CyberSagacity

WHITEPAPER · CLOUD

Application security in the cloud.
The shared-responsibility gap.

Cloud migration accelerated delivery — but it did not transfer cyber-risk to your provider. Every CSP's Shared Responsibility Model places application security squarely on you, while fragmented tools can't produce the evidence to prove it. CyberSagacity is the missing control.

PUBLISHED
2026

AUDIENCE
CISO · Cloud · AppSec · Board

FORMAT
Whitepaper

CYBERSAGACITY.COM

EXECUTIVE SUMMARY

Cloud did not transfer your risk. It magnified it.

Every major CSP — AWS, Azure, Google, Oracle — uses a Shared Responsibility Model that places full accountability for application security on the customer.

CSP contracts explicitly limit provider liability and disclaim responsibility for customer workloads. Meanwhile AppSec tools are fragmented, inaccurate, noisy, and blind to business impact — unable to produce the evidence those agreements demand.

CyberSagacity closes the gap — normalizing, correlating, ranking, and financially quantifying defects, turning AppSec into a measurable, business-aligned risk discipline.

THE CLOUD CHANGED EVERYTHING — EXCEPT WHO OWNS APPLICATION RISK

CSPs secure the cloud.
You secure what's in it.

CSP Responsibility

SECURITY OF THE CLOUD

- Global infrastructure & physical security.
- Hardware, compute, storage, networking.
- Hypervisors & virtualization layers.
- Managed-service control planes.

Customer Responsibility

SECURITY IN THE CLOUD

- Application code — business logic, defects, vulnerabilities.
- CI/CD pipelines, identity & access, configuration.
- Data protection, encryption, retention.
- OSS & third-party supply chain; DevSecOps evidence.

Applications — and the vulnerabilities within them — remain 100% the customer's responsibility. Not guidance; contractual reality.

CSPS LIMIT THEIR LIABILITY AND PLACE THE RISK ON YOU

The provider's liability is capped. Yours is unlimited.

01

No app-security guarantee

CSPs secure their platforms, not your workloads. Insecure code is not their concern.

02

Misconfig = your liability

Faulty storage permissions, misconfigured IAM, secrets in code, unpatched libraries, pipeline tampering, business-logic flaws.

03

Liability caps protect the CSP

Across AWS, Azure, Google, and Oracle, provider liability is typically capped at **12 months of fees or less**.

04

Breaches = full customer exposure

Revenue loss, customer churn, regulatory penalties, litigation, compliance failures, board scrutiny, insurance complications.

> **The cloud accelerates delivery — but does not absorb application-layer risk.**

WHY TRADITIONAL APPSEC TOOLS ARE FAILING THE CLOUD ERA

Fragmented, inaccurate, and blind to business impact.

01

Fragmentation creates chaos

SAST, DAST, SCA, MAST, IAST, ASPM, container, IaC, and cloud-posture tools all operate in silos.

02

Accuracy is unacceptable

High false positives, silent false negatives, inconsistent ontology, minimal overlap, contradictory severity.

03

No business context

Can't answer which defects are real, which carry financial exposure, or whether SRM obligations are met.

04

Cannot be governed

No enterprise can produce governance evidence across 10–20 tools without normalization, correlation, and financial assessment.

Tools aren't trusted, prioritization is guesswork, and regulators see inadequate assurance.

CYBERSAGACITY'S VALUE PROPOSITION

The intelligence layer missing from modern AppSec.

01

Corrected, correlated defect intelligence

Unifies SAST, DAST, SCA, MAST, IAST, and more into a single canonical defect record.

02

Statistical accuracy modeling

Quantifies false positives/negatives and tool reliability from tens of thousands of rules and millions of historical defects.

03

Financial & regulatory quantification

Scores each defect by business-impact likelihood, loss expectancy, and consequences (PCI, HIPAA, SOX, FFIEC, GDPR).

04

SRM compliance engine

Produces evidence that customer-side responsibilities are continuously met across AWS, Azure, GCP, and Oracle.

05

Enterprise-grade reporting

Board visibility, CFO financial translation, regulator-ready documentation, and CI/CD-integrated developer prioritization.

→

The new standard

Normalize, quantify accuracy, rank by financial risk, and generate defensible, audit-ready SRM evidence. Traditional tools cannot.

CYBERSAGACITY VS. TRADITIONAL APPSEC

What it takes to satisfy the SRM.

Capability	Traditional Tools	CyberSagacity
Defect correlation	✗	✓
Cross-tool accuracy models	✗	✓
Financial risk quantification	✗	✓
Regulatory impact mapping	✗	✓
Cloud SRM compliance evidence	✗	✓
Portfolio-level analytics	LIMITED	DEEP
Board / executive reporting	WEAK	STRONG
Developer prioritization	NOISY	ACTIONABLE

SHARED RESPONSIBILITY — AWS · AZURE · GOOGLE · ORACLE

The provider changes. The liability doesn't.

SRM element	AWS	Azure	Google	Oracle
Infrastructure security	Provider	Provider	Provider	Provider
Application security	**Customer**	**Customer**	**Customer**	**Customer**
Identity & access	**Customer**	**Customer**	**Customer**	**Customer**
Data protection	**Customer**	**Customer**	**Customer**	**Customer**
Misconfiguration risk	High	High	Moderate	Moderate
Liability coverage	Very limited	Limited	Limited	Limited
Governance expectations	Increasing	Increasing	Increasing	Increasing

> **No CSP protects you from misconfiguration — and the financial fallout is always yours.**

STRATEGIC IMPLICATIONS FOR CISOS, BOARDS & REGULATORS

You cannot outsource AppSec to your cloud provider.

- You cannot manage modern risk with decade-old tools.
- You cannot satisfy SRM obligations without correlated, accurate intelligence.
- You cannot report exposure without financial quantification.

Boards and regulators increasingly treat the inability to measure application-layer risk as a **material deficiency** — on par with poor IAM or data governance.

CONCLUSION

Cloud migration hasn't reduced application security risk — it has magnified, accelerated, and exposed it. CSP contracts make it explicit: the customer owns application-layer security and all resulting liability.

Outcome-driven AppSec is no longer optional — it is foundational. CyberSagacity provides the analytical foundation.