Magic Quadrant for Software Supply Chain Security

17 June 2026 - ID G00843814 - 45 min read

By Aaron Lord, Johnny Walters, and 1 more

The SSCS market is emerging as a stand-alone capability set that protects organizations from third-party software risks, including open-source and third-party AI. Software engineering and security leaders should use this Magic Quadrant to help select vendors that can protect their software factories from upstream providers.

Market Definition/Description

Gartner defines software supply chain security (SSCS) tools as solutions that reduce business technology risk by protecting against compromise from third-party software. Using threat intelligence, software composition analysis, software bills of materials and third-party governance, SSCS tools identify risk and ensure software integrity from acquisition through delivery, supporting SaaS and hybrid models and improving DevSecOps maturity.

Software supply chains extend beyond organizational boundaries and encompass external entities, in addition to internal systems. Internal systems include software delivery pipelines, software dependencies and software development environments. External entities include partners, open-source software (OSS), containers, AI models and vendors. Organizations have greater control over internal systems and little to no control over external entities. SSCS tools protect organizations from insider threats and compromised external entities.

Software powers most critical infrastructure today. Therefore, a lack of understanding of who built the software, how it was built and what its ingredients are poses a danger not

only to businesses but also to society at large. Software engineering teams can use SSCS tools to automate the enforcement of security and compliance policies and meet regulatory and government mandates.

SSCS tools help an organization achieve these tangible outcomes:

- Identify and mitigate security and compliance risks arising from the widespread use of third-party software, including open-source and commercial software, third-party AI large language models (LLMs), Model Context Protocol (MCP) servers and containerized workloads.
- Reduce developer friction and lost productivity due to attacks on tools, environments, pipelines and infrastructure used for software development and delivery.
- Guard the organization from attacks on upstream software dependencies and downstream software users from compromised products.
- Protect the organization's intellectual property, which increasingly and mostly resides in software.
- Satisfy governance and regulatory requirements by making the software delivery infrastructure auditable and automating the enforcement of application security policies.

Mandatory Features

The mandatory features for this market include:

Third-Party Software Risk Protection

- Perform software composition analysis (SCA) of third-party software for exploitable vulnerabilities. That can include one or more of the following inputs:
  - Artifact registries
  - Static analysis of source code (ex. Maven or pip manifest files)
  - Static analysis of container definitions (ex. Dockerfiles)
  - Image registries
  - Binary, executable or compiled software analysis

    - Runtime analysis during software execution
- Evaluation of third-party software licenses to ensure compliance with organizational software and legal policies.
- Governance of third-party software consumption to apply consistent software supply chain security policy.

Software Bill of Materials (SBOM)

- Collection, storage and continuous analysis of SBOMs to identify third-party risk within the components used to create software.
- Generation of SBOMs for downstream users of produced software.

Threat Intelligence

- Utilization of up-to-date threat research and threat intelligence feeds to continuously identify known risks in third-party software.
- Compiles and organizes vendor, third-party provider and open-source reputation to protect the business from risks stemming from unmaintained or deprecated software (also known as abandonware).

Optional Features

The optional features for this market include:

- Integration into artifact management systems, source control managers (SCM) and build tools.
- Support the generation of machine-readable documents (e.g., VEX, CSAF) for effective vulnerability disclosure and prioritization of common vulnerabilities and exposures (CVEs) affecting the delivered software.
- Support reachability analysis to analyze and prioritize risk by identifying whether applications depend on vulnerable code fragments and/or affected dependencies.
- Protection from third-party AI components including large language models (LLMs) and Model Context Protocol (MCP) servers.
- Support SBOM life cycle management functions to enable discovery, access and secure exchange of SBOMs between multiple suppliers and consumers through a

common exchange point.

- Trigger a workflow to replace an artifact that is either tampered with or affected by a vulnerability during or after its build and deployment. This workflow could involve automatically creating user stories to track the upgrade, accompanied by a corresponding upgrade impact analysis.
- Provide developer workspace security by analyzing plugins and extensions for developer tools like integrated developer environments (IDEs).
- AI-augmented workflows for improving both developer and security experience by analyzing security posture data, and recommending alternatives to third-party software.
- Detect and prevent unauthorized access by human and machine identities to software development life cycle (SDLC) tools and environments.
- Provide an accurate and complete inventory of development tools, developer identities and software artifacts to gain full visibility into the path, from development to delivery.
- Governance of software delivery pipeline security posture by detecting and fixing misconfigurations in DevOps tools (e.g., source-code repositories, artifact registries).

Magic Quadrant

Figure 1: Magic Quadrant for Software Supply Chain Security

Gartner

Vendor Strengths and Cautions

ActiveState

ActiveState is a Niche Player in this Magic Quadrant. It offers ActiveState Curated Catalog, which provides built-from-source open-source components, SBOM life cycle management, continuous threat intelligence, and third-party software governance. ActiveState Curated Catalog can be deployed as SaaS or customer-managed (on-premises or private cloud).

ActiveState's operations primarily support customers in the U.S. and Canada. Its clients tend to be medium-to-large enterprises in regulated industries such as financial services, healthcare, government, and infrastructure. Since 2025, ActiveState has expanded its

secure container offering, significantly increased its rebuilt component library, and introduced AI-assisted build and dependency resolution capabilities with human-in-the-loop controls.

Strengths

- **Innovation:** ActiveState focuses on delivering preremediated, built-from-source OSS rather than prioritizing detection. Customers benefit from reduced vulnerability exposure without requiring developers to triage or upgrade dependencies.
- **Offering (product) strategy:** ActiveState operates its own build infrastructure, which aligns with SLSA Level 3, and it rebuilds components internally rather than relying on upstream binaries. This gives customers higher assurance of provenance and reduces exposure to compromised build pipelines.
- **Market understanding:** ActiveState demonstrates a strong understanding of the buying criteria used by enterprises in regulated industries, structuring its offering around predefined remediation SLAs, audit-ready artifacts (signed SBOMs and VEX), and policy-driven curated catalogs. Customers benefit from clear timelines for vulnerability resolution (five to 10 business days for critical and high issues).

Cautions

- **Product or service:** ActiveState is missing several common features compared with other vendors in this Magic Quadrant, including secrets detection, software pipeline security posture, and developer workspace security.
- **Customer experience:** ActiveState does not offer an IDE plugin or developer workspace integrations. Organizations seeking rich, interactive developer guidance or conversational remediation inside IDEs will need complementary tools.
- **Geographic strategy:** ActiveState is primarily serving customers in the U.S., Canada, and Western Europe.

Apiiro

Apiiro is a Leader in this Magic Quadrant. It offers the Apiiro Platform, which provides software composition analysis with deep code analysis, an extended bill of materials (xBOM), third-party software governance, continuous threat exposure management,

software pipeline security posture, and AI supply chain security. Apiiro Platform can be deployed as SaaS or as an on-premises subscription.

Apiiro's operations are in the U.S.and Europe, and its clients tend to be large enterprises in regulated industries with complex SDLC environments and thousands of developers. Since 2025, Apiiro has introduced the Guardian Agent for agentic development security, expanded AI development governance, and shifted its pricing and roadmap focus toward outcome-driven, prevention-first workflows.

Strengths

- **Offering (product) strategy:** Apiiro integrates SCA into a broader, graph-based application security model. This benefits customers by prioritizing vulnerabilities based on exploitability, reachability, runtime exposure, and business impact.
- **Innovation:** Apiiro's Guardian Agent enables autonomous vulnerability and compliance prevention and remediation across IDEs, CI/CD pipelines, and AI coding agents. This helps engineering and security teams manage the heightened security risks from increased AI-driven development velocity.
- **Market responsiveness:** Apiiro's expanded AI development governance and Guardian Agent demonstrate that it is rapidly adapting to emerging risks, including AI supply chain threats. Customers benefit from using Apiiro's capabilities for securing AI in the traditional SDLC and in the SDLC for AI applications.

Cautions

- **Operations:** Apiiro's platform is more complex than other vendors in this Magic Quadrant. Customers should expect a steep learning curve when operationalizing the platform, particularly when multiple teams are responsible for different parts of the SDLC.
- **Sales execution/pricing:** Apiiro's average deal size is much higher than other vendors in this Magic Quadrant. Customers considering Apiiro's services will need to carefully consider if it will fit within their budgets.
- **Marketing strategy:** Organizations with simpler SDLCs or limited AI adoption may not fully utilize the platform's capabilities, making it difficult to justify the cost and operational effort.

Arnica

Arnica is a Niche Player in this Magic Quadrant. It offers the Arnica Platform, which provides pipelineless SCA, continuous SBOM generation, license and reputation analysis, secrets scanning, and real-time developer notifications through collaboration tools. Arnica Platform can be deployed as SaaS or as an on-premises subscription.

Arnica's operations are primarily focused in North America and Europe, and its clients tend to be medium-to-large enterprises with fast release cycles and high AI-assisted development adoption. Since 2025, Arnica has expanded its platform's AI code governance, introduced agentic rules enforcement, and extended its identity graph to attribute AI-generated code to human owners.

Strengths

- **Customer experience:** Arnica's pipelineless approach scans every code push and routes findings privately via Slack or Teams. This approach improves developer engagement and accelerates remediation without adding workflow friction.
- **Innovation:** Arnica detects AI coding tools and MCP server configurations directly from source repositories and can enforce guardrails at generation time. Customers can govern AI-assisted development without requiring new developer workflows.
- **Product or service:** Arnica dynamically recalculates threat severity using the Common Vulnerability Scoring System (CVSS), Exploit Prediction Scoring System (EPSS), known exploited vulnerabilities (KEV) status, function-level reachability, dependency depth, and SDLC context. As a result, customers receive fewer low-priority alerts and clearer remediation paths.

Cautions

- **Offering (product) strategy:** Arnica intentionally limits the scope of its SBOMs to packages, versions, and licenses, excluding broader infrastructure or extended BOM constructs. Customers who require holistic supply chain inventory will need additional tooling.
- **Market understanding:** Arnica does not support ingestion of customer-provided threat intelligence feeds. Organizations with custom or proprietary intelligence programs will find this restrictive.

- **Operations:** Arnica operates with a relatively small sales and services footprint. This smaller scale may not appeal to risk-averse enterprise buyers seeking a more established and financially entrenched partner.

Black Duck

Black Duck is a Leader in this Magic Quadrant. It offers Black Duck SCA, which includes deep open-source discovery across sources, binaries, and containers; vulnerability and exploit intelligence curated through Black Duck Security Advisories; advanced license compliance; and SBOM generation and ingestion. Black Duck SCA can be deployed as single-tenant SaaS or customer-managed deployments, supporting regulated and air-gapped environments.

Black Duck's operations are primarily focused in North America, Europe, Asia/Pacific and the Middle East, and its clients tend to be large enterprises and software producers in regulated industries, including automotive, industrial, financial services, and technology. Since 2025, Black Duck has expanded its AI Model Risk Insights offering, VEX and SBOM life cycle management, and AI-assisted remediation, while continuing to invest in regulatory alignment related to the EU Cyber Resilience Act (EU CRA) and AI governance requirements.

Strengths

- **Market understanding**: Black Duck demonstrates strong understanding of regulated software supply chains, emphasizing defensible SBOMs, license obligations, and vulnerability disclosure workflows. This focus helps customers satisfy auditors, regulators, and downstream buyers with evidence-grade artifacts rather than best-effort scans.

- **Innovation**: Black Duck Security Advisories (BDSAs) combine human curation with AI-assisted research across more than 50 vulnerability sources. This enables customers to prioritize true exploit risk and remediation paths with higher confidence than reliance on raw CVE feeds alone.

- **Product or service**: Black Duck supports use cases beyond cloud-native development, including embedded systems, firmware, and binary-only software scanning. This allows customers with heterogeneous delivery models to standardize on a single SCA platform rather than maintaining multiple tools.

Cautions

- **Customer experience**: Black Duck's broader workflows remain governance-centric and highly structured, which may not resonate with organizations seeking fully conversational, automation-first, or developer-owned remediation.
- **Operations**: Black Duck's emphasis on comprehensive analysis increases scan duration, data volume, and workflow complexity. Customers operating at high commit velocity or with decentralized teams need to carefully scope scans and adjust CI/CD usage to avoid pipeline friction.
- **Sales strategy:** Black Duck's platform focuses on large enterprise use cases and contexts, which can preclude smaller organizations. Customers should closely validate packaging, edition coverage, and onboarding effort to ensure the platform's capabilities align with their team size and operating model.

Chainguard

Chainguard is a Leader in this Magic Quadrant. It offers Chainguard Containers, Chainguard Libraries, and Chainguard VMs. These products provide secure-by-default container images, language libraries, and virtual machine images rebuilt from source with signed SBOMs, SLSA 3-aligned provenance, and continuous CVE remediation. These offerings can be deployed through customer-controlled environments using Chainguard's OCI-compliant registries and SaaS management console.

Chainguard's operations are primarily in North America and Europe, with growing reach through partners in Asia/Pacific, Latin America, and the Middle East. Its customers are mainly large enterprises and public-sector organizations in regulated sectors such as financial services, healthcare, technology, and defense. Since 2025, Chainguard has expanded its secure artifact catalog beyond containers into libraries and VMs, increased FIPS-validated coverage, and invested in Chainguard Factory automation and AI-assisted rebuild workflows.

Strengths

- **Market understanding:** Chainguard demonstrates strong alignment with compliance-driven and malware-resilient software supply chain requirements. Customers benefit from a secure-by-default model that addresses regulatory mandates such as FedRAMP, NIS2 Directive, and the EU CRA without relying on reactive scanning and patching.

- **Innovation:** By delivering minimal, curated images with near-zero known CVEs, Chainguard reduces vulnerability noise before artifacts enter customer pipelines. This allows security teams to reallocate effort from triage to higher-impact risk management activities.
- **Offering (product) strategy:** Chainguard integrates through standard OCI registries, SBOM formats, and signed provenance rather than proprietary plugins. This allows customers to consume Chainguard artifacts within existing CI/CD, SCA, and CNAPP tools without restructuring their toolchains.

Cautions

- **Customer experience:** Chainguard offers limited support for in-IDE inspection or in-line remediation workflows. Organizations seeking rich, interactive developer guidance or conversational remediation inside IDEs will likely need complementary tools.
- **Operations:** Chainguard's model provides little flexibility to consume arbitrary upstream packages. Customers with highly customized or niche dependencies may encounter gaps in catalog coverage that require additional engineering effort or alternative sourcing strategies.
- **Product or service:** Chainguard is tightly coupled to its build-from-source Chainguard Factory, curated artifact catalog, and continuous rebuild workflows, creating a risk of vendor lock-in. Organizations that later choose to replace Chainguard will need to re-establish their supply chain foundations, including artifact sourcing, provenance generation, and CVE remediation processes.

Checkmarx

Checkmarx is a Leader in this Magic Quadrant. It offers Checkmarx One, a unified platform that provides software composition analysis, container security, malicious package detection, SBOM generation and ingestion, secrets detection, and AI supply chain security. Checkmarx One can be deployed as a cloud-native SaaS platform, integrated across IDEs, SCMs, CI/CD pipelines, and artifact repositories.

Checkmarx's operations are primarily in North America and Europe, with an established customer base in Asia/Pacific and an expanding presence in selected EMEA markets. Its customers are mainly large enterprises and regulated organizations across the financial

services, healthcare, government, and technology sectors. Since 2025, Checkmarx has expanded AI supply chain security, enhanced reachability-based prioritization and risk orchestration, and increased investment in AI-assisted remediation and developer-side prevention.

Strengths

- **Innovation:** Checkmarx correlates vulnerability severity, exploitability, and reachability with application code context to focus attention on actual risks. Its in-house research team further enriches this prioritization with curated CVE analysis and malicious package intelligence, reducing noise from unverified or misleading advisory data.
- **Customer experience:** Checkmarx embeds supply chain security directly into developer workflows through deep IDE integration, real-time detection, and AI-assisted remediation. Developers can address vulnerable or malicious dependencies earlier in the SDLC without relying solely on centralized security review gates.
- **Offering (product) strategy:** Checkmarx's single-platform architecture supports centralized governance across multiple security engines, allowing organizations to normalize risk signals and enforce policy consistently without managing disparate tools. This approach is particularly beneficial for enterprises consolidating application security and supply chain oversight.

Cautions

- **Sales execution/pricing:** Checkmarx's subscription-based and forthcoming consumption-based pricing is higher than average compared to vendors in this Magic Quadrant. Customers should validate long-term cost predictability as AI-driven remediation and agent-based features increase utilization.
- **Sales strategy:** Checkmarx focuses on large enterprise use cases and context, which can preclude smaller organizations. Customers should closely validate packaging, edition coverage, and onboarding effort to ensure the platform's capabilities align with their team size and operating model.
- **Product or service:** Checkmarx's granular policy control requires careful initial and ongoing configuration to align with an organization's risk tolerance. Poorly tuned policies can either suppress relevant findings or generate excessive noise, requiring ongoing calibration by experienced security teams.

Cycode

Cycode is a Leader in this Magic Quadrant. It offers an Agentic Development Security Platform, which includes Cycode Complete ASPM, Cimon for runtime pipeline security, and Cycode Maestro. The platform covers third-party risk protection, third-party software governance and reputation analysis, SBOM life cycle management, AI supply chain security, and continuous threat intelligence. Cycode can be deployed as a multitenant or single-tenant SaaS, or as an on-premises or air-gapped subscription.

Cycode's operations are in North America, EMEA and Asia/Pacific. Its clients tend to be medium-to-large enterprises operating complex, distributed software development environments, including the technology and telecommunications, and banking, finance, and investment services sectors. Since 2025, Cycode has delivered Maestro (an agentic orchestration layer), native AI bill of materials (AIBOMs) generation, AI security governance capabilities to provide visibility into AI-generated code and tools, and AI teammates for autonomous risk detection and remediation.

Strengths

- **Product or service:** Cycode's platform actively discovers and enforces policies that govern the use of AI components (e.g., LLMs, AI libraries, and MCP servers) across the SDLC, including integration with AI coding assistants.
- **Offering (product) strategy:** Cycode's product strategy is focused on software supply chain threats specific to agentic coding tools and AI supply chain risk reduction capabilities.
- **Market responsiveness:** Cycode has adapted its offerings in response to recent supply chain attacks (such as Shai Hulud) and increased enterprise use of AI coding assistants. Cycode has released a runtime pipeline protection called Cimon, published relevant threat intelligence playbooks, and introduced AI asset inventory and governance controls.

Cautions

- **Customer experience:** Cycode customers with highly customized or legacy build environments have reported onboarding complexity and long operationalization times. Additionally, some users have experienced alert volume challenges when aggregating supply chain signals.

- **Operations:** Cycode has a relatively leaner team dedicated to its SSCS offerings compared to other vendors evaluated. Cycode is also lacking FedRAMP public-sector certification that is commonly required by highly regulated government entities in the United States.
- **Overall viability:** Cycode maintains a comparatively smaller customer base and overall market presence than other vendors evaluated. While a Leader in this Magic Quadrant, smaller-scale vendors may not appeal to risk-averse enterprise buyers seeking a more established and financially entrenched partner.

Endor Labs

Endor Labs is a Visionary in this Magic Quadrant. It offers Endor Labs Supply Chain, Endor Open Source, Endor CI/CD, and Endor SBOM Hub, which provide third-party risk protection, third-party software governance and reputation analysis, SBOM life cycle management, AI supply chain security, and continuous threat intelligence. Endor Labs' products can be deployed as SaaS or as an on-premises subscription.

Endor Labs' operations are in North America, the Netherlands, and India. Its clients tend to be technology-forward organizations that view secure software as core to their competitive differentiation, including in the technology and telecommunications; banking, finance, and investment services; and manufacturing sectors. Since 2025, Endor Labs has delivered software composition analysis (SCA) for C/C++, AI component governance, a package firewall, Endor Outpost, and compliance guidance for PCI DSS 4.0 and EU CRA.

Strengths

- **Product or service:** Endor Patches is a remediation-focused product designed to provide drop-in, security-only patches for hard-to-upgrade libraries and end-of-life software. This product helps customers to reduce the risk of introducing breaking changes into an application.
- **Market responsiveness:** Endor Labs introduced Endor Outpost in July 2025. It provides an on-premises subscription deployment for organizations with strict compliance and sovereignty requirements.
- **Innovation:** Endor Labs uses an Open Policy Agent (OPA) engine that enables customers to centrally govern and enforce risk standards as "security-as-code" using

Rego, a declarative query language, across their software supply chain.

Cautions

- **Business model:** Endor Labs is introducing daily scan limits for non-main branches and pull/merge requests. This significant shift in pricing can lead to confusion and higher prices for new and current customers.
- **Operations:** Endor Labs holds fewer compliance certifications than most vendors in this Magic Quadrant, supporting only SOC 2 Type II, and is lacking FedRAMP public-sector certification. This limits the company's ability to satisfy requirements for highly regulated industries.
- **Geographic strategy:** Endor Labs has limited mind share and market share in the Asia/Pacific region relative to other vendors in this evaluation.

FOSSA

FOSSA is a Niche Player in this Magic Quadrant. It offers the FOSSA platform, which includes FOSSA SCA, Binary Composition Analysis, SBOM Management, and fossabot. The platform covers software composition analysis, third-party software governance, open-source license compliance, SBOM life cycle management, continuous threat intelligence, and binary composition analysis. FOSSA can be deployed as a SaaS or as an on-premises subscription.

FOSSA's operations are primarily in North America, with an increasing focus on the EU. Its clients tend to be enterprise organizations in sectors including technology and telecommunications; services; manufacturing; banking, finance, and investment services; and automotive and medical devices. Since 2025, FOSSA has delivered a public preview of fossabot (an agentic software supply chain maintenance platform with auto-fix remediation), snippet detection capabilities for agentic workflows, C/C++ scanners for vendor dependencies, binary composition analysis for firmware, an FDA SBOM toggle, and a new automated malware detection solution.

Strengths

- **Overall viability:** FOSSA has a larger, more established enterprise customer base than many of the startups in this market. Its broad market footprint provides a more stable foundation for the vendor when compared to other smaller, emerging competitors in this Magic Quadrant.

- **Marketing strategy:** FOSSA's focus on generative engine optimization (GEO) and increased investment in Europe are designed to boost visibility. Its open-source license compliance capabilities are especially beneficial to customers in Europe due to evolving regulations such as the EU CRA.
- **Market responsiveness:** FOSSA effectively identifies emerging compliance and technology trends through strategic account syncs, advisory boards and regulatory research. In response, it has delivered capabilities such as code snippet detection and binary composition analysis.

Cautions

- **Product or service:** FOSSA lacks several common features, including AI supply chain risks, software pipeline security posture, and developer workspace security.
- **Offering (product) strategy:** FOSSA remains focused on delivering capabilities already offered by other vendors in this Magic Quadrant, and its product roadmap does not address emerging SSC risks related to AI coding assistants.
- **Innovation:** FOSSA's development remains narrowly focused on traditional SCA and licensing. It lags behind competitors who are innovating toward consolidated software supply chain security platforms.

GitHub

GitHub is a Niche Player in this Magic Quadrant. It offers GitHub Enterprise (Cloud or Server), with capabilities available via GitHub Code Security, GitHub Secret Protection, and GitHub Advanced Security (GHAS). These capabilities include Dependabot, dependency graph, dependency review, CodeQL code scanning, secret scanning and Copilot Autofix. The platform covers software composition analysis, third-party software governance, SBOM life cycle management, continuous threat intelligence, and provenance and artifact integrity. GitHub can be deployed as a SaaS or as an on-premises solution.

GitHub's operations are global, extending across North America, EMEA and Asia/Pacific. Its clients tend to be organizations with a significant software footprint, multiple development teams and frequent release cycles, often operating in regulated or high-risk industries. Since 2025, GitHub has delivered Virtual Registry via linked artifacts for code-to-cloud traceability and artifact risk visibility.

Strengths

- **Product or service:** GitHub supports software pipeline security posture by allowing administrators to configure branch protections and use GitHub Actions workflows to generate and validate cryptographic artifact attestations. Its curated Advisory Database aggregates vulnerability and malware data from ecosystem advisories, maintainer disclosures, and community submissions.
- **Overall viability:** GitHub is a wholly owned subsidiary of Microsoft. GitHub is backed by Microsoft's financial resources and can leverage Microsoft's enterprise security and cloud foundations to scale its supply chain security offerings.
- **Offering (product) strategy:** GitHub focuses on embedding security into developer workflows by developing agentic capabilities to autonomously triage, prioritize, and remediate risks within pull requests and backlogs. The vendor's roadmap also emphasizes AI supply chain posture management, enhanced malware protections, and enforceable artifact attestations to improve release integrity.

Cautions

- **Innovation:** GitHub has yet to release fully autonomous, end-to-end agentic security workflows for backlogs and pull requests, while its leading competitors in this Magic Quadrant already offer these capabilities.
- **Sales execution/pricing:** GitHub recently transitioned its security business to a meter-based billing model. This significant shift in pricing model complicates long-term cost forecasting for prospective buyers.
- **Market understanding:** GitHub's capabilities for third-party reputation analysis lag its competitors, as it does not analyze open-source project popularity, maintenance activity or maintainer credibility.

JFrog

JFrog is a Leader in this Magic Quadrant. It offers the JFrog Software Supply Chain Platform, which includes JFrog Artifactory, JFrog Xray, JFrog Curation, JFrog Runtime, JFrog AppTrust, JFrog Advanced Security and JFrog AI Catalog. The platform covers software composition analysis, software licensing analysis, third-party software governance, continuous threat intelligence, SBOM life cycle management, third-party

reputation analysis and binary artifact management. JFrog can be deployed as a SaaS, on-premises, or in a hybrid model.

JFrog's operations span North America, Latin America, Asia/Pacific and Europe. Its clients tend to be Global 2000 enterprises scaling agent-led development across hybrid and multicloud environments in regulated sectors, including finance, healthcare, government and automotive. Since 2025, JFrog has delivered its Compliant Version Selection (CVS) capability within JFrog Curation, JFrog AI Catalog, JFrog AppTrust, an MCP server, IDE plugins, and extended support for SBOM Evidence with VEX in CycloneDX and SPDX 3.0 formats.

Strengths

- **Innovation:** JFrog AppTrust attaches security attestations to software packages, ensuring that artifact integrity and provenance are continuously verified at each stage of the SDLC. This policy-as-code governance enables customers to automate evidence collection and strictly enforce compliance gates from build to deployment.
- **Offering (product) strategy:** JFrog is evolving its artifact repository into a dynamic, self-healing supply chain platform. By prioritizing agent-agnostic pipeline security and automated vendor substitution, JFrog helps steer development workflows toward safe artifacts without impeding release velocity.
- **Operations:** JFrog supports global enterprise deployments with operational teams that are trained across its entire platform portfolio. It supports high resilience in mission-critical environments by offering a contractual, in-region 99.99% uptime SLA.

Cautions

- **Sales execution/pricing:** JFrog's pricing for product subscriptions is higher than other vendors evaluated in this Magic Quadrant.
- **Sales strategy:** JFrog alters its list pricing and discounting practices annually and anticipates modifying pricing models to match the AI economy. This sharply contrasts with competitors in this Magic Quadrant who project flat pricing or aggressive discounts to capture market share.
- **Product or service:** JFrog's ability to govern and enforce policies on IDE plugins and extensions is limited to Visual Studio Code-based environments. The platform's

security and governance controls for emerging AI agent skills recently exited its proof-of-concept phase.

Lineaje

Lineaje is a Visionary in this Magic Quadrant. It offers Full-Lifecycle Software Supply Chain Security, which includes Gold Open Source, SCA360, SBOM360 and SBOM360 Hub, Third Party Risk Manager, and UnifAI. The platform covers third-party risk protection, third-party software governance and reputation analysis, SBOM life cycle management, AI supply chain security, and continuous threat intelligence. Full-Lifecycle Software Supply Chain Security can be deployed as SaaS or as an on-premises subscription.

Lineaje's operations are in North America and India. Its clients tend to be large organizations where software is critical for their business, in highly regulated sectors including banking, finance, and investment services; government; and technology and telecommunications. Since 2025, Lineaje has delivered Gold Open Source, agentic remediation for source code and containers in SBOM360, AI supply chain with UnifAI, and AI bill of materials (AIBOM) in SBOM360.

Strengths

- **Product or service:** Lineaje's UnifAI product is a unified, autonomous AI policy manager that is designed to develop, secure and govern agentic AI applications. It acts as a control layer directly inside AI development workflows, allowing users to centrally enforce corporate AI standards before applications are deployed.
- **Innovation:** In April 2025, Lineaje launched Gold Open Source, an enterprise-grade subscription service that provides developers with safe, curated, and high-integrity open-source packages and images. The product is designed to eliminate open-source risks without disrupting existing development workflows.
- **Market responsiveness:** Lineaje has responded to recent trends for AI supply chain security by introducing Lineaje AI Labs in 2025. AI Labs provides threat detection policies by asset type that are designed for autonomous insertion at build time and secure operation at runtime, delivered through UnifAI.

Cautions

- **Operations:** Lineaje operates with fewer full-time engineers dedicated to its SSCS product compared to most vendors in this Magic Quadrant. This raises vendor viability concerns amid a rapidly evolving threat landscape and a highly competitive market.
- **Marketing execution:** Lineaje's visibility in the market is below average for vendors in this Magic Quadrant, as evidenced by fewer than average Lineaje product reviews in Gartner Peer Insights. This limited customer awareness may limit growth for Lineaje.
- **Business model:** In 2026, Lineaje is reducing the number of discounts it offers and increasing its negotiated pricing for products. This significant shift in pricing can lead to confusion and higher costs for new and current customers.

Mend.io

Mend.io is a Visionary in this Magic Quadrant. It offers the Mend platform, which includes Mend SCA, Mend AI, and Mend Renovate. The platform covers third-party software risk protection, third-party software governance, SBOM life cycle management, AI supply chain security, and the ability to provide automated remediation of software dependencies. The Mend Platform can be deployed as a SaaS or as an on-premises subscription.

Mend.io's operations are mainly in North America, with some presence in Europe and Asia/Pacific. Its clients tend to be high-growth organizations in highly regulated sectors including banking, finance and investment services; technology and telecommunications; and government. Since 2025, Mend.io has delivered the Merge Confidence feature and new capabilities for securing AI-powered applications, agentic SCA, and expanding reachability analysis.

Strengths

- **Product or service:** Mend Renovate automatically identifies deprecated packages through registry metadata and seamlessly issues alerts or pull requests, enabling developers to transition to supported, secure alternatives. Its newly added Merge Confidence feature uses crowdsourced data from millions of updates to predict if version bumps will break a build. It can be integrated in numerous AI code editors.
- **Innovation:** Mend.io's AI Security Dashboard centralizes AI observability and surfaces unmanaged or unauthorized AI usage, such as "shadow Hugging Face." Its AI bill of

materials (AIBOM) provides visibility into the vulnerabilities, security postures, origins, licensing, and versions of all AI components present in an application.

- **Offering (product) strategy:** In 2025, Mend.io expanded its strategic partnerships and ecosystem integrations to include GitGuardian, HeroDevs, Invicti, JetBrains, Microsoft Defender and Wiz.

Cautions

- **Market understanding:** Unlike most vendors in this Magic Quadrant, Mend.io does not feature capabilities to provide cryptographic provenance for software deliverables. The platform also lacks software pipeline security and developer workspace security.
- **Customer experience:** In several Gartner Peer Insights reviews, Mend.io customers have reported a lack of visibility into current scan queues and volumes, occasionally slow response times and required follow-ups from Mend.io. They also reported that scanning results required a lot of manual effort, leading to alert fatigue.
- **Geographic strategy:** Mend.io has limited mind share and market share in the Middle East region relative to other vendors in this evaluation.

OX Security

OX Security is a Leader in this Magic Quadrant. It offers the OX Security platform, which includes OX VibeSec, OX Code and OX Cloud. The platform covers third-party software risk protection, third-party software governance and reputation analysis, SBOM life cycle management, software pipeline security posture, and continuous threat intelligence. OX Security can be deployed as a SaaS or as an on-premises subscription.

OX Security's operations are mainly in North America, with some presence in the EMEA. Its clients tend to be midmarket organizations where software is core to revenue and AI-driven development is accelerating, especially in sectors like technology and telecommunications; banking, finance, and investment services; and healthcare. Since 2025, OX Security has delivered expanded runtime correlation for issue prioritization, no-code enforcement workflows and enhanced SBOM capabilities.

Strengths

- **Innovation:** OX Security released its VibeSec product, an AI-native security engineering capability embedded directly into AI code generation workflows. It

validates code before it is committed, blocks risky packages in real time, and enforces organizational security policies on AI-generated code.

- **Offering (product) strategy:** OX Security stands out due to its software pipeline security posture, which combines continuous posture monitoring, identity risk management, and automated integrity enforcement with Pipeline Bill of Materials (PBOM). The PBOM is OX Security's proprietary extension of traditional SBOMs, designed to provide dynamic, end-to-end lineage across the SDLC.
- **Sales execution/pricing:** OX Security's pricing for a license subscription to its products is less expensive than most vendors in this Magic Quadrant.

Cautions

- **Product or service:** OX Security lacks binary software analysis, which is gaining traction for most other vendors in this Magic Quadrant.
- **Operations:** OX Security lacks FedRAMP public-sector certification that is commonly required by highly regulated government entities in the United States.
- **Customer experience:** In several Gartner Peer Insights reviews, OX Security's customers noted issues with reporting and alerts, including limited time frames for historical metrics and a lack of customization options.

RapidFort

RapidFort is a Niche Player in this Magic Quadrant. It offers the RapidFort Platform, which includes RapidFort Analyzer, RapidFort Curated Images, RapidFort Profiler, and RapidFort Optimizer. The platform covers third-party software risk protection (primarily by curating OS images and monitoring execution behavior), third-party software governance and reputation analysis, SBOM life cycle management, and continuous threat intelligence. RapidFort can be deployed as a SaaS or as an on-premises subscription.

RapidFort's operations are primarily in North America and EMEA. Its clients tend to be high-growth software organizations operating large fleets of containerized applications in sectors including banking, finance, and investment services; healthcare; and government. Since 2025, RapidFort has expanded artifact life cycle management and has delivered vulnerability applicability intelligence, artifact hardening generation, and a curated catalog of hardened images.

Strengths

- **Offering (product) strategy:** RapidFort continuously updates its catalog of hardened base OS and customer-requested application images. The catalog is powered by RapidFort's managed private OS package repositories, which are FIPS 140-2 and FIPS 140-3 certified and offer standard Linux distributions like Ubuntu, Red Hat, Alpine, and Debian.
- **Innovation:** RapidFort's Runtime Bill of Materials (RBOM) identifies exactly which software components are actively executing within a workload. It captures this execution behavior and component usage through runtime instrumentation, such as eBPF-based Kubernetes monitoring.
- **Customer experience:** In several Gartner Peer Insights reviews, RapidFort's customers report fast response times and knowledgeable support staff.

Cautions

- **Product or service:** RapidFort lacks several common features, including an IDE plugin, developer workspace security, and automated remediation. Additionally, RapidFort's platform is primarily designed for virtualized and containerized environments and has limited application in organizations with largely noncontainerized environments.
- **Sales execution/pricing:** RapidFort does not offer a seat-based licensing model for enterprise organizations. Enterprise customers should consider if RapidFort's licensing models will fit their requirements.
- **Geographic strategy:** RapidFort is currently serving customers in North America and EMEA only, although it plans to expand into Asia/Pacific by late 2026.

ReversingLabs

ReversingLabs is a Visionary in this Magic Quadrant. It offers Spectra Assure, which includes Spectra Intelligence, Spectra Assure Community, and Spectra Core. The platform covers third-party software risk protection (primarily using binary analysis), third-party software governance and reputation analysis, SBOM life cycle management, and continuous threat intelligence. Spectra Assure can be deployed as a SaaS subscription, an on-premises subscription, or a hybrid of both SaaS and on-premises.

ReversingLabs' operations are mainly in North America and EMEA. Its clients tend to be large organizations with complex software ecosystems in highly regulated sectors, including banking, finance, and investment services; technology and telecommunications; and oil and gas. Since 2025, ReversingLabs has delivered extended bill of materials (xBOM) capabilities for compiled commercial software, third-party software onboarding controls, expanded AI/ML security coverage, and expanded threat intelligence capabilities.

Strengths

- **Offering (product) strategy:** ReversingLabs' platform emphasizes binary analysis for third-party software risk protection more than any other vendor in this Magic Quadrant. Instead of having downstream consumers receive SBOMs from upstream providers, Spectra Assure enables downstream consumers to self-scan software from upstream providers and create SBOMs.
- **Innovation:** ReversingLabs recently delivered a preventative control plane that evaluates third-party software in a controlled "Security DMZ." This ensures that the software is safe and secure before entering the corporate network.
- **Customer experience:** ReversingLabs' Spectra Assure can be integrated into engineering workflows to build safe software, while also offering CISOs, procurement teams, and compliance officers features for managing third-party risk from commercial third-party software. Customers provided an average score of 4.9 for Spectra Assure in Gartner Peer Insights.

Cautions

- **Product or service:** ReversingLabs lacks some common features, including software pipeline security posture, runtime analysis and an IDE integration. ReversingLabs' automated remediation feature does not apply to source code because it focuses on binary analysis.
- **Geographic strategy:** ReversingLabs has limited mind share and market share in the Asia/Pacific region relative to other vendors in this evaluation.
- **Operations:** ReversingLabs lacks FedRAMP public-sector certification that is commonly required by highly regulated government entities in the United States.

Sonatype

Sonatype is a Leader in this Magic Quadrant. It offers Sonatype Nexus One, which includes Sonatype Nexus Repository, Sonatype Repository Firewall, Sonatype Lifecycle, Sonatype Guide, and Sonatype SBOM Manager. The platform covers third-party risk protection, third-party software governance and reputation analysis, SBOM life cycle management, and continuous threat intelligence. Sonatype can be deployed as SaaS, on-premises, and air-gapped subscriptions.

Sonatype's operations are mainly in North America, Europe and Asia/Pacific. Its clients tend to be medium-to-large organizations running software development at scale, particularly in regulated industries including banking, finance, and investment services, government, and healthcare. Since 2025, Sonatype has delivered Sonatype Guide for AI dependency management, integrated malware detection, Hugging Face and AI model governance, expanded SBOM capabilities, and air-gapped environment updates.

Strengths

- **Product or service:** Sonatype's Nexus One platform is a unified, overarching solution that provides full-spectrum control across the entire SDLC. Sonatype approaches automated remediation through its agentic dependency management, which merges deterministic, rule-based upgrades with GenAI capabilities.
- **Innovation:** In November 2025, Sonatype launched Sonatype Guide, an interactive tool that provides real-time feedback on security, licensing, and quality as code is written by developers and AI agents. This new feature shifts security to the earliest point in the development cycle.
- **Customer experience:** In several Gartner Peer Insights reviews, Sonatype customers have stated a positive experience with the company's customer support and with their assigned customer success engineer.

Cautions

- **Offering (product) strategy:** Sonatype is lacking some common product features, including software pipeline security posture, developer workspace security and secrets detection.
- **Business model:** Sonatype is transitioning from user-based pricing to a usage/consumption-based pricing model. This significant shift in pricing can lead to confusion for new and current customers.

- **Operations:** Sonatype lacks FedRAMP public-sector certification that is commonly required by highly regulated government entities in the United States.

Veracode

Veracode is a Niche Player in this Magic Quadrant. It offers Veracode Software Composition Analysis (SCA), Veracode Risk Manager, Veracode Package Firewall, and Veracode Threat Research. These products cover third-party software risk protection, third-party software governance and reputation analysis, SBOM life cycle management and continuous threat intelligence. Veracode can be deployed as SaaS, on-premises subscriptions, or a hybrid of both.

Veracode's operations are mainly in North America and Europe. Its clients tend to be large organizations that have daily or weekly software releases and dedicated security budgets, including in the healthcare, government, and banking, finance, and investment services sectors. Since 2025, Veracode has delivered Veracode Package Firewall, Software Supply Chain Intelligence (SSCI), and integrated supplemental data from the open-source vulnerabilities (OSV) threat feed into its threat research product.

Strengths

- **Offering (product) strategy:** Veracode acquired Phylum in response to customer feedback highlighting a need for stronger controls around open-source packages. This acquisition led to the launch of Veracode Package Firewall.
- **Innovation:** Veracode Fix was first to market for automated vulnerability remediation. It relies on specialized and controlled prompting, as Veracode trains the LLM with secure coding examples derived from its 20 years of remediation guidance.
- **Operations:** Veracode holds a large number of operational, organizational and compliance certifications, including EU-U.S. Data Privacy Framework, FedRAMP, FIPS 140-2, FISMA, GDPR, SOC 2 Type II, and ITIL.

Cautions

- **Market understanding:** Veracode's vision for how to address SSCS during the next five years lags behind most other vendors in this Magic Quadrant. Key gaps include runtime context analysis, secure-by-design, systems of record, and establishing a chain of trust.

- **Sales execution/pricing:** Veracode's pricing for a license subscription to its products is higher than the average of vendors in this Magic Quadrant.
- **Product or service:** Veracode's products lack critical features that other vendors in this Magic Quadrant offer, including cryptographic provenance for software deliverables, AI supply chain security, and a weak continuous threat intelligence capability. The ability for Veracode to integrate with artifact registries only recently shipped in mid-2026.

Inclusion and Exclusion Criteria

To qualify for inclusion, vendors must offer a software supply chain security technology that provides all of the mandatory features outlined in the Market Definition. The following features must be present:

Third-Party Software Risk Protection

- Perform software composition analysis (SCA) of third-party software for exploitable vulnerabilities. That can include one or more of the following inputs:
  - Artifact registries
  - Static analysis of source code (ex. Maven or pip manifest files)
  - Static analysis of container definitions (ex. Dockerfiles)
  - Image registries
  - Binary, executable, or compiled software analysis
  - Runtime analysis during software execution
- Evaluation of third-party software licenses to ensure compliance with organizational software and legal policies.
- Governance of third-party software consumption to apply consistent software supply chain security policy.

Software Bill of Materials (SBOM)

- Collection, storage and continuous analysis of SBOMs to identify third-party risk within the components used to create software.
- Generation of SBOMs for downstream users of produced software.

Threat Intelligence

- Utilization of up-to-date threat research and threat intelligence feeds to continuously identify known risks in third-party software.
- Compiles and organizes vendor, third-party provider, and open-source reputation to protect the business from risks stemming from unmaintained or deprecated software (also known as abandonware).

Evaluation Criteria

Ability to Execute

We evaluated the following criteria to assess the vendor's Ability to Execute. Below is a description of what we specifically looked for in each criterion.

Product or service: Software composition analysis, third-party software governance, software bill of materials life cycle management, continuous threat intelligence, third-party reputation analysis, and all other additional features.

Overall viability: Financial performance, ownership structure, customer segmentation by industry, and investment planning.

Sales execution/pricing: Customer acquisition, average deal size, pricing strategy, customer contract, and sales resource (FTE) allocation.

Market responsiveness/record: Release frequency, market dynamics and organizational response, and market intelligence and agility.

Marketing execution: Brand messaging, marketing campaign effectiveness, estimated marketing budget, and audience profiling.

Customer experience: Customer satisfaction assessment, customer satisfaction incentives, customer advisory board, and customer impact assessment.

Operations: Workforce distribution, and product certifications and compliance.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Low
Customer Experience	Medium
Operations	Medium

Source: Gartner (June 2026)

Completeness of Vision

We evaluated the following criteria to assess the vendor's Completeness of Vision. Below is a description of what we specifically looked for in each criterion.

Market understanding: Competitive analysis, understanding of market disruption, market foresight, differentiation strategy, and SSCS vision.

Marketing strategy: Marketing adaptability and persona targeting and messaging.

Sales strategy: Sales strategy agility, growth focus clarity, pricing strategy transparency, ideal customer definition and approach, and licensing/pricing model innovation.

Offering (product) strategy: Product enhancement roadmap, product strategy prioritization, customer feedback integration, and SSCS agility.

Business model: Business model clarity, business model evolution, stakeholder value proposition, and technology business model.

Vertical/industry strategy: Vertical focus adaptability, vertical growth strategy, industry standards responsiveness, and industry SSCS compliance standards.

Innovation: Recent innovation delivery, future innovation planning, intellectual property strength, and

R&D investment commitment.

Geographic strategy: Geographic focus adaptability, geographic growth strategy, and regional standards responsiveness.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (June 2026)

Quadrant Descriptions

Leaders

Leaders provide mature offerings that meet market demand and have demonstrated the vision necessary to sustain their market position as requirements evolve. The hallmark o Leaders is that they focus on and invest in their offerings to the point where they lead th market and can affect its overall direction. As a result, Leaders can become the vendors to watch as you try to understand how new market offerings might evolve.

Leaders for SSCS trend toward innovative methods for third-party software risk protection. They offer a full SBOM life cycle management product, full contextualizatior of findings within an organization's ecosystem, and developer-enabling controls that allow for SSCS to scale. Leaders in the SSCS market have also made large investments AI supply chain security.

Leaders typically respond to a wide market audience by supporting broad market requirements. However, they may fail to meet the specific needs of vertical markets or other more specialized segments.

Challengers

Challengers have a strong Ability to Execute but may not have a plan that will maintain a strong value proposition for new customers. Larger vendors in mature markets may be positioned as Challengers because they choose to minimize risk or avoid disrupting their customers or their own activities.

Although Challengers are typically large and have significant financial resources, they may lack strong vision, innovation or an overall understanding of market needs. For SSCS, Challengers have excelled in offering conventional tooling for third-party software risk protection but are not keeping pace with market trends for leading innovations.

Challengers can become Leaders if their vision develops. Over time, large companies may fluctuate between the Challengers and Leaders quadrants as their product cycles and market needs shift.

Visionaries

Visionaries align with Gartner's view of how a market will evolve, but their ability to deliver against that vision is less proven. In growing markets, this status is typical. In more mature markets, it may reflect a competitive strategy for a smaller vendor — such as selling an innovation ahead of mainstream demand — or a larger vendor trying to break out of a rut or differentiate itself.

For vendors and customers, Visionaries fall into the higher-risk-higher-reward category. They often introduce new technology, services or business models, and they may need to build financial strength, service and support, and sales and distribution channels. For the SSCS market, Visionaries have followed the trends and innovations for third-party software risk protection, but have yet to prove their execution capabilities.

Whether Visionaries become Challengers or Leaders may depend on if customers accept the new technology or the vendors can develop partnerships that complement their strengths. Visionaries are sometimes attractive acquisition targets for Leaders or Challengers.

Niche Players

Niche Players do well in a segment of a market, or they have a limited ability to innovate or outperform other vendors in the wider market. This may be because they focus on a particular functionality or geographic region, or because they are new entrants to the market. Alternatively, they may be struggling to remain relevant in a market that is moving away from them. Niche Players in SSCS have stuck to conventional methods for third-party software risk protection or have not invested in features that would make them a Challenger or Visionary, like AI software supply chain or software pipeline security posture.

For end users, assessing Niche Players is more challenging than assessing vendors in other quadrants. Some could make progress, while others do not execute well and may not have the vision and means to keep pace with broader market demands.

A Niche Player may be a perfect fit for your requirements. However, if it goes against the direction of the market — even if you like what it offers — then it may be a risky choice because its long-term viability may be threatened.

Context

Software supply chain security (SSCS) has long been included as a standard capability within the application security testing (AST) market. The market for AST tools has greatly expanded in the past six years, so much so that a single Magic Quadrant can never fully cover all possible vendors. Gartner took the first step last April by recognizing SSCS with its own Market Guide. Since then, customer interest for SSCS has increased and SSCS capabilities are already widely deployed and deliver high value. It is clear that SSCS now warrants its own independent Magic Quadrant.

Market Overview

Software supply chain security (SSCS) has grown from a niche concern into a top enterprise priority, supported by a rapidly maturing market. Gartner estimates that SSCS market revenue exceeded $2.8 billion in 2025, up from $2.5 billion in 2024 and $2.2 billion in 2023. Gartner forecasts that the SSCS market will exceed $5 billion in revenue by 2030. [1]

Software engineering leaders and cybersecurity leaders increasingly need continuous, contextual protection rather than episodic scanning. In response, SSCS vendors have released security capabilities that span the full life cycle of third-party components and build artifacts.

Three dominant forces are now shaping the market:

- Regulatory pressure that mandates provenance and auditability
- Broad adoption of SBOMs and attestations as minimum compliance artifacts
- A strategic pivot from post-facto detection toward prevention and continuous assurance embedded in developer toolchains

As a result of these forces, SSCS products have recently evolved in five ways:

- The EU Cyber Resilience Act, financial-sector mandates and U.S. federal requirements like FedRAMP are driving feature roadmaps for attestations, SBOM/VEX ingestion and audit-ready evidence.

- Interest in controls for AI assets and LLM supply chains has risen markedly, with buyers asking for discovery, governance and lineage for models and related artifacts alongside traditional open-source components.
- Vulnerability triage now favors using exploitability analysis and runtime reachability, and security scanning tools integrate directly into SCM, CI/CD, registries and developer workflows (such as IDE checks, pull-request gates and pipeline workflows).
- Binary-first analysis and deep artifact forensics are emerging as important differentiators for shipped software complementing manifest-level SCA.
- OS image security, curated registries and rebuild factories are growing, as vendors seek to harden the upstream supply and offer pre-vetted components.

As a leader for software engineering or cybersecurity, use our evaluation to compare the top vendors in the SSCS market and capabilities of their products. Identify vendors that deliver the SSCS capabilities you need now and offer a compelling vision that aligns with your organization's strategic direction.

This is the first iteration of the Magic Quadrant for Software Supply Chain Security. It is replacing Gartner's **Market Guide for Software Supply Chain Security**.

⊕ Evidence

⊕ Evaluation Criteria Definitions