How Scribe Security Aligns with Gartner’s 2025 Software Supply Chain Security Market Guide

INVINCIBLE PRODUCT SECURITY

Additional information is available at https://scribesecurity.com/

How Scribe Security Aligns with Gartner’s 2025 Software Supply Chain Security Guidance

Executive Summary

The April 2025 Gartner Market Guide for Software Supply Chain Security (SSCS) outlines a strategic shift: organizations must move beyond fragmented, reactive security measures and adopt comprehensive platforms that deliver **visibility**, **integrity**, and **governance** across the software development lifecycle (SDLC). Gartner highlights three critical capabilities that define a state-of-the-art SSCS solution:

1. **Complete visibility** into all software components and development activity

2. **Proven software integrity** through artifact signing and provenance tracking

3. **Improved security posture** via automated policy enforcement and compliance

Scribe Security’s platform is purpose-built to meet and exceed these expectations. It delivers **continuous assurance** by embedding security into every step of the SDLC—automating SBOM generation, enforcing policy-as-code guardrails, signing and attesting to software artifacts, and producing verifiable, audit-ready evidence of compliance.

This article outlines how Scribe maps directly to Gartner’s vision. For **technology companies**, it provides real-time supply chain risk management without slowing delivery. In **financial services**, Scribe enables scalable compliance with frameworks like **SSDF**, **SLSA**, **DORA**, and **FedRAMP**. In **healthcare and medical devices**, it helps satisfy **FDA premarket and postmarket** cybersecurity requirements. And for **regulated software suppliers**, Scribe automates the generation and sharing of attestations and **SBOMs** to meet emerging **EU CRA** and **U.S. government mandates EO 14028 and EO 14144**.

In a security environment where speed, trust, and proof are essential, Scribe Security offers a unified solution that empowers CISOs, product security leaders, and DevSecOps teams to build secure software at scale—while aligning with Gartner's definition of a modern SSCS platform.

Gartner's 2025 Market Guide: Key Supply Chain Security Requirements

In April 7, 2025, Gartner released a Market Guide for Software Supply Chain Security (SSCS) that highlights how modern software delivery is under attack and what capabilities organizations need to protect it. Gartner notes that attackers are increasingly targeting the software supply chain – including open-source and commercial code dependencies, third-party APIs, and DevOps toolchains – to introduce vulnerabilities or malicious code. This complex web of components and processes creates **visibility gaps**. Many organizations struggle to see all the software artifacts, developer identities, and pipeline dependencies in their environment, which makes it hard to spot risks. The guide emphasizes that this lack of end-to-end visibility allows hidden vulnerabilities to slip through.

Another major risk Gartner calls out is **integrity**: without proper validation of artifact integrity, attackers can inject compromised components into build or delivery pipelines. **Improper artifact integrity validation** in the CI/CD process can enable attackers to "poison" the pipeline and tamper with software releases. In other words, if builds and dependencies aren't verified and secured, the final software product could be subverted without detection.

Gartner also observes that many organizations have a **weak security posture in their software factories** due to insufficient automation. The absence of automated enforcement of security policies and the failure to detect misconfigurations in development infrastructure leave the door open for supply chain attacks. Security efforts are often fragmented – teams might focus on application code vulnerabilities but overlook the security of build systems, deployment scripts, or open-source imports (we wrote about this in a past article: How Scribe Security Aligns with Gartner's Leader's Guide to Software Supply Chain Security). This piecemeal approach results in gaps that attackers can exploit.

To address these challenges, Gartner advises software engineering leaders to evaluate SSCS tools by how well they support three critical use cases: improving visibility, protecting integrity, and enhancing security posture across the SDLC. In practice, this means organizations should seek solutions that:

- **Provide comprehensive visibility** into software components (e.g. via SBOMs and dependency analysis) and an audit trail of all actions in the development pipeline. This helps close the visibility gap by mapping out third-party code risks and changes in the SDLC.

- **Protect the integrity of software artifacts and processes** by using strong cryptographic measures (signing, verification, provenance tracking) to ensure every build component is authentic and unchanged. This guards against tampering and ensures only approved, compliant artifacts make it through the pipeline.

- **Improve the security posture of the software delivery process** through automated policy enforcement and misconfiguration detection. Essentially, “guardrails” in CI/CD should be applied to continuously check for policy violations or insecure settings so that insecure practices are caught early and consistently.

Addressing SSCS Compliance Requirements

Gartner further notes that such tools should help organizations meet emerging **regulatory and compliance demands**. Governments and industry regulators are increasingly requiring software producers to document how software was built and what’s inside it. Lacking insight into “who built the software, how it was built, and what its ingredients are” is now recognized as a systemic risk to critical infrastructure and society. Therefore, modern SSCS platforms must support capabilities like automated compliance checks and the generation of attestations to prove adherence to security standards.

In summary, the 2025 Gartner guidance urges organizations to **unify their software supply chain security strategy**. Instead of ad-hoc measures, companies need a platform that **gives full visibility into software components and pipeline activities, enforces integrity at every step, and automates security governance**. Next, we examine how Scribe Security’s platform aligns with these state-of-the-art recommendations.

How Scribe Security's Platform Capabilities Aligned to Gartner's Guidance

Scribe Security offers a software supply chain security platform designed around the same principles highlighted by Gartner. In fact, **Gartner names Scribe as a representative vendor providing SSCS capabilities** as part of an Application Security Posture Management approach. Scribe's solution can be described as a **continuous assurance platform** that provides visibility, control, and trust throughout the software development lifecycle (SDLC). It does so by automating SBOM management, embedding security guardrails in pipelines, leveraging attestations for compliance, and protecting the integrity of every build artifact.

Scribe Security's "ScribeHub" approach integrates policy enforcement, risk management (SBOM, vulnerabilities, anti-tampering), and attestation of evidence across the development pipeline. It embeds into source control, CI/CD, and release processes, then provides a sharing mechanism for verified compliance evidence. (What is Scribe? I The Scribe Documentation Site)

By design, Scribe addresses the **core SSCS requirements** defined by Gartner – it gives organizations end-to-end **visibility** into their software supply chain, ensures the **integrity** of code and builds, and automates governance to strengthen the security **posture** of the SDLC. In the sections below, we break down how Scribe delivers on each of these key capabilities and map them to Gartner's guidance. We also highlight real-world use cases in technology, finance, healthcare, and other regulated sectors, demonstrating how Scribe's continuous assurance model balances rapid development with robust security and compliance.

Automated SBOM Management for Full Visibility

One of Gartner's top recommendations is to **"reduce visibility gaps in the software supply chain"** by tracking third-party code and pipeline activities (e.g. via SCA and SBOMs). Scribe directly fulfills this need through automated Software Bill of Materials (SBOM) management and comprehensive supply chain discovery. The platform automatically discovers assets across the SDLC – scanning source code repositories, build systems, container registries, and more – to **inventory all software components and dependencies** in your environment. As code is built and released, Scribe can auto-generate SBOMs (and even AI-BOMs) for each artifact straight from the CI pipeline. This means every open-source library, third-party package, and internal module that goes into a software product is accounted for in a machine-readable SBOM.

By centralizing these SBOMs, Scribe gives security teams a **live, unified view of the "ingredients" of their software**. This greatly improves visibility into upstream open-source risk. For example, if a new critical vulnerability in an open-source library is announced, Scribe's SBOM database can immediately reveal which applications or services include that library. Scribe augments SBOM data with real-time risk insights – integrating vulnerability intelligence (CVSS scores, threat context like EPSS and KEV lists, OpenSSF Scorecard, license risks, etc.) and even generating VEX (Vulnerability Exploitability eXchange) advisories to indicate which components are exploitable. Security teams get a "single source of truth" for component risk. **Full SDLC visibility** is a core benefit: organizations gain comprehensive insight into their software inventory and its risk posture, eliminating blind spots. Scribe's platform **centralizes SBOMs and security attestations**, ensuring that any vulnerable or non-compliant component can be quickly identified and addressed before release (You can read a real-world case study about this: Automating Software Supply Chain Visibility & Risk Management in a F-500 Financial Services Firm).

Beyond component inventory, Scribe also provides an **audit trail of all SDLC activities**. As the product builds progress through the pipeline, Scribe gathers evidence and logs (build metadata, code commit history, test results, etc.) as part of its continuous assurance. This creates a forensic record and context around each software artifact. Gartner highlighted the importance of such auditability for compliance and governance. With Scribe, every change, from code commit to package deployment, can be traced and tied back to who made it and whether it met SDLC security requirements. The Scribe platform **continuously gathers and examines evidence from the software development and build processes to confirm that the software was built securely,** validating things like code integrity, that code reviews were performed, security tests passed, only approved dependencies were used, and commits came from authorized developers (What is Scribe? | The Scribe Documentation Site). All this evidence is attached to the SBOM and build record, giving unparalleled visibility into not just *what* is in your software, but *how* it was built.

For organizations in **high-tech and SaaS** industries, this level of visibility is crucial. These companies often rely heavily on open-source and rapid iterative development; Scribe's automated SBOM tracking ensures that even in fast-paced environments, every component is tracked and vetted. It helps answer the questions their customers or auditors might ask: "Which open-source libraries are you using, and are they safe?" In regulated contexts like healthcare, visibility is not just a nice-to-have but a requirement. **Medical device developers,** for instance, must provide SBOMs for every software component in a device per FDA guidelines. Scribe's platform was built to help meet such needs: it **"generates SBOM and manages the associated risk throughout the SDLC,"** giving medical device manufacturers comprehensive visibility into third-party and proprietary code (How Scribe Security Helps Medical Device Manufacturers Meet FDA Cybersecurity Guidelines). This capability helps them comply with FDA premarket cybersecurity submissions, which demand SBOMs and documented risk management for each software component.

In summary, Scribe delivers the **visibility** outcome that Gartner calls for by **illuminating the entire software supply chain**. Through SBOM management and evidence collection, it creates a transparent view of all software assets and their security status. This empowers CISOs and Product Security leaders to answer the fundamental question, *"What's in our software, and is it safe?"* with confidence and data to back it up.

Ensuring Software Integrity and Trust through Signing and Attestations

The next major capability Gartner highlights is **protecting software integrity throughout the delivery process**. Scribe addresses this by introducing strong integrity controls like cryptographic signing, provenance tracking, and security attestations into each step of the SDLC.

The Scribe platform ensures that every build artifact – from compiled binaries to container images – is automatically signed and accompanied by tamper-proof provenance metadata. By signing artifacts and generating attestations, Scribe guarantees that any consumer of the software (whether an internal deployment or an external customer) can verify exactly where an artifact came from and that it hasn't been altered.

Gartner specifically recommends implementing signing and verification to ensure provenance and prevent the use of unverified or "noncompliant" artifacts. Scribe's solution was built with this in mind. It establishes a robust **chain-of-custody for software**, where each step (source, build, package) can be attested. In practice, as soon as the code is built, Scribe's agent signs the artifact and records metadata like the builder identity, source commit, timestamps, and checksums into an attestation. These attestations are cryptographically sealed, making them tamper-evident. Scribe's platform then **verifies these signatures and attestations at every stage of the SDLC** so that only artifacts with valid provenance and policy adherence can progress down the pipeline (a real-world case study demonstrating this: How a Financial Data Giant Transformed Software Supply Chain Security using Scribe). This mechanism directly **prevents software tampering by protecting the integrity of the software delivery** process. If an attacker tried to inject a malicious component or alter a build, the missing or mismatched signature would flag it, and Scribe could block the deployment.

In the case of the financial services firm mentioned earlier, this integrity feature was pivotal. All artifacts in their pipelines were "**cryptographically signed, ensuring software provenance and resilience against tampering**", which helped the firm achieve compliance with supply chain integrity standards like SLSA Level 2. By integrating with the organization's key management (e.g. vault) and using conditional signing policies, Scribe ensured that every build output was trustworthy. This gave the AppSec and DevSecOps teams confidence that no unauthorized code was slipping through. In fact, the firm's Head of Product Security noted that *"today, we have provable software integrity… and real-time insights – without slowing our developers down."* This is the essence of **trust** that Scribe provides: development doesn't grind to a halt, yet security is baked into every artifact.

Machine-Readable Attestations of Secure Software Development

Attestation-based compliance is another aspect of Scribe's integrity protection. Each attestation serves as verifiable proof that security requirements were met (or not) for a given build or release. Scribe's platform collects a wide range of evidence (test results, dependency scans, code review records, etc.) and attaches these attestations to the artifacts. This creates a permanent record that the artifact was built in accordance with the organization's security policies (and, by extension, industry standards). ScribeHub **"acts as a hub where software producers and consumers can exchange evidence, attesting to the safety of their software products" (**What is Scribe? | The Scribe Documentation Site**).** In other words, a software producer can provide customers or regulators with these signed attestations to prove the software's integrity and security posture. This is increasingly important as customers and regulators ask for SBOMs and proof of secure development practices before trusting software in their supply chain (e.g. (EO14144).

From a **DevSecOps leadership perspective**, these integrity features drastically improve assurance. Traditional approaches might rely on manual code reviews or scanner outputs to claim an artifact is safe.

Scribe instead delivers provable security: every artifact has a cryptographic pedigree and documented compliance with security controls. This is exactly what Gartner meant by addressing the integrity gap – ensuring software is delivered as intended, without hidden malware or untracked changes.

It also helps with **incident response**: if a vulnerability is found post-release, teams can quickly trace back through attestations to see how that code was built, who approved it, and whether any integrity checks failed.

For highly regulated industries and critical systems, this level of trust is often mandated. **Financial services** firms and **healthcare software** providers, for instance, have audit and compliance requirements to show that production code is authorized and unaltered. Scribe's tamper-proof attestations and artifact signing meet these needs by producing **"clear, auditable evidence of security controls and compliance"** for each software release. In regulated environments (like banking, where frameworks such as PCI-DSS or DORA demand strict change control, or medical devices where FDA expects evidence of secure development), Scribe provides the technical means to both enforce integrity and demonstrate it to third parties.

Ultimately, Scribe's focus on signing and attestations, along with its extensive gating capabilities, turns the software factory into a **zero-trust environment**: nothing goes out unless it can prove it's been built securely and hasn't been tampered with. This establishes a foundation of **trust** in the software supply chain, aligning perfectly with Gartner's call to protect software integrity end-to-end.

Strengthening SDLC Security Posture with Automated Guardrails

The third critical capability area, according to Gartner's guidance, is improving the overall **security posture of the software delivery process** through automation. This is about embedding security into the CI/CD pipeline itself – ensuring secure configurations and practices are consistently enforced, thus reducing the chance for human error or oversight. Scribe addresses this via a concept often referred to as **"guardrails-as-code"** or policy-as-code. Essentially, Scribe allows security and compliance teams to define rules and **automated security policies that integrate with CI/CD pipelines**, so that deviations are caught in real time and remediated. It's the manifestation of the holy grail in software security - Secure by Design!

Gartner pointed out that the **lack of automated tools to enforce security policies and detect misconfigurations** weakens an organization's software delivery security. Scribe fills that gap with its policy engine and huge pre-built SDLC controls library (160 policies-as-code). With Scribe, teams can codify their security requirements – for example, "all dependencies must be from approved sources," "no critical vulnerabilities allowed in builds," "container images must not run as root," or "CI pipelines must have MFA enabled for critical steps." These policies are then enforced by Scribe's platform across the SDLC. If a developer or pipeline action violates a policy, Scribe can block the build or deployment and alert the team, much like an automated checkpoint. This ensures **continuous compliance** with internal standards and external regulations.

"Automated governance & policy enforcement – Scribe enforces automated guardrails across your development and deployment pipelines. At build time, deployment, or out-of-band, a policy-as-code framework ensures SDLC governance that adapts to your security and compliance requirements." (Scribe Product Datasheet).

In short, it's like having a security coach and gatekeeper embedded in the process rather than relying on after-the-fact reviews.

By integrating these guardrails, Scribe significantly strengthens the security posture of the software factory. Misconfigurations in DevOps tooling – a common source of breaches – can be detected and fixed early. For instance, Scribe can flag if a Jenkins instance or GitHub action is using insecure settings and prompt remediation, closing those attack avenues. The platform's **unified policy framework** means that whether the code is in development, in CI build, or in deployment, the same security standards apply and are checked automatically. This unification was reflected in the case of the financial data company: they implemented **"conditional signing policies and automated verification gates, enabling continuous compliance checks"**, and used Scribe's risk scoring to prioritize and quickly remediate any policy violations. Over 10 distinct security guardrails were enforced automatically in their pipelines, eliminating manual review steps and ensuring 100% of artifacts met the company's security criteria. The result was a much stronger security posture (no more unknown rogue processes or unreviewed code getting through) and improved operational efficiency – the firm cut down manual compliance work by 50%, freeing up the AppSec team for higher-value risk mitigation.

From an AppSec manager's perspective, this kind of frictionless SDLC governance is a game-changer. Scribe provides "full visibility into the assets in the SDLC and their risk posture" coupled with "automating policy enforcement" to achieve "frictionless SDLC governance".

Security checks no longer rely on developers remembering every guideline; instead, the system actively verifies and enforces them. Importantly, these guardrails are implemented in a developer-friendly way – integrated into CI/CD tools – which helps avoid the dreaded slowdown or friction that security often introduces. Developers get immediate feedback if something is amiss, and many issues can be auto-remediated or simply blocked with clear instructions, rather than resulting in a late-stage surprise. This alignment with DevOps is crucial for DevSecOps leaders who need to balance **speed and security**.

Scribe's approach effectively operationalizes Gartner's recommendation to *"automate policy enforcement in the SDLC and detect misconfigurations in DevOps tooling"*. By codifying security policies and embedding them, Scribe boosts the SDLC's immune system. For example, consider a **tech company** delivering cloud software: They can define guardrails such as requiring all code changes to go through peer review and security scanning. Scribe will automatically check for evidence of code review and scan results (as part of its attestation collection) – if a step is missed, it can halt the process at the Admission Controller or, even sooner, by breaking the build. Likewise, in a **banking environment**, policies might enforce that certain high-risk applications include additional threat modeling or that cryptographic libraries meet compliance standards; Scribe can ensure these rules are continuously met, satisfying internal audit and external regulators. As Gartner noted, by 2028 the majority of large enterprises will have deployed such SSCS tools – and Scribe is providing that capability today by **making the entire software delivery infrastructure auditable and controlled via code**.

In essence, Scribe's guardrails-as-code give security teams control over the software factory without creating a bottleneck. This improves the overall posture by systematically reducing configuration errors and insecure practices. The outcome is a DevSecOps process where security is proactive and preventative rather than reactive. Organizations can demonstrate that their SDLC is governed by consistent security policies – a powerful assurance for stakeholders and often a requirement for industry compliance.

Continuous Assurance at Scale: Balancing Speed with Security and Compliance

A key promise of Scribe's platform is enabling **continuous assurance** – the idea that security and compliance are continuously verified throughout the software lifecycle, not just at one or two gates. This model is particularly valuable for organizations that need to move fast **and** meet stringent security or regulatory requirements. By aligning with Gartner's outlined capabilities (**visibility, integrity, posture**) in an automated fashion, Scribe helps different industries achieve this balance at scale.

Consider the **financial services sector**: As illustrated in a Scribe case study, a leading financial data firm integrated Scribe across 200+ development environments and saw transformative results. They moved from a fragmented, reactive approach to a **proactive, automated security posture**. The outcome was **"full SDLC visibility"** (comprehensive insight into all dev environments and components), combined with **automated security and compliance** (over 10 security policies enforced with zero manual intervention). This gave the company real-time awareness of software risks and the ability to prevent non-compliant software from ever reaching production. Importantly, they achieved this **without impacting developer productivity** – *"streamlined compliance — without disrupting development velocity"*. The continuous attestation and guardrail model actually removed manual bottlenecks (reducing compliance-related work by 50% for the security team) and improved collaboration between AppSec and developers (issues were caught and fixed earlier, accelerating remediation). For a CISO in finance, this means they can confidently report that their software factory is under control and meets frameworks like CIS, NIST SSDF, SLSA or even new laws like the Digital

Operational Resilience Act (DORA), all while supporting the business's rapid innovation.

In the **healthcare and medical devices** realm, continuous assurance is equally crucial. Medical device manufacturers face strict FDA cybersecurity guidelines that demand evidence of risk management and security across the device lifecycle. Scribe's platform was practically tailor-made for this scenario:

ScribeHub "embeds security directly into the SDLC, automates continuous attestations, and generates verifiable evidence – providing medical device makers the tools they need to meet FDA requirements and safeguard their products" (How Scribe Security Helps Medical Device Manufacturers Meet FDA Cybersecurity Guidelines)*.*

For example, each software component of a medical device can be accompanied by an attestation that it was developed according to FDA-recommended secure development processes and has a corresponding SBOM. Post-market, if a vulnerability emerges, the manufacturer can quickly identify affected devices via SBOMs and use the attestations to show regulators or hospital clients that proper processes were followed in developing a patch. This continuous trail of evidence significantly eases compliance with healthcare regulations and standards (like **IEC 62304** or the **FDA's premarket guidance**), which historically involved tedious documentation. Scribe automates much of that, letting medical software teams focus on innovation and patient safety rather than paperwork. Manufacturers using Scribe can maintain *"clear, auditable evidence of security controls and compliance"* for regulatory review, turning a compliance burden into a byproduct of their normal DevOps workflow and competitive advantage.

Tech companies and software vendors outside of heavily regulated industries also benefit from this model. Many enterprise customers and government agencies now require their software suppliers to provide SBOMs and **security attestations** (a trend driven by initiatives like the U.S. Executive Order on Cybersecurity 14144 and the EU Cyber Resilience Act). Scribe enables software providers to adopt a "secure-by-design" stance and then prove it. They can easily share SBOMs, vulnerability disclosures, and attestations with stakeholders, fostering trust in their products. For instance, a SaaS company can use Scribe to automatically produce a security attestation for each release, which can be provided to clients during due diligence. This not only meets customer requirements but can become a **competitive advantage – a demonstration of transparency and commitment to security**.

In the fast-paced tech world, having Scribe's guardrails means developers can use modern tools (including generative AI for code, as some do) with confidence that any risky dependency or insecure config will be caught. It's a safety net that lets innovation continue at high speed, aligning with the Gartner future vision where DevSecOps maturity is enhanced by such integrated SSCS tools.

Lastly, for **software suppliers in regulated industries** or selling to the government, Scribe's continuous assurance provides a scalable way to meet mandates without slowing down. For example, U.S. federal software acquisition rules now require vendors to self-attest to following the NIST Secure Software Development Framework (SSDF). Scribe comes with pre-built policy blueprints mapped to standards like NIST SSDF and SLSA. This means organizations can quickly implement those controls in their pipeline and automatically collect evidence for each practice.

Scribe "streamlines adherence with industry frameworks like SLSA, SSDF… using prebuilt blueprints and automated evidence collection" (Scribe Product Datasheet).

The platform essentially operationalizes these compliance frameworks. So when it's time to sign an attestation for the government or undergo an audit, all the evidence is readily available and trustable. In the EU, the forthcoming Cyber Resilience Act will similarly require software producers to maintain secure development processes and documentation; Scribe's capabilities are directly aligned with these needs.

Across all these use cases, Scribe's value proposition is a **unified, continuous approach to software supply chain security**. It provides the visibility, control, and trust mechanisms that Gartner's 2025 Market Guide identifies as essential, and it does so in a way that scales with development and doesn't hinder speed. The platform's **"attestation-based continuous assurance"** model allows organizations to **prove** their security and compliance at any point – a powerful benefit as security becomes not just an internal concern but a market differentiator and legal requirement.

Conclusion

Gartner's latest guidance for software supply chain security calls for an integrated strategy that embeds security throughout the software lifecycle, rather than piecemeal point solutions. Scribe Security's platform exemplifies this integrated, comprehensive approach. It delivers on **visibility** by inventorying software components and risks (automated SBOMs and evidence trails), on **integrity** by ensuring every artifact is signed and verifiable (attestations and provenance), and on security **posture** by enforcing policies and best practices via code (CI/CD guardrails and continuous compliance checks). These capabilities map one-to-one with the core requirements outlined in Gartner's 2025 Market Guide (Apr 7 2025).

For CISOs, Heads of Product Security, and DevSecOps leaders, adopting a platform like Scribe means gaining **unprecedented control and insight** into the software factory without sacrificing agility. It provides confidence that software releases haven't been compromised and that development processes meet the highest standards of security – all backed by data and cryptographic proof. This continuous assurance enables organizations to shift from a reactive stance (trying to fix issues late or respond to supply chain incidents) to a proactive and **"secure-by-design"** culture. As evidenced in industry use cases, companies can achieve strong supply chain security **"with real-time insights – without slowing developers down"**.

In an era of escalating supply chain attacks and increasing regulatory scrutiny, Scribe Security's platform offers a scalable solution that aligns perfectly with Gartner's state-of-the-art guidance. It empowers organizations to maintain **visibility, control, and trust** across the entire SDLC, thereby balancing rapid software innovation with robust risk mitigation and compliance. In short, Scribe delivers the tools and automation needed to protect the modern software supply chain at scale – turning what Gartner calls a strategic imperative into an operational reality for enterprises.