Service Overview

SynAck Solutions delivers comprehensive security assessments of Microsoft Azure, Office 365, and Entra ID (Azure AD) environments. Our certified operators evaluate your cloud tenant configuration, identity and access management, data protection controls, and IaaS workload security against Microsoft security baselines and industry best practices to identify misconfigurations and security gaps before they are exploited.

Every engagement covers the full Microsoft cloud stack — from Entra ID identity configuration and conditional access policies through Office 365 collaboration security to Azure IaaS resource exposure and network segmentation. We assess your environment as an attacker would, identifying privilege escalation paths, data exfiltration risks, and lateral movement opportunities across your cloud estate.

Business Value

- Identify misconfigurations across Entra ID, Office 365, and Azure IaaS before breach
- Validate conditional access policies, MFA enforcement, and privileged identity controls
- Assess data protection: sharing policies, DLP rules, and sensitivity labelling effectiveness
- Meet compliance obligations: ISO 27001, Essential Eight, APRA CPS 234, ACSC Cloud Guidelines
- Detect over-permissioned service principals, app registrations, and managed identities
- Evaluate Azure network security: NSGs, firewalls, private endpoints, and public exposure
- Receive prioritised remediation guidance mapped to Microsoft Secure Score and CIS benchmarks

What's Included

- Entra ID configuration review: authentication methods, password policies, and legacy protocols
- Conditional access policy assessment: coverage gaps, bypass conditions, and MFA enforcement
- Privileged identity review: PIM configuration, standing admin access, and role assignments
- App registrations and service principal permission audit
- Office 365 security: Exchange Online, SharePoint, OneDrive, and Teams configuration
- Email security: anti-phishing, anti-malware, Safe Links, Safe Attachments, DMARC/DKIM/SPF
- Data protection: external sharing policies, guest access, and DLP rule effectiveness
- Azure IaaS: virtual machine security, storage account exposure, and key vault configuration
- Network security: NSGs, Azure Firewall, private endpoints, and public IP exposure
- Branded report: executive summary, findings, CIS benchmark mapping, remediation guidance
- Delivery in four formats: Word, PDF, interactive HTML, and Google Doc

Assessment Coverage

The engagement covers your Microsoft cloud environment across three pillars:

- Entra ID (Azure AD): tenant configuration, authentication, conditional access, PIM, app registrations, B2B/guest access, directory roles, and identity protection policies
- Office 365: Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, and Microsoft 365 Defender configuration
- Azure IaaS: subscriptions, resource groups, virtual machines, storage accounts, networking, key vaults, managed identities, and RBAC assignments

Multi-tenant and hybrid (on-premises AD + Entra ID) environments are supported.

What's Excluded

- Internal or external network penetration testing (available separately)
- Web application penetration testing (available separately)
- AWS or GCP cloud assessments (available as separate engagements)
- Social engineering or phishing campaigns
- Implementation of remediation changes (advisory and guidance provided)
- Ongoing continuous monitoring (advisory on tooling and configuration provided)

Methodology

Our methodology aligns with the CIS Microsoft Azure Foundations Benchmark, CIS Microsoft 365 Foundations Benchmark, and the ACSC Cloud Security Guidelines. Assessment covers identity security, data protection, workload hardening, network controls, and logging/monitoring. Findings are mapped to CIS controls and Microsoft Secure Score recommendations.

Engagement Timeline

A typical assessment runs 5-10 business days depending on tenant complexity and number of subscriptions. Final report delivery within 5 business days of assessment completion. Re-assessment of remediated findings available within 30 days at 30% of initial engagement cost.

Get Started

Contact us to discuss your environment and receive a tailored proposal. We will assess your tenant scope, agree on read-only access requirements, and schedule the assessment at a time that suits your operations.

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

ABN 88 667 784 956