# 评估和选择

# DEVSECOPS 解决方案

# 的七个建议


JFrog

# 评估和选择 DEVSECOPS 解决方案的七个建议

越来越多的公司意识到确保 DevOps 流水线的安全至关重要，因此，对 DevSecOps 产品的需求一直在强劲增长。然而，在进入 DevSecOps 市场寻找解决方案后，IT 和 DevOps 专业人员很快就发现，DevSecOps 工具和框架数量庞大，令人难以选择。由于选择过多，他们往往会产生决策疲劳和分析瘫痪，因为他们试图了解应该选择哪些安全解决方案，以及如何将它们集成到软件开发流水线中。

为什么 DevSecOps 会受到大家的关注呢？为了跟上创新的步伐，开发人员对开源软件 (OSS) 的使用呈指数级增长，使其在应用程序开发流水线中得到广泛应用。随着越来越多的源代码来自“外部”，收集和理解其内容成为关键所在。

在本电子书中，我们将介绍哪些类型的工具和技术可以最有效地减少 OSS 中可能包含的漏洞。然后，我们将分享一些建议，帮助您在评估市场（尤其是在软件成分分析 (SCA) 领域）上的多种不同解决方案时辨别优劣，做出更好、更明智的决定。

# 开发现状

如今，典型的应用程序使用多达 90% 的 OSS 组件，这些组件来自公开可用的开源库。这一趋势使得应用程序中存在的漏洞数量不断增加，进而导致漏洞被利用，信息被窃取。为此，各公司将更多的安全检查措施集成到其 DevOps 流水线。

但是，安全专业人员和开发人员到底需要哪些类型的工具来确保其生产软件的安全性和稳定性呢？平心而论，开发团队针对软件开发生命周期 (SDLC) 的不同领域提供了几种 DevOps 安全工具：

- 代码分析（静态和动态）
- 软件成分分析（针对第三方 OSS）
- 运行时安全性分析（包括容器）

理想情况下，团队应致力于采用所有这些工具来确保 SDLC 安全无虞，但在本博客中，我们将重点关注软件成分分析，该工具旨在减少 OSS 组件和二进制文件中的漏洞和许可违规。

# DEVSECOPS 的七个必备条件

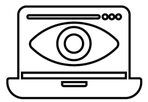
在选择 **DevSecOps** 工具，应确保以下 **7** 点：

**1.需要能够本地管理和理解所有制品的工具**

在团队着手识别哪些 OSS 组件存在漏洞之前，他们首先需要一个通用的 DevOps 平台。作为基本要求，该平台应统一管理所有制品和二进制文件，不论这些制品和二进制文件是什么类型，采用何种技术。DevOps 平台需要知道使用和创建了哪些制品以及制品的依赖项是什么。

**2. 使用最好的燃料**

最有效的解决方案需要全面的漏洞信息，比如 JFrog 安全研究团队所维护的漏洞信息，以确保漏洞知识库处于最新状态。即便是世界上最好的汽车，如果没有好的燃料来推动，也会一无是处。



**3. 重视可见性和影响分析**

DevSecOps “赢家”不仅知道您的二进制文件使用了哪些 OSS 库和组件，还能了解如何解压和扫描它们并洞悉所有底层和依赖项，甚至包括打包在 Docker 镜像和压缩文件中的底层和依赖项。能够了解组织所用制品和依赖项结构的解决方案可以提供可见性，并确定软件生态系统中任何漏洞或许可违规的影响。

**4. 需要支持容器和云原生框架**

解决方案应支持基于容器的发布框架，这种框架正迅速成为云原生部署的事实标准。深入、递归地理解容器技术并深入探究每一层，这将确保漏洞无处藏身。遗憾的是，有些扫描工具不支持容器，或者对容器的所有不同层和传递依赖项了解不够。

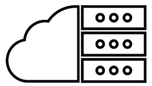
### 5.自动化管理

就 DevSecOps 而言，与公司安全部门合作实现自动化管理十分重要。管理系统必须能够自动执行公司政策，无需人为干预即可采取相应措施。主要功能应包括：

- 通过不同渠道（如电子邮件、即时通讯和 Jira）就违反安全或合规规定的情况发出通知
- 阻止下载
- 使依赖于易受攻击组件的构建失败
- 防止部署易受攻击的发布包

### 6. 覆盖整个流水线

DevSecOps 解决方案的特色在于知道如何利用制品的详细数据并将其与制品仓库、构建和容器中所有二进制文件的安全扫描结合起来。能够贯穿整个 SDLC 并持续检测和监控漏洞及违规行为（即使在生产部署之后）的平台将脱颖而出。



### 7. 拥抱混合解决方案

即使您目前没有使用混合基础架构，您将来也会这么做。现在选择适当的工具和解决方案，为您的云端之旅提供支持，这有助于确保您的 DevSecOps 流水线在任何地方都具有一致性和标准。

## 结论

DevSecOps 将不再只是 CIO 的一个心愿。现在，它是必不可少的 IT 战略，需要成为任何 SDLC 的必要组成部分。即使企业已经选择了合适的 DevSecOps 解决方案，领导者也需要确保在各个团队中实施完善的 DevSecOps 流程。其中包括需要继续就应用安全最佳实践对开发人员和 DevOps 从业人员进行培训。开发人员和安全专业人员比例通常是 250:1，因此让各个开发团队掌握安全知识是减少漏洞的必要之举。

选择一个能够管理仓库、二进制文件、CI/CD 自动化、OSS 组件分析并支持容器化发布框架的 DevSecOps 平台似乎是一项艰巨的任务。此外，支持本地、云、多云和混合部署也是一个难题。不过，可以从解决方案需求清单入手。我们希望这七条建议能为您提供一个坚实的基础，帮助您向供应商提出正确的问题，规避市场噪音，做出明智的决策。

# 关于 JFROG

JFrog 的使命是创造一个从开发人员到设备之间畅通无阻的软件交付世界。秉承“流式软件”的理念，JFrog 软件供应链平台是统一的记录系统，帮助企业快速安全地构建、管理和分发软件，确保软件可用、可追溯和防篡改。集成的安全功能还有助于发现和抵御威胁和漏洞并加以补救。

JFrog 的混合、通用、多云平台可作为跨多个主流云服务提供商的自我托管和 SaaS 服务。全球数百万用户和 7000 多名客户，包括财富 100 强企业中的 89 家，依靠 JFrog 解决方案安全地开展数字化转型。有关更多信息，请参见 www.jfrogchina.com