



DECISION PASSPORT

Choose a SAST tool

Do not sign a multi-year contract yet; run a trial on your own code first,
then pick Checkmarx if you must self-host or scan COBOL, or Snyk if your
code is modern and cloud is allowed.

Confidence: not assigned. 28 evidence records.

Blocked. Human decision pending.

Before acting: Nobody in the record owns the scanner, the repository access,
or the legacy COBOL slice that a trial needs.

Read this record before deciding.

EXECUTIVE SUMMARY

Recommendation

Do not sign a multi-year contract yet; run a trial on your own code first, then pick Checkmarx if you must self-host or scan COBOL, or Snyk if your code is modern and cloud is allowed.

Checkmarx CxSAST can be deployed in a private data center or hosted. Snyk offers a Free plan at \$0 / month and a Team plan from \$25 / month. Those Snyk prices are for small teams, so ask Snyk for an Enterprise quote, because compliance reporting and COBOL early access are Enterprise only.

CONFIDENCE	EVIDENCE	READINESS	HUMAN DECISION	FORMAL APPROVAL
Not assigned	28 records	Blocked	Pending	Not required

Confidence describes the strength of the recorded analysis. It is not the probability that an option is best.

Before acting

1. Nobody in the record owns the scanner, the repository access, or the legacy COBOL slice that a trial needs.
2. Open question: What primary programming languages and frameworks are in your core codebases?
3. Open question: Are you required to run on premises or can you use a multi tenant cloud solution?

Principal risks

RISK	SEVERITY	REQUIRED ACTION
Snyk's current language documentation says interfile analysis is available for supported languages except COBOL, and its COBOL docs list supported dialects and file formats.	High	Verify before committing: Run a Snyk scan on a representative COBOL sample with planted cross-file flaws and check whether the report lists them.
Fortify is described in the decision evidence as needing significant ongoing administration and specialized tuning.	High	Verify before committing: Name the staff and weekly hours assigned to run and tune Fortify, and confirm in a trial that scans stay current.
Checkmarx says pricing is customized by modules, SaaS or self-hosted deployment, and developer count, with no one-size-fits-all list price.	Medium	Verify before committing: Require itemized module, seat, deployment, renewal, and overage terms; compare each line with required coverage and users before purchase.

EXECUTIVE SUMMARY, CONTINUED

What would change the recommendation

- **Snyk wins** if your written language inventory shows no COBOL, policy allows cloud scanning, and a Snyk trial on your sample repositories finds the planted test flaws.
- **Checkmarx says** pricing is customized by modules, SaaS or self-hosted deployment, and developer count, with no one-size-fits-all list price.

What limits confidence

- We do not have evidence of your programming languages, whether you must run on premises, or whether you have staff to run an engine.

IN THIS RECORD

01	Question and decision frame	4
02	Argumont Verdict	5
03	Decision Hinges	6
04	Residual risks and unresolved questions	6
05	Human Decision and approvals	9
06	Evidence record	11
07	Record	18

Prepared from Passport v2, saved by Argumont. Later revisions create a separate version. Source links open external publications; numbered citations link to the evidence appendix.

RECORD IDENTITY

DECISION	dec_4d94bb5095f64cf1a441ff419d0a73a2
PASSPORT	pass_79ef486fad6f45939846bcfc6818adbe
SAVED BY	Argumont
SAVED AT	2026-10-11 13:51:19 UTC
CONTENT SHA-256	8c7b90a269ae8af28fa4b69aeae4b954f2158b5013dfc4fd64f317b618350b9a

The content hash identifies the saved JSON record. This PDF changes presentation only.

QUESTION AND DECISION FRAME

THE QUESTION AS ASKED

As a financial organization, we need to buy a SAST tool. Should we buy Checkmarx or Synk, or are there excellent alternatives we are not aware of?

OPTION	HOW IT ENTERED	DESCRIPTION
Checkmarx	Named in the question	
Snyk	Named in the question	
Veracode	Raised during analysis	Enterprise application security platform offering comprehensive SAST with centralized policy governance and compliance reporting tailored for regulated financial institutions.
Fortify	Raised during analysis	Enterprise SAST solution by OpenText with deep code analysis capabilities and flexible on-premise deployment options widely adopted in banking environments.

WHAT MATTERS	WHAT IT MEANS
Effectiveness in vulnerability detection	Ability to identify potential security threats
Integration with existing infrastructure	Compatibility with current systems and tools
Cost and licensing	Total cost of ownership and licensing fees
Ease of use and deployment	Simplicity of installation and operation
Support and updates	Quality of vendor support and frequency of updates

Decided about

A specific software enterprise agreement from a SAST vendor for your organization.

Open questions

- What primary programming languages and frameworks are in your core codebases?
- Are you required to run on premises or can you use a multi tenant cloud solution?

QUESTION AND DECISION FRAME, CONTINUED

Constraints

- Nobody in the record owns the scanner, the repository access, or the legacy COBOL slice that a trial needs.

ARGUMENT VERDICT

RECORDED VERDICT

Do not sign a multi-year contract yet; run a trial on your own code first, then pick Checkmarx if you must self-host or scan COBOL, or Snyk if your code is modern and cloud is allowed.

Checkmarx CxSAST can be deployed in a private data center or hosted. Snyk offers a Free plan at \$0 / month and a Team plan from \$25 / month. Those Snyk prices are for small teams, so ask Snyk for an Enterprise quote, because compliance reporting and COBOL early access are Enterprise only. Veracode is reported to send code off-premises, so it loses if your rules keep source code in-house. Fortify requires significant ongoing administration and specialized tuning compared to modern developer-centric SAST tools. Pick Fortify only if you can name the staff who will run and tune it. Two facts flip this: whether your core code includes COBOL or other legacy languages, and whether policy forces source to stay on your own servers. It comes down to whether the bank must self-host or scan COBOL.

LEADING OPTION	No single option selected
CONFIDENCE	Not assigned
CONFIDENCE BASIS	Strength of the analytical record: evidence quality, unresolved load-bearing claims, source independence, and Verdict sensitivity. It is not the probability that this option is best, and it is not an Outcome probability.
ISSUED	2026-10-11 13:21:47 UTC
VERDICT VERSION	1

STRONGEST SURVIVING OBJECTION

Checkmarx says pricing is customized by modules, SaaS or self-hosted deployment, and developer count, with no one-size-fits-all list price.

OPTIONS COMPARED

OPTION	RECORDED ASSESSMENT
Veracode	Veracode is reported to send code or compiled files off-premises, so it loses if your rules require code to stay in-house.

ARGUMENT VERDICT, CONTINUED

OPTION	RECORDED ASSESSMENT
Snyk	Snyk loses if you rely on it for COBOL, because its cross-file analysis excludes COBOL.

Dissenting view

Checkmarx's bank case rests on vendor case studies, and a 393% ROI at another institution is not a price comparison against Snyk.

Remaining uncertainty

We do not have evidence of your programming languages, whether you must run on premises, or whether you have staff to run an engine.

DECISION HINGES

Conditions that could change the conclusion.

NO.	WHAT WOULD CHANGE THE CONCLUSION
01	Snyk wins if your written language inventory shows no COBOL, policy allows cloud scanning, and a Snyk trial on your sample repositories finds the planted test flaws.

RESIDUAL RISKS AND UNRESOLVED QUESTIONS

RISK REGISTER

4 recorded risks

RISK	SEVERITY	LIKELIHOOD	EVIDENCE
01 Checkmarx says pricing is customized by modules, SaaS or self-hosted deployment, and developer count, with no one-size-fits-all list price.	Medium	Medium	Researched
02 Snyk's current language documentation says interfile analysis is available for supported languages except COBOL, and its COBOL docs list supported dialects and file formats.	High	Medium	Researched
03 Public user feedback describes difficulty locating policy settings, challenges running SAST and DAST together, and a hard initial deployment and training period.	Medium	Medium	Researched
04 Fortify is described in the decision evidence as needing significant ongoing administration and specialized tuning.	High	Medium	Researched

RESIDUAL RISKS AND UNRESOLVED QUESTIONS, CONTINUED

RISK DETAILS

RISK 01 / MEDIUM

Checkmarx says pricing is customized by modules, SaaS or self-hosted deployment, and developer count, with no one-size-fits-all list price.

A quote that includes modules or seats beyond the actual need could raise total cost after procurement; the trigger is a mismatch between licensed scope and active use. Severity is medium because it can materially raise spend, but the amount is not established. Probability is medium because pricing is explicitly tailored, not because an overrun is proven. Mitigation: require an itemized quote with renewal and seat-count terms, then compare it against a fixed set of required scans and users. Verify by reconciling the quote to that list; revisit if seats, modules, or renewal price exceed the agreed scope. Residual risk remains because renewal terms and final price are not known.

WHAT TO DO

Verify before committing: Require itemized module, seat, deployment, renewal, and overage terms; compare each line with required coverage and users before purchase. Verify against actual usage and review if scope or renewal price grows.

CATEGORY

Financial

RISK 02 / HIGH

Snyk's current language documentation says interfile analysis is available for supported languages except COBOL, and its COBOL docs list supported dialects and file formats.

If important COBOL code depends on flows across files, findings could miss those relationships; the trigger is relying on Snyk alone for that code. Severity is high only if such code is material to the systems in scope, otherwise low; the COBOL inventory is unknown. Probability is medium conditional on that use because the documented limitation is specific, but actual missed findings are unproven. Mitigation: map languages and frameworks, then test representative COBOL and modern code against agreed security cases before selection. Verify results and coverage reports; reopen the choice if required flows or frameworks are not analyzed. Residual risk remains for untested code and frameworks.

WHAT TO DO

Verify before committing: Run a Snyk scan on a representative COBOL sample with planted cross-file flaws and check whether the report lists them.

CATEGORY

Evidence uncertainty

RESIDUAL RISKS AND UNRESOLVED QUESTIONS, CONTINUED

RISK 03 / MEDIUM

Public user feedback describes difficulty locating policy settings, challenges running SAST and DAST together, and a hard initial deployment and training period.

If policy setup and team training are not completed, scans or release gates could be delayed or applied inconsistently. Severity is medium because this could disrupt security review and delivery; probability is low to medium because these are individual reports, not proof of this organization's outcome. Mitigation: test the required policies, integrations, and scan workflow in a representative evaluation before purchase. Verify that teams can find and apply the required controls and complete the workflow; review if policy exceptions or failed integrations persist. Whether code or binaries must leave the organization's network for the proposed setup is unproven so far, so do not treat that as an established weakness. Residual risk remains until deployment and custody terms are confirmed.

WHAT TO DO

In an evaluation, test required policy setup, integrations, and combined scan workflow with representative teams. Confirm data-handling and deployment terms in writing; review if controls or integrations fail in practice.

CATEGORY

Schedule

RISK 04 / HIGH

Fortify is described in the decision evidence as needing significant ongoing administration and specialized tuning.

If the organization lacks staff time or expertise, rules and findings may not be maintained, slowing reviews or reducing useful coverage; the trigger is choosing an on-premise engine without confirmed operating capacity. Severity is medium to high depending on workload and service expectations. Probability is uncertain because dedicated staff are unverified; the administration burden is supported, but failure at this organization is not proven. Mitigation: confirm available operator capacity and include setup, tuning, and support effort in an evaluation using representative code. Verify through documented operating tasks and scan upkeep during the evaluation; reconsider if required maintenance cannot be sustained. Residual risk remains until staffing and workload are confirmed.

WHAT TO DO

Verify before committing: Name the staff and weekly hours assigned to run and tune Fortify, and confirm in a trial that scans stay current.

CATEGORY

Evidence uncertainty

What remains open

- The financial organization has dedicated security staff to manage and tune an on-premise static analysis engine. An unresolved issue remains: only financial organization is user-confirmed. Staff, COBOL load, and air-gap need are not confirmed, yet they carry the Fortify recommendation while Fortify itself is described as heavy to administer. Evidence is still needed: a user statement that they already staff an on-premise SAST engine, or a public Fortify requirement that such staff is mandatory for a bank-sized deployment. The recorded assessment is unverified.
- Veracode relies on a cloud-hosted scanning model where code or compiled artifacts are transmitted off-premises. An unresolved issue remains: if this is true, Veracode may be disqualified for a bank that cannot send source out. If it is false, the custody attack on Veracode collapses and Fortify loses its main contrast. Evidence is still needed: current Veracode documentation stating whether SAST requires

RESIDUAL RISKS AND UNRESOLVED QUESTIONS, CONTINUED

transmitting source or binaries off-premises and whether a private or on-premises scan path exists. The recorded assessment is unverified.

- Fortify requires significant ongoing administration and specialized tuning compared to modern developer-centric SAST tools. An unresolved issue remains: that downside undercuts Fortify on ease of use unless the unverified staff claim is true. It is not a reason to pick Fortify over Checkmarx self-hosted or Snyk Team. Evidence is still needed: a public comparison of admin hours, rule-tuning labor, or failure to operate Fortify without a dedicated engine team versus Checkmarx or Snyk. The recorded assessment is unsupported.
- Vendor ROI on another institution is not a comparable price for this purchase versus Snyk Team at 25 dollars a month.

What is still contested

- Checkmarx One pricing depends on selected modules, deployment model (SaaS or self-hosted), and developer seat count.
- Checkmarx pricing is based on developer seats, applications, and usage.
- Checkmarx does not publish list pricing on its website.
- Checkmarx SAST supports languages including Java, JavaScript, TypeScript, Python, C#, C/C++, Go, PHP, Ruby, Swift, Kotlin, COBOL, and PL/SQL.
- Interfile analysis in Snyk Code is available for all supported languages except COBOL.
- Snyk Code on Enterprise plans provides reporting for compliance frameworks including SOC 2, PCI DSS, HIPAA, and ISO 27001.
- Veracode relies on a cloud-hosted scanning model where code or compiled artifacts are transmitted off-premises.
- The financial organization has dedicated security staff to manage and tune an on-premise static analysis engine.

HUMAN DECISION AND APPROVALS

The analytical Verdict and the human authorization are recorded separately.

DECISION OWNER	Not assigned in this sample
ASSIGNED APPROVER	Not assigned in this sample
RISK OWNER	Not assigned in this sample
EXECUTION READINESS	Blocked
READINESS BASIS	Nobody in the record owns the scanner, the repository access, or the legacy COBOL slice that a trial needs.

HUMAN DECISION AND APPROVALS, CONTINUED

HUMAN DECISION

The organization has not recorded its decision.

FORMAL APPROVAL

Not required for this decision.

EVIDENCE RECORD

What the record holds, and what is not yet established.

EVIDENCE SUMMARY

19 recorded claims

CLAIM	STATUS	STRENGTH	SOURCES
Checkmarx One pricing depends on selected modules, deployment model (SaaS or self-hosted), and developer seat count. Checkmarx	Partly supported	Not recorded	[4], [12]
Checkmarx pricing is based on developer seats, applications, and usage. Checkmarx	Partly supported	Not recorded	[2]
Checkmarx does not publish list pricing on its website. Checkmarx	Partly supported	Not recorded	[2], [9]
Checkmarx SAST supports languages including Java, JavaScript, TypeScript, Python, C#, C/C++, Go, PHP, Ruby, Swift, Kotlin, COBOL, and PL/SQL. Checkmarx	Partly supported	Not recorded	[2], [6]
Checkmarx SAST scans 30+ languages including Java, JavaScript, TypeScript, Python, C#, Go, Rust, Apex, and COBOL. Checkmarx	Partly supported	Not recorded	[2], [6]
Snyk offers a Free plan at \$0 / month and a Team plan from \$25 / month. Snyk	Supported	Not recorded	[3]
Snyk Code includes 100 tests / month on the Free plan and 1,000 tests / month on the Team plan. Snyk	Supported	Not recorded	[3], [5]
Interfile analysis in Snyk Code is available for all supported languages except COBOL. Snyk	Partly supported	Not recorded	[4], [11]
Snyk Code on Enterprise plans provides reporting for compliance frameworks including SOC 2, PCI DSS, HIPAA, and ISO 27001. Snyk	Partly supported	Not recorded	[3], [5]

EVIDENCE RECORD, CONTINUED

CLAIM	STATUS	STRENGTH	SOURCES
Snyk Code supports 16 language groups including Apex, C/C++, COBOL, Dart and Flutter, and Go. Snyk	Partly supported	Not recorded	[4], [6]
Snyk Code restricts Early Access language analysis for Rust, Groovy, COBOL, Dart/Flutter, and Objective-C to Enterprise plans. Snyk	Partly supported	Not recorded	[3]
Veracode relies on a cloud-hosted scanning model where code or compiled artifacts are transmitted off-premises. Fortify	Partly supported	Not recorded	[10]
Fortify requires significant ongoing administration and specialized tuning compared to modern developer-centric SAST tools. Fortify	Supported	Not recorded	[7], [13]
Checkmarx does not publish flat list pricing publicly and prices by developer seats, application count, and deployment model. Checkmarx	Supported	Not recorded	[4]
Veracode requires code or compiled artifacts to be transmitted off-premises to its cloud-hosted scanning infrastructure. Veracode	Partly supported	Not recorded	[10]
Checkmarx CxSAST can be deployed in a private data center or hosted. Checkmarx	Supported	Not recorded	[8]
Checkmarx says a large financial services company reduces remediation time by 83% with Checkmarx. Checkmarx	Supported	Not recorded	[7]
Checkmarx says a European financial services institution achieves 393% ROI with Checkmarx. Checkmarx	Supported	Not recorded	[2]
A global financial software developer scanning tens of millions of lines of code across Java and C++ selected Checkmarx CxSAST as an on-premise alternative. Checkmarx	Supported	Not recorded	[1]

EVIDENCE RECORD, CONTINUED

CONFIRMED BY THE ORGANIZATION

Financial organization

OPTION Shared across the decision

NOT YET CONFIRMED

The financial organization has dedicated security staff to manage and tune an on-premise static analysis engine.

Only the organization can confirm this.

OPTION Fortify

Unknowns

- The financial organization has dedicated security staff to manage and tune an on-premise static analysis engine.

SOURCE REGISTER

REF.	PUBLISHER	RECORDED TYPE	QUALITY
[1]	Casestudies.com	Secondary source	Secondary
[2]	Casestudies.com	Secondary source	Secondary
[3]	Snyk.io	Secondary source	Primary
[4]	Casestudies.com	Secondary source	Secondary
[5]	Docs.snyk.io	Secondary source	Primary
[6]	Docs.checkmarx.com	Secondary source	Secondary
[7]	Casestudies.com	Secondary source	Secondary
[8]	Info.checkmarx.com	Secondary source	Secondary
[9]	Docs.checkmarx.com	Secondary source	Secondary
[10]	Veracode.com	Secondary source	Primary
[11]	Docs.checkmarx.com	Secondary source	Secondary
[12]	Docs.cortex.io	Secondary source	Secondary
[13]	Checkmarx.com	Secondary source	Secondary

SOURCE DETAILS

EVIDENCE RECORD, CONTINUED

STRONG

[1] Case Study: Leading Financial Software Provider achieves a more secure SDLC with Checkmarx CxSAST

The case study states that a financial platform developer scanning tens of millions of lines of Java and C++ chose Checkmarx CxSAST as an on-premise solution.

PUBLISHER	Casestudies.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source
Open source: www.casestudies.com	

STRONG

[2] Case Study: European Financial Services Institution achieves 393% ROI and rapid, secure software delivery with Checkmarx

The case study reports that a European financial services institution achieved a 393% ROI with Checkmarx.

PUBLISHER	Casestudies.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source
Open source: www.casestudies.com	

STRONG

[3] Snyk official pricing

The Snyk plans page reports a Free tier and a Team tier starting at \$25/month.

PUBLISHER	Snyk.io
STANCE	Support
RETRIEVED	2026-10-11 13:13:07 UTC
SOURCE QUALITY	Primary
SOURCE TYPE	Secondary source
Open source: snyk.io	

EVIDENCE RECORD, CONTINUED

MODERATE

[4] Case Study: Global Financial Services Company achieves stronger multi-language application security and developer-driven SDLC adoption with Checkmarx

Global Financial Services, a 125-year-old firm that processes more than 23 billion consumer self-service transactions worldwide, needed to replace its legacy SAST tooling with a more accurate, flexible static code analysis solution.

PUBLISHER	Casestudies.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source

Open source: www.casestudies.com

MODERATE

[5] Snyk official documentation

PUBLISHER	Docs.snyk.io
STANCE	Support
RETRIEVED	2026-10-11 13:13:07 UTC
SOURCE QUALITY	Primary
SOURCE TYPE	Secondary source

Open source: docs.snyk.io

MODERATE

[6] Checkmarx SAST

PUBLISHER	Docs.checkmarx.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source

Open source: docs.checkmarx.com

EVIDENCE RECORD, CONTINUED

STRONG

[7] Case Study: a large financial services company reduces remediation time by 83% with Checkmarx

The case study states that a large financial services company reduced remediation time by 83% with Checkmarx.

PUBLISHER	Casestudies.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source

Open source: www.casestudies.com

STRONG

[8] Checkmarx Static Application Security Testing (SAST)

The Checkmarx datasheet states that CxSAST can be deployed in a private data center or hosted.

PUBLISHER	Info.checkmarx.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source

Open source: info.checkmarx.com

LINK NOT RETAINED

[9] General and Server Settings**- 9.7.0 Required Prerequisites for Installing Checkmarx SAST**

PUBLISHER	Docs.checkmarx.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source
PAGE LINK	Not retained

EVIDENCE RECORD, CONTINUED

MODERATE

[10] Veracode official pricing

PUBLISHER	Veracode.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:07 UTC
SOURCE QUALITY	Primary
SOURCE TYPE	Secondary source
Open source: www.veracode.com	

LINK NOT RETAINED

[11] Installation Guide

. The Reporting Service consists of four components, and that setup consists of the following steps from a high-level perspective: 1. Run the auth script on the CxManager server. 2. Install the Cx Reporting Manager. 3.

PUBLISHER	Docs.checkmarx.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source
PAGE LINK	Not retained

MODERATE

[12] Checkmarx - Integrations - Cortex Docs

This integration is supported for [Checkmarx Static Application Security Testing (SAST)](<https://checkmarx.com/cxsast-source-code-scanning/>).... Before getting started, create a user with access to the `sast\_rest\_api` scope.... If you're using a self-hosted instance of Checkmarx, you'll need to verify that your Cortex instance is able to reach the Checkmarx instance.

PUBLISHER	Docs.cortex.io
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source
Open source: docs.cortex.io	

EVIDENCE RECORD, CONTINUED

MODERATE

[13] How a Financial Giant Maximized Its AppSec ROI

PUBLISHER	Checkmarx.com
STANCE	Support
RETRIEVED	2026-10-11 13:13:15 UTC
SOURCE QUALITY	Secondary
SOURCE TYPE	Secondary source
Open source: checkmarx.com	

RECORD

CURRENT

Verdict record 1

Do not sign a multi-year contract yet; run a trial on your own code first, then pick Checkmarx if you must self-host or scan COBOL, or Snyk if your code is modern and cloud is allowed.

ISSUED	2026-10-11 13:21:47 UTC
CONFIDENCE	Not assigned