SERVICE BRIEF

# Azure Security.

An independent CIS-benchmarked assessment of your Azure security posture.

THE PROBLEM & THE APPROACH

**Azure tenants accumulate misconfigurations and silent risk over time. Without a structured review, it is hard to see where the real exposure sits.**

**CNNECT's Azure Security Assessment** delivers a CIS-benchmarked review of your Azure subscriptions covering identity, network, storage, compute, database, keys, logging, and governance with status, evidence, and remediation guidance for every finding.

## Key challenges addressed

EIGHT COMMON RISKS

01 Privileged accounts and admins without MFA or conditional access.

02 Storage accounts and databases exposed to public networks.

03 Network security groups permitting unrestricted inbound access.

04 Encryption gaps across data services, disks, and storage tiers.

05 Key Vault secrets and certificates lacking rotation or RBAC scoping.

06 Diagnostic logging, audit retention, and Defender coverage gaps.

07 Guest users and over-privileged role assignments unreviewed.

08 No mapping of the estate to a recognised security benchmark.

SERVICE OVERVIEW

# An objective view of your Azure posture.

This assessment evaluates your Azure subscriptions against the CIS Microsoft Azure Foundations Benchmark a recognised industry standard covering identity, governance, network, storage, compute, database, keys, monitoring, and logging.

Every control is tested against the live state of your tenant. Findings are recorded with status, evidence, and remediation context an objective view of your posture.

PHASE 01 · DISCOVERY

## Discovery

We confirm subscriptions, tenants, and management groups in scope, establish secure read-only access, and map the environment to be assessed.

- Subscription & tenant inventory
- Read-only access provisioning
- Scope confirmation & signoff
- Control framework mapping

PHASE 02 · ASSESSMENT

## Assessment

We evaluate every subscription against the CIS Microsoft Azure Foundations Benchmark covering identity, network, storage, compute, database, keys, logging, and governance.

- CIS Benchmark control execution
- Evidence capture per finding
- Severity & status classification
- Prioritised remediation guidance

TYPICAL TIMELINE

**2 – 3 weeks**

From kick-off to delivered findings report.

INVESTMENT

**From £4,750**

Final price agreed after scoping.

WHAT'S INCLUDED

FIVE DELIVERABLES

01 Scoping document 02 Findings report 03 Executive summary 04 Remediation guidance 05 Findings review

NEXT STEPS

## Discuss your environment or request an example findings report.

**hello@cnnect.com**

**+44 20 7173 5320**

CNNECT.COM