Case Study

Scribe

Continuous Assurance at Scale: How a Financial Data Giant Transformed Software Supply Chain Security

THE CHALLENGE:

Gaining Control Over Software Supply Chain Risks

A leading U.S.-based financial services firm, specializing in risk management solutions, faced growing concerns around software supply chain security. Despite having a mature AppSec program and multiple scanning tools in place, the company struggled to gain end-to-end visibility across its complex development ecosystem. With numerous decentralized environments and diverse toolsets, security teams found it difficult to assess software risks, prioritize vulnerabilities, and enforce consistent policies.

The company's CISO recognized the unique value of an attestation-based approach to secure software development. Few solutions could deliver cryptographically signed, tamper-proof attestations across the software development lifecycle (SDLC)—critical for compliance, audit readiness and incident response. In addition, Scribe's policy-based guardrails and automation features aligned with the firm's goal of reducing manual workloads and enhancing developer-security collaboration.

THE SCRIBE SECURITY SOLUTION:

Continuous Assurance for the Entire SDLC

The organization fully integrated Scribe into the standardized DevOps pipeline used across the company. Scribe's platform automated SBOM collection, enforced zero-trust security policies, and streamlined compliance—without disrupting development velocity. The company successfully moved from reactive risk management to proactive, automated, secure SDLC policy verification and enforcement.

1. **Automated SBOM and Attestation Collection**
   - Scribe's Valint Agent was deployed across all development pipelines to collect high-fidelity SBOMs at multiple build stages..
   - Reports from third-party tools (SAST, SCA, ASPM) were ingested to support unified policy evaluation and enforcement.

2. **Tamper-Proof Signing & Provenance Verification**
    - All artifacts were cryptographically signed, ensuring software provenance and resilience against tampering.
    - SLSA Level 2 compliance was achieved via signed provenance records and integration with the company's key vault infrastructure.
3. **Policy-Driven Guardrails & Risk Prioritization**
    - The firm implemented conditional signing policies and automated verification gates, enabling continuous compliance checks.
    - Scribe's unified risk scoring engine helped prioritize remediation across all findings—from vulnerabilities to posture violations.
    - Centralized dashboards provided the AppSec team with a real-time "single pane of glass" view of software supply chain risks

RESULTS:

Scalable, Proactive Risk Management Across the SDLC

- **Full SDLC Visibility**: Gained comprehensive insight across 200+ development environments, eliminating blind spots. SBOMs and security attestations are centralized, ensuring timely mitigation and prevention of software versions that don't meet mandatory SDLC requirements.
- **Automated Security & Compliance:** Over 10 security guardrails enforced automatically eliminating manual reviews; 100% of artifacts signed and verified.
- **Operational Efficiency:** Reduced manual compliance tasks by 50%, freeing AppSec teams to focus on strategic risk mitigation.
- **Accelerated Remediation:** Risk prioritization and improved collaboration between AppSec and developers led to significantly faster issue resolution.

Customer Feedback

"We've achieved strong adoption of Scribe's policy engine across our development pipelines. Continuous attestations and automated compliance have eliminated manual security bottlenecks, improved risk visibility, and strengthened SDLC resilience. Today, we have provable software integrity, scalable guardrails, and real-time insights—without slowing our developers down."

Head of Product Security, Leading Financial Services Company

Conclusion: Software Supply Chain Security at Scale

For financial institutions, securing the software supply chain is no longer a nice-to-have—it's mission-critical. This company's experience demonstrates how Scribe Security helps large, regulated enterprises shift from fragmented, reactive security to a unified, automated approach that enables continuous compliance and proactive risk mitigation. Scribe provides the tools, automation and visibility needed to protect software factories at scale—without slowing innovation