JFrog XRAY

解决方案简介

无法控制，何谈安全

挑战

在不断演变的攻击手法和形形色色的安全点解决方案之间，开发者的软件供应链中存在诸多盲点和缺口。那么，他们如何保持开发速度而不牺牲用户对产品的信任？

解决方案

JFrog Xray 是一款应用程序安全工具，将安全自动化及相关知识直接集成到 DevOps 工作流中，更快地交付可信软件版本。JFrog Xray 通过强大的软件成分分析巩固您的软件供应链，并扫描从 IDE 直至分发到边缘设备的整个流水线。

Kroger

> *Xray 用作一种安全解决方案，帮助您确定已发布到 Artifactory 实例的哪些 Docker 镜像存在漏洞，并深入探究这些 Docker 镜像中所有不同的层，准确弄清楚需要修复哪些内容。*
>
> **BRAD BECKTELL，KROGER 的 DEVOPS 工程师**

容器上下文分析

业内首创的高级容器扫描，可识别开源软件漏洞并确定其优先级，处理在您的应用程序中是否真正可被利用。

基础设施即代码 (IaC)

保护存储在 JFrog Artifactory 中的 IaC 文件，及早发现可被利用的云和基础设的施错误配置。

恶意包检测

使用 JFrog 独有的已识别恶意包数据库，发现并消除不需要或意外的包。

增强的 CVE 修复数据

利用关键 CVE 增强修复来加速缓解漏洞影响，使开发人员、DevOps 和安全团队能够更多地了解如何轻松、智能地解决漏洞，通常只需要编写简单的代码或进行配置更改。

以开发人员为导向的特性

安全知识直接集成到最受欢迎的 IDE 和 Docker Desktop，通过 CLI 的漏洞扫描以及用于发现 Git 代码库漏洞的 Frogbot 扫描器，随时可供开发人员使用。

暴露的机密

检测存储在 JFrog Artifactory 的任何容器中暴露的机密，防止密码、API 密钥、内部令牌或凭证意外泄漏。

以安全为导向的功能

借助现成可用的软件物料清单 SBOM、行业标准的 SPDX 和 CycloneDX 以及新的安全 UI 屏幕，使合规变得轻而易举，所有安全扫描都显示在一起。

库和服务的不安全使用

发现公共 OSS 库和服务的使用或配置是否不安全从而面临被攻击的风险。

增强的 CVE 数据和严重性评估

了解关键 CVE 和相关的额外分析，使开发人员、DevOps 和安全团队能够了解各种 OSS 和商业环境的问题。该能力基于我们专业的安全研究团队提供的增强分析。

操作风险策略

轻松处理开源软件风险，如包维护问题和技术负债。

XRAY 与其他软件比较

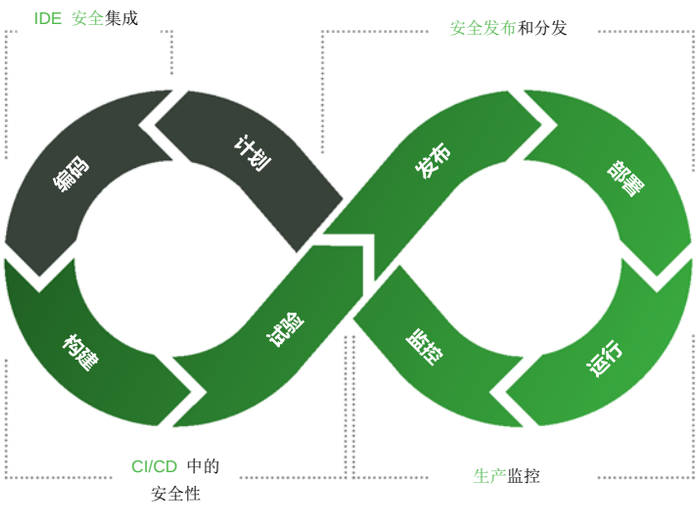
	JFrog	Sonatype	Snyk	Synopsys	GitLab	GitHub
增强的软件成分分析	●	●	○	●	○	○
服务暴露	●	○	○	○	○	○
机密检测	●	○	○	○	●	●
IaC 安全	●	○	●	●	●	○
基于上下文 CVE 分析的优先排序	●	○	●	●	○	○
统一的制品安全管理平台	●	●	○	○	○	○
全面的混合云和多云支持	●	○	○	○	○	○

用整体解决方案应对当今的安全挑战

提供可信软件，通过强大的保护措施降低风险、强化品牌，在整个软件供应链中免遭各种安全威胁。

以速度和规模进行创新，在保护您的软件和客户的同时，使得自动化的安全保障成为 SDLC 工作流的自然组成部分，最大限度地减少识别、优先排序和修复漏洞所需的工作。

始终如一地实施软件安全控制和最佳实践，**简化**安全法规、各项标准和内部政策的**合规性**。



v1.0220505

关于 JFrog

JFrog 通用、混合、多云的 JFrog Platform 助力全球成千上万的 DevOps 组织构建、保护、分发任何软件制品并将其连接到任何环境。

法律声明