

OPSWAT.

# SBOM

Automated SBOM Generation for  
Source Code, Containers, and Binaries



Modern applications are assembled from open-source and third-party components, and the component inventory is what determines whether a team can answer “are we affected?” after a new CVE.

OPSWAT SBOM (Software Bill of Materials) gives development, security, and GRC teams a machine-readable inventory of every open-source and third-party component in their software. It identifies known vulnerabilities, validates licenses, and exports SBOMs in CycloneDX and SPDX—in the CI/CD pipeline or as part of MetaDefender™ Core file scanning.

15+

Languages and  
ecosystems scanned

7M+

Open-source components  
in the OPSWAT library

4

Export formats: CycloneDX,  
SPDX, JSON, PDF

ms

File scans in milliseconds;  
container images in minutes

## Key Features



### Source Code Analysis

Scans projects with dependency manifests and lock files across 15+ languages, including Java, JavaScript/Node.js, Python, Go, PHP, Ruby, and .NET.



### Container Image Scanning

Inspects every layer of a container image to inventory OS and application packages and surface their vulnerabilities.



### Binary Analysis

Detects components and vulnerabilities in compiled artifacts—Java archives with full dependency mapping; C#/C++ binaries by file signature and metadata.



### Nested Dependency Check

Recursively resolves every library and its transitive dependencies, so visibility extends past first-level packages.



### Vulnerability Detection

Cross-references components against GHSA, CVE, EUVD, and OSV, plus a 7M+ component library, with severity ratings and patch status.



### License Detection & Policy

Identifies hundreds of license types, ships with a pre-selected restricted-license list, and flags or blocks non-compliant components.



### Standardized SBOM Export

Generates reports in CycloneDX, SPDX, and JSON, aligned with NTIA minimum elements, EU CRA, and CERT-In guidance, plus a human-readable PDF.



### SBOM Validation & Enrichment

Ingests external CycloneDX and SPDX SBOMs, rescans and validates components, fills missing fields, and adds current vulnerability and license data.

Benefits

Dependency Visibility

Inventories components across source code, containers, and binaries, including transitive dependencies.

Fits Inside the Build

Scanning runs as part of the pipeline, so SBOM generation doesn't hold up a release.

Faster Incident Response

When a new CVE drops, the answer to “are we affected?” comes from a current inventory—not a manual audit across repositories.

Regulatory Readiness

Produces SBOM artifacts in the formats named by E0 14028, the EU Cyber Resilience Act, and CERT-In guidance, plus customer procurement requests.

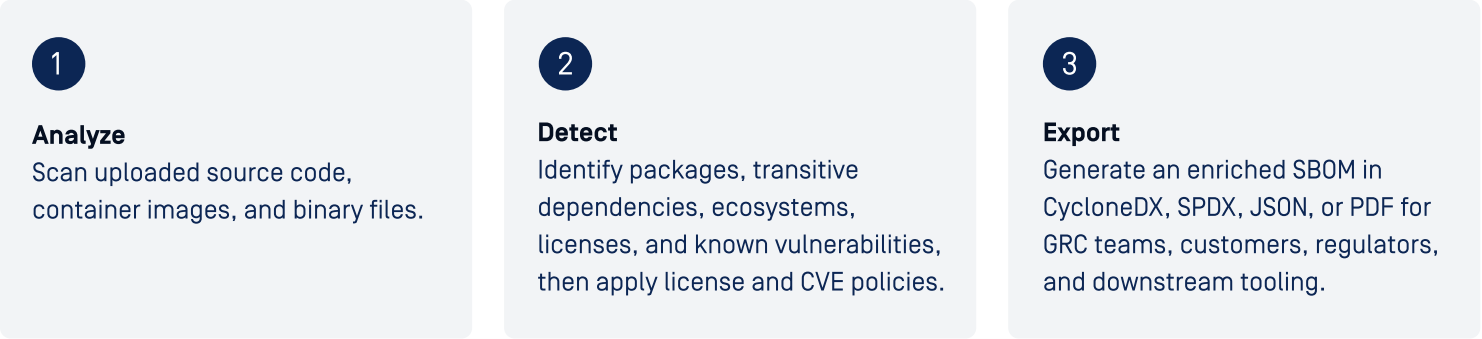
License Risk Control

Flags copyleft and restricted licenses before release, while swapping a component is still cheap.

Malware, Secrets, and SBOM in One Pass

Runs alongside Metascan™ Multiscanning and Proactive DLP™ in MetaDefender™ Core, so a single scan covers malware, hardcoded secrets, and vulnerabilities.

How OPSWAT SBOM Works



15+ languages and ecosystems: Java, JavaScript/Node.js, Python, Go, PHP, Ruby, .NET, and more

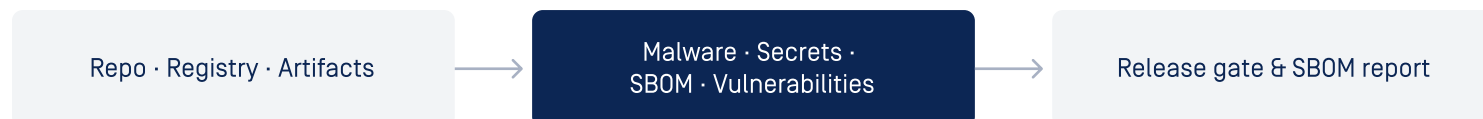
Specifications

| Inputs                                                                                                                                                                                                                                                                       | Detection                                                                                                                                                                                                                                                                  | Output & Integration                                                                                                                                                                                     | Performance                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Source Code</b><br/>Dependency or lock files;<br/>15+ ecosystems</p> <p><b>Containers</b><br/>Images scanned layer by layer</p> <p><b>Binaries</b><br/>Java archives; C#/C++ by<br/>signature</p> <p><b>Existing SBOMs</b><br/>CycloneDX &amp; SPDX for validation</p> | <p><b>Data Sources</b><br/>GHSA, CVE, EUVD, OSV</p> <p><b>Library</b><br/>7M+ third-party OSS components</p> <p><b>Policy Actions</b><br/>Block on known CVEs or<br/>unapproved licenses</p> <p><b>License Lists</b><br/>Configurable, pre-selected<br/>restricted set</p> | <p><b>Formats</b><br/>CycloneDX, SPDX, JSON, PDF</p> <p><b>Products</b><br/>MetaDefender Core,<br/>MetaDefender Software<br/>Supply Chain</p> <p><b>Standards</b><br/>NTIA elements, EU CRA, CERT-In</p> | <p><b>Source Code</b><br/>Milliseconds per file scan</p> <p><b>Containers</b><br/>Minutes per image, scaling with<br/>size and layer count</p> <p><b>Pipeline</b><br/>Runs inline without holding up<br/>a release</p> |

## Use Cases by Product

### Secure the Build Pipeline | MetaDefender Software Supply Chain

Connect source repositories, container registries, and artifact repositories. Every commit and image is scanned for malware [Metascan], hardcoded secrets [Proactive DLP], and vulnerabilities, with an SBOM generated automatically.



### Scan SBOM on Any File Workflow | MetaDefender Core

Run SBOM as a MetaDefender Core engine. Archives, packages, and container images submitted for scanning are inventoried—and blocked when they contain known CVEs or unapproved licenses.



### Validate Vendor SBOMs | SBOM Validation & Enrichment

Procurement and GRC teams ingest supplier-provided CycloneDX or SPDX SBOMs, rescan the components, and fill missing fields—getting back a report with current vulnerabilities, severities, and license data.



## Use Cases by Industry

### Government & Defense

Produce attestation-ready inventories carrying the NTIA minimum elements—and validate contractor-supplied SBOMs instead of taking them on faith.

### Energy & OT/ICS

Decompose vendor firmware and binaries inside air-gapped networks, correlate against current vulnerability data, and make patch-or-isolate decisions without disrupting operations.

### Finance

Keep a living inventory across internal applications and vendor software so audit and regulator questions get same-day answers, not a two-week fire drill.

### Manufacturing & Device Makers

Generate the EU CRA-ready SBOM customers now require—produced as a standard build artifact, with license gates catching copyleft issues before shipment.

## Compliance Drivers OPSWAT SBOM Supports

### US EO 14028 / NTIA (United States)

**Applies to:** Suppliers of software to US federal agencies

**Requires:** SBOMs carrying the NTIA minimum elements—component, version, supplier, unique IDs, dependency relationships, author, and timestamp

**OPSWAT SBOM:** Captures the NTIA minimum data elements automatically and exports in SPDX or CycloneDX

### EU Cyber Resilience Act (European Union)

**Applies to:** Manufacturers of products with digital elements sold in the EU

**Requires:** An SBOM covering at least top-level dependencies, plus vulnerability management across the product lifecycle

**OPSWAT SBOM:** Continuous SBOM generation in CI/CD with vulnerability correlation that includes the EU's EUVD database

### NIS2 (European Union)

**Applies to:** Essential and important entities across critical sectors

**Requires:** Supply chain security and vulnerability handling obligations

**OPSWAT SBOM:** Supplies the component inventory and vulnerability data that supply chain risk management and vulnerability handling run on

### CERT-In SBOM Guidelines (India)

**Applies to:** Organizations serving Indian government and critical sectors

**Requires:** SBOMs with license, patch status, end-of-life, checksums, and usage restrictions, refreshed at every release

**OPSWAT SBOM:** Collects component, risk, and licensing fields, and regenerates SBOMs on every build

Also supports sector rules—FDA, NHTSA, IMDRF, and Japan ESPA—with standardized, shareable SBOMs plus license and CVE policy enforcement before release.

## See what's actually in your build before an auditor or customer asks.

Talk to an Expert  
[opswat.com/get-started](https://opswat.com/get-started)  
[sales@opswat.com](mailto:sales@opswat.com)



OPSWAT is a global leader in IT, OT, and ICS critical infrastructure cybersecurity, trusted by more than 2,100 organizations worldwide. Built on a “Trust no file. Trust no device.”™ philosophy, the MetaDefender platform secures files, devices, and software supply chains.

## OPSWAT.

Protecting the World's Critical Infrastructure