MEND

Software Bill of Materials

The Challenge

A massive increase in cyberattacks against the software supply chain has led to a flurry of new governmental regulations aimed at protecting critical infrastructure and private sector software. New U.S. federal government regulations require that every piece of software contain a software bill of materials (SBOM) – a formal, machine-readable inventory of all components and dependencies used in building software. Accurately creating and managing SBOMs can be a difficult process that slows the development cycle or worse – fails to identify vulnerabilities in your software.

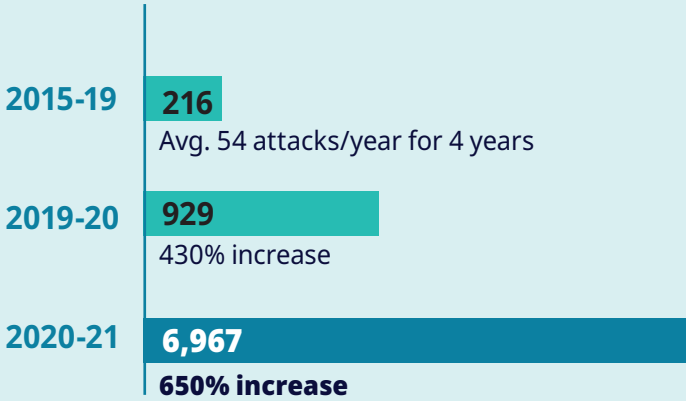
The Solution

Mend SBOM quickly and effectively enables you to create SBOMs that meet regulatory requirements, giving you unmatched visibility into what makes up your software. But it doesn't stop there. **Mend SBOM also gives you a path to remediation for vulnerable components found in software – helping developers code more securely and protecting software users, while also ensuring the security of the software supply chain.**

How Serious Are Software Supply Chain Attacks?

66% of attacks use **code from suppliers** to expand the attack

60% of attacks target **personal data and intellectual property**



How Does Mend SBOM Work?

Mend makes creating SBOMs simple.

Mend SBOMs are generated in SPDX format to create a machine-readable inventory of software components, their dependencies, and their hierarchical relationships, including:

- Identification of all open source libraries
- Tracking and documenting each component, including direct and transitive libraries
- Automatic updates when components change
- Identification of vulnerabilities
- Path to remediation that ensures updates are backward compatible and won't break the build

Why Does Mend SBOM Focus on Open Source Code?

Because that's where attackers focus their efforts

Open source software is used in 96% of all commercial codebases.

Open source software powers 75% of the public cloud workload.

The codebase in an average application is 60-80% open source.

Almost 10,000 vulnerabilities were found in open source code in 2020 alone.

Key Benefits of Mend SBOM

1. **Detection**
   Gain increased insight into your open source inventory, as well as identify security vulnerabilities and license compliance requirements.
2. **Transparency**
   Ensure components are up to date and increase visibility into the software supply chain. Improve adherence to policies and regulations.
3. **Remediation**
   Identify affected software, understand the associated risk, and determine the steps to remediate any defects.
4. **Reduced Operating Costs**
   Quantify and manage risks, while consolidating assets and impro ving security

Why Does Mend SBOM Focus on Open Source Code?

With Mend SBOM, the identification of vulnerable components is fully integrated into the cycle of addressing those risks. Mend SBOM helps developers:

- Keep code up to date
- Identify all open source components, including transitive dep
- Ensure vulnerabilities are quickly identified
- Reduce alerts by guaranteeing no false positives
- Prioritize vulnerabilities based on their potential impact
- Remediate issues quickly and easily