CyberSagacity

MARKET ANALYSIS WHITEPAPER

Target segments for an advanced Application Security Analytics platform.

Where the intelligence layer above AST tooling delivers the most measurable value — across security teams, regulated enterprises, cloud providers, and risk advisors.

PUBLISHED
2026

AUDIENCE
CISO · AppSec · GRC · Investors

FORMAT
Market Analysis Whitepaper

EXECUTIVE SUMMARY

The AST market has matured. The intelligence layer above it has not.

Most medium-to-large organizations already operate a mix of SAST, DAST, SCA, IAST, MAST, pen testing, ASPM, and ASOC tools. What remains immature is the intelligence layer that makes sense of these fragmented, noisy outputs.

CyberSagacity's Security Analytics platform — **SATraits™** and **SATriage™** — sits above this tooling stack. It ingests, corrects, normalizes, and correlates AST results across vendors and environments, then ranks them by true risk, business impact, and compliance exposure.

Instead of asking *"Which tool should we buy next?"*, CyberSagacity's customers ask and answer: **which vulnerabilities actually matter, where are we over- or under-protected, and what is the quantified financial and regulatory risk associated with our current exposures?**

SEGMENT 01

Security & DevSecOps Teams

Operational owners of AST tools and AppSec outcomes.

SEGMENT 02

Large Enterprises & Regulated Industries

Multi-tool, high-regulation environments with significant breach impact.

SEGMENT 03

Cloud & Infrastructure Providers

Platforms embedding security into cloud, DevOps, and multi-tenant services.

SEGMENT 04

Compliance & Risk Management Firms

Auditors, GRC consultancies, red teams, M&A due-diligence providers.

SEGMENT 01 · SECURITY & DEVSECOPS TEAMS

The operators and enforcers of AST and AppSec tooling.

Definition

Security & DevSecOps Teams are the primary operators of AST and AppSec tooling. Typical roles include CISOs and Directors of Application / Product Security, Security Engineers, AppSec Analysts, DevSecOps Engineers, and Security Champions embedded in engineering squads.

Their mandate: integrate security into the SDLC and CI/CD pipelines without breaking delivery velocity.

Market Dynamics

Adoption Level: Very High. Heavy users of SAST, DAST, SCA, IAST, pen tests, ASPM/ASOC, plus SIEM and SOAR. The problem is not tool scarcity — it is **signal scarcity**: overlapping, conflicting, and misclassified findings.

Drivers of Adoption

- **Threat modeling & risk management** — exposure must be understood and prioritized.
- **Automated security in CI/CD** — security gates across build/test/deploy.
- **Reducing MTTD & MTTR** — detect and fix material issues fast.

Key Challenges

- **Security vs. speed tension** — oversensitive controls slow teams; undersensitive controls invite breaches.
- **Noise & false positives** — large backlogs with minimal actionable prioritization.
- **Fragmented data** — different tools, formats, and severities with no unified truth.

SEGMENT 01 · CYBERSAGACITY FIT & COMPANIES

From drowning in noise to driving measurable risk reduction.

CyberSagacity delivers:

- A single normalized view of vulnerabilities across SAST/DAST/SCA/IAST/pen tests.
- Statistical correction of vendor severities and mislabeling.
- Risk-based prioritization weighted by exploitability, business criticality, and regulatory exposure.
- Integration with Jira and CI/CD to push actionable work into existing pipelines.

> **Stop counting findings. Start measuring risk reduction.**

Representative Companies

Netflix
High-velocity DevSecOps, complex microservices.

Capital One
Cloud-first financial institution with strong security posture.

Salesforce
Large SaaS platform with multi-tenant AppSec.

Adobe
Global software provider with mature secure-SDLC programs.

Shopify
High-scale e-commerce with aggressive release cycles.

Microsoft
Massive internal AST usage across product engineering orgs.

SEGMENT 02 · LARGE ENTERPRISES & REGULATED INDUSTRIES

Where application failures cause material financial, regulatory, and reputational damage.

Definition

Organizations where applications carry outsized risk, including **BFSI** (banking, payments, capital markets, insurance, fintech), **Healthcare & Pharmaceuticals** (hospitals, payers, EMR vendors, medical and research systems), **Government & Defense** (civil agencies, defense, intelligence, critical infrastructure), **Retail & E-commerce**, and **Energy & Utilities**.

These organizations usually run multiple AST vendors — Veracode, Checkmarx, Synopsys, Fortify — plus consulting-led pen tests and in-house tools.

Market Dynamics

Adoption Level: High. AST is table stakes, often deployed for years. Compliance pressure spans PCI-DSS, SOX, HIPAA/HITRUST, GDPR/CCPA, FFIEC, NIST 800-53/CSF, CMMC, FedRAMP, and sector regulators. Architectural complexity: legacy monoliths alongside microservices, APIs, mobile, and cloud workloads.

Drivers of Adoption

- **Regulatory compliance & audit readiness** at scale.
- **Risk mitigation** in high-value, highly targeted sectors.
- **Enterprise governance** — board and regulator expectations for demonstrable control effectiveness.

Key Challenges

- **Legacy systems** that are hard to test and hard to replace.
- **Multi-tool complexity** — Checkmarx + Veracode + Fortify + Black Duck + pen testing = conflicting data.
- **Scale** — thousands of applications, millions of findings, limited remediation bandwidth.

SEGMENT 02 · CYBERSAGACITY FIT & COMPANIES

CyberSagacity becomes the AppSec system of record.

CyberSagacity:

- Measures coverage, overlap, and gaps across all tools.
- Corrects vendor-centric severity ratings and harmonizes taxonomies.
- Maps each defect to specific governance controls and business services.
- Quantifies financial, operational, and regulatory risk so CISOs and boards can make informed tradeoffs.

> **From "we run tools" to "we can prove where we're exposed, what matters most, and how risk is trending."**

Representative Companies

JPMorgan Chase
Global bank with extensive regulated application estate.

UnitedHealth Group
Major healthcare and insurance provider under HIPAA/HITRUST.

Walmart
Global retail and online commerce, massive transaction volumes.

HSBC
Multinational bank with multi-jurisdiction regulatory complexity.

Pfizer
Regulated R&D, manufacturing, and clinical trial systems.

U.S. Dept. of Veterans Affairs
Large citizen-facing government application portfolio.

SEGMENT 03 · CLOUD & INFRASTRUCTURE PROVIDERS

Where security is both table stakes and differentiator.

Definition

Providers of shared platforms and core infrastructure: **Public Cloud** (AWS, Microsoft Azure, Google Cloud, Oracle Cloud, IBM Cloud), **Managed Infrastructure** (Equinix, DigitalOcean), **Telecom & Network** providers running large-scale platforms and APIs, and **Edge / CDN / Security service** providers (Cloudflare, Akamai, Fastly).

Market Dynamics

Adoption Level: High. Heavy use of internal AST, IaC scanning, container security, API security, CSPM, and runtime analysis. Operate under a **shared responsibility model**: they secure the underlying infrastructure and control planes while enabling customers to secure workloads.

Drivers of Adoption

- **Security as a market differentiator** and revenue-generating service.
- **Multi-tenant isolation** and platform trust.
- **Compliance & certification** demands (SOC 2, ISO 27001, FedRAMP, sector-specific).

Key Challenges

- **Scale & complexity** across regions, tenants, and product lines.
- **Cloud-native patterns** (containers, serverless, IaC, APIs) that don't map cleanly to old AST models.
- **Customer heterogeneity** — from startups to regulated enterprises.

SEGMENT 03 · CYBERSAGACITY FIT & COMPANIES

Internal intelligence — and a customer-facing analytics service.

Two primary modes

1. Internal security analytics. Normalizes and prioritizes vulnerabilities across AST, IaC, container, API, and runtime tools. Supports internal security, risk, and compliance with accurate, prioritized intelligence.

2. Customer-facing analytics (OEM / embedded). Provides tenants with risk dashboards built from their own AST and cloud security outputs. Enhances platform value and differentiation via analytics-driven security posture views.

> **Deep cross-tool insight internally — and a monetizable analytics layer externally.**

Representative Companies

Amazon Web Services
Global hyperscale cloud provider.

Microsoft Azure
Heavy enterprise and public-sector presence.

Google Cloud Platform
Strong in Kubernetes, data, and ML workloads.

IBM Cloud
Hybrid cloud with regulated-industry focus.

Oracle Cloud Infrastructure
Cloud targeting databases, ERP, regulated sectors.

Cloudflare
Edge network and security provider, large application footprint.

SEGMENT 04 · COMPLIANCE & RISK MANAGEMENT FIRMS

The firms that assess, validate, and attest to client security posture.

Definition

External firms whose business is assessing and attesting to client security posture: **Big-4 and regional audit/advisory** firms, **Governance, Risk, and Compliance (GRC)** consultancies, **penetration testing and red-team** firms, and **M&A due-diligence and third-party risk** assessors.

They use AST outputs, pen test findings, and custom tools to deliver audits, certifications, advisory reports, and due-diligence opinions.

Market Dynamics

Adoption Level: Moderate to High. These firms use AST data extensively, but often in **episodic, engagement-based** contexts rather than continuous operations. Their core challenge: standardizing and comparing risk across many clients, industries, and tool vendors.

Drivers of Adoption

- **Regulatory and audit requirements** — clients must show evidence of testing and remediation.
- **Third-party and supply-chain risk** — assessing vendors' AppSec postures.
- **M&A and investment due-diligence** — evaluating latent security debt and risk of software assets.
- **Advisory and benchmarking** — maturity assessments and roadmap recommendations.

Key Challenges

- **Manual-heavy processes** — documents, interviews, and static reports.
- **Heterogeneous toolchains** — every client runs a different mix of SAST/DAST/SCA/pen tests/cloud tools.
- **Inconsistent risk scoring** across vendor severities and taxonomies.
- **Report defensibility** — findings must withstand regulator, board, or buyer scrutiny.

SEGMENT 04 · CYBERSAGACITY FIT & COMPANIES

CyberSagacity becomes a standardization engine.

For Compliance & Risk Management firms, CyberSagacity:

- Ingests disparate AST, pen test, and security data across multiple clients and tools.
- Applies a consistent scoring and classification model across engagements.
- Maps findings to recognized frameworks (NIST, ISO 27001, PCI-DSS, HIPAA).
- Produces repeatable, defensible analytics and reports that reduce labor and increase consistency.

This enables new service offerings: **quantified AppSec risk scoring** for vendor risk programs, **M&A due-diligence packages** with clear exposure estimates, and **benchmarking services** across portfolios or industries.

Representative Companies

Deloitte
Global audit and advisory firm with major cyber practice.

PwC
Big-4 firm providing security, risk, and compliance advisory.

KPMG
Global firm with extensive GRC and cyber capability.

EY (Ernst & Young)
Big-4 with dedicated cyber risk and advisory services.

Accenture
Large consulting firm with security and GRC practices.

NCC Group / Mandiant
Specialized penetration testing, red teaming, cyber advisory.

CONCLUSION · THE SHARED PAIN

Not a lack of scanners.
A lack of clarity, consistency, and business-aligned insight.

SEGMENT 01
Security & DevSecOps Teams
Own the tools — and are drowning in noise.

SEGMENT 02
Large Enterprises
Must prove — not just claim — that they are managing risk and compliance.

SEGMENT 03
Cloud Providers
Must secure multi-tenant platforms at scale and increasingly productize security insights.

SEGMENT 04
Compliance & Risk Firms
Must normalize and defend assessments across diverse client environments.

CyberSagacity's Security Analytics platform addresses this gap directly. It **corrects and normalizes** outputs from SAST, DAST, SCA, MAST, IAST, pen tests, and cloud-native tools; **correlates and de-duplicates** findings across vendors and environments; **prioritizes by true risk** — exploitability, business criticality, and regulatory impact; **maps to governance frameworks** and quantifies potential financial and operational loss; and delivers **executive- and auditor-ready reporting** that turns technical noise into strategic decisions.

> **In a market saturated with tools that find vulnerabilities, CyberSagacity leads where outcomes are actually determined — making findings accurate, contextual, prioritized, and defensible.**

APPENDIX 01 · CROSS-SEGMENT SUMMARY

AST adoption by sector.

SEGMENT	ADOPTION LEVEL	TYPICAL METHODS	KEY CHALLENGES
Security & DevSecOps Teams	**Very High**	SAST, DAST, SCA, automation, ASOC / ASPM	Noise, tool sprawl, dev friction
Large Enterprises & Regulated	**High**	SAST, DAST, SCA, IAST, pen test	Legacy complexity, cost, making sense of multiple tools
Cloud & Infrastructure Providers	**High**	Cloud-native AST, IaC, container, CSPM	Shared responsibility, cloud-native complexity
Technology & Software Development	**Moderate–High**	SAST, IAST, SCA, container security	False positives, limited AppSec headcount
Compliance & Risk / Audit Firms	**Moderate–High**	SCA, DAST, pen testing, binary analysis	Manual processes, evolving regulations

APPENDIX 02 · GLOBAL APPLICATION SECURITY MARKET

A multi-tens-of-billions market, growing at mid-teens CAGR.

Global AppSec Market (Broad)

Current revenues sit in the **$10–17B range** with a mid-teens CAGR through the next decade — implying ~$25–35B by 2030.

$10.4B

2024 revenue, reaching $34.8B by 2033 at 14.3% CAGR.

IMARC GROUP

$13.6B

2025 revenue, growing to $30.4B by 2030 at 17.4% CAGR.

MORDOR INTELLIGENCE

$8.98B

2024 revenue, reaching $25.1B by 2030 at 18.7% CAGR.

GRAND VIEW RESEARCH

Dedicated AST Segment

Smaller than broad AppSec, growing at comparable or slightly higher rates — and **fragmented across many SAST / DAST / SCA vendors**. This is the layer CyberSagacity's analytics sits above.

$4.77B

AST tools, 2024 — projected to $17.9B by 2033 at 15.7% CAGR.

BUSINESS RESEARCH INSIGHTS

$3.41B

AST projected 2025, exceeding $10B by 2033 at ~15% CAGR.

DATAINSIGHTS MARKET

Largest Vertical Contributors

- **BFSI** — ~30–35% of AppSec revenues. Largest and most mature.
- **IT & Telecom / Software** — roughly 20–25%, second-largest.
- **Healthcare** — ~10–15%, fastest-growing major vertical.
- **Government & Public Sector** — ~10–15%.
- **Retail & E-Commerce** — ~10–15%.

APPENDIX 03 · THE VENDOR LANDSCAPE

Most commonly referenced AST vendors, by industry.

TECHNOLOGY & SOFTWARE

Developer-centric

- **Snyk** — SCA, container, IaC
- **GitHub Advanced Security** — code scanning, SCA
- **GitLab Secure** — SAST, DAST, dependencies
- **SonarQube** — SAST + code quality
- **Contrast Security** — IAST, RASP

GOVERNMENT & DEFENSE

DoD-compliant stack

- **Checkmarx** — SAST/IAST (DoD "Iron Bank")
- **Synopsys** — Coverity, Black Duck
- **Micro Focus Fortify**
- **HCL AppScan**
- **Veracode**

FINANCIAL SERVICES

Banking & capital markets

- **Veracode** — SAST, DAST, SCA
- **Synopsys** — Coverity + Black Duck
- **Checkmarx**
- **Micro Focus Fortify**
- **HCL AppScan**

HEALTHCARE & PHARMA

HIPAA-aligned

- **Veracode**
- **Synopsys** — Coverity, Black Duck
- **Checkmarx**
- **Micro Focus Fortify**
- **HCL AppScan**

RETAIL & E-COMMERCE

PCI-driven, CI/CD-heavy

- **Veracode**
- **Synopsys**
- **Checkmarx**
- **Micro Focus Fortify**
- **Burp Suite / OWASP ZAP**

ENERGY & UTILITIES

OT/ICS-aware

- **Veracode**
- **Checkmarx**
- **Micro Focus Fortify**
- **NTT Application Security**
- **Synopsys**

TELECOM & MEDIA

Carrier-scale

- **Veracode**
- **Checkmarx**
- **Synopsys**
- **Micro Focus Fortify**
- **HCL AppScan**

CROSS-VENDOR REALITY

No single tool wins.

- 5+ vendors per enterprise on average.
- <20% defect coverage per tool.
- <1% cross-tool correlation.
- **→ analytics layer required.**