced security features of Xray announced include:

- Scanning of Infrastructure-as-Code (IaC) files in Artifactory for early discovery of cloud and infrastructure misconfigurations.
- Detection of exposed secrets in containers stored in Artifactory to stop any accidental leak of internal tokens or credentials.
- Container contextual analysis to help prioritize open source software (OSS) vulnerabilities based on their exploitability.
- Identification of the insecure use of libraries and services, including configuration issues and security malpractices, to help harden containerized applications.

IDC's Point of View

Securing the software supply chain is significantly important and substantially complex for virtually every organization. Many entry points into the software supply chain constitute a considerable risk that has gone unaccounted for in many organizations. In IDC's 2022 *DevSecOps Adoption, Techniques and Tools Survey* (IDC #US48599822, Aug 2022), respondents were asked about their confidence level in various aspects of DevSecOps, and the confidence score for the security of their software supply chain was the lowest. In addition, when asked what the two biggest application security gaps or exposures were in their organization, the growing use of open source by development teams and the vulnerability of the software supply chain were ranked number two and three behind security policy management.

The security of the software supply chain is fundamental to ensuring the fortification of modern applications. Unfortunately, supply chain attacks can go undetected and exponentially impact software producers and consumers, and that lack of visibility can lead to significant propagation of compromised code, leading to a secondary wave of vulnerabilities or exploits. Therefore, in addition to securing independent components of their applications, organizations should lock and guard all digital entry points into their software factories. Organizations must take a holistic approach because focusing only on one dimension of the software supply chain is both unscalable and inadequate.

The foundation for JFrog's new software supply chain capabilities come from the Vdoo acquisition in June 2021. Acquiring Vdoo allowed JFrog to scan applications in context, examining the environment binaries run in, using contextual threat analysis and application scanning that prioritizes critical security gaps and intelligence that covers code service and operating system changes. Further, the acquisition provided JFrog with an in-house security research team to better provide insights into threats and remediation options.

The delivery of software supply chain security capabilities as part of a DevOps platform is a key differentiator for JFrog. When software supply chain security is integrated as part of a DevOps platform, it provides end-to-end visibility and auditability, which can't be achieved as easily using stitched together standalone tools. Additionally, with Artifactory, a universal binary management solution, at the heart of their platform, all an organization's binaries, packages, and components are stored in one place, becoming a single source of truth for the supply chain. With this approach, organizations can develop and deploy applications quickly and more efficiently without managing dozens of tools and integrations while reducing the number of points of security failure as data is transferred between tools.

JFrog's binary-centric solution also offers certain advantages in terms of software supply chain security. Conventional scanning solutions are programming language and framework dependent and are not capable of scanning completed binaries. Binaries represent the finished product and contain more information about the makeup of the application than can be found in the source code alone. JFrog’s focus on the binary reveals issues not visible to tools focused solely on source code.

The importance of binary scanning became apparent during the December 2021 Log4j vulnerability event (*The Log4j Vulnerability: Widespread Impact and How DevOps Teams Can Respond*, IDC #lcUS48600422, Dec 2021) when organizations scrambled to try and find the Log4j vulnerability. Organizations using a binary-centric solution, such as Xray, could scan their applications and third-party commercial binaries and quickly identify their real exposure to the vulnerability.

Artifactory is not only storing binaries but tracking them through the software development lifecycle, providing a fully traceable record of their provenance and usage. Additional features, such as checksum verification, help to provide more certainty that every component is what it claims to be and hasn’t been compromised. By centralizing binaries and enabling metadata-based searchability in Artifactory, JFrog provides organizations with a clearer path to finding and fixing vulnerabilities.

JFrog's advanced security features also address several key software supply chain attack vectors. Many successful attacks on cloud services result from misconfigurations in IaC or exposed secrets. These exposed credentials are sought after by bad actors because exploits can unlock the door to an organization's critical data. When misconfigurations in Iac or exposed secrets go undetected, they frequently get replicated and shared amongst application environments, resulting in minor errors becoming larger runtime attack surface vulnerabilities. Additionally, because IaC is written in declarative languages, it requires less skill to reverse engineer, and attackers can more easily determine where assets are and how to access them. JFrog will initially support IaC scanning for Terraform state files on AWS and secrets detection for Python, JavaScript, and Java, so it will be important to expand their coverage expeditiously.

With limited security resources and knowledge, organizations must focus on the threats that truly matter. Not all security vulnerabilities present the same levels of risk, so DevOps and security teams need to have a common understanding of priorities and stack rank those risks. The actual risk to your application might differ depending on the technical stack, viable business importance, location (i.e., externally exposed), underlying data, and so on. It is equally essential to provide developers with real-time feedback in the tools they are working with so that vulnerabilities can be remediated before they even have the chance to become exploitable.

The software bill of materials (SBOM) for virtually every application using open source contains some potential vulnerabilities. However, development teams only have so much bandwidth and must focus on the vulnerabilities that present the most significant risk associated with a given deployment. So, filtering out the vulnerabilities that are not exploitable can help to ensure that the vulnerabilities that are real threats for possible exploitation are addressed. JFrog's container contextual analysis looks to solve this problem by identifying whether OSS vulnerabilities within an application are exploitable. Additionally, JFrog enriches these findings with knowledge and findings from JFrog's security research team's analysis. Although not the flashiest, these features are key in helping organizations to improve their overall software supply chain security efficiently.

Key Takeaways

- Many enterprises are looking to simplify their security tooling and leverage platforms that provide a comprehensive approach to DevSecOps and software supply chain security. JFrog offers a compelling solution to meet this need.
- Organizations seeking to improve the security of their software supply chains should consider how the JFrog advanced security capabilities can help them to improve their overall application security posture.
- Existing JFrog customers should explore how to integrate these new capabilities into their current DevOps pipelines to improve the security of their software supply chain more seamlessly.
- JFrog's new advanced security features strengthen the company's position in the overall DevSecOps tools and growing software supply chain security marketplace. However, the software supply chain security market is evolving, with new competitors entering the space. IDC expects continued innovation, mergers, and acquisitions in this area as vendors work to mature solutions and address these challenges, so JFrog will face continued competition.

Subscriptions Covered:
DevOps Analytics, Practices and Automation, DevSecOps and Application Security