eSurelTy

AZURE & AWS SECURITY ASSESSMENTS

Uncover hidden risks and compliance gaps in Azure/AWS—before attackers and auditors do.

Why Cloud Security Can't Be Assumed

Cloud breaches are driven by preventable issues: misconfigured storage, weak access controls, and exposed APIs. Under the shared responsibility model, Azure and AWS secure the cloud infrastructure; your team is responsible for securing data, identities, and configurations.

eSurelTy's Azure and AWS Security Assessments expose those weaknesses and align your environment with CIS Benchmarks and frameworks such as HIPAA, PCI DSS, ISO 27001, and NIST 800-53.

Cloud Complexity and Hidden Risk

The rapid adoption of multi-cloud and hybrid environments introduces blind spots:

- Misconfigurations: Insecure storage, open ports, and public-facing assets.
- IAM Weaknesses: Overly permissive roles, inactive accounts, and poor key management.
- API Vulnerabilities: Exposed endpoints enabling unauthorized access and data exfiltration.
- Compliance Drift: Untracked policy changes that break alignment with internal standards and external frameworks.
- Cloud Sprawl: Unmanaged assets increasing exposure without visibility or ownership.

Even with reputable providers, your configuration choices determine your real security posture.

Azure & AWS Security Aligned to CIS Benchmarks

eSurelTy follows the Center for Internet Security (CIS) Benchmark standards to deliver a structured assessment that stands up to technical scrutiny and executive review.

Our Methodology Includes:

Environment Discovery

- Inventory Azure and AWS resources, subscriptions, accounts, regions, and connected services.

Network & Firewall Audit

- Assess network segmentation, security groups, routing rules, exposed services, and entry points.

CIS Benchmark Alignment

- Compare current configurations against CIS-recommended baselines for each platform and service.

Logging & Monitoring Review

- Evaluate audit logging, security event collection, alerting configuration, and log retention.

Identity & Access Review

- Validate least-privilege implementation, MFA enforcement, and role-based access control.

Compliance Verification

- Map findings to HIPAA, PCI DSS, ISO 27001, and NIST 800-53 controls to support audit readiness.

Data Security Analysis

- Confirm encryption in transit and at rest, key management practices, backup policies, and data retention.+-

Actionable Reporting

- Deliver a prioritized remediation roadmap tied to measurable risk reduction and clear ownership.

Contact Us

info@eSurelTy.com

www.eSurelTy.com

Deliverables That Strengthen Security and Coverage

Cloud Security Assessment Report (PDF & Interactive)

- Current-state overview of your Azure and/or AWS environment.
- CIS Benchmark scores and control coverage views.
- Detailed list of misconfigurations, vulnerabilities, and risky patterns.
- Executive summary that translates technical risk into business impact.

Remediation & Governance Plan

- Action plan categorized by risk level and implementation effort.
- Policy and standards recommendations for IAM, encryption, network segmentation, and access governance.
- Guidance on integrating findings into change management and configuration baselines.

Continuous Improvement Roadmap

- Options for periodic reassessment to confirm progress and prevent drift.
- Recommendations for automation, guardrails, and monitoring to sustain hardening efforts.

Why Choose eSurelTy

- CIS Benchmark expertise – Deep experience applying CIS controls to real-world Azure and AWS deployments.
- Certified professionals – CISSP, CISA, CEH, OSCP, and cloud-certified engineers working directly on your engagement.
- Platform-agnostic depth – Strong coverage across Azure, AWS, and hybrid architectures.
- Real-world cloud experience – Findings prioritized based on exploitability and business impact, not just theoretical risk.
- Actionable reporting – Outputs written for both technical teams and executives, enabling fast decision-making and remediation.
- Ongoing partnership – Availability for retesting, validation of fixes, and advisory support as your environment evolves.

What You Gain

An Azure & AWS Security Assessment from eSurelTy provides::

- Verified alignment with CIS Benchmarks and major security frameworks.
- Reduced likelihood and impact of cloud breaches caused by preventable errors.
- Stronger, evidence-backed documentation for internal and external audits.
- Clear visibility into critical misconfigurations, identity risks, and exposed services.
- A practical, ordered plan for remediation that your teams can execute.
- For organizations that carry cyber insurance, the assessment generates the cloud control evidence carriers increasingly expect to see when validating coverage requirements.

Strengthen Your Cloud Security Posture

Identify, quantify, and reduce risk in your Azure or AWS environment with a focused Cloud Security Assessment and a clear snapshot of your most critical vulnerabilities.

Schedule your Azure & AWS Security Assessment

Contact Us

info@eSurelTy.com

www.eSurelTy.com