WHY YOU NEED THE JFROG SECURITY PACK

Modern applications commonly consist of 90% open source software (OSS) dependencies, exposing your code to potential hidden security vulnerabilities and even expensive and complex license compliance issues. Neither of these problems are desirable outcomes for any company to deal with.

Ensuring license compliance in OSS dependencies is a growing concern for legal teams and CEOs alike. No-one wants to be on the receiving end of a failed audit, or an expensive Intellectual Property or license infringement case. Knowing what OSS is being used, by who and in which builds and production releases is of primary concern.

We are all painfully aware of the cost of security breaches. You only have to think back to the recent SolarWinds breach, or further back to the notorious Equifax hack, which cost them Billions. Not only that there is also the risk of being out of compliance with software licenses, which can land you in a complex and expensive intellectual property battle. Not to mention that you could be subject to an audit of your software and a failed audit can be subject to steep fines, depending on the industry you’re in.

User access is also a major concern for DevOps teams as you roll out the JFrog Platform across new users, teams and sites. With the Security Pack you can connect to other identity management tools you use like Active Directory, Okta, and others to automatically manage the onboarding, offboarding and changing permissions of users.

You can also integrate with Hashicorp Vault to enable easy secrets management for things like signing keys, which can be stored in a centralized vault and then accessed by the platform when needed, without having to upload them.

“Xray allows us to be able to scan through all the different Docker layers and find out what binaries are actually being included in here; and that way we have a process in place that we can actually go and notify a team and help them understand that there are vulnerabilities in your build pack.”

Brad Becktell, DevOps Engineer, Kroger
WHAT’S INCLUDED IN THE SECURITY PACK

With the security pack you get enhanced security and compliance features included with JFrog Xray as well as enhanced platform security features. The security pack extends the capabilities of JFrog Xray with two major improvements:

- Leading Vulnerability Intelligence
- Automated License Compliance

The Security Pack also gets extended with three new platform security features:

- System For Cross-domain Identity Management (SCIM) 2.0
- Hashicorp Vault Integration
- Private Endpoints that support AWS PrivateLink

LEADING VULNERABILITY INTELLIGENCE

The Security Pack includes the industry leading vulnerability intelligence VulnDB that is provided by Risk Based Security. Their database is meticulously maintained and updated every time a new vulnerability is discovered. VulnDB is derived from a proprietary search engine and the thorough analysis of thousands of disclosed vulnerabilities by their world-renowned research team.

Not only does it cast a wider net for you, it also brings you awareness of any new vulnerabilities much sooner than the NVD. This is critical for you to stay ahead in the fight to keep your code clean of any vulnerabilities or license problems.

- Gain confidence with the most timely and comprehensive vulnerability intelligence VulnDB
- Most comprehensive intelligence on the market with over 247,000 vulnerabilities, covering products of 27,000 vendors, including vulnerabilities not found in CVE/NVD
- Extended Vulnerability Metadata with each vulnerability containing an extended classification system and CVSS metrics to provide ratings for remediation and prioritization

AUTOMATED LICENSE COMPLIANCE

The Security Pack provides the ability to define and automate license compliance policies to identify the usage of a component that does not comply with your organization’s legal guidelines. Different mitigation behavior can be set based on the context of the type of license and where the component is being used.

Upon detection of license violations, you can notify users in several different ways including: sending emails, Slack messages, creating a Jira ticket or through any other system via Webhooks. Besides creating violations and notifications the system lets you setup enforcement actions, including blocking the download of a binary, failing a build and preventing the distribution of a Release Bundle. Safeguard your production software releases with the security pack, your biggest security and compliance ally in the world of DevSecOps.
SYSTEM FOR CROSS-DOMAIN IDENTITY MANAGEMENT (SCIM) 2.0

SCIM alleviates the pain and difficulty of manually managing the access rights and permissions of users who are joining, changing roles, teams or leaving in a secure and compliant manner. It supports managing what each of those users are allowed to do. If any part of this process is manual it can mean human error, resulting in security, compliance or operational issues. To address this situation we have an automatic way to update the platform with any change in users or a change in their roles, with the user management tools that you are likely using already, like Active Directory, Okta or another identity management tool which support SCIM 2.0.

We have a set of APIs which enable you to link your user management tool with our platform enabling automatic updates on user changes, such as a user leaving, coming back or needing to associate them with a new role. The platform will get automatic updates when a user needs to be modified. It supports user level and group level roles and how they are associated with each other.

---

HASHICORP VAULT INTEGRATION

Establish an external Hashicorp Vault integration with your JFrog Platform Deployment. Vault is a tool to manage secrets such as signing keys. The secrets are kept centrally in the vault and don't need to be uploaded into the Platform. The Platform knows to associate with or grab the relevant keys or secrets from the vault. It supports multiple signing key types such as GPG, RSA or Trusted keys used to sign packages or release bundles.

---

AWS PRIVATELINK

Secure your network traffic by utilizing AWS PrivateLink. Easily establish a secure network connection originating from your own AWS Virtual Private Cloud (VPC) into your JFrog Cloud (SaaS) instance on AWS - without sending the traffic through the public Internet. The ability to set up private endpoints allows for private connectivity between VPCs, AWS services and your on-premises networks. This makes it easy to connect services across different accounts and VPCs to simplify your architecture. See the 6-step process to get started using PrivateLink endpoints.

---

THE SECURITY PACK IS AVAILABLE IN THE CLOUD FOR ENTERPRISE & ENTERPRISE+ SUBSCRIPTIONS

redbox. splunk> puppet

For more information please contact us at www.jfrog.com

The Liquid Software Company