Service Overview

SynAck Solutions provides comprehensive security evaluation across AWS, Google Cloud Platform, Microsoft Azure, and hybrid cloud environments. We go beyond automated CSPM scanning with expert-led review of cloud architecture, IAM configuration, network segmentation, data protection controls, Infrastructure as Code templates, and workload security — including inter-cloud trust relationships and hybrid connectivity.

Business Value

- Identify misconfigurations and security gaps across AWS, Azure, GCP, and hybrid environments
- Validate IAM policies follow least-privilege and contain no privilege escalation paths
- Ensure network segmentation effectively isolates workloads and data tiers
- Assess Infrastructure as Code templates for security issues before they propagate
- Verify data protection controls meet regulatory requirements for encryption and key management
- Evaluate identity federation and cross-cloud trust for authentication weaknesses
- Support compliance under APRA CPS 234, ISO 27017/27018, and the Privacy Act 1988

What's Included

- Multi-cloud architecture review covering AWS, Azure, GCP, and hybrid connectivity
- IAM deep-dive: role analysis, privilege escalation paths, and service account review
- Identity federation assessment: SAML, OIDC, cross-cloud trust, and MFA enforcement
- Network security review: VPC/VNet design, security groups, peering, and private endpoints
- Data protection assessment: encryption (KMS, CMK, SSE), key rotation, and access logging
- Infrastructure as Code review: Terraform, CloudFormation, Bicep, and Pulumi templates
- Container and Kubernetes security: EKS, AKS, GKE configuration, RBAC, and pod security
- Serverless assessment: Lambda, Azure Functions, Cloud Functions execution roles and secrets
- Logging and monitoring review: CloudTrail, Azure Monitor, GCP Cloud Audit Logs
- CIS Benchmark compliance assessment for each in-scope cloud platform
- Detailed technical report with risk-rated findings and remediation guidance

Scope

The assessment covers cloud environments as agreed during scoping. Multi-cloud, single-cloud, and hybrid configurations are all supported.

- AWS accounts: IAM, VPC, S3, EC2, RDS, Lambda, EKS, CloudTrail, and GuardDuty
- Azure subscriptions: Entra ID, VNets, Storage, VMs, App Services, AKS, and Monitor
- GCP projects: IAM, VPC, Cloud Storage, Compute, Cloud SQL, GKE, and Audit Logs
- Hybrid connectivity: VPN, ExpressRoute, Direct Connect, and Cloud Interconnect
- Infrastructure as Code repositories used for environment provisioning
- Container orchestration: EKS, AKS, GKE clusters and container registries

What's Excluded

- Penetration testing of cloud-hosted web applications (available separately)
- Remediation of identified issues — guidance provided; hands-on remediation available separately
- Cloud cost optimisation and FinOps analysis
- Migration planning or cloud architecture design services
- SaaS application configuration review (M365, Salesforce — available separately)
- Source code review of applications deployed on cloud infrastructure

Methodology

Our methodology aligns with CIS Benchmarks for AWS, Azure, and GCP, the NIST Cybersecurity Framework, ISO 27017, and the CSA Cloud Controls Matrix. Automated CSPM scanning is complemented by manual expert review. Findings are risk-rated based on exploitability and data exposure impact, mapped to APRA CPS 234 and ASD Essential 8.

Engagement Timeline

A typical multi-cloud assessment completes within three to five weeks depending on the number of cloud accounts and architecture complexity. Detailed report and executive summary delivered within ten business days. Remediation re-assessment available within 90 days.

Get Started

Contact SynAck Solutions to schedule a multi-cloud security assessment. We'll map your cloud footprint, define priorities, and deliver a clear picture of your security posture across every environment.

info@synack.au | https://www.synack.au

ABN 88 667 784 956