Mend.io

Enhance Supply Chain Security with Proactive SBOM Management

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.

While organizations use them today to create software inventories and analyze, track, and understand exactly which components make up their software supply chain, that's not enough.

Using SBOMs to create software inventories to meet compliance or industry requirements is a great start. However, the possibilities beyond compliance are even more compelling. Ultimately, the real value lies in evolving SBOMs from informational resources to actionable business tools.

Once an organization has SBOM capabilities in place, there are opportunities to turn that SBOM information into action. From automated vulnerability analysis to proactive application lifecycle prediction, SBOMs can help organizations stay productive and safe in a dynamic software environment.

Moreover, as SBOM tools evolve and add more analytical capabilities, new ways to take action with SBOMs will appear.

To take advantage of the coming opportunities and competitive value generated by SBOM maturation, organizations need to build a solid foundation by accurately creating, implementing, and managing SBOMs. Doing so allows them to quickly take advantage of the opportunities that SBOMs will bring for turning information into action.

The Evolution Of SBOMs

SBOMs are still developing, so naturally their uses are also evolving. We can see the first steps towards action as companies start developing SBOM tools into analytical platforms that can help organizations understand and inventory software environments, and take proactive action based on that information.

Generally, SBOM usage starts with generating an inventory of software components. Some industries, compliance requirements, or software licenses may even require it. But to really take action with SBOMs, organizations need up-to-date SBOM inventories, not static, out-of-date ones.

Generating a static inventory of software components for an SBOM is a little like taking a still image from a movie—it's representative, but it doesn't tell the whole story. That's because applications and software fundamentally differ from a manufactured product like a car, whose original parts are fixed once it leaves the factory. In contrast, software constantly evolves: new versions are released, vulnerabilities are discovered, functionality is changed.

The result is that today's SBOMs essentially try to tell a dynamic and evolving story through a static snapshot of an application at one point in time. While helpful and a great starting point, it's not the complete picture of any organization's software environment.

Action Opportunities

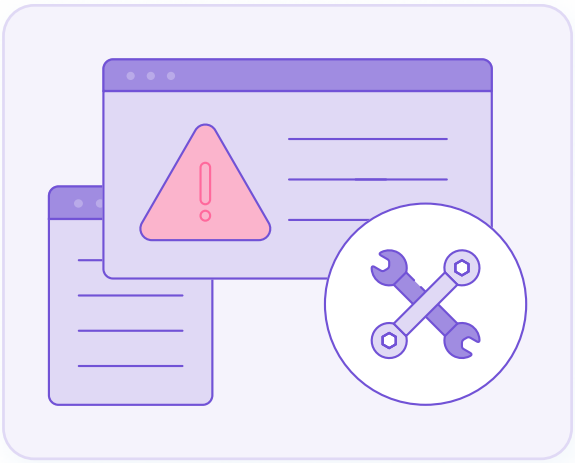
Ultimately, many envision SBOMs as a dynamic tool that provides a live data feed rather than that static snapshot. While no SBOM tools currently provide that capability, organizations can take steps in that direction by updating their static SBOMs more frequently and generating software inventories more often, essentially emulating a dynamic SBOM through multiple fixed points.

Thus, the critical step in being able to take action with SBOMs is to have SBOM inventories that are updated as close to continually as possible. And for most companies, that's impossible with manual SBOM solutions.

Since there's no feasible way to manually manage the volume of SBOM information, organizations from software manufacturers to software consumers need to automate everything related to SBOM management. Therefore, the first step in taking action with SBOMs is to automate their consumption and production, including the generation of software inventory and the ingestion of SBOMs from suppliers. Let's take a look at how important SBOM capabilities such as vulnerability remediation, inventory management, and open source license compliance are increasingly being automated.

Vulnerability Remediation

Up-to-date inventories are essential if companies want to use SBOM information to identify and remediate software vulnerabilities, which are both dynamic and time urgent. One important way to take action with SBOM information is by using SBOM data to **automate vulnerability analysis and remediation**.



Organizations can leverage software inventories—as long as they're current—to correlate vulnerabilities and flag them for remediation. Ideally, organizations can then take the next step and automate the remediation of vulnerabilities. This may involve a "shift left" approach that works back to the original source repository to remediate vulnerabilities for a new version or patch.

Mend SBOM: Essential Capabilities For Vulnerability Remediation

Exploitability data

Exports VEX files to demonstrate whether a vulnerability is exploitable.

Automated policy enforcement

Enables granular policies per project, product, application type, or organization. Allows you to set policies for each stage of the SDLC: planning, development, deployment, and production. Policies can be conditional on security parameters such as severity or a specific CVE.

Prioritization

Analyzes how affected libraries are actually used in your code. Eliminates 70-80% of vulnerability alerts that have no impact on the current project.

Shift left

Scans popular repos, including GitHub repos, using its GitHub integration. Browser extension gives developers information about components as they browse the web.

Shift right

Tracks the Bill of Materials of the latest build for every version you deploy. Alerts teams in real time and provides remediation guidance when new vulnerabilities are reported.

Third-party support

Third-party SBOMs can be consumed by Mend.io's SBOM, allowing organization's to manage supply chain risk with greater visibility.

Vulnerability remediation

Sources patches and suggested fixes from hundreds of trusted open source communities. Offers developers multiple remediation options, with scoring.

Pinpointing vulnerabilities in code

Provides a complete trace analysis for each vulnerability. Shows which part of your code touches the vulnerable functionality, down to the line number.

Key Benefits Of Mend SBOM

01

Actionable automation

Effective automation that automatically updates open source dependencies and packages across all applications, eliminating error-prone manual processes.

02

Accurate risk assessment

Automated dependency identification provides an accurate and up-to-the minute risk assessment and ensures license compliance.

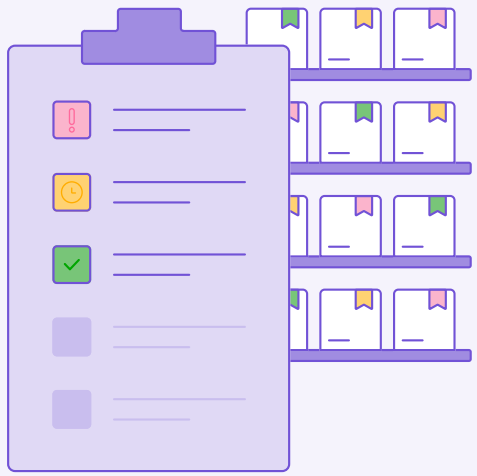
03

Prioritize high-risk vulnerabilities

Not all vulnerabilities pose a risk. By knowing whether your code reaches vulnerable functions, you can prioritize remediation based on actual risk.

Inventory Management

SBOM information can be helpful for more than just identifying, fixing, and communicating software vulnerabilities within an organization's IT environment. Companies can also use SBOM data to eliminate technical debt. Organizations can use the information contained in SBOM software inventories to analyze applications, understand how "old" or "brittle" each application is, and rate the quality of the application.



For example, an automated SBOM evaluation of an application might show that the application has components that are seven versions from the latest, opening up the organization to potential security or performance risks. In general, older applications are more likely to break or malfunction. By using SBOM information to analyze the average age of applications, organizations can identify which ones should be updated or addressed. In addition, the more out-of-date an application is, the harder it will be to update without significant resource investments.

Mend SBOM: Essential Capabilities For Inventory Management

Integrations with DevOps tools

Integrates with IDEs, package managers, repos, build tools, CI servers, and AST tools. Alerts about problems and guides teams as they select and download components.

Automated policy enforcement

Automates selection, approval, and tracking of open source components. Policies defined per SDLC stage, product, and organization.

Open source components database

Aggregates information about open source components from hundreds of sources, multiple times a day.

Reporting

Provides built-in reports for open source Bill of Materials, due diligence, risk, and attribution at the project, product, or organization level..

Automated dependency identification

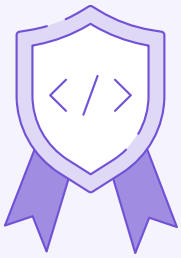
Comprehensive dependency identification automatically identifies all open source and third-party components in an application, including direct and transitive dependencies. Complies with NIST standards and is available in SPDX and Cyclone DX formats.

Languages and frameworks coverage

Supports over 200 languages, frameworks, and development environments.

Open Source License Compliance

It is important to establish an open source usage policy and block inappropriate or overly restrictive open source licenses. You must also ensure that you are meeting license requirements for all of the open source components used in your software. Management, security, legal teams, and third parties such as investors conducting due diligence need complete visibility over open source licensing.



Mend SBOM: Essential Capabilities For License Compliance

Accuracy

100% license detection accuracy with unique ability to associate folders and libraries. Shows licenses for the entire dependency tree. Supports multiple licenses for one component.

Reporting and auditing

Offers a wide range of reports built for all relevant organizational roles. Provides visibility for internal teams—R&D or IT management, security, legal, management.

Languages and frameworks coverage

Supports over 200 languages, frameworks, and development environments.

Automated policy enforcement

Automates the license approval process. Extends license tracking and approval to the full dependency tree of each package. Can automatically approve, reject, or initiate a manual workflow, depending on license type.

Shift left

Provides a native Github integration—scans GitHub repos and discovers license information. Provides a browser plugin that helps avoid problematic licenses at the selection stage. Integrates with DevOps tools at all stages of the SDLC and alerts about license issues.

Real-time alerts

Alerts which license types are in your software and provides a full risk analysis.

Competitive Advantage Through Actionable SBOMs

SBOMs are a critical first step to managing and securing the software supply chain since data from SBOMs can be aggregated, enriched, and analyzed to significantly lower software supply chain risk and make compliance easier.

But the tipping point away from static SBOMs is coming soon, and proactive organizations now have the opportunity to turn SBOM informational resources into actionable information platforms that can help generate business value and competitive advantage.

Organizations that want to create value from SBOMs should develop internal SBOM programs and implement an SBOM automated management platform. By automating, enriching, and analyzing SBOM information, organizations can move them from information resources to actional information that can impact everything from an organization's security stance to its competitive advantage in the market.

Mend.io

Contact an expert to learn more about proactive application security

Schedule a demo