Software bill of materials is the first step to improve software supply chain security

THIS CONTENT HAS BEEN PROVIDED BY ANCHORE

Jeremy Bryan, solutions architect and technical lead, Anchore

anchore

A confluence of events, including the SolarWinds breach and the subsequent White House executive order on cybersecurity, has pushed software supply chain security center-stage for the federal government and the ecosystem of contractors that do business with it. It's a top priority for many executives, but traditional notions of cybersecurity are proving inadequate to the current landscape, and the path forward isn't always clear. So where do they start?

Security accelerants

It's important to zero in on the factors that affect how agencies or an organization are impacted by current security risks in the software supply chain. And to do that, organizations need to understand the perfect storm of "accelerants" – as Jeremy Bryan, DevSecOps solutions architect at Anchore, calls them – that led to these current circumstances. Those accelerants would be the evolution of cloud platforms and cloud-native development practices, the increase of software containerization and the adoption of modern build and deployment methods.

"First, cloud platforms have not only allowed innovation at remarkable rates, they are enabling organizations to reach broader audiences faster," Bryan said. "Growing cloud adoption has, in turn, accelerated the use of cloud-native development techniques like software containerization. Using software containers has, in turn, encouraged increased use of open source software. This combination of cloud deployment, modern development techniques and expanded use of open source software is creating new threats for both software producers and software consumers."

Bryan also noted the rise in importance and awareness.

"The intersection of increased software container adoption and increased supply chain security concerns is impacting container initiatives across the board," he said. "We see that in our recent Anchore survey of 425 IT, security and DevOps leaders, that 64% of respondents have been affected by software supply chain attacks in the last year. This issue is growing in size each day."

"In the absence of applying new techniques to secure the software development pipeline, you have the security breaches that we're seeing," Bryan added. "Those elements combined have helped to accelerate the visibility of software supply chain security. Traditional security means just can't keep up, IT security organizations and even accreditation processes really cannot keep up with the pace at which organizations are able to build and release software now. We can consume new releases of software faster than ever before. And it's only going to continue to ramp up from here."

Role of the SBOM

This is where Bryan sees the concept of a software bill of materials (SBOM) squarely fitting into the

picture. Before an organization can make sense of the software supply chain, it has to understand the software building blocks it is using. An SBOM is often compared to the ingredients list on packaged food in the grocery store. It's an articulated list of all of the components that are in that package. That could include open source components, vendor components, or pieces of software a systems integrator built.

Having this level of transparency and visibility into the software supply chain gives organizations new opportunities to assess their risk disposition, and provides new, more secure footing and perspective for performing risk management. But just having an SBOM isn't enough; organizations have to make a plan for how to manage software supply chain security over time. A single software package could have thousands of components or more. That's a lot of information to aggregate, make sense of, and put to use in a meaningful, efficient way on an ongoing basis.

"I think that's a question that we're really sort of in the infancy of figuring out how to do," Bryan said. "Once you start to think about sharing SBOM information between organizations, you need to start thinking about standard formats to exchange the data, as well as tooling to automate the process and leverage the information to improve your security posture."

Supply chain trust

Because an SBOM becomes a foundation for trust between software suppliers and software consumers, it has to be in a format that each can read and understand. The industry has developed several SBOM standards and enabling frameworks, but there is not a definitive singular standard. One key area being developed is new approaches to guarantee that an SBOM hasn't been tampered with, by way of cryptographically signed attestations.

There's also the question of how these artifacts will be folded into existing accreditations and federal requirements, like Defense Department cybersecurity assessments or risk management and cybersecurity frameworks from the National Institute of Standards and Technology.

"The idea of creating this level of component transparency across the software supply chain is foundational to protect against future attacks more effectively," Bryan said. "As the cloud-native software development and containerization efforts continue to mature, traditional accreditation methods have opportunities to make equally significant strides. We are already starting to see new requirements being developed by the US government based on the executive order."

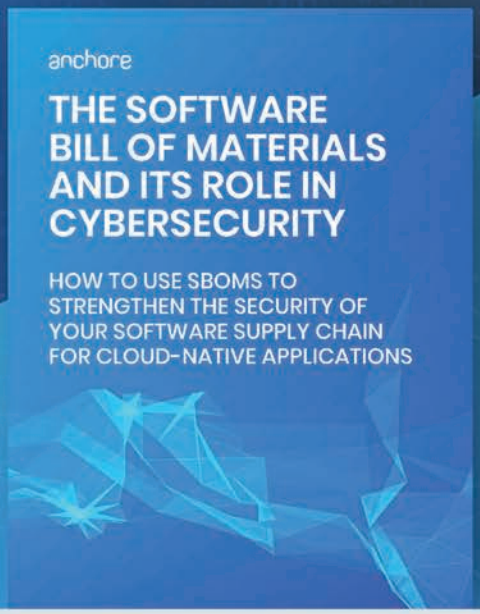
To improve their software supply chain security, organizations need to establish a strong foundation; they need to begin by looking at their development practices, pipelines and tooling, and assess how they can embed security into each step of the development process. That will require input and cooperation from all stakeholders, from security to development to leadership teams.

"It's not a situation where you can say 'I'm done, I did this thing once, and it's complete.' Software supply chain security is evolving, and it's going to be ever evolving. And organizations really have to pragmatically look at their software development practices," Bryan said. "Organizations can begin to formulate their security approach by understanding what an SBOM is, why it is important and how it fits into their current processes. They also must engage both business and technology leaders early so they understand the importance and value of a strong security posture in software development. Ultimately, both software producers and software consumers will need to work together to secure the software supply chain and prevent future attacks."

anchore

SECURE THE SOFTWARE SUPPLY CHAIN: SAVE THE WORLD

Accelerating software development is critical for deploying applications—but not at the expense of security. 64% of organizations surveyed reported they had been affected by software supply chain attacks in 2020. It's never been more important to ensure your software supply chain is secure. The Software Bill of Materials (SBOM) can be the key. Check out our white paper, **The Software Bill of Materials and its Role in Cybersecurity** to learn where to start.



DOWNLOAD THE WHITE PAPER >