Case Study

Scribe

Securing an Air-Gapped Software Supply Chain in a Leading Bank

A Blueprint for Securing Software Factories

THE CHALLENGE:

Closing Security Gaps in an Isolated Development Environment

A leading global bank operated an air-gapped development environment within a private Azure cloud, ensuring that internal software and financial data remained fully isolated from external threats.

However, this disconnected infrastructure created security blind spots for the Application Security (AppSec) team. The CISO lacked real-time visibility into vulnerabilities, code provenance and whether security policies were consistently enforced. Despite using multiple scanning and threat detection tools, they could not track developer actions, enforce remediation timelines or verify software integrity in an automated way. The result was delayed security responses, manual compliance burdens and unverified software risks within the bank's SDLC.

They needed a scalable, automated solution to enforce policies, gain real-time security insights and ensure airtight software integrity—without compromising the air-gapped security model.

THE SCRIBE SECURITY SOLUTION:

Continuous Assurance for Air-Gapped Development

The bank deployed Scribe Security's Continuous Assurance Platform, enabling automated software security enforcement, risk visibility and cryptographic integrity verification—all within its air-gapped ecosystem. Key capabilities included:

1. **Automated SBOM Generation & Security Attestations**

   - Scribe Valint Agent was deployed across all pipelines to generate high-accuracy SBOMs and ingest third-party scanner reports (e.g., Nexus IQ, Checkmarx) for policy enforcement.
   - Ensured tamper-proof, cryptographically signed attestations, enabling compliance and forensic analysis

© Copyright 2025 Scribe Security.

2. **Policy-Based Security Guardrails & Risk Prioritization**
    - Automated policy enforcement for software dependencies, code signing and vulnerability remediation.
    - Risk scoring & prioritization ensured faster decision-making.
    - Policy violation alerts provided real-time security insights for proactive mitigation.
3. **Secure Code Signing & Tamper-Proof Integrity Verification**
    - 100% of software artifacts cryptographically signed, ensuring tamper resistance & compliance.
    - Integrated seamlessly with the bank's existing key vault & attestation store.
4. **Air-Gapped Deployment & Secure Cross-Domain Communications**
    - Lightweight, containerized deployment to fit the bank's infrastructure
    - Used existing cross-domain solutions to securely import threat intelligence updates into the air-gapped environment.

RESULTS:

Business Impact & Security Gains

- **Full Supply Chain Risk Visibility -**
    - Automatic inventory of software risks, ensuring no blind spots in software dependencies.
    - Automated risk scoring of software components across all development teams
- **Strong Security & Compliance -**
    - 100% of software artifacts are cryptographically signed, ensuring tamper resistance & auditability
    - 10+ security policies enforced, cutting compliance review time by 40%
- **Operational Efficiency & Risk Reduction—**
    - Eliminated software supply chain security bottlenecks, allowing development teams to move faster without introducing risk
    - Faster vulnerability remediation & automated security due to improved communications and common language between developers and AppSec teams

© Copyright 2025 Scribe Security.

Customer Perspective

"Scribe gave us the missing visibility and control we needed in our air-gapped development environment. We now enforce policies automatically, verify software integrity with cryptographic proof and remediate risks faster—with zero disruption to developers. It's transformed how we manage software supply chain risk."

CISO, Leading Global Bank

Proactive Software Supply Chain Risk Management for Air-Gapped Environments

As financial institutions face mounting software supply chain threats and escalating regulatory demands, timely and continuous software risk management has become a business necessity. While air-gapped development environments offer strong isolation from external threats, they often suffer from limited visibility, manual processes, and gaps in policy enforcement—making them vulnerable to internal and supply chain-based risks.

This leading global bank chose a proactive approach by implementing Scribe Security's Continuous Assurance Platform. Unlike traditional tools that struggle to function in disconnected environments, Scribe provides automated attestation, policy enforcement and cryptographic integrity verification—tailored for secure, air-gapped deployments.

By bridging the visibility and enforcement gap, Scribe enabled the bank to strengthen software integrity, streamline compliance, and accelerate secure development—all without compromising the air-gapped security model. It's a blueprint for how modern financial institutions can secure their software factories—regardless of infrastructure constraints.

© Copyright 2025 Scribe Security.