WHITE PAPER

HIKVISION

# Hikvision
# Securing the Software Supply Chain: SBOMs to Protect Your Organization

Building Security Posture with Software Transparency

# Contents



HIKVISION®

## INTRODUCTION: WHY SBOMS?

In 2020, SolarWinds suffered a massive breach with the injection of malicious code into a patch update for one of its products. By March 2021, 18,000 organizations and enterprises had installed the malicious patch onto their SolarWinds systems, from Fortune 500 companies to the U.S. government. The incident revealed an uncomfortable truth: Today's cyber threat actors have become increasingly sophisticated at exploiting software supply chains to conduct attacks. Whether threatened by crime groups or intelligence groups, even organizations deploying best practices for cybersecurity are faced with mounting cyber risks from their suppliers being infiltrated. Software supply chain threats are considered a top attack vector as threat actors introduce malicious tools and programs into vendor products and services at each level of the development cycle, presenting new threat considerations for enterprises that render many previous approaches to cyber defense obsolete. A Software Bill of Materials, or SBOM, is now considered by cyber industry players and the federal government as a clear solution to the increasing software supply chain attacks.

Often compared to a nutrition facts label for software providers, SBOMs enable organizations to get a clear picture of the "ingredients" of the programs and applications they rely on. SBOMs safeguard enterprises and applications through transparency; security teams are able to identify outdated software, low-quality tools, non-trustworthy vendors and other potential issues within their enterprise software through a framework that identifies each component of the software supply chain. By enabling transparency into their software components and providers, SBOMs help organizations achieve Zero Trust security posture.

In May 2021, the White House issued an Executive Order on Cybersecurity, advocating for SBOMs. The executive order states that, "A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. […] The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM and using it to analyze known vulnerabilities are crucial in managing risk." Industry observers suggest that future federal guidance may require many organizations, regardless of presence in critical industries, to utilize SBOMs as part of their security posture.

## SOFTWARE SUPPLY CHAIN VULNERABILITIES: UNDERSTANDING THE THREAT AND CHALLENGE

Software supply chain threats are present wherever software is deployed. Today, software development typically requires the reuse of open source, external and third-party software. The combination of a lack of transparency, increasing cyber threat environments and widely divergent quality standards of software providers, means enterprises often lack an understanding of the security and quality of the applications they deploy. By communicating the individual components and origins of software, SBOMs enable developers, security teams and the broader IT function to understand where software is reused, what vulnerabilities exist, and where room for improvement is needed. SBOMs further enable companies to transparently communicate software supply chain risks to their customers and partners.[1]

## WHAT IS A SOFTWARE SUPPLY CHAIN ATTACK?

Cyber threat actors increasingly target the software supply chain. According to the Cybersecurity and Infrastructure Security Agency (CISA), software supply chain attacks involve attackers targeting software providers in order to compromise the software with malicious code before customers receive it. This can come in the form of compromise before the product is released, or the malicious code can be delivered via software updates and patches. CISA notes that these attacks can affect all software users, including downstream partners and associated organizations, with consequences for the private and public sector.[2]

For example, a cyber threat actor may compromise an employee from a company that makes human resources software. By using the employee login credentials, they may insert code into a patch update or hotfix for a popular software tool. When the patch is delivered to customers, it may give a threat actor remote access to the HR software at each company where it is installed. This allows the threat actor to not only gain access to the sensitive data in the HR software, but also pivot from that HR system to find and attack other systems at the same company, such as financial servers, manufacturing lines, or internal email and network shares. In some cases, the attacker may specify a small number of targets, yet adversely affect millions of users.

Another example is the compromise of an open-source application – such as the one we just saw with Log4j – which can be catastrophic across industries and impact more than just companies, but can also have real ramifications for consumers as well as the internet at large. We also saw this back in 2014 with Heartbleed, a serious vulnerability within OpenSSL, another open-source tool used widely on the Internet that is typically embedded in other code. So, while there was a patch, the fact that the vulnerable code was part of so many other applications and tools meant that patching everything would never happen, because so many web apps and tools that were no longer supported would be using that code. In that case, the flawed SSL heartbeat option on one computer was bugged with a malicious heartbeat message, which released secret information to the other computer. Specifically, the vulnerable computer divulged contents from the server's memory, or RAM.[3]

[1] June 2021, Security Boulevard, What is an SBOM? A deep dive.

[2] April 2021, Cybersecurity and Infrastructure Security Agency, Defending Against Software Supply Chain Attacks.

[3] September 2017, CSO Online: What is the Heartbleed bug, how does it work and how was it fixed?

# KEY BENEFITS OF SBOMS IN BUILDING ROBUST SECURITY POSTURE

## SOFTWARE HERD IMMUNITY

According to the National Telecommunications and Information Administration (NTIA),[4] organizations receive a broad range of security and business benefits from an SBOM approach. NTIA notes that enterprises can achieve a form of amplified "herd immunity" from SBOM adoption. This concept involves a group of enterprises and organizations coordinating their cybersecurity preventative activities in order to reduce individual risk, which mitigates broader risk for the overall group. For instance, if one player in the software ecosystem identifies and thus avoids a vulnerability in its software, it can have downstream effects for its partners and customers by collectively protecting them from attacks.

## IMPROVING QUALITY OF SUPPLIERS

With the transparency and accessibility of information afforded by SBOMs, organizations can avoid including unsupported or sub-par quality software components in their products. In the physical security industry, like others, organizations stand to benefit from an improvement in their processes and mechanisms for detecting and remediating problematic software components. This, in turn, enables enterprises to be more selective with their partners and vendors.

## SPEEDING UP VULNERABILITY MANAGEMENT

Organizations can accelerate the timeline for fixing deployed systems, according to NTIA. For instance, enterprises today may factor in timetables of months or years for addressing systems with many points of vulnerability that can experience delays in responsible disclosure. NTIA notes that "accurate SBOMs can collapse this chain of delays to allow all stakeholders to begin assessing vulnerabilities immediately and measure remediation performance throughout the supply chain."

Think of all of the connected devices within a home ranging from routers to laptops and other mobile devices, to printers, streaming devices and more. What many don't necessarily think about are which operating systems are running throughout their home (i.e., Linux, iOS/Android and Windows/MacOS). What happens if there is a vulnerability in Linux or one of its key components? What is the likelihood an average consumer knows about that vulnerability and then has the tools to know to patch it accordingly? Alternatively, if all devices within that house had an SBOM, it would be easy to identify which devices were vulnerable, allowing the individual to patch or otherwise mitigate the vulnerability. Without an SBOM, a home network could be compromised and allow a threat actor into the network for an indeterminate amount of time.

[4] November 2019, National Telecommunications and Information Administration (NTIA), Roles and Benefits for SBOM Across the Supply Chain.

## ESTABLISHING SBOM BEST PRACTICES: TRANSPARENCY AND RISK MITIGATION WITH SUPPLY CHAIN CLARITY

Both DevOps and IT organizations are responsible for implementing SBOM frameworks. According to the Linux Foundation, working across NTIA standards is a bare minimum requirement for organizations. Released in July 2021 and aligned to President Biden's Executive Order on Cybersecurity, the NTIA offers three minimum key components to an SBOM, which "comprise three broad, interrelated areas":[5]

| **Minimum SBOM Elements** | |
|---|---|
| Data Fields | *Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, & Timestamp.* |
| Automation Support | *Support automation, including via automatic generation & machine-readability, to allow for scaling across the software ecosystem. Data formats used to generate & consume SBOMs include SPDX, CycloneDX, & SWID tags.* |
| Practices & Processes | *Define the operations of SBOM requests, generation & use including: Frequency, Depth, Known Unknowns, Distribution & Delivery, Access Control, & Accommodation of Mistakes.* |

For end users of software, it is critical for IT and security teams to understand the key elements of an SBOM in order to build and maintain inventory of the software components present on their systems, particularly ones critical to business functions like finance, security and operations. These best practices are particularly key for critical industries more frequently targeted by threat actors, or more at-risk for high-profile attacks, such as healthcare, energy and financial services.

Security teams and those accountable for software supply chain security should look to SBOMs that are accurate and continuously updated. By building a database of applications and network assets with up-to-date SBOMs deploying best practices, organizations can better understand the quality of the software on their networks, as well as the factors affecting their security risk profiles from the software provider levels.

## MAKING THE CASE TO STAKEHOLDERS: OUTLINING THE VALUE OF SBOMS

While regulatory guidance continues to evolve, the primary aim of SBOMs is to give a full picture of vulnerabilities and sources of all software components to each player in an ecosystem, including vendors, customers and other stakeholders.[6] Further, SBOMs should help automate the process of identifying vulnerabilities by providing a continuously updated single source of truth for all software suppliers.

Organizations should not look at SBOMs as a cure-all for supply chain threats, but rather as a critical mitigation tool in the constant battle against cyber intrusions and threat actors. Given the complexity of software systems and configurations, deploying SBOMs as a software provider – or understanding them as an end user – can take investment in stakeholder alignment and process development across the enterprise. Without SBOMs, organizations cannot understand their exposure to cyber threats.

[5] July 2021, NTIA: The Minimum Elements For a Software Bill of Materials (SBOM) Pursuant to Executive Order 1408 on Improving the Nation's Cybersecurity.
[6] August 2021, Security Boulevard, What is an SBOM? A deep dive.

## SBOM'S ROLE IN ACHIEVING ORGANIZATIONAL SECURITY AND BUSINESS PRIORITIES

Regulatory guidance is emerging that may ultimately require end users of software to take into account SBOMs for critical software. In the interim, organizations should begin the process of aligning stakeholders – such as CFO and compliance functions, IT and security, and operations – with the process of reviewing, evaluating and utilizing SBOMs to build robust security practices and posture.

To make the SBOMs case to business leaders outside of the security function, consider the following points:

- With software supply chain qualification and validation, suppliers are held to more rigorous standards that offer a competitive advantage.
- SBOMs enable enterprises to identify and avoid vulnerabilities in both software developed and software purchased or acquired.
- SBOMs improve business decisions around what companies to enter into business engagements or relationships with.
- By better understanding software components, origins and vulnerabilities, SBOMs can help eliminate silos in organizations and enable leaders to more objectively understand the products and services present within their networks, from the state of compliance to evolving regulatory needs, to the threat posed by lower quality and vulnerability-prone software components.
- Organizations that prioritize software supply chain security enjoy competitive advantages and mitigate business losses and challenges resulting from security incidents.

## THE RACI CHART: IDENTIFYING ROLES AND RESPONSIBILITIES ACROSS THE SBOM END USER

Let's take a look at the key roles needed to build an understanding of SBOMs within a medium to large enterprise. With best practices indicating that all software on an enterprise network should be evaluated for known vulnerabilities and other potential risk factors, enterprises should design a stakeholder process that enables users to identify gaps in their security posture through the lens of SBOMs

| | Software User | Project Sponsor | IT Security |
|---|---|---|---|
| Initiate Application Review or Purchase Decision | A | R | C |
| Evaluate Software Supply Chain Security with SBOM | C | I | R |
| Make Decision on Responsible Deployment of Enterprise Software | A | R | C |

| |
|---|
| **Responsible:** This team member works to complete the task, and every task assigned needs one responsible party who would complete the job. It is fine to assign a task to more members. |
| **Accountable:** This team member delegates work and is the only one who reviews the deliverable before it is complete. In some tasks, the Responsible party can also serve as the Accountable one. You have to make sure that only one Accountable person is assigned to each job or deliverable. |
| **Consulted:** These team members are typically the ones who would provide suggestions either on how it will impact their future projects or their domain of expertise on the deliverable itself. However, it's a fact that every deliverable strengthens with review and consultation from more than one team member. |
| **Informed:** These team members are informed about the project's progress instead of being roped into every deliverable's details. |

## ACHIEVING ZERO TRUST CYBERSECURITY POSTURE WITH SBOMS

SBOMs are key to achieving Zero Trust, a cybersecurity posture we outlined in Hikvision's white paper, *Securing a New Digital World with Zero Trust*. By prioritizing software disclosures and understanding the applications and related enterprise assets within the network, organizations can replace trust with transparency;[7] if an organization regularly and accurately updates SBOMs, that can provide insight into components that might previously have required a degree of trust with software suppliers that can no longer be justified in today's threat environment.

When deployed properly, SBOMs should provide a 360-degree view of an organization's risk exposure to software supply chain threats. If IT and security leaders understand the security practices of their vendors, they can identify their risk exposure to attacks conducted via vulnerable software components or other third-party mistakes and issues. Further, SBOMs provide a window into determining which software partners are most up to date on security best practices.[8]

## CONCLUSION: A MORE SECURE FUTURE THROUGH SBOMS

Organizations have never faced more cyber risk than today's threat environment, one in which threat actors no longer need to infiltrate organizations through their employees' login credentials or application vulnerabilities, but can instead conduct attacks at scale via software supply chain attacks. SBOMs enable enterprises to build a more secure cybersecurity posture by understanding their exposure to the cyber risk of these attacks, in addition to the vulnerabilities present on their networks by outdated/obsolete and risky software components.

To protect against accelerating cyber threats, business and technology leaders should embrace the SBOM framework to build robust security posture and put into effect practices to better understand their applications and systems and require their software vendors and partners to provide transparency through SBOMs. By using the SBOM framework and automating processes to ensure vulnerabilities and potential weak spots are regularly documented in a consistent, accurate repository, enterprises can advance on their journey to a true Zero Trust cybersecurity posture that defends against the threat actors increasingly targeting vulnerabilities in software providers.

[7] June 2021, CSO, Government-mandated SBOMs to throw light on software supply chain security.
[8] September 2021, CPO Magazine, Attackers are getting smarter. Can your SBOM keep up?

## RESOURCES


- September 2017, CSO Online, What is the Heartbleed bug, how does it work and how was it fixed?
- November 2019, National Telecommunications and Information Administration (NTIA), Roles and Benefits for SBOM Across the Supply Chain.
- October 2020, National Telecommunications and Information Administration (NTIA), SBOM FAQ.
- March 2021, Linux Foundation, Materials (SBOM) with Open-Source Standards and Tooling.
- April 2021, Cybersecurity and Infrastructure Security Agency, Defending Against Software Supply Chain Attacks.
- April 2021, FOSSA, Software Bill of Materials: Formats, Use Cases, and Tools.
- June 2021, CSO, Government-mandated SBOMs to throw light on software supply chain security.
- June 2021, Federal Register: Software Bill of Materials Elements and Considerations.
- July 2021, ITPro Today, Generating a Software Bill of Materials Is Becoming Essential.
- July 2021, National Telecommunications and Information Administration (NTIA), The Minimum Elements for a Software Bill of Materials (SBOM).
- July 2021, Security Boulevard, The Software Bill of Materials and Software Development.
- August 2021, Security Boulevard, The Future of the SBOM.
- August 2021, Security Boulevard, What is an SBOM? A deep dive.
- September 2021, CPO Magazine, Attackers are getting smarter. Can your SBOM keep up?

Hikvision USA Inc.
18639 Railroad Street
City of Industry, CA 91748

Hikvision Canada Inc.
4848 Levy Street
Saint-Laurent, Quebec H4R 2P1

Contact Information
Toll-Free: +1 866-200-6690 (U.S. and Canada)
Phone: +1 909-895-0400
Email: sales.usa@hikvision.com
**hikvision.com**

Connect with us:



HIKVISION®