CyberSagacity

SOLUTION BRIEF · CLOUD

# Application security in the cloud.
# Closing the shared-responsibility gap.

Cloud providers secure the infrastructure. You secure everything you run in it. Cloud doesn't reduce application security risk — it magnifies it, and the accountability is contractually, operationally, and legally yours.


PUBLISHED
2025

AUDIENCE
CISO · Cloud · AppSec · Governance

FORMAT
Solution Brief


CYBERSAGACITY.COM

THE SHARED RESPONSIBILITY MODEL

# They secure the cloud.
# You secure what runs in it.

Every major CSP — AWS, Azure, GCP, Oracle — follows the same model. Your responsibility includes:

- Code & business logic, and CI/CD pipelines.
- IAM & secrets management; data protection & encryption.
- OSS & third-party components; workload configuration.
- Proof of governance & compliance.

> **Application vulnerabilities remain your accountability — contractually, operationally, and legally.**

WHERE EXPOSURE COMES BACK TO YOU

# The CSP's liability is capped. Yours is not.

CSP contracts explicitly disclaim responsibility for customer workloads:

- CSPs do not guarantee application security.
- Misconfigurations, insecure code, and unpatched OSS are **full customer liability**.
- CSP financial exposure is contractually capped — yours is not.

Your potential losses:

- Denial of service & data exfiltration.
- Revenue impact & customer-outage fallout.
- Regulatory enforcement.
- Litigation, insurance, and board/auditor scrutiny.

THE REALITY

**Cloud doesn't reduce AppSec risk — it magnifies it.**

WHY TRADITIONAL APPSEC TOOLS FAIL UNDER SRM

# Most enterprises run 10–20 tools — and still can't prove compliance.

01
**Fragmented, conflicting results**
No two scanners agree; naming, severity, and coverage all differ.

02
**Unreliable accuracy**
False positives waste time; false negatives open exploitable holes.

03
**No business or compliance context**
Tools can't answer what matters financially, operationally, or regulatorily.

04
**No governance evidence**
Boards, auditors, and regulators require proof — not scanner noise.

**The outcome: organizations cannot demonstrate they are satisfying their SRM obligations.**

CYBERSAGACITY — THE MISSING INTELLIGENCE LAYER

# Fragmented data becomes defensible, financially grounded intelligence.

01

### Corrected & correlated defects

A unified canonical view across SAST, DAST, SCA, MAST, IAST, PenTest, and cloud findings — eliminating duplicates and contradictions.

02

### Statistical accuracy modeling

Research on millions of defects identifies false positives, false negatives, true tool coverage, and cross-tool reliability.

03

### Financial & regulatory quantification

Each defect scored by loss expectancy, business impact, and compliance exposure (PCI, HIPAA, SOX, GDPR, CMMC).

04

### Automated SRM compliance evidence

Audit-ready presentation of technical controls across AWS, Azure, GCP, and Oracle.

05

### Executive-grade reporting

CISO/board exposure summaries, CFO-grade ROI modeling, actionable engineering prioritization, and clean auditor documentation.

CYBERSAGACITY VS. TRADITIONAL APPSEC

# What separates noise from defensible evidence.

| Capability | Traditional Tools | CyberSagacity |
|---|---|---|
| Defect correlation | ✗ | ✓ |
| Accuracy modeling | ✗ | ✓ |
| Financial risk quantification | ✗ | ✓ |
| Regulatory impact mapping | ✗ | ✓ |
| SRM compliance evidence | ✗ | ✓ |
| Board / executive insight | WEAK | STRONG |
| Developer prioritization | NOISY | ACTIONABLE |

STRATEGIC VALUE

# You own application-layer risk — fully and legally.

| Without CyberSagacity | With CyberSagacity |
| --- | --- |
| ○ You cannot prove SRM compliance. | ● You see all defects clearly and focus on what matters. |
| ○ You cannot quantify exposure. | ● You reduce measurable risk. |
| ○ You cannot prioritize intelligently. | ● You strengthen governance posture. |
| ○ You cannot demonstrate AppSec ROI. | ● You establish a defensible AppSec foundation. |

THE BOTTOM LINE

CSPs secure their platforms. You own application-layer risk. CyberSagacity makes cloud AppSec clear, accurate, quantifiable, compliant, and defensible.

**Outcome-driven, evidence-backed AppSec is now foundational — CyberSagacity makes it achievable.**