Why do you need Sparrow SecureHub?

Verification of SBOM tampering and forgery comes first.

If a tampered or forged SBOM is shared, discrepancies with actual data can cause confusion in SW supply chain management. Therefore, verifying the authenticity and integrity of the SBOM is essential.

It is difficult to manage distributed SBOMs.

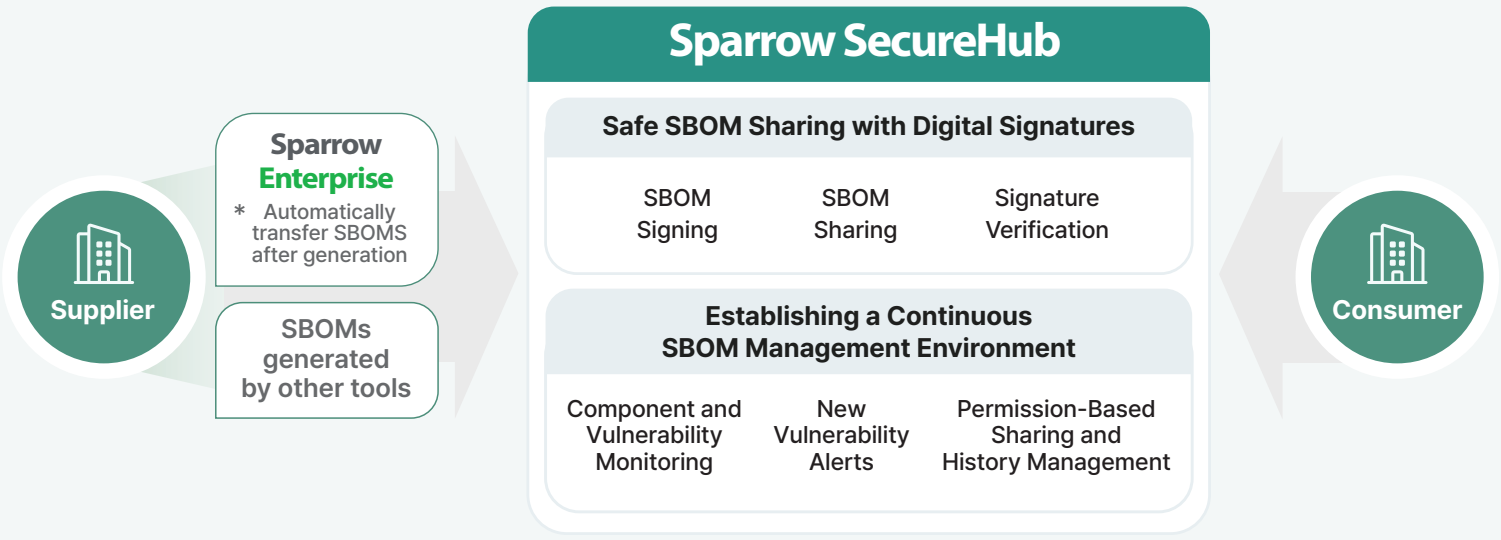
Once an SBOM is transferred from a supplier, it is hard to track who stored it, when, and which version was shared. In addition, whenever new vulnerabilities are discovered, it can be cumbersome to update each distributed SBOM individually.

New vulnerabilities are continuously discovered.

Issues in software components can evolve into new vulnerabilities. Governments also recommend continuous monitoring of SBOMs to track and manage the occurrence of vulnerabilities in software components as part of “software supply chain security guidelines.”

Sparrow SecureHub ?

A platform enabling both sides of the software supply chain to securely and transparently exchange SBOMs and manage them with ease.



Key Features

- SBOM Registration/ Request
- Add Digital Signatures and Verify Authenticity
- Share SBOMs
- Generate Reports and Monitor Vulnerabilities
- Manage Permissions and Sharing History

Expected Benefits

01 Build a trusted SBOM sharing environment where all SW supply chain participants can share safely

Supplier

Self Attestation
Prove authenticity with digital signatures issued from a trusted source.

Consumer

Ensuring Transparency
Verify the authenticity and integrity of SBOMs through signature verification.

02 Enable prompt vulnerability response and continuous vulnerability monitoring

Automate SBOM sharing history and modification tracking

Receive real-time alerts when new vulnerabilities arise

→ Identify affected components when vulnerabilities are discovered

→ Reduce response time to new vulnerabilities

03 Prepare for SBOM-based software supply chain security regulations

By Industry

When manufacturing digital medical devices
(FD&C Act 524B MDR 745, IVDR 746, Digital Medical Device Regulation)

When a financial institution needs to identify and respond to security vulnerabilities in advance
(Checklist for Financial Institutions on Software Supply Chain Security)

By Country

When supplying software to the U.S. federal government
(U.S. Executive Order 14028)

When selling products containing EU software to the European market
(Cyber Resilience Act)

Have questions about Sparrow SecureHub?

We're here to help

✉ E. slaes@sparrow.im

Sparrow Website