CyberSagacity

POSITIONING PAPER · ARTIFACT № 2

The End of Application Security Theatre.

Tools, dashboards, and findings don't equal assurance. CyberSagacity replaces activity metrics with validated, measurable, audit-defensible intelligence.

PUBLISHED
2026

AUDIENCE
CISO · AppSec · Engineering · Audit

FORMAT
Positioning Paper

CYBERSAGACITY.COM

EXECUTIVE SUMMARY

Application security has become performative.

Organizations deploy an expanding array of Application Security Testing (AST) tools, generate massive volumes of findings, and report activity as progress — yet breaches continue to accelerate, known vulnerabilities remain unaddressed, and leaders lack defensible insight into real risk.

This is **Application Security Theatre**: the illusion of security created by tools, dashboards, and process theatre that cannot be objectively validated, financially justified, or aligned to business outcomes.

THE PROBLEM · APPLICATION SECURITY TOOLS AND PROCESSES HAVE NOT KEPT PACE WITH SOFTWARE

Software now underpins every business. Software development has changed irrevocably.

Continuous delivery
Microservices have multiplied release volume.

Cloud-native & APIs
Distributed systems have expanded attack surfaces.

AI-generated code
Defect creation is accelerating at unprecedented scale.

AI-assisted adversaries
Attackers operate with automation and AI exploitation.

Yet the mechanisms intended to secure software remain largely unchanged. Despite decades of tooling investment, the application security ecosystem continues to produce questionable, inconsistent, and often misleading results. Tools identify “findings,” not risk. They generate severity labels without context, prioritize without evidence, and provide no objective way to validate whether coverage, accuracy, or remediation effort meaningfully reduces exposure.

The gap between what organizations believe they have secured — and what attackers exploit — continues to widen.

DEFINING APPLICATION SECURITY THEATRE

The false confidence created when organizations mistake tool activity for risk reduction.

It emerges when teams are unable to do five fundamental things.

01 · Coverage

Verify the coverage or correctness of AST tool output.

02 · Severity

Distinguish true defect severity from scanner-generated noise.

03 · Impact

Link vulnerabilities to business, operational, or compliance impact.

04 · Exposure

Quantify financial exposure and loss potential.

05 · Priority

Prioritize remediation based on real, defensible risk.

The result is predictable: software ships with latent defects, attackers exploit them quickly, and post-incident analysis reveals that the vulnerabilities were “known,” misclassified, deprioritized, or ignored entirely.

This is not a tooling shortage. It is an intelligence failure.

THE EVIDENCE IS UNAMBIGUOUS

Software quality is declining. Breaches are becoming routine.

Software quality is declining

Industry research is consistent and unequivocal. Development velocity and automation have increased release frequency — not release quality. Organizations lack objective insight into defect accuracy, false positives, false negatives, or overlap across tools.

90%+

Of software contains defects. More than 50% contains serious vulnerabilities.

SOURCE · GARTNER, 2025

Breaches are becoming routine

Attackers continue to favor application-layer exploits because they offer direct access to data, identity systems, and business logic.

67%

Of organizations experienced at least one application-layer breach in the last year.

SOURCE · VERACODE, STATE OF SOFTWARE SECURITY 2025

More scanning has not produced better security outcomes.

KNOWN VULNERABILITIES DRIVE THE MAJORITY OF INCIDENTS

This is not a zero-day problem.
It is a prioritization and accuracy problem.

60%

Of breach victims were compromised via a known, unpatched vulnerability.

PONEMON INSTITUTE & SERVICENOW

62%

Of breached organizations were unaware they were vulnerable prior to the incident.

PONEMON INSTITUTE

56%

Of external attacks leverage known application vulnerabilities.

FORRESTER, STATE OF APP SECURITY 2025

Adversaries do not require novel techniques. They rely on scale, automation, and the predictable failure of organizations to correctly identify what matters.

CISA CONFIRMS THE REALITY

CISA leadership has been explicit: most exploited vulnerabilities fall into defect classes that have been understood for decades — SQL injection, broken access control, insecure deserialization, XSS, API misconfigurations.

The industry knows what is wrong. It simply cannot measure or manage it effectively.

AI IS AMPLIFYING THE FAILURE

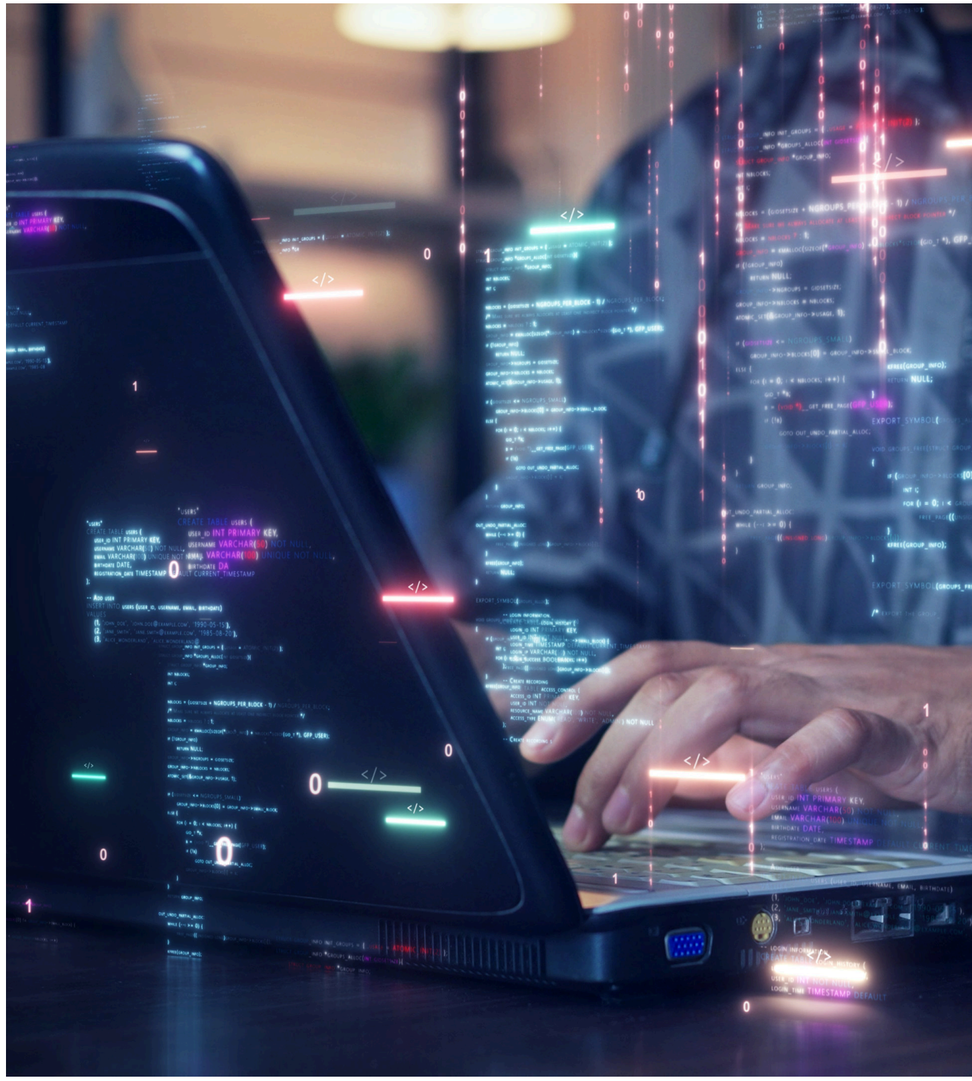
AI is now a material contributor to production systems.

AI-generated code is changing development at scale:

- AI generates **more than 25%** of new code at Google.
- Up to **30%** of Microsoft's code is AI-generated.
- Nearly **half** of AI-generated code contains insecure patterns or vulnerabilities. *(CSET, 2024)*

Generative models optimize for syntactic correctness, not secure design. They scale defect creation faster than traditional AppSec tools can evaluate accuracy or impact.

> **Application Security Theatre is not just continuing — it is accelerating.**



WHY TODAY'S APPSEC TOOLS CANNOT FIX THIS

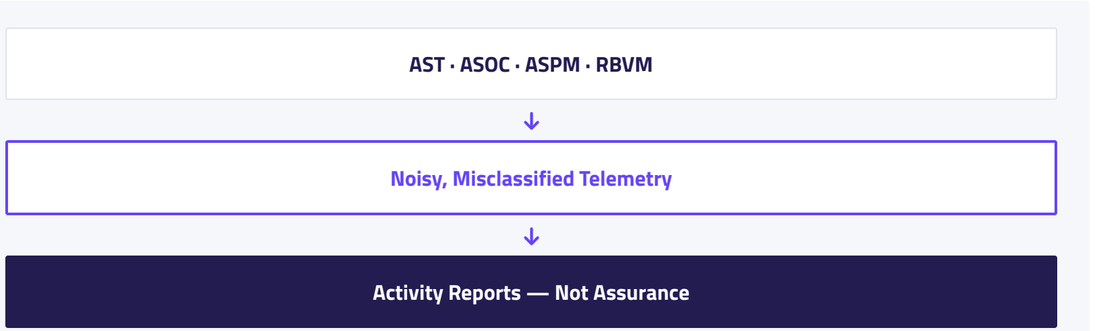
Modern AST tools are necessary — but insufficient.

They scan, label, and report. They do not validate. They do not quantify loss. They do not model exposure. They do not provide an objective standard for determining whether an AppSec program is effective.

Without an independent intelligence layer:

- There is no way to measure tool accuracy.
- No way to compare coverage across tools.
- No way to align remediation with real risk.
- No way to justify security investment in business terms.

> **In short — without intelligence, tools produce activity, not assurance.**



CYBERSAGACITY'S RESEARCH

No single tool covers more than **20%** of known vulnerabilities. Cross-tool correlation averages **less than 1%**.

THE ANSWER · CYBERSAGACITY

The only Application Security Intelligence Platform designed to end the theatre.

CyberSagacity ends this illusion. By applying statistical risk modeling, actuarial science, and business-aligned intelligence to noisy AST data, CyberSagacity delivers what the AppSec ecosystem fundamentally lacks: accuracy, verification, prioritization, and proof.

Rather than generating more findings, CyberSagacity transforms existing AST output into **validated, prioritized, and financially quantified** risk intelligence — so organizations can prove what matters, eliminate waste, and protect business value. CyberSagacity's **SATraits™** and **SATriage™** platforms apply proprietary statistical modeling and actuarial science to:

Accuracy & severity
Measure defect accuracy and severity objectively. Strip scanner noise.

Coverage gaps
Identify what scanners miss and misclassify across the full stack.

Cross-tool correlation
Correlate defects across tools and real attack paths.

Risk quantification
Quantify technical, operational, regulatory, and financial risk.

ROI-ranked priority
Rank remediation by real risk reduction and ROI.

Does not infer. Measures.
Defensible prioritization grounded in evidence — not opinion.

CONCLUSION · ENDING THE ILLUSION

The era of Application Security Theatre is over. Security you can prove has arrived.

Application Security Theatre has persisted because organizations lacked a way to independently verify effectiveness, accuracy, and impact. CyberSagacity provides that missing intelligence layer.

By delivering a single, consistent, data-driven view of application risk, CyberSagacity enables CISOs, developers, and executives to make informed decisions, demonstrate measurable risk reduction, and transform application security from a cost center into a disciplined, economically grounded control.

Without CyberSagacity	With CyberSagacity
○ AI amplifies noisy, inconsistent signals.	● AI operates on validated, high-integrity telemetry.
○ Teams chase low-value or incorrect findings.	● Remediation aligns to true risk and exploitability.
○ Critical exposure stays hidden behind tool noise.	● Hidden exposure becomes visible and measurable.
○ Security becomes a bottleneck — or an illusion.	● Security becomes faster, sharper, and defensible.

Learn more at www.cybersagacity.com →