ソリューションシート

SECURITY PACK

セキュリティとコンプライアンスの範囲を拡大

JFrogのセキュリティパックが必要な理由

今日のアプリケーションは、一般的に最大90%がオープンソースソフトウェア（OSS）に依存しているため、潜在的なセキュリティの脆弱性や高いコストで複雑なライセンスコンプライアンスの問題がコードに潜んでいます。いずれの問題も企業にとって望ましいものではありません。

OSS に依存しているソフトウェアのライセンスのコンプライアンスを保証することは、法務部門やCEOにとって同様に大きな懸念材料です。監査に失敗したり、高額な知的財産権やライセンス侵害の裁判に巻き込まれたりすることは誰にとっても避けたいことです。どのOSSが誰に、どのビルドやリリースで利用されているかを把握することが最大の悩みです。

最近のLog4jの脆弱性インシデントやSolarWindsの不正アクセス、あるいはもう少し遡って数十億ドルの損失を出した悪名高いEquifaxのハッキングなど、セキュリティ侵害のコストは誰もが痛感していることでしょう。それだけでなくソフトウェアライセンスのコンプライアンスを逸脱し、複雑で費用のかかる知的財産権争いに巻き込まれるリスクもあります。もちろんソフトウェア監査の対象となる可能性もあり、監査に失敗すると業種によっては高額な罰金が科せられる場合もあります。

ユーザーアクセスとセキュリティは、新しいユーザー、チーム、サイトにJFrog Platformを導入するDevOpsチームにとって大きな懸念事項です。JFrogのセキュリティパックを活用することでActive DirectoryやOktaなどの他のID管理ツールと接続しユーザーのオンボーディング、オフボーディング、権限の変更を自動的に管理できます。

また、Hashicorp Vaultとインテグレーションし、署名キーなどのシークレット管理を容易に実施し、一元管理されたアクセス場所に保管され、必要に応じてプラットフォームからアクセスできるためアップロードする必要がありません。

> "Xrayは異なるDockerレイヤーをすべてスキャンし、実際にどのバイナリが含まれているかを検出できます。実際にビルドに脆弱性がある場合はチームに通知し、処理するプロセスを確立できます。"
>
> KROGER（クローガー）
> DevOpsエンジニア
> **BRAD BECKTELL（ブラッド・ベックテル）**

セキュリティパックに含まれるもの

セキュリティパックには強化されたセキュリティとコンプライアンス機能が含まれており、プラットフォームのセキュリティ機能も強化されています。

- 主要な脆弱性インテリジェンス —VulunDB脆弱性データベースの活用
- 自動化されたライセンスコンプライアンス —きめ細かく設定可能なポリシー
- 強化されたCVEデータ —より正確で詳細な脆弱性データのためのステップ・バイ・ステップでの修正機能
- コンテキスト分析 —誤検知(false positive)を軽減し、修復の優先順位を決定するCVE分析
- 業界標準のSBOM —CycloneDXおよびSPDXレポート用のエクスポート機能

プラットフォームのセキュリティ機能：

- クロスドメインID管理システム(SCIM)2.0
- Hashicorp Vaultインテグレーション
- AWS Privatelinkをサポートするプライベートエンドポイント

先進的な脆弱性インテリジェンス

業界をリードする脆弱性データベースであるVulnDBを搭載したリスクベースのセキュリティを提供します。脆弱性データベースは新しい脆弱性が発見されるたびに更新し維持されています。このデータベースは広大な範囲をカバーするだけでなくNVD(National Vulnerability Database)よりもはるかに早く新しい脆弱性を報告します。これは自分たちのコードを脆弱性やライセンスの問題から守るためにとても重要です。

- 最もタイムリーで包括的な脆弱性データ
- ベースであるVulnDBにより**信頼性を向上**
- NVDに記載されていない脆弱性を含む、27,000以上のベンダー製品をカバーする247,000件以上の脆弱性を網羅した**業界最高峰のデータベース**
- 各脆弱性に拡張された分類システムとCVSSメトリクスを含む**拡張脆弱性メタデータ**により、改善策と優先順位付けのためのレーティングを提供

自動化されたライセンス・コンプライアンス

ライセンスコンプライアンスポリシーを定義および自動化し、組織の法的ガイドラインに準拠していないコンポーネントの利用状況を特定します。ライセンスの種類やコンポーネントがどこでどのように使用されているかというコンテキストに基づきさまざまな軽減処理を設定できます。

ライセンス違反を検出すると、電子メール、Slackメッセージ、JiraやServiceNowのチケットの作成、Webhooksを経由した他のシステムとの連携など、さまざまな方法でユーザーに通知できます。違反や通知の作成に加えて、バイナリのダウンロードのブロック、ビルドの失敗、リリースバンドルの配布を禁止するなどの強制アクションを設定することができます。

拡張CVEデータ

JFrogセキュリティ・リサーチチームは、よりクリティカルなCVEの分析と調査にリソースを費やし、さらに多くの脆弱性の洞察と脆弱性を軽減するためのデータを作成します。これにより開発者、DevOps、セキュリティチームは脆弱性の軽減方法とステップバイステップの修復ガイダンスを容易に理解できるようになります。

コンテキスト分析

コンテキスト分析はバイナリのコンテキストを考慮した上で、スマートにスキャンします。これはCVEリストで依存関係を照合するという単純な作業ではなく、CVEに適用されるかどうかを判断するためにバイナリ内のCVEとの関連性からバイナリ環境を調べる全体的な分析を実行します。これにより煩わしい誤検知がなくなり、チームはクリティカルな脆弱性にのみ集中できます。

業界標準のSBOM

サイバーセキュリティに関する米国大統領令に基づき、ソフトウェアアプリケーションの精査が義務付けられ、ソフトウェアベンダーはアプリケーションを構成するすべてのオープンソースのソフトウェアコンポーネントのリストを提供する必要があります。この措置はアプリケーションのSBOM（ソフトウェア部品表）があるか、アプリケーションがSBOMを作成する機能を備えてる必要性を意味します。JFrog Platformは詳細なSBOMを作成するために必要なすべてのソフトウェアコンポーネントのメタデータを備えているだけでなく、業界標準のフォーマットであるCycloneDXやSPDX形式でエクスポートできます。

クロスドメインID管理（SCIM）2.0のシステム

SCIMは安全かつコンプライアンスに準拠した方法で、ユーザーの追加、権限の変更、グループの削除などのアクセス権とパーミッションを手動で管理する労力と煩雑さから開放します。また、SCIMは各ユーザーに許可されている権限の管理もサポートします。これらの作業のいずれかが手動である場合にはヒューマンエラーが発生する可能性が高くなりセキュリティ、コンプライアンス、運用上の問題を引き起こします。このような状況に対応するため、Active Directory、Okta、SCIM 2.0をサポートするその他のID管理ツールなど、既存のユーザー管理ツールでユーザーの変更や権限の変更に応じてプラットフォームを自動的に更新する方法を用意しています。

HASHICORP VAULTインテグレーション

JFrog PlatformのデプロイメントにHashicorp Vaultをインテグレーションします。Vaultは署名キーなどのシークレットを管理するツールです。シークレットはVaultに一元的に保管されるためプラットフォームにアップロードする必要はありません。JFrog PlatformはVaultから関連するキーやシークレットを関連付けたり取得できます。パッケージやリリースバンドルの署名に使用されるGPG、RSA、信頼されたキーなど複数の署名キーをサポートします。

AWS PRIVATELINK

AWS PrivateLinkを利用してネットワークのトラフィックを保護します。パブリックなインターネットにトラフィックを送信することなく、独自のAWS仮想プライベートクラウド（VPC）からAWS上のJFrog Cloud（SaaS）インスタンスへのセキュアなネットワーク接続を容易に確立できます。プライベートエンドポイントを設定することでVPC、AWS、オンプレミスネットワーク間のプライベート接続が可能になります。これにより異なるアカウントやVPC間のサービスを簡単に接続し、アーキテクチャを簡素化できます。

PrivateLinkエンドポイントを使い始めるには6ステップのプロセスをご覧ください。

セキュリティパックはEnterpriseおよびEnterprise+サブスクリプションにてご利用いただけます

redbox. splunk> puppet

JFrog Japan 株式会社

〒100-0004 東京都千代田区大手町1-9-2 Global Business Hub Tokyo | TEL: 03-4243-1049 | Webサイト：jfrog.com/ja/ | ブログ：jfrog.com/ja/blog/
お問い合わせ：jfrog.com/ja/contact-us/

SS-202210-D