

Company Name: TestifySec

Company Statement: TestifySec simplifies compliance by automating evidence collection and policy checks, tracking, reducing security risks, and ensuring faster, safer software releases. Through unifying developer and cybersecurity teams, they create transparency and accountability with their open-source and commercial products.

Technology Description: TestifySec uses a build pipeline observer, that automates the collection and management of trusted telemetry, and then acts on evidence-based supply chain attestations. It yields a lower residual risk of a software supply chain attack by amplifying the Sec in DevSecOps.

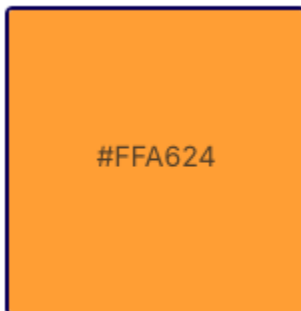
Mission Statement: Ensuring everyone has access to secure software by simplifying evidence collection, reducing security risks, and ensuring faster, safer software releases.

Everyone Deserves Secure Software

Company logo



Company Colors



Orange
Color



Dark Navy Blue
Color



Light Blue
Color

Company Core Values

Trust, Innovate, Customer Centric, Collaboration, Empathy, Adaptability

Platform Features

TestifySec simplifies compliance by automating evidence collection and policy checks, tracking, reducing security risks, and ensuring faster, safer software releases. This enables an automated governance and compliance experience aligned with NIST 800–204D and Secure Software Development Framework (SSDF) guidance. It begins with a build pipeline observer that automates the collection and management of verifiable evidence and trusted telemetry, enabling visibility into the SDLC process. Integrating seamlessly with CI/CD pipelines to automate security checks, our platform is able to continuously monitor source code, build artifacts, and deployments ensuring compliance adherence can be enforced at any point of the SDLC process, continuing through day two operations.

Key features include:

- Pipeline Observation: Flexible observability allows collecting evidence for any existing CI/CD step. The extensible framework allows detailed collection of common telemetry and can be expanded for custom use cases.
- Evidence Collection Store: Evidence is stored in an auditable centralized repository. This repository allows efficient querying, scalable policy evaluation, and exporting for auditing and retention across a large amount of telemetry.
- Automated Vulnerability Discovery and Management: Continuous scanning against evidence containing Software Bill of Materials (SBOMs) and Vulnerability Exchange (VEX) statements provide visibility into vulnerabilities detected, while excluding false positives in code, dependencies, libraries, system packages, and containers.
- Policy Evaluations: A flexible policy framework can ensure continuous evaluation of customized organizational specific security policies, standards, and requirements.
- Admission Control: Applying policy evaluation and decisions audit logging during application deployments ensure deploy-time adherence. Continuous auditing ensures adherence over time.
- Verified Reporting: Policy decisions and compliance postures can be exported to PDF documents, including references to the evaluated policy and all evidence used.

TestifySec mitigates the risk of software supply chain attacks by reinforcing the security aspects of DevSecOps, offering end-to-end security coverage for the software development process. It integrates seamlessly with major CI and infrastructure providers, supports air-gapped environments, and adheres to open standards such as in-toto and PKI for robust security compliance.

Target Market

- Our target market is organizations who prioritize security, compliance and governance across their software supply chain. This includes government agencies like the Department of Homeland Security, Department of Defense, and their

partners. We have worked closely with Lockheed Martin on providing evidence and telemetry collection to reduce risk and deliver software faster. This also includes the financial services and banking industry.

Keywords for Brand Identity	Keywords for Design Element	Market and Audience	Tone and Messaging
Security	SImplicity	DevSecOps	Authority
Trust	Clean Lines	Developers	Collaboration
Compliance	Modern Aesthics	Cyber Security	Trustworthy
Governance	Professional	SOfware Supply Chain	Strategic
Transparency	Approachable	Air-gapped environments	Evidence Based
Innovation	High Tech	Compliance driven	Resilient
Modern	Secure	enterprise	Comprehensive
Robust	Seamless	defense	Proactive
Resilience	Versatile	finance	Seamless integration
Confidence	Future-oriented	Open source	Zero-trust Principles