# flexera

# Reduce risk, enhance software reliability

## Now you can:

- **Ingest third-party SBOMs** you've received from your software suppliers to assess impact to your organization, including new vulnerabilities and more

- **Construct SBOMs** for applications in your estate, including software built internally, SaaS applications, vendor software and more

- **Assess the impact of newly reported security vulnerabilities** against your IT estate and develop mitigation or remediation plans

## What you get

- A comprehensive list of all third-party components in a shipped/hosted app

- Third-party elements, including commercial-off-the-shelf (COTS) and open source software (OSS) components

- A defined relationship between components; who is bringing what to where

- Addendums available in standard industry formats, which can provide advanced vulnerability information regarding impact to your applications, such as Vulnerability Disclosure Report (VDR) and Vulnerability Exploitability eXchange (VEX)

Flexera One IT Visibility SBOM Management is a comprehensive SBOM management and compliance solution offering transparency, security and compliance in the software supply chain. With advanced automation, deep scanning and cloud-based accessibility, it also manages software complexities by tracking producers, third-party code and internal modules, aiding in compliance and risk management.
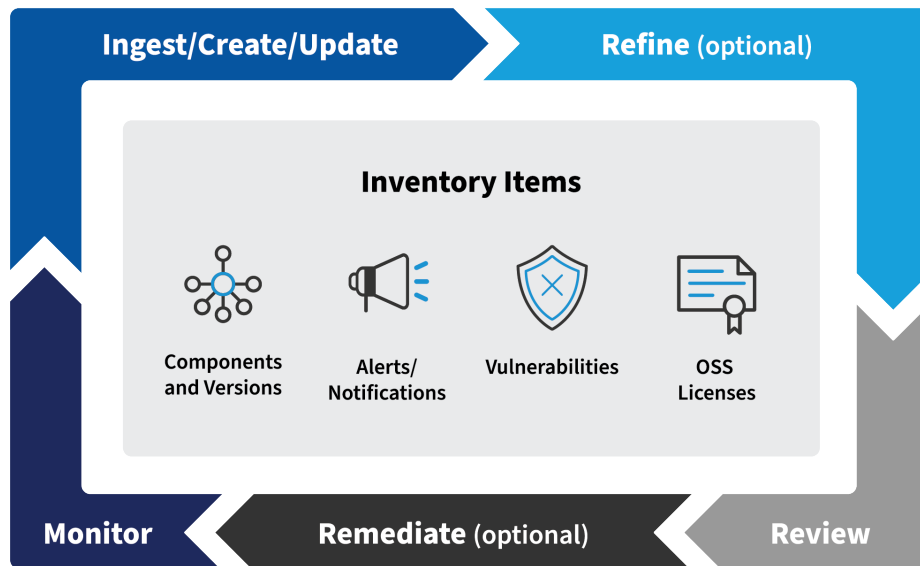
---

» **DEFINITION**

**Software Bill of Materials (SBOM)**

An SBOM is a formal and queryable record containing the details and relationships of various components used in building software.

- NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

---

**Software Bill of Materials for Consumers**

| Ingest/Create/Update | Refine (optional) |
|---|---|

**Inventory Items**

Components and Versions | Alerts/Notifications | Vulnerabilities | OSS Licenses

| Monitor | Remediate (optional) | Review |
|---|---|---|

## IT organizations face growing software challenges

When it comes to risk management, having an SBOM is an essential element of mitigating cyber threats because it empowers you to know where to find malicious code in an application that your organization has deployed. The SBOM provides a source of truth for components in use across your enterprise to reduce organizational risk due to:

- **Continued OSS growth:** Software providers consistently leverage OSS to accelerate time to market and drive innovation. On average, Flexera sees 2,500 OSS components per application, which accounts for 80% or more of an application's content (Revenera Audit Services, 2023)

- **Increased security exploits:** The software supply chain is constantly under attack from hackers, with the frequency and sophistication of exploits continually increasing. On average, it takes organizations 277 days to identify and contain a breach. (IBM/Ponemon Institute Report, 2023)

- **Continued expansion of SBOM mandates:** Regulations across the world (US Cyber EO 14028 and EU CRA) are requiring enhanced cybersecurity and software supply chain integrity. This includes gaining transparency and assessment into software composition and security vulnerabilities for remediation. It applies to regulated industries, including financial (SEC Cyber Rules), medical, transportation, energy and more

- **Disconnected supply chains:** Lack of transparency into software supply chain leads to lack of

**» INSIGHT**

**2,500**
Average number of open-source items discovered per audit project. **Up 14% YOY**

**REVENERA AUDIT SERVICES, 2023**

accountability. Additionally, software buyers have to trust their suppliers without much knowledge of what's in the mission-critical software they rely on to run their business

- **Emerging SBOM initiatives:** New vendors and applications are constantly emerging, and it's time consuming and tedious to keep track of everything in your organization's software estate

## IT Visibility SBOM Management

The software industry's reliance on OSS—along with a sharp increase in dependencies—and the frequency of security exploits has created a perfect storm for supply chain security, which is why Flexera is focused on greater completeness and accuracy of SBOMs.

SBOMs are rarely 100% perfect, but it goes without saying that it's highly preferable for an SBOM to be as complete and accurate as possible. This means including all relevant components in a piece of software, as well as all subcomponents, direct and resolved transitive dependencies, associated licenses and true-positive security vulnerabilities. It also means taking into account as much supporting detail as possible, including the relationships between the SBOM parts, which indicate their origin.

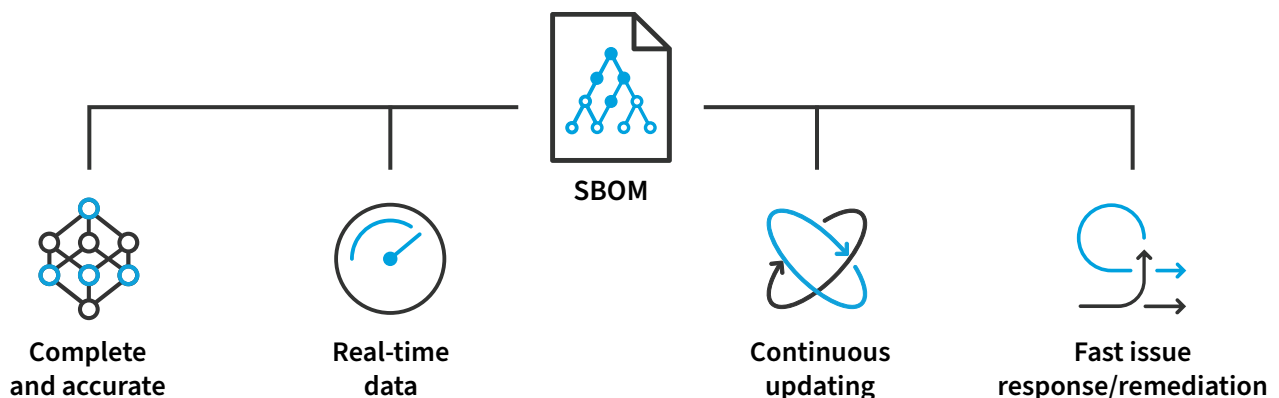With Flexera One's SBOM Management, you can achieve:

- **Compliance with regulations:** comply with National Cyber Security regulations, EU CRA and other regulatory bodies

- **Unified Flexera One platform:** Offering a central solution for all SBOM related needs, from ingestion of third-party SBOMs to real-time monitoring of vulnerabilities

- **Proactive approach:** Emphasis on real-time monitoring, ensuring your organization stays ahead of potential threats and vulnerabilities

- **Versatility:** Suitable for a wide range of industries and organizational sizes, ensuring broad usage and application

## Qualities of an SBOM



SBOM

Complete and accurate

Real-time data

Continuous updating

Fast issue response/remediation

SBOM Management in Flexera One IT Visibility shows you what's being used in real time; therefore you can expedite reactions to security risks and facilitate a rapid response to threats with speed and accuracy.

Maintain actionable SBOMs for more application control and transparency. With all open source code and third-party components catalogued, when the next high-profile vulnerability hits, your IT and security teams will have access to unified data to quickly uncover potential exposure and fix problems—both in the code internally scanned and in the software components coming from outside the organization.

## SBOM source of truth

**Industry standard formats**

**Impact analysis**

**Usage insights**

**Alerts**

## About Flexera

Flexera saves customers billions of dollars in wasted technology spend. A pioneer in Hybrid ITAM and FinOps, Flexera provides award-winning, data-oriented SaaS solutions for technology value optimization (TVO), enabling IT, finance, procurement and cloud teams to gain deep insights into cost optimization, compliance and risks for each business service. Flexera One solutions are built on a set of definitive customer, supplier and industry data, powered by Technopedia, that enables organizations to visualize their Enterprise Technology Blueprint™ in hybrid environments—from on-premises to SaaS to containers to cloud.

More than 50,000 customers subscribe to Flexera's technology value optimization solutions, delivered by 1,300+ team members worldwide. Learn more at **flexera.com**

**» NEXT STEPS**

Evaluate your organization's SBOM needs

**FIND OUT MORE**

**flexera**™