GitLab | TESTIFYSEC

# Deploy Witness with GitLab CI for verified SSDF compliance

GitLab is the most comprehensive AI-powered DevSecOps platform in the market today, offering a powerful suite of products to help create secure software faster.  GitLab is designed as an open-source platform to allow easy integration with leading technology partners. That open-source foundation can provide more value to GitLab users through integrations by which organizations can share data between GitLab and the partners' tools.

GitLab now offers integration with TestifySec to generate and verify attestations for every step in the Software Development Lifecycle (SDLC) by helping to enforce policy, ensure traceability, and further mitigate supply chain risks.

## Executive summary

As enterprises secure their production infrastructure, attackers are increasingly shifting their focus to the supply chain. The complex nature of software supply chains, coupled with organizations managing countless tools across diverse environments, creates a need to go beyond visibility, and creates an urgent need for enforcement and mitigation.

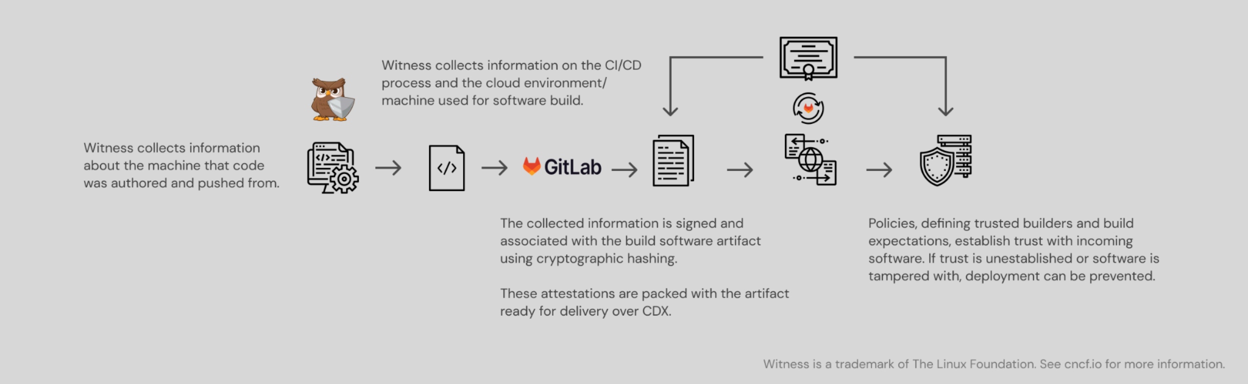
TestifySec unites developers and cybersecurity teams in defending against software supply chain threats by integrating zero trust principles into build pipelines. TestifySec creates transparency and accountability with its open-source and commercial products that observe, manage, and act on metadata at each step of the software generation process.

With a team of security and defense experts, TestifySec is renowned for its influential work in security research and extensive experience in building and securing critical systems, primarily in the defense, banking, and critical infrastructure markets. The company's contributions, such as the CNCF's reference architecture paper for the Secure Software Factory & Software Supply Chain Best Practices, the Cloud Native Security Whitepaper, and various NIST publications, underscore that commitment.

> *"Supply chain attestations are the foundation of effective supply chain security and I believe **Witness** is the most comprehensive solution for generating build attestations."*
>
> **Justin Cormack, CTO, Docker**

## Solution overview

Witness and Archivista are open-source projects created and maintained by TestifySec that are now part of the Cloud Native Computing Foundation (CNCF). Leveraging the in-toto framework for securing the integrity of software supply chains, Witness integrates with pipeline orchestrators to capture build process telemetry, actively enforce development policies, and generate evidence-based supply chain attestations. Archivista manages storage, retrieval, and retention of software build pipeline attestations and trusted telemetry observed by Witness. Deploying Witness with GitLab CI enables organizations to generate and verify attestations for every step in the SDLC, regardless of the execution environment.



Witness collects information about the machine that code was authored and pushed from.

Witness collects information on the CI/CD process and the cloud environment/ machine used for software build.

The collected information is signed and associated with the build software artifact using cryptographic hashing.

These attestations are packed with the artifact ready for delivery over CDX.

Policies, defining trusted builders and build expectations, establish trust with incoming software. If trust is unestablished or software is tampered with, deployment can be prevented.

Witness is a trademark of The Linux Foundation. See cncf.io for more information.

## Solution benefits

Witness gathers and catalogs metadata about the environment, processes, materials, and artifacts within the GitLab CI/CD pipeline; the input files, the command itself, the command execution environment including the Operating System and user details, and finally, the output of the process. Witness then cryptographically hashes and timestamps each piece of metadata to create trusted telemetry detailing every step in the SDLC. These signatures act as checks to help ensure that precisely the expected operations occurred, and that the results haven't been tampered with. The small executable footprint of Witness enables its use wherever GitLab runners are executed, including air-gapped environments.

The evidence gathered by Witness compliments SBOMs, extending transparency into the software creation process itself. Employing Witness within your CI/CD pipeline helps comply with NIST SP 800-218, Secure Software Development Framework (SSDF). The collection of this evidence reduces risks for organizations that are obligated to issue an SSDF attestation to their customers and subject to SEC filings to report a material breach within the supply chain.

**Streamline Authority to Operate (ATO) Process:** Remove bottlenecks by enabling this process across the Department of Defense to enforce, manage, and verify software development policy compliance.

**Air-Gapped Capability:** Reduce risk by enabling cryptographic verification of system updates in air-gapped or highly secure environments.

**Verifiable Compliance:** Enhance overall security posture through cryptographic proofs and automated compliance checks.

### About TestifySec

TestifySec unites developers and cybersecurity teams in defending against software supply chain threats by integrating zero trust principles into build pipelines. TestifySec creates transparency and accountability with our open-source and commercial products that observe, manage, and act on metadata at each step of the software generation process. Everyone deserves secure software. For more information, visit https://testifysec.com.

### About GitLab

GitLab is the most comprehensive AI-powered DevSecOps platform that empowers organizations to maximize the overall return on software development by delivering software faster and efficiently, while strengthening security and compliance. With GitLab, every team in your organization can collaboratively plan, build, secure, and deploy software to drive business outcomes faster with complete transparency, consistency, and traceability. For more information, email us at: alliance@gitlab.com or visit us here.

GitLab