Futurum

sonatype

Securing Your Software Supply Chain: A Boardroom and C-Suite Imperative

MARCH 2025

Introduction

Software is the underpinning of virtually all modern business processes. Once considered a background function supporting operations, today's software is central to an organization's ability to compete, innovate, and provide differentiated digital experiences. This transition is largely powered by the adoption of open-source components in software, which has had a profound effect on innovation and development speed. In fact, open-source components make up as much as 90% of modern software applications, which puts pressure on teams to ensure these components are safe from vulnerabilities and, increasingly, open-source malware.

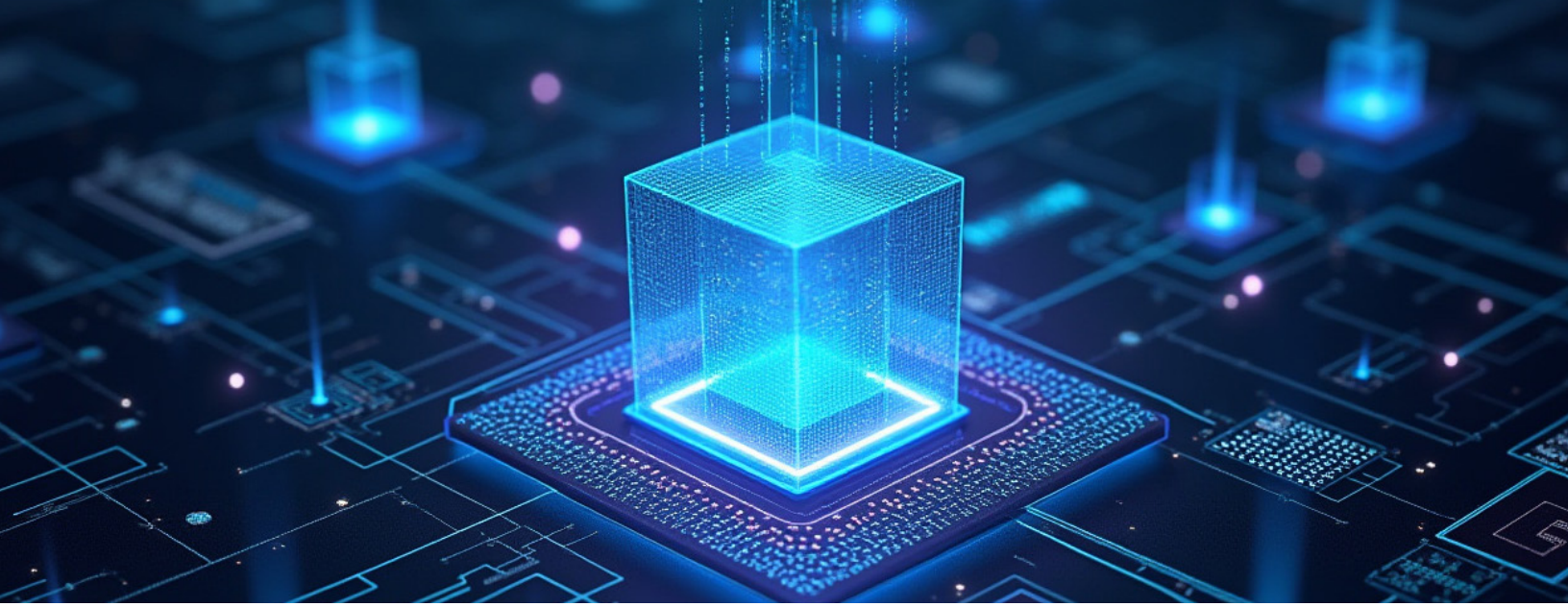
As our reliance on software grows, the security attack surface becomes increasingly vulnerable to established and emerging security threats. Business leaders must consider the security of their software supply chain with the same importance as its development. Financially motivated, nation-state, and malicious bad actors see the software development and assembly process as a target-rich attack surface to gain a foothold in our software.

Leaders today face a security imperative - securing the software supply chain.

In response to these growing threats and their impact, regulatory and policy organizations globally are converging on an expanding set of software security requirements, including what could prove to be significant fines and damages. In 2024 alone, businesses, including Advanced Computer Software, Unisys, Avaya Holdings, and Check Point Software, received fines from the UK's Information Commissioner's Office, the U.S. Securities and Exchange Commission (SEC), and other regulatory bodies for security and disclosure violations.

Given their current trajectory, the costs of not meeting or violating regulatory compliance requirements on software supply chain security will result in increasingly punitive fines.

This research brief aims to guide business leaders through the topics and questions they must address in the C-suite and boardroom to improve software supply chain security. Commissioned by Sonatype, this paper explores the challenges, benefits, and impacts of such efforts. We further address the conversations leaders need to have to ensure the alignment, technology, preparation, and timing required to meet key regulatory initiatives.



Rising Threats and Regulation

Organizations are doing their best to respond to these threats, but are struggling. For example, more than three years after discovering a critical vulnerability in Log4j, about 30% of organizations are still using compromised versions. The scale of the risks and the pace at which they are evolving demand that software security emerge from behind the scenes of development to the board and C-suite level's visibility and oversight. Part of the issue is that software supply chain security strategies are inconsistent and not in widespread use. Futurum Research's 2025 analysis of 866 organizations shows that while 63% of organizations create software bills of materials (SBOMs) and perform software composition analysis (SCA), SBOMs are made for only half of their releases.

Cybersecurity has primarily focused on defensive policies, technologies, and responses to threats seeking to find and exploit vulnerabilities and weaknesses in production networks, systems, and applications. These defensive measures and response protocols remain critical but do not address the increasing threats to applications and the underlying software components used to build and operate them.

Software development organizations once generally considered software from open-source, online, and image repositories such as GitHub and Docker Hub, as well as code package managers for Python, Java, and others, to be secure enough for use. Today, attackers see the software development community as the new, target-rich surface of attack. Nefarious code can be distributed much more broadly when attackers compromise software upstream in the supply chain, including open-source projects, software libraries, and container and system images.

Attacks on software upstream in the software supply chain are analogous to the camel's nose under the tent. They give attackers the inside track to embed nefarious code into software downloaded via repositories, code libraries, and package managers that organizations deploy compromised code into hundreds, if not thousands, of environments.

Several successful attacks garnered the industry's and regulators' attention, including XZ Utils and the previously mentioned Log4Shell open-source used in Linux, Okta identity management software, Equifax's use of Apache Struts, and SolarWinds' distribution of compromised security software. The industry benchmark 2024 State of the Software Supply Chain report found rapid growth in malware-infected open-source software. Over 512,847 malicious open-source software packages were logged during 2024, a 156% increase year-over-year.

Despite the efforts of open-source projects, online repositories, and software package managers to secure the software they create and deliver, organizations must take additional steps to ensure that the software they develop does not contain or utilize malware-compromised components. Regulators are determined to enforce compliance among software organizations, making it clear that failure to improve software supply chain security could result in penalties.

Globally, 2025 and 2026 are inflection point years for security regulations and policies, led primarily by the U.S. and the EU. A common element in these regulatory efforts is the move to greater transparency and security in software. Many of them include specific requirements for the production of SBOMs and SCA reports for software delivered to government and/or commercial customers, stricter security frameworks, and shortened security incident reporting requirements.

For example, the Digital Operational Resilience Act (DORA) doesn't explicitly require SBOMs, but its guidance strongly encourages practices that align with SBOM usage, including mandating third-party risk assessment and sharing threat intelligence. These essential security requirements for EU financial institutions entered enforcement in January 2025. The EU Cyber Resilience Act (CRA) grants manufacturers until December 2027 to comply with their cybersecurity standards, including requirements to provide transparency into software components. Similarly, the Network and Information Security 2 Directive (NIS2), which has stricter cybersecurity requirements, is slated to go into effect in October 2026 with requirements for vulnerability management and visibility.

Changes in the EU member states' product liability laws are underway due to the enactment of the Product Liability Directive (PLD), which extends the liability of some software products and is to be completed by December 2026.

In the U.S., Executive Order 14028 mandates software vendors to the federal government to provide SBOMs detailing components used in software supplied to government agencies. As a presidential executive order rather than a signed law, 14028 is less definitive and can be changed, relaxed, or withdrawn by current and future administrations.

Software Security - A C-Suite and Board Room Matter

The evolving threat landscape, coupled with increased scrutiny of how software supply chains are managed, requires strategic guidance and oversight at the highest organizational levels. This means that security is no longer solely the responsibility of IT, security, and compliance organizations. Executives must understand that software security is not just about preventing attacks but also protecting the business.

C-suite and board-room engagement is one key element to establishing a culture of security. Executives at the C-suite and board-room levels must facilitate discussions and ask tough questions across all parts of the business.

5 Questions and Topics for the C-Suite and Boardroom

1. What is the current software supply chain risk exposure across the organization?
2. Do we have the software security policies and processes to address the threats and compliance requirements?
3. How do we hold our software and online services suppliers accountable for software supply chain security?
4. What investments are we making, or do we need to make, in technologies such as SBOM and SCA?
5. What is our software security plan, and who is accountable for leading the charge?

Conversely, IT, security, and compliance leaders must be prepared to report the following critical information in business terms regularly:

- The organization's security posture
- Software security risks and their business impact
- Preparedness for current and pending regulatory reporting
- Benchmarking against regularly updated resources such as the Software Chain Report
- Benefits delivered from security investments.

Key Software Security Technologies

SBOMs, SCA, repository firewalls, and software security testing are all sources of attestation and information for auditors and compliance to meet business and regulatory requirements.

SBOM Automation and Management: Not only are SBOMs vital to meeting current and future regulatory requirements, they're essential to fully understanding software and its dependences on external or third-party sources that are operating within the business. SBOM creation must be a continuous and automated part of the software development lifecycle (SDLC). An SBOM management technology can serve as a repository for monitoring, auditing, and reporting internally, and to auditors, regulators, and customers. An SBOM manager can also serve to retain SBOMs provided to the organization by external software suppliers and partners.

SCA Automation and Management: SCA technology provides detailed insights into the interdependencies between software, internally and from outside sources, open-source, vulnerabilities, and license compliance requirements.

Repository Staging or Firewall: Any code or binary from an external source requires additional vetting for security vulnerabilities. It has been a common practice to download software (code and binaries), images, and libraries directly from online repositories such as GitHub and software package managers.

Software Security Testing: Software teams are well accustomed to performing a number of static and dynamic software tests specifically looking for software vulnerabilities introduced during development. While not a comprehensive solution, software vulnerability testing remains a vital element of creating and releasing secure software.

Guidance for Improving Software Security

Implementing any type of cybersecurity initiative is no quick fix or silver bullet, and addressing software security is no different. Improving security requires a multifaceted approach that involves people, processes, and technology. Below are some important steps to take to improve software security.

Conduct a software security risk assessment and threat analysis to prioritize improvements with the greatest impact.

Implement SBOM management, continuous SBOM generation, and SCA integrated into development workflows and processes such as continuous integration and continuous deployment (CI/CD).

Develop a software incident response process, similar to what security teams have for a security intrusion or breach, to enable software teams to assess and respond to vulnerabilities in critical or high-priority situations.

Create secure coding standards and implement security reviews as part of ongoing code reviews.

Establish policies and vetting processes regarding software acquired from external repositories, libraries, and package managers.

Perform ongoing audit and testing and updates to ensure software security measures are effective.

Analyst Take

Underpinning any software or cybersecurity initiative by establishing a commitment to creating a culture of security, beginning with the C-suite. Policies, investments in security, technologies, and process improvements are easily set aside over time without ongoing attention and prioritization by leaders.

Organizations increasingly recognize the importance of software security and are allocating budgets to address it. Research by Futurum conducted in early 2025 shows that 27% to 35% of organizations plan to significantly increase spending on application security over the next 12-18 months. Similarly, 41% to 45% of organizations plan to moderately increase their software security spending over the same time period.

	Software Bill of Materials (SBOM)	Software Composition Analysis (SCA)	Secure Code and Library Repository	Secure Open-source Solutions	DevOps Toolchain Security	App Security Incident Response
Significant Increase	**30%**	**27%**	**31%**	**32%**	**35%**	**34%**
Moderate Increase	**42%**	**41%**	**44%**	**42%**	**42%**	**45%**

Source: Futurum Intelligence: DevOps and Application Development Decision Maker Survey 2025

At the same time, even widely available software security testing technologies are not fully implemented by software teams. Futurum's research shows that one-third of organizations use application security testing tools on 75% or more of the software their organizations create.

Now is the time to address software security. Business and technology leaders must align business and security strategies, priorities, and investments. The regulatory environment is difficult to predict and evolves quickly, requiring communication and collaboration with business, software, and security leaders, teams, and partners.

Important Information About This Report

AUTHORS

Mitch Ashley
Vice President & Practice Lead, DevOps
& Application Development | The Futurum Group

Daniel Newman
CEO | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

sonatype

ABOUT SONATYPE

Sonatype is a leading software supply chain management company that helps organizations build secure, high-quality software at scale. With its industry-leading platform, Sonatype enables teams to automate open source governance, enforce security policies, and maintain compliance across the entire development lifecycle. A key part of Sonatype's solution is its support for generating and managing Software Bills of Materials (SBOMs), providing transparency and traceability into software components. By empowering organizations to understand what's in their software, Sonatype helps reduce risk and drive innovation with confidence.

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.