Scribe

Scribe Platform Overview

END-TO-END SOFTWARE SUPPLY CHAIN SECURITY
IN A ZERO TRUST APPROACH

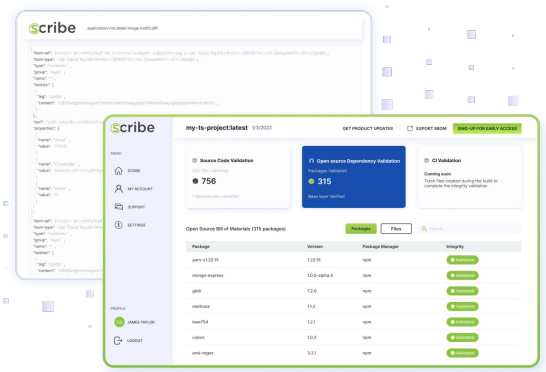
Software supply chain attacks are on the rise and with it, the need to build transparent, evidence-based trust in software

In recent years, software supply chains, both open source and proprietary CI/CD pipelines, have become more attack-prone than ever before. in 2022, Gartner listed digital supply chain as a top trend to watch and a major rising attack surface. The integrity of your code, your customers, and your brand reputation is at risk. Even one bad software component or a security gap in your CI/CD, that might lead to malicious access to your development environment can be enough.

Security professionals, software engineers and DevOps teams are challenged with building transparent, evidence-based trust in the software they use or deliver.

Scribe Platform: The first evidence-based security trust hub

Scribe serves as a hub for software producers and consumers to share attestations (cryptographically signed evidence) to software's trustworthiness - across teams and organizations.



Scribe continuously attests your software's trustworthiness, so stakeholders can:

- ✔ Ensure a secure development process
- ✔ Build and enforce SDLC processes
- ✔ Validate that the code is tamper-free
- ✔ Gauge compliance to standards such as SSDF and SLSA

Immediate value for both DevOps and Security professionals

Share SBOMs and transparency reports on software products

Excellent visibility to your code security aspects and actionable insights for timely mitigation and continuous improvement

Hardened, fully governed development processes and CI/CD pipelines

Continuous, attestation- based compliance with SSDF and SLSA

Validated code integrity & provenance throughout the product lifecycle

Auditable enforcement of security development policies and industry standards

SCRIBE KEY FEATURES

Supports a workflow for sharing SBOMs across teams and organizations

Organizations are often unaware of the full extent of open-source dependencies in their software. Furthermore, if such information exists, it is not methodically tracked, aggregated or communicated to stakeholders.

Monitoring and sharing SBOM is a best practice that is becoming widely required by customers and regulators alike to mitigate software supply chain risks.

Scribe can automatically generate your software product SBOM, along with information about vulnerabilities, reputation, provenance and evidence of its secure development and build. You can select what to share across internal teams or with your customers across enterprise boundaries.

Validates Software builds for provenance and integrity

Every file is tracked and hashed, from its origin to the built artifact, throughout the SDLC. Scribe flags suspicious modifications while accounting for legitimate changes such as linting and compilation. With its open-source package intelligence service, Scribe authenticates the open-source components, assuring that they were not maliciously modified.

Scribe cryptographically signs and validates critical evidence with customer keys, throughout the software development lifecycle. This method provides resistance against tampering. It can also be regarded as extending the well-known concept of software signing to the SDLC.

Handles published vulnerabilities (CVEs) and their relevance to your product (VEX)

Generate CVE reports and track newly published CVEs, based on the SBOMs that are managed in your Scribe Security Hub. Communicate to stakeholder whether a CVE is not relevant to your product with standards based VEX (Vulnerability Exploitability eXchange) advisory.

Governs SDLC Security

Scribe allows you to set a local or organizational SDLC policy that governs your minimum security level. You can whitelist open-source components, mandate certain security tests, or flag severe warnings from tools checking for CVEs in your pipeline, mandates the identification of committers and signage of commits. Software customers can govern, by policy, artifacts delivered from their vendors (e.g., in a subcontracting relationship).

SCRIBE KEY BENEFITS:

Automatically generate, and manage SBOMs and security insights.

Validate your code integrity and provenance.

Track the vulnerabilities in your containers, dependencies, and pipelines.

Detect code tampering.

Continuously demonstrate compliance with supply chain regulation and best practices.

Selectively share all this, in a controlled manner, with stakeholders internally or externally.

ABOUT SCRIBE

Scribe was founded by cyber security and cryptography veterans on a mission to build and provide innovative end-to-end software supply chain security solutions.

We applied our expertise to create a novel platform that leverages leading concepts and frameworks to deliver uncompromising security to code artifacts, from production to delivery throughout the entire software lifecycle.