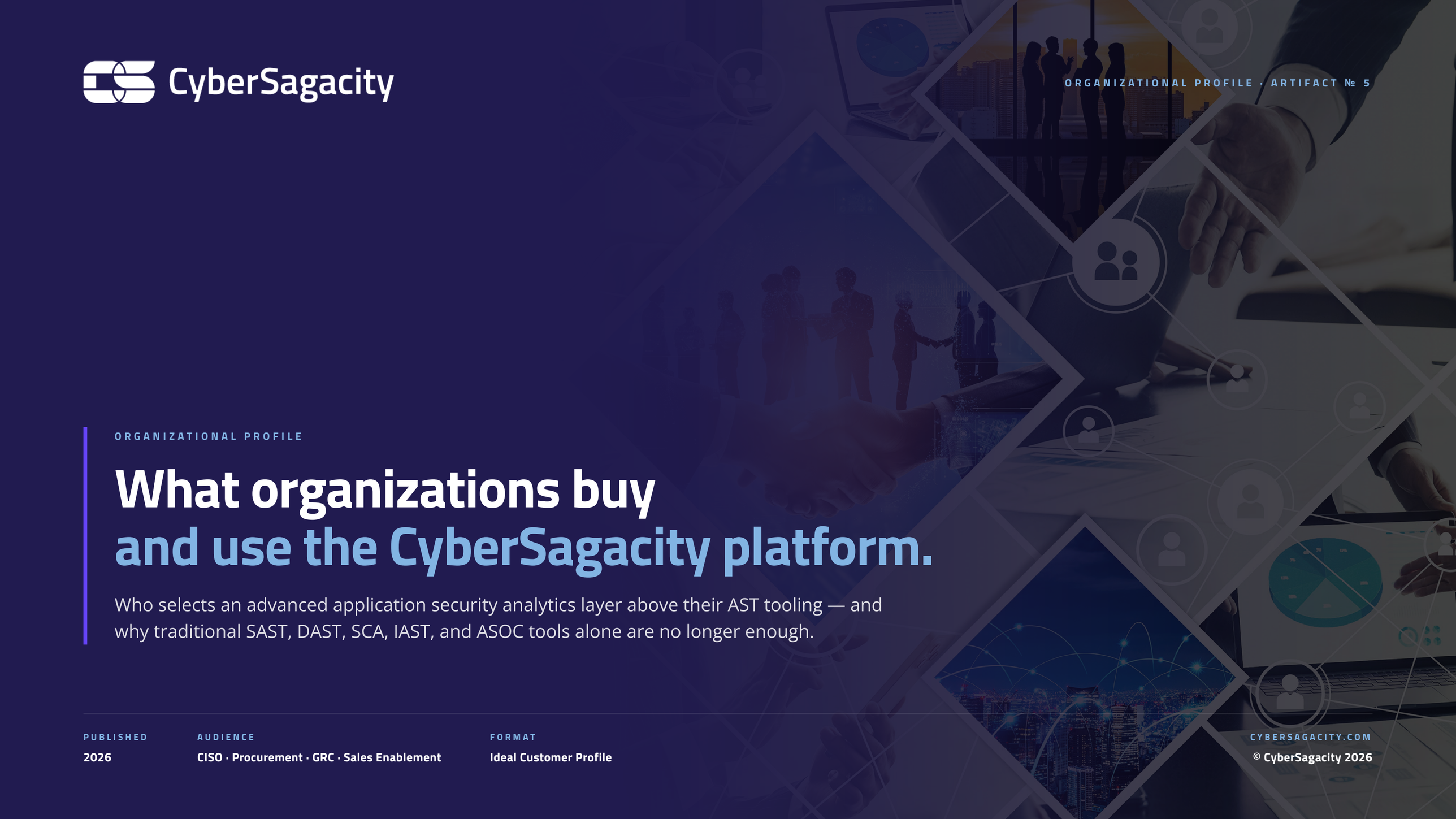
CyberSagacity



ORGANIZATIONAL PROFILE

What organizations buy and use the CyberSagacity platform.

Who selects an advanced application security analytics layer above their AST tooling — and why traditional SAST, DAST, SCA, IAST, and ASOC tools alone are no longer enough.

PUBLISHED
2026

AUDIENCE
CISO · Procurement · GRC · Sales Enablement

FORMAT
Ideal Customer Profile

CYBERSAGACITY.COM

EXECUTIVE SUMMARY

For organizations facing the realities of modern software risk.

CyberSagacity's SATraits™ and SATriage™ platform is designed for organizations that develop or deploy software and are facing fragmented AST tools, overwhelming noise, inconsistent severity scoring, and a lack of business-aligned insight.

The customers who adopt CyberSagacity are users of AST tools who recognize that **traditional SAST, DAST, MAST, SCA, PenTest, ASPM, and ASOC tools are no longer sufficient.** They seek a high-fidelity analytics layer — one that corrects, normalizes, correlates, and prioritizes all application-security findings.

This paper defines **who buys and relies on** CyberSagacity's platform, **why**, and what characteristics define the **ideal customer profile**.

> **From detection to decision-grade intelligence — for the organizations at the forefront of cybersecurity and regulatory accountability.**

SECTION 01 · ORGANIZATIONS THAT RELY ON TRADITIONAL AST TOOLS

Enterprises that need to manage the noise, false positives, and unclear priorities.

CyberSagacity's platform is most valued by organizations that are hitting the limits of traditional AST tooling. These enterprises experience:

- Excessive false positives and false negatives.
- Tool overlap producing redundant or contradictory results.
- Inconsistent or meaningless severity scoring.
- Inability to determine which vulnerabilities matter.
- Bloated backlogs and slow remediation cycles.

These buyers need more than detection — they require **precision analytics** capable of mapping vulnerabilities to consequence, exploitability, compliance, and financial exposure.

Industries served

Financial services & fintech	Healthcare & life sciences
E-commerce & consumer brands	SaaS & cloud technology
Telecom & media	Energy & utilities
Critical infrastructure	Defense, aerospace & government

SECTION 02 · LARGE, FAST-MOVING DEVELOPMENT ORGANIZATIONS

Software-centric enterprises facing scale and complexity.

CyberSagacity's customers typically maintain

- Multi-team development organizations.
- Large application portfolios.
- Microservices and API-driven architectures.
- High-velocity CI/CD pipelines.
- Hybrid cloud environments.
- Heavy reliance on open-source and third-party components.

They choose CyberSagacity because it provides

- **Cross-tool coverage analytics.**
- **True defect classification and severity correction.**
- **Prioritization based on business impact** — not guesswork.
- **Executive-ready metrics and dashboards.**
- **Risk quantification** to support decision-making.

> **They cannot afford slow or inaccurate AppSec tooling.**

SECTION 03 · REGULATED ENTERPRISES NEEDING DEFENSIBLE, AUDIT-READY EVIDENCE

Where accuracy is not optional — it is legally and financially mandatory.

CyberSagacity is selected by organizations obligated to meet strict regulatory frameworks:

PCI DSS	HIPAA / HITRUST	SOX / FFIEC
GDPR / CCPA	NIST 800-53 / CSF	CMMC / FEDRAMP

These enterprises must demonstrate consistent, defensible control evidence.

They choose CyberSagacity because it

- Normalizes and corrects tool output.
- Maps every defect to governance controls.
- Quantifies compliance exposure.
- Provides audit-ready documentation and reporting.

> **For these customers, accuracy is not optional — it is legally and financially mandatory.**

SECTION 04 · BREACH-EXPOSED, AUDIT-FLAGGED, OR BOARD-PRESSURED ORGANIZATIONS

Buyers motivated by risk events, material findings, or executive mandates.

A significant portion of CyberSagacity customers arrive after:

- A major breach or third-party compromise.
- A compliance failure or audit deficiency.
- A regulator, customer, or board inquiry.
- An M&A due-diligence gap.
- A failed or stalled AppSec transformation initiative.

They require

- Clarity on true vulnerability severity.
- Quantified risk for executive decision-making.
- Prioritization based on impact, not tool noise.
- Evidence-based remediation recommendations.

> **CyberSagacity becomes the trust layer that unifies and validates all AppSec data.**

SECTION 05 · DEVSECOPS, PRODUCT SECURITY & ENGINEERING TEAMS

Teams focused on reducing bottlenecks and improving productivity.

Engineering and security teams adopt CyberSagacity because it:

- Eliminates noise, duplicates, contradictions, and misclassifications.
- Reduces time wasted on non-issues.
- Prioritizes work by risk, exploitability, and financial outcome.
- Improves developer productivity and remediation speed.
- Integrates seamlessly into CI/CD workflows.

> **Less friction. More clarity. Better alignment with business outcomes.**

These teams have spent years operating multiple AST scanners and have learned firsthand that adding more tools does not add more clarity. They want a system that turns the raw output of those tools into work that moves the needle — at the speed of their delivery pipelines.

CYBERSAGACITY'S IDEAL CUSTOMER PROFILE

Six characteristics shared across our ideal customers.

01 · DEPENDENCE

High application dependence

Digital products, services, or operations rely heavily on software integrity.

02 · STACK

Multi-tool AST environment

Several SAST/DAST/MAST/SCA/PenTest/ASPM/ASOC tools in use, seeking a unified intelligence layer.

03 · VISIBILITY

Visibility gaps & backlog problems

Struggle to understand which vulnerabilities matter and which tool outputs are reliable.

04 · COMPLIANCE

Compliance pressure

Need accurate, defensible reporting tied to regulatory control frameworks.

05 · BOARD

Executive or board attention on risk

Security findings must translate into business, financial, and operational terms.

06 · OUTCOMES

Outcome-driven security

Seek measurable improvements in security posture — not just more data.

CONCLUSION

Traditional AST tools detect. CyberSagacity validates, correlates, prioritizes, and explains.

CyberSagacity's advanced analytics platform is purchased by organizations that have recognized a fundamental truth: **traditional AST tools are necessary but insufficient.** They detect — but they do not validate, correlate, prioritize, or explain risk.

CyberSagacity fills this critical gap by delivering:

- Corrected and normalized findings.
- True severity and exploitability ranking.
- Coverage and accuracy analytics across tools.
- Compliance mapping for every defect.
- Quantified financial and operational risk.
- Executive-ready reporting and dashboards.

> **CyberSagacity is the platform they choose when they need clarity, confidence, and quantifiable outcomes from their AppSec investments.**

These are the capabilities demanded by the organizations at the forefront of cybersecurity, digital transformation, and regulatory accountability.

Learn more at www.cybersagacity.com →