IDC ANALYZE THE FUTURE

IDC ANALYST BRIEF

Sponsored by: Revenera

While many organizations presume that open source software (OSS) is free of charge, there are often undetected security and licensing liabilities that must be tracked and mitigated. This type of management is best accomplished with automated software composition analysis (SCA).

Addressing the Hidden Cost of Embedding Open Source Software

November 2020

Written by: Jim Mercer, Research Director, DevOps and DevSecOps

Introduction

Today's digital climate is impelling organizations to digitally transform their business. Adding fuel to the digital transformation (DX) movement is the 2020 pandemic, which suddenly forced every organization, both large and small, to support contactless commerce. Microsoft CEO Satya Nadella summarized this pandemic DX phenomenon by stating, "We have seen two years' worth of digital transformation in two months." In the modern digital ecosystem, the impatience of the digital end user for speed and convenience is propelling organizations to deliver new software updates faster using DevOps development methodologies. Historically, application development teams wrote virtually all their own proprietary code, but this approach is too slow and error prone and makes it difficult to quickly adapt to market changes. As organizations try to deliver new innovations and value to their customers, they are increasingly turning to open source software (OSS). Resistance to OSS has waned over the past few years, and modern DevOps teams are now more predisposed to seek out OSS solutions to help them more rapidly deliver value to their end users.

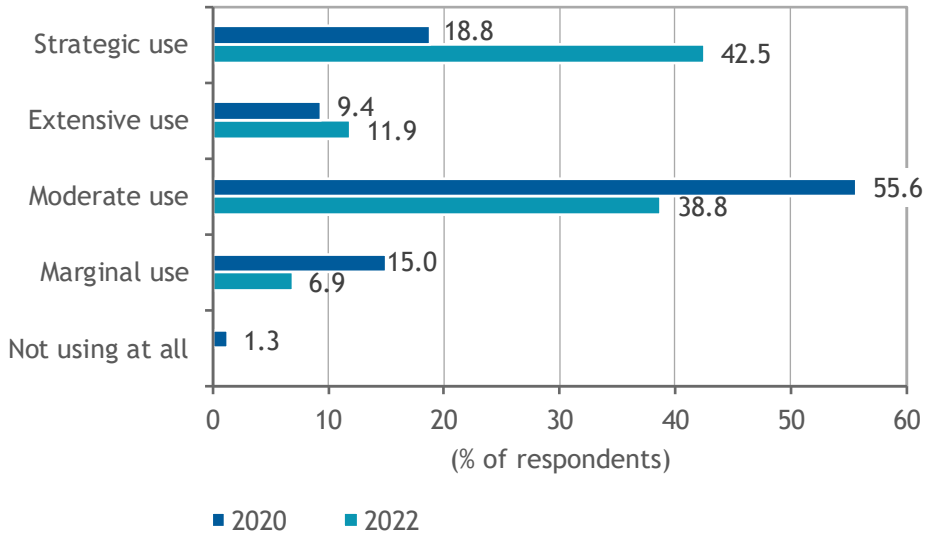
Software composition analysis scans applications for open source software usage and identifies security vulnerabilities and license risks.

Infusion of Open Source Software

A recent IDC survey illustrates how DevOps teams are increasingly comfortable using OSS in their applications; nearly 43% of respondents said their usage of OSS will be considered strategic by 2022 (see Figure 1). DevOps teams are increasing their use of OSS, and the technology is becoming an essential building block of application development and is being used strategically by DevOps teams to build new, innovative applications.

FIGURE 1: ***Use of Open Source Software Grows***

Q *Which of the following best describes your use of open source today and in two years?*



n = 160

Source: IDC's U.S. DevOps Survey, 2020

Open Source Software Comes with a Cost

While OSS is generally thought to be free of charge, there are underlying hidden costs and risks that need to be considered, and paramount among those costs and risks are security and licensing liabilities. Just like software written in-house, OSS can introduce vulnerabilities and security exposures that can be exploited by bad actors, and there are thousands of different types of license terms that can expose an organization to serious legal implications. Given the pervasiveness of OSS usage, these vulnerabilities and licensing issues can present serious risks to organizations.

Organizations should realize that when OSS components are included in their application code, they implicitly inherit all the subsequent components used by those components as well as the transitive/indirect dependencies. To ensure that they are protected from known common vulnerabilities and exposures (CVEs), organizations need to track direct and indirect software components using a software bill of material (SBOM). An SBOM is akin to a manufacturing bill of materials (BOM) — an inventory that tracks the parts needed to create a product. If a defect is found in a part, the BOM enables manufacturers to identify the affected products. As an OSS consumer, a DevOps team has control over its own code and implicit control over the components included within the application. However, the team has no control over the transitory dependencies that come with any OSS components included in their applications.

Despite having a reputation for being "free," OSS is governed by licensing terms just like commercial off-the-shelf (COTS) software. Although some open source licenses are more widely used, there are thousands of different license combinations within the OSS ecosystem. Therefore, organizations using open source need to mitigate risk by ensuring compliance with the various licenses used within their applications. Potential problems include expired, missing,

incompatible, or copyleft licenses. A copyleft or reciprocal license requires that any software product embedding the OSS component, even if it is just a few lines out of code, make its entire source code available for free, along with the rights to modify and distribute it. Also, licensing issues can arise when open source terms conflict with the terms of commercial or other OSS licenses within the same code base. OSS license discernment and compliance are even more critical if an organization is creating software that is packaged, embedded, or commercial SaaS.

It is in an organization's best interests to track OSS and license usage via an SBOM to avoid potential vulnerabilities and violations. While organizations have tried different approaches for managing OSS used by their software development teams to mitigate these issues, the volume of open source used in the code base of a modern application makes tracking labor intensive and fraught with errors.

This has led to the growth of software composition analysis (SCA) solutions that automate the visibility into OSS use for the purpose of risk management, security, and license compliance.

Benefits of Software Composition Analysis

Given the number of OSS components that applications use today, every organization should be using or considering the use of an SCA solution. Using SCA to scan applications provides several key benefits, including:

- **Visibility.** Over time, as more OSS artifacts are added, it is easy for application development teams to lose track of all the components they are using in their application. SCA should provide an inventory or catalog of OSS artifacts in your application by creating an SBOM, although SCA solutions differ in their completeness and SBOM accuracy. Teams are often surprised to see OSS artifacts that they did not even know were in use by the application. This provides an opportunity to do some pruning of components that may no longer be needed or licenses that don't comply with your policies, decreasing the size of your application footprint and reducing your overall security exposure.
- **Detection.** Fundamental to SCA is the actual detection of known vulnerabilities in your application. Detection typically provides insights into the actual vulnerability and its severity (i.e., critical, major, minor), the scope of exposure, and guidance on updated versions of the OSS artifacts that can be used to remediate the vulnerability.
- **Discovery of transitive dependencies.** When you embed OSS components in your code, you inherit the dependencies that are included within those OSS components. These inherited software components will be included as part of the SCA SBOM. These layers of inherited dependencies are often multitiered and complex. This is critical information because any known vulnerabilities in those inherited components can leave your application vulnerable. SCA solutions build a dependency graph showing the transitive OSS artifacts and at what tier they are included in the SBOM. SCA vendors may take different approaches to building the SBOM (i.e., programming language, build packages, file scans), and because precision matters, it is best to use a solution that takes multiple approaches to identify OSS dependencies.
- **Identification of outdated OSS components.** SCA will provide a list of known vulnerabilities included in your embedded OSS components. However, there is latency in creating CVEs, and lesser-known vulnerabilities are surfacing all the time. An SCA solution will identify when OSS components in the SBOM have been updated because this is the best way to proactively avoid vulnerability exposure.

- **Licensing.** Once the SCA solution generates a license report, you can assess the license compliance of the OSS components that make up your application. This will help you understand your risk and whether the OSS license is permissive, public domain, proprietary, and so forth and share this information with legal and compliance teams.
- **Trust.** When organizations use DevOps, software delivery is ungated and continuous. However, there is little point in using DevOps to produce better software faster if it is encumbered by security vulnerabilities and potential license compliance violations. SCA enables organizations to be confident and trust that they have done proper due diligence to protect themselves and their stakeholders without hindering DevOps velocity.

The reports generated from SCA are applicable to multiple stakeholders and enable the following capabilities:

- **Security.** Scan and report on applications with known vulnerabilities.
- **Procurement.** Uncover and manage OSS components already in use.
- **Compliance.** Understand and set policies to ensure appropriate compliance and risk tolerance.
- **Legal/IP team.** Mitigate legal risks by ensuring proper license IP due diligence.
- **Merger and acquisition (M&A) team.** Mandate OSS disclosures as part of technical due diligence (TDD) as required by underwriters covering M&As.
- **End users/customers.** Reassure end users that their personal data is not being unduly exposed to bad actors. Some customers may explicitly request OSS audits as part of their supply chain demands.
- **DevOps/engineering.** Improve the speed of security validation and reduce the application vulnerability exposure of applications and services.

Further, via the automation and tracking of the SBOM and licensing, an SCA solution can significantly reduce the operational cost of using OSS components. It can measurably reduce the number of FTE resources required for tracking and managing OSS components and licenses. Additionally, it allows organizations to shift remediation of OSS vulnerabilities to the left of the DevOps pipeline, reducing the amount of time and effort spent on repairs.

Considerations

While adopting an SCA solution is an important part of protecting your organization against bad actors, several aspects should be considered as part of evaluating competitive solutions:

- **Accuracy.** For teams adopting an SCA solution, accuracy matters, and erroneous results can be costly in terms of time and risk exposure. While results with false positives can add unnecessary work, a false negative is even worse because the SCA tool is not finding a vulnerability when one exists in your application. This leaves organizations more exposed with a greater risk that some vulnerabilities may be missed. Organizations should consider both the accuracy and the comprehensiveness of the scans. At the end of the day, an SCA solution that does not provide a full view of your OSS risk exposure could provide a false sense of security confidence.

- **Remediation.** The process of addressing OSS security and licensing issues identified in the SBOM needs to occur swiftly while ensuring proper due diligence and tracking. An SCA solution that offers security remediation management with integrations into defect tracking systems and monitoring to notify the appropriate stakeholders can help ensure a smoother security stabilization workflow across your application estate.
- **SaaS only.** Some SCA solutions are available as SaaS only. These solutions may not be suitable for security-conscious customers concerned about protecting their own software IP or customers that have compliance requirements around data residency. Organizations must consider these requirements when selecting an SCA solution and may be better served with a solution that is designed for on-premises scanning that can be customized to meet unique scanning requirements.
- **DevOps pipeline.** To achieve continuous analysis, an SCA solution needs to enable seamless integration into the DevOps software delivery pipeline, including integrations with developer IDEs and CI/CD tools.

Conclusion

The digital economy is here to stay, and the 2020 pandemic has forced every organization, both large and small, to support contactless commerce and accelerate its DX efforts. In the modern digital ecosystem, the impatience of the digital end user for speed and convenience is propelling organizations to deliver new software updates faster using DevOps development methodologies. As organizations try to rapidly deliver new innovations and value to their customers, they are increasingly turning to OSS.

Many organizations initially presume that OSS is free of charge, but undetected security and licensing liabilities often need to be tracked and mitigated, and this requires the use of an SCA solution. An SCA solution can track the complex graph of transitive dependencies by building an SBOM and tracking licensing terms and conditions. This ability reduces the number of resources that are required for tracking and managing OSS components and licenses. In doing so, an SCA solution can protect the organization from security vulnerabilities and license violations and ultimately help the organization avoid a costly security breach.

About the Analyst

Jim Mercer, *Research Director, DevOps and DevSecOps*

Jim Mercer is a Research Director within IDC's DevOps Solutions research practice. In this role, he is responsible for researching, writing, and advising clients on the fast-evolving DevOps market. Mr. Mercer's core research includes topics such as rapid enterprise application development, modern microservice-based packaging, application security, and automated deployment and life-cycle/management strategies as applied to a DevOps practice.

MESSAGE FROM THE SPONSOR

About Revenera

Revenera helps product executives build better products, accelerate time to value and monetize what matters. Revenera's leading solutions help software and technology companies drive top line revenue with modern software monetization, understand usage and compliance with software usage analytics, empower the use of open source with software composition analysis, and deliver an excellent user experience—for embedded, on-premises, cloud and SaaS products.

To learn more, visit ***http://www.revenera.com/protect.html***.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com