InfoSight
www.infosightinc.com

CLOUD SECURITY ASSESSMENTS

See every risk. Prove every control. Eliminate guesswork.

☎ 305-828-1003
✉ info@infosightinc.com

Cloud attacks are no longer edge cases.

Most involve exactly what leadership assumes is "handled by the provider": misconfigurations, machine identities, over-permissioned roles, exposed APIs, orphaned storage, unmanaged SaaS, and weak control over third parties in your tenant. Recent guidance and incident data keep confirming the pattern: cloud failures are overwhelmingly customer-side configuration, identity, and monitoring gaps—not missing features from AWS, Azure, or Google Cloud.

WHY CLOUD RISK LOOKS DIFFERENT NOW

Modern cloud estates break old security assumptions:

⚠ **Misconfiguration as the default breach path:** Public buckets, open management ports, insecure Kubernetes, unmanaged keys, disabled logging, and flat networks remain the leading cause of cloud compromise.

⚠ **Identity is the new perimeter:** Over-privileged service accounts, stale roles, token misuse, and federation missteps give attac: ers system-wide reach off a single phish or stolen credential.

⚠ **API and SaaS sprawl:** Uninventoried APIs, third-party integrations, AI services, and shadow SaaS create hidden data flows your policies never see but attackers actively probe.

⚠ **Cloud-native ransomware and data extortion:** Direct attacks on storage, databases, backups, and pipelines target the services executives assume are "resilient by default."

⚠ **Regulators and customers want evidence, not narratives:** CISA, CIS, and major cloud providers now publish prescriptive baselines; directives like BOD 25-01 and secure-by-design expectations are pushing organizations to prove they meet modern standards across tenants, workloads, and SaaS.

If your cloud environment has grown faster than your guardrails, attackers will find the misalignment before an audit does.

HIGH-SPEED CLOUD. SLOW, FRAGMENTED ASSURANCE

Most organizations:

- Depend on the shared responsibility model but lack a shared understanding internally of who owns what.
- Assume "we're fine" because core services are in AWS, Azure defaults—while IAM, logging, backups, and network controls drift.
- Run point-in-time reviews that never keep pace with new accounts, regions, services, M&A, or DevOps changes.
- Can't translate technical findings into board-ready language tied to business processes, revenue impact, or regulatory expectations.

INFOSIGHT'S CLOUD SECURITY ASSESSMENT IS BUILT TO CONFRONT THIS GAP DIRECTLY, FROM ATTACKER VIEW TO EXECUTIVE VIEW.

STANDARDS-ALIGNED, THREAT-LED, TENANT-DEEP

Our assessment is cloud-native, provider-agnostic, and aligned to:

- CIS Benchmarks for AWS and Azure
- NIST CSF 2.0, Zero Trust principles, CISA/NSA cloud security guidance, BOD 25-01/SCuBA where applicable
- Your internal policies, industry regulations, and contractual obligations

FROM ASSUMPTIONS TO DEFENSIBLE, MEASURABLE OUTCOMES.

Deliverables are provided through InfoSight's Mitigator Vulnerability & Threat Management Platform for ongoing tracking, exports, and reporting.

- **Executive risk narrative:** Plain-language summary that ties findings to business processes, customer impact, regulatory exposure, and board priorities.
- **Attack-path–driven findings:** Not just "failed checks," but mapped exploit paths: which misconfigurations, identities, and assets chain together into real scenarios.
- **Prioritized remediation plan:** Clear sequencing by business impact and attacker value, with focus on identity, configurations, and data exposure that materially reduce risk fastest.
- **Control validation and evidence pack:** Screenshots, configs, and references aligned with CIS, NIST CSF 2.0, and other frameworks to support audits, insurers, and customer security reviews.
- **Actionable guidance for your teams:** Concrete, cloud-native remediation steps your internal staff or partners can execute without guesswork.

This is a cloud assessment that proves where you stand, what breaks first, and exactly how to close it—measured, repeatable, defensible.

MITIGATOR®
VULNERABILITY & THREAT MANAGER

RELATED ASSESSMENTS

- Vulnerability & Penetration Testing for external and internal attack surface validation.
- Red Team Exercises to test detection and response across hybrid and cloud-native paths.
- Code, Mobile & API Security Testing to secure the applications and services your cloud relies on.
- Social Engineering Assessments to connect identity, access, and user behavior risk to your cloud exposure.

TAKE THE NEXT STEP

Turn hidden cloud misconfigurations into verified fixes—schedule your Cloud Security Assessment with InfoSight.

KEY COMPONENTS (TAILORED PER CLIENT ENVIRONMENT):

Cloud Asset and Exposure Mapping
Full discovery across accounts, subscriptions, regions, VNets/VPCs, containers, serverless, data stores, identities, and external attack surface to expose unknown assets, shadow IT, and stale resources.

Identity, Access, and Privilege Analysis
Deep review of IAM design, roles, groups, policies, keys, tokens, SSO/federation, workload identities, Just-In-Time access, and admin boundaries. Flags privilege escalation paths, toxic combinations, and abuse-ready permissions.

Data Protection and Storage Controls
Validation of encryption at rest/in transit, KMS usage, key management, public exposure, backup robustness, retention, and segmentation for sensitive and regulated data.

Network and Segmentation Effectiveness
Assessment of security groups, NACLs, private endpoints, ingress/egress controls, service endpoints, peering, and isolation between environments (prod/non-prod/third-party). Identifies lateral movement paths an attacker would actually use.

Logging, Detection, and Telemetry Readiness
Verification of cloud-native logging (CloudTrail, Activity Logs, etc.), audit coverage, retention, and integration with your detection stack. Identifies blind spots that turn small incidents into prolonged compromises.

Configuration Benchmarking and Hardening
Automated and manual comparison against CIS Benchmarks and leading practices. Pinpoints misconfigurations with clear mapping to risk, exploitability, and compliance impact.

DevOps, CI/CD, and API Review
Inspection of pipelines, secrets management, images, IaC, API gateways, service mesh policies, and deployment patterns to ensure "secure by default" at build and release.

Third-Party, SaaS, and Marketplace Risk
Validation of how external services integrate with your tenant: scopes, tokens, consent, and controls that prevent partners and tools from becoming your weakest link.

Execution is performed by senior security engineers and architects with real-world offensive and defensive experience—not automated reports pushed from a tool.

WHY INFOSIGHT?

✓ **Deep experience** across regulated industries where cloud mistakes are material, not theoretical.

✓ **Expertise spanning offensive testing,** architecture, compliance, and operations—no siloed view.

✓ **Independent validation:** we measure your controls against modern attacker behavior and authoritative baselines, not vendor marketing.

✓ **Delivered and tracked via Mitigator, giving leadership a single pane of glass for posture, trends, and remediation progress.**