ANALYST BRIEF

Sponsored by: Revenera

Like the supply chain for physical products, the software supply chain demands a security framework. Because when you rely on third-party software, including open source software, *you are responsible* for the quality and security of the software you produce.

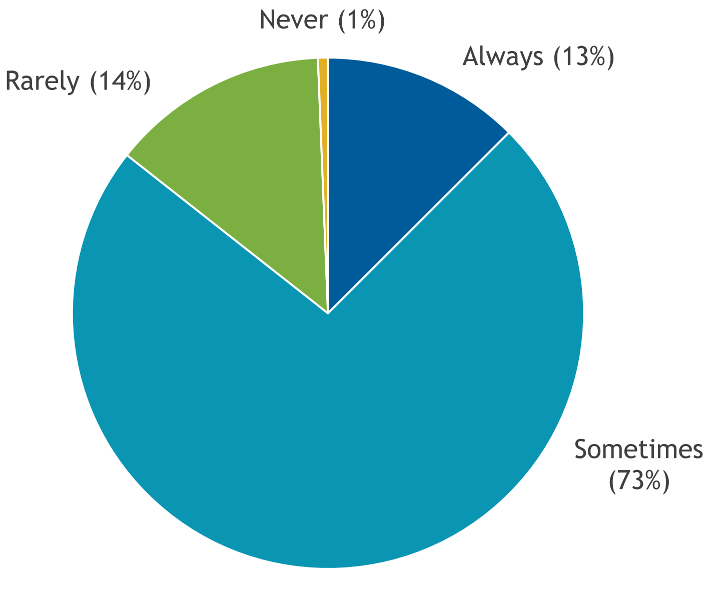
The Open Source Blind Spot Putting the Business at Risk

June 2022

Written by: Jim Mercer, Research Director, DevOps and DevSecOps and Nancy Gohring, Research Director, Future of Digital Innovation

FIGURE 1: ***Open Source Has Gone Mainstream***

Q ***How often do you try to find open source options over other kinds of software?***



n = 160

Source: IDC's DevOps and Accelerated Application Delivery Survey, 2021

Introduction

Digital products and services are the tools that enterprises of all kinds use to drive revenue, differentiate, and disrupt. Those digital products and services are increasingly complex, with most applications built on a mix of open source, commercial, and internally developed software as well as legacy applications running mission-critical functions. Virtually all those software sources rely on some open source software to deliver essential functionality for end users.

In a study of DevOps professionals, IDC found that 86% of respondents said they sometimes or always try to find open source options over other kinds of software (refer back to Figure 1). However, most organizations are unaware of the extent to which they already use open source and underestimate their dependency on it, a dependency that comes with some risks. IDC research found that 68% of organizations that use any kind of open source software acknowledged they had been impacted by a vulnerability or compromise associated with an open source technology over the past two years. Threats from open source vulnerabilities impact net-new applications that enterprises are building, critical legacy applications, and software offered by suppliers.

As enterprises expand the use of open source software, so do the challenges they face in understanding the scope of open source software used throughout the organization and the corresponding exposure. Without clear insight into the software supply chain, the business faces significant risk associated with exposure to vulnerabilities and risk associated with improper licensing.

Our increasing dependence on embedded software in all facets of life has made the software supply chain a critical issue — sometimes threatening to human life. Examples include the 2020 ransomware incident that impacted a hospital in Germany, causing it to turn away patients, including one who later died, and, in 2021, a bad actor who attempted to poison a Florida city's water supply by gaining access to the SCADA control system.

Securing the Software Supply Chain

The software supply chain should be considered a critical area of corporate risk. A plan for protecting the software supply chain should become part of the organization's governance, risk, and compliance (GRC) blueprint. Doing so will ensure that you're prepared for the next exploit. The plan should encompass tracking all third-party and commercial software bill of materials (SBOM) parts, not just open source software. In addition, it should ensure visibility into applications running in the cloud. A sprawling network of connected applications and cloud-connected tools can conceal weak links, and bad actors need just one insecure connection point to infiltrate your environment.

To manage software complexity and the associated elevated risk environment, enterprises must adopt several best practices throughout the application development life cycle, starting with securing the software supply chain. Doing so includes using an enterprise-grade software composition analysis (SCA) solution that should provide:

» **A software bill of materials:** Akin to a manufacturing BOM, an SBOM offers insight into the quality standards of your suppliers. SBOMs provide an inventory of open source and commercial software used in applications that were internally built as well as those offered by commercial-off-the-shelf (COTS) third-party software vendors, ensuring visibility into components your suppliers use. An SBOM delivers the transparency required to ensure that if a vulnerability occurs in a software component, you know whether your organization uses that component and should take action. A modern SCA solution should be able to produce SBOMs in industry-standard formats such as CycloneDX and the Software Package Data Exchange (SPDX).

- **Software licensing support:** Maintaining license compliance is critical to avoid possible conflicts or litigation. 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 of code, make its entire source code available for free and the rights to modify it. Licensing litigation is serious and potentially costly. An SCA solution should identify license issues and include a policy engine that automatically enforces licensing compliance standards. Using a framework such as OpenChain, an international standard (ISO/IEC 5230:2020) for open source license compliance, helps to ensure that your program yields a trusted and consistent outcome.

- **An ability to scan container images for vulnerabilities:** Modern cloud-native applications use microservices deployed via containers. Developers need to be equipped to find container vulnerabilities early in the software development life cycle (SDLC) to ensure they cannot be exploited when moved into production.

- **The ability to seamlessly integrate SCA scans into DevOps/CI/CD pipelines:** Continuously analyzing the software supply chain ensures that even as your organization releases software faster, you have clear insight into all the software components in use.

- **Enhanced collaboration between DevOps and security teams:** Software supply chain security and open source software licensing policies should be developed in partnership between DevOps, security, and legal teams. This collaboration is critical as you do not want to be unprepared when the next high-impact vulnerability materializes. Because the next Log4J type of vulnerability will arise, enterprises must exercise appropriate due diligence to ensure they are ready.

- **Timely security alerts**: When a new vulnerability emerges, you want to know as soon as possible to remediate the problem quickly. Your SCA solution should alert you about new security vulnerabilities for cataloged SBOM parts as the security state of OSS components often changes over time.

Benefits

Enterprises that take the right approach to secure the software supply chain stand to benefit in several ways, including:

- Building a strong relationship of trust with customers due to heightened transparency and a strong security posture

- Using scarce developer resources efficiently by focusing their work on projects that aim to achieve strategic business objectives rather than mitigating security incidents

- Avoiding the security and compliance issues that may cost the company both revenue and reputation (Cost savings may include the time, money, and opportunity associated with pulling developers off other work required to remediate security incidents.)

Considerations

Employing a modern SCA solution is essential in securing the software supply chain. However, not putting in place the proper process and integrations, including building strong collaboration between DevOps and security teams and creating a plan as part of a governance, risk, and compliance policy, will derail successful outcomes.

Software Supply Chain Best Practices

- Form a product security incident response team (PSIRT) to protect the software supply chain.
  - It should become a part of your corporate GRC blueprint to manage IT and software risks to the business.
  - The next Log4J-like exploit is inevitable. You can't be caught flat-footed – you need to be ready.
- Don't forget about your COTS. You need a comprehensive SCA solution that can scan binaries and software build dependencies.
  - Many independent software vendors (ISVs) use open source software liberally.
- Inventory everything to know what you have, and understand the composition of your applications and the pervasiveness of open source components across your application portfolio.
  - It helps to know where your greatest exposure lies and assess the ease of exploiting the code.
- Evaluate your application software inventory to understand where you have the highest levels of exposure. Some considerations might be: Is it on premises or in the cloud? What layers of protection are in place? Where are there gaps?
  - Cloud adoption has quickly become the norm rather than the outlier – applications running in the cloud can be attractive targets for bad actors.
  - A sprawling network of connected applications and cloud-connected tools can conceal weak links, and bad actors need just one insecure connection point to infiltrate your environment.
- Manage the software supply chain like you manage any other critical corporate risk.
  - Continuously analyze the software supply chain by integrating SCA scans into the DevOps CI/CD pipelines.

Executive Order 14028

Also, while your organization may not be a U.S. government agency or do business with the government, it is only a matter of time before you are affected by Executive Order 14028. This unprecedented government action is a mandate to protect against supply chain and infrastructure attacks on software. It emphasizes that the prevention, detection, assessment, and remediation of cyberincidents is a top priority and essential to national and economic security. Furthermore, it emphasizes the need for the private sector to follow suit. Included in the guidance are key directives such as:

- Establish and maintain a software inventory or an SBOM.
- Rapidly mitigate known vulnerabilities to reduce the exposure time.

- Continually monitor software components against a database of known vulnerabilities.
- Build as much assurance for included code (i.e., open source software, libraries, and packages) as for code that you natively develop.

As more organizations adopt these standards, they will expect the same due diligence from their business partners or vendors. Software composition is increasingly becoming a part of compliance regulation language in standards such as PCI, healthcare (FDA), automotive (NHTSA), energy (NERC), consumer (FTC), and multiple EU agencies (cloud, IoT, medical, payments, telco).

Key Trends

Just look to the headlines for evidence that implementing the right tools and processes that secure the software built by enterprises is perhaps more important than ever before. All the following trends will pressure organizations to provide more transparency and attestation regarding the composition of the software they use and build:

- Among the more dangerous areas of vulnerability are those applications that may not be under much security scrutiny but likely contain vulnerable components since they are rarely updated. Two recent examples — Log4J and Spring4Shell — demonstrate bad actors that exploited open source software vulnerabilities. They both targeted benign components of Java applications, with many organizations largely unaware of the prevalence of usage across their application estates.
- Geopolitical risks, most notably the Russia-Ukraine War, pose increasing risks to enterprises. IDC anticipates increased activity from rogue nation-states or activist hacker groups that attack wherever they can find a weakness.
- Emerging regulations, including Executive Order 14028, will continue to pressure the enterprise. The follow-on Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will give the enterprise more impetus to secure its growing software environments.
- Civil penalties will become a reality. On January 4, 2022, the Federal Trade Commission (FTC) warned companies and their vendors to take reasonable steps to remediate OSS vulnerabilities such as the Log4J vulnerability (CVE-2021-44228). In its warning, the FTC stated that it intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure due to Log4J or similar known vulnerabilities in the future. There is already a precedent for this, as Equifax ended up paying $575 million for a data breach caused by an unpatched vulnerability in the OSS Apache Struts.

Conclusion

The imperative to deliver digital products and services has caused a notable shift: Whereas most enterprises were once primarily consumers of software, they are now becoming software suppliers as well. However, most of the applications they build today are heterogeneous and complex, elevating risk. Vulnerabilities in open source, internally developed, and commercial software could all have an impact if not properly managed. A loss of trust by customers, damage to your brand, and potential fines for failing to comply with increased regulatory controls are all at stake.

A plan for protecting the software supply chain that includes a robust SCA solution, an SBOM, and an open source license compliance and security policy is key to avoiding impact from inevitable future attacks. Ultimately, even if you predominantly rely on commercial third-party software, including open source software, you are responsible for the quality and security of the software you produce.

About the Analysts

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 and DevSecOps markets. 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.

Nancy Gohring, *Research Director, Future of Digital Innovation*

Nancy Gohring is Research Director for IDC's Future of Digital Innovation market research service. She focuses on software innovation programs in the enterprise and their potential to drive efficiencies into corporate processes, generate new revenue streams, respond to customer demand, and improve competitiveness. Her research examines ways that enterprises can best execute on the four pillars of software innovation — plan, source, develop and distribute — and highlights leading enterprises that have developed successful new approaches to these competencies.

MESSAGE FROM THE SPONSOR

About Revenera

Revenera provides Software Composition Analysis solutions that help organizations manage their software supply chain and the license compliance and security issues inherent in their open source and third-party software. Code Insight from Revenera produces a precise open-source inventory of what's in a codebase, including all subcomponents, hidden dependencies, and associated licenses.

https://www.revenera.com/software-composition-analysis

IDC Custom Solutions

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

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.