mend.io

The Future of SBOMs

mend.io

The Future of SBOMs

Moving Beyond Information to Action

Software bills of materials (SBOMs) are reaching the tipping point. 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 implementing SBOM generation capabilities. Doing so allows them to quickly take advantage of the opportunities that SBOMs will bring for turning information into action.

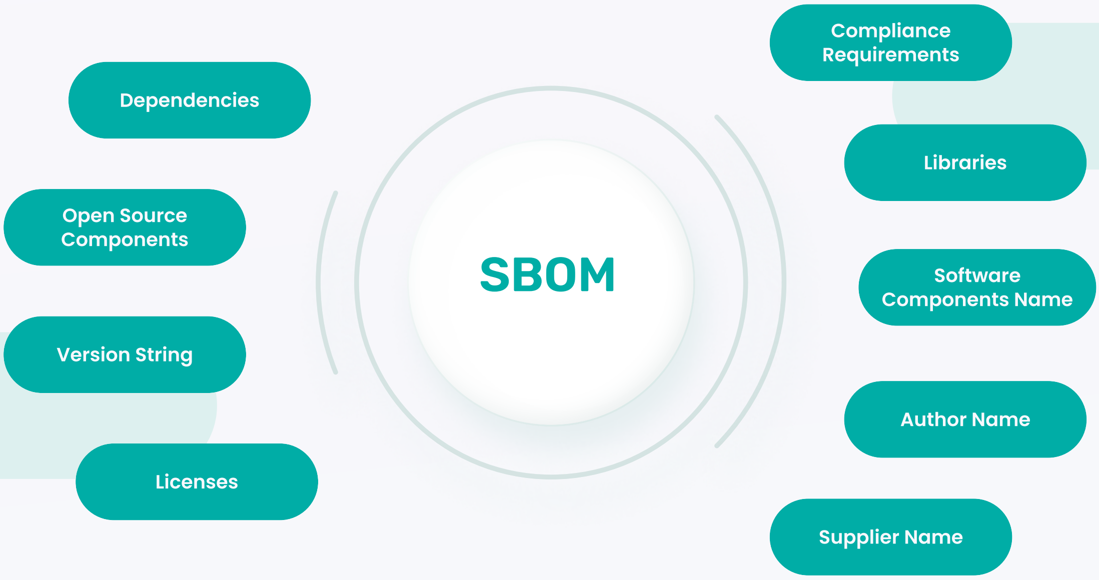
The Evolution of SBOMs

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 But to really take action with SBOMs, organizations need up-to-date SBOM inventories, not static, out-of-date ones.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.



From Static to Dynamic

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.

This capability is essential if companies want to use SBOM information to identify and remediate software vulnerabilities, which are both dynamic and time urgent. If an organization relies on SBOM inventories to identify vulnerabilities, those inventories must be up to date.

Thus, the critical step in being able to take action with SBOMs is to have up-to-date SBOM inventories, as close to continuous ones as possible. And for most companies, that's impossible with manual SBOM solutions. There's no way that organizations can manage SBOMs by hand if their goal is to be able to take action with them.

SBOM Action Opportunities

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.

Once an organization has automated its SBOMs, it will have a foundation for leveraging SBOM information to deliver business benefits.

As SBOM specifications, practices, regulations, and guidance evolve, companies will be able to move beyond collecting information to using that information to take action.

Consider the following possibilities:

Automating vulnerability analysis and remediation.

An 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.

Automating the communication of vulnerabilities.

Finding vulnerabilities and fixing them is critically important for any organization. But if you are a software supplier, it can be just as essential to communicate software vulnerabilities that might affect the users of your software. This leads to the next great way to take action with SBOM data: automating the communication of vulnerabilities to outside companies or partners. When vulnerabilities are discovered, automation could work to notify impacted users – potentially even with patching or remediation advice.

Proactively managing your application life cycle.

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.

Competitive Advantage Through Actionable SBOMs

SBOMs are a critical first step to managing the software supply chain and its security 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 for 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.

Learn more about SBOMs

mend.io