WHY DOES YOUR BUSINESS NEED A SOFTWARE BILL OF MATERIALS (SBOM)?

digicert®

Dependencies on multiple components gathered from all along the software supply chain put your code at risk. But that's just one part of the picture. There's more for businesses to consider.

BROKEN LINKS IN THE SOFTWARE SUPPLY CHAIN

Nearly all cybercrime operates on dark corners and obscurity. When your dev team taps into the intricate, complex, and often unknown code throughout the software supply chain, you risk introducing openings and malware into your build. Cybercriminals don't want you to be able to see what they've slipped into the code you're picking up from open source, third-party, libraries, and other teams. The obscurity of the unknown is their best tool for targeting your software.

When your business can see all the components in the software you're building, you gain the kinds of visibility into your complete code that allows you to greatly reduce risk while increasing efficiency and putting together a better product. That's where a Software Bill of Materials comes into play. It shines a light on all components, making it very difficult for cybercriminals to obscure the threat they're trying to introduce into your build.

2022 reports from several top research groups document a massive number of software supply chain attacks—and they're only increasing.

1700+

Total number of breaches

400 MILLION+

Total people affected worldwide

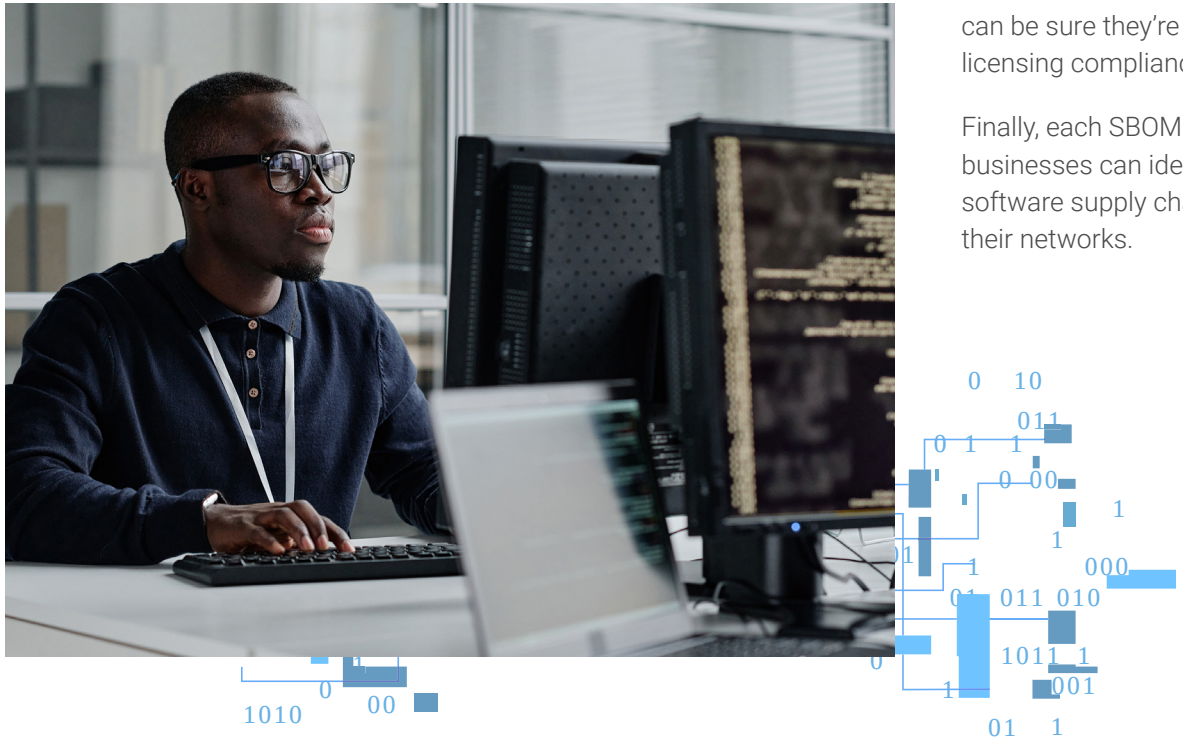
$4.5+ MILLION USD

Total cost of damages to orgs per breach

WHAT IS AN SBOM?

There are several best practices like code signing that helps organizations protect their code. But if a threat can be introduced from outside your team, through the software supply chain, the only way to protect the complete package is to know everything that's in that build—no matter who wrote it and where it comes from. That's where an SBOM comes in.

A Software Bill of Materials is a record of all the components contained in a piece of software. They are often likened to a list of ingredients on a nutrition label in food packaging in some countries. However, the point of the SBOM is not just to provide information about the "health" of the software, it's also a tool that allows people to trace and eliminate or mitigate an individual code component that contains vulnerabilities or malware. Compared to a nutrition label, an SBOM offers a far more dynamic approach, enabling developers and IT professionals to effectively reduce risk by integrating with other security tools.



HOW DOES AN SBOM PROTECT BUSINESSES?

From a technical standpoint, it's easy to see the security advantages to a Software Bill of Materials. But the SBOM also offers business protection—and value—beyond basic software security.

Risk management

Unfortunately, as many companies have discovered over the past few years, everyone thinks "It won't be me," until it is. The resources involved in deploying SBOMs are minimal compared to the cost of a large data breach.

As a detailed inventory of all components in a software project, Software Bills of Materials allows a business to identify potential vulnerabilities or security issues and deal with them quickly—sometimes even before someone on the outside can break in. If someone exploits a vulnerability before it's detected, an SBOM can isolate the point of entry and patch it before the breach grows to a critical point.

Each SBOM contains licensing terms for each component, so Developers can be sure they're using components that meet legal and business licensing compliance.

Finally, each SBOM reveals dependencies on external components, so businesses can identify where they're reliant on different parts of the software supply chain, and better control which software they use on their networks.

Efficiency

For software creators, an SBOM gives the ability to look downstream and assess the potential impact of a vulnerability on products and services using their software. And for commercial components, an SBOM helps software makers evaluate the security practices of different vendors, so they can make informed decisions about which components to use in their builds.

If an incident occurs, it's easier for software creators to locate the problem, and communicate to their customers and users while they help to fix the problem.

Finally, having an SBOM helps open-source management teams boost efficiency by cutting down the amount of time spent fixing non-compliant code. And an SBOM improves overall efficiency by reducing the amount of time spent remediating early-stage problems. An SBOM speeds time-to-market and helps Developers stick to their budget.

Transparency

Visibility into all corners of their digital information is what gives businesses the ability to protect and manage that information. Because an SBOM inventories all components, businesses can see every part of a software's building blocks. This not only allows for the detection of security threats, it also shows how these components move through the supply chain by specifying versions, so businesses can track updates, patches, and new threats.

This form of transparency makes it much easier to meet regulatory compliance. When software is protected and transparent, and businesses stay in compliance with government and industry standards, that helps to protect the brand reputation. Utilizing SBOMs is not only a best security practice, it also shows a commitment to data protection and responsible software development.

They are also advantageous for companies during the merger and acquisition process. When all the software is already inventoried, it takes less time to analyze the code, and it reduces the risk of delivering or inheriting security or licensing issues that could expose the business to breaches and the subsequent legal and public fallout.

THE CLEAR BUSINESS ADVANTAGE

While a Software Bill of Materials isn't the only solution to the problems in the software supply chain, it's a powerful, proven, and resource-friendly part of fighting data theft, ransomware, and the other kinds of software vulnerabilities that regularly do damage to businesses. When you deploy SBOMs, you actively foil the efforts of cybercriminals trying to use obscurity to slip harmful code into your software. A Software Bill of Materials is one of the most effective methods for protecting your business and the entire software supply chain.

You can learn about securing the entire software supply chain here:
digicert.com/software-trust-manager