

Overview: Assessment of Microsoft 365, Azure, and Entra ID

Assess

Assessment of Microsoft Entra ID

Overview: Rapid, holistic assessment using insights from interviews and automated vulnerability assessment

- Domain, forest, and trust configurations
- Authentication controls, Azure IAM, Authenticator / MFA
- Secure Kerberos configuration
- Group policy security
- Use of Azure Active Directory Identity Protection, Identity Governance, and Conditional Access Policies

Assessment of Microsoft 365 and Azure Security Posture

Overview: Assessment using both best-practice frameworks (like CIS) and proprietary KS measurements

- Use of Microsoft Purview (data protection)
- Azure / Microsoft 365 alerting and logging configuration
- Use of Microsoft Defender (suite)
- Security of App Service, APIs, and external integrations
- Use of native features (e.g., Defender for Cloud) to protect workloads and groups

Report



Maturity ratings across the assessed scope to provide an independent benchmark for future assessments

Both Azure and Active Directory

High Priority - Enhance access review processes: augment the existing Azure account review process with Azure Access Reviews to formalize and document reviews of privileged Azure AD and subscription-level roles. Additionally, expand on-premises AD reviews to consider permissions (e.g. Domain Admin membership), not just account visibility / existence.

Active Directory

High Priority - Harden group more exposure domain permissions accounts that are severely exposed.

High Priority - Harden Domain print spooler and ensure DC authentication protocols.

Azure

Low Priority - Improve account and remove stale accounts (e.g. admin).

Low Priority - Use Azure management where possible.

Low Priority - Enable and (policy creation, security group to defined monitoring and

Low Priority - Harden and protect App Service Apps as access as well as requiring it

AZURE ASSESSMENT

This assessment evaluates the security posture CIS three subscriptions, PROD, CORE, and NON-PROD, using the Center for Internet Security's (CIS) Azure Benchmark (Azure Benchmark). The Azure Benchmark categories covered for each are summarized below.

CATEGORY	CORE	PROD	NON-PROD
Identity and Access Management			
Microsoft Defender for Cloud			
Storage Accounts			
Database Services			
Logging and Monitoring			
Networking			
Virtual Machines			
Key Vault			
App Service			

X Section and findings included below

N Not included - addressed by PROD subscription

Y Not included - compliant or no relevant findings

Z Not included - Azure service not used or N/A

Security assessment report, targeted based on nature of compromise – delivered as detailed findings and executive summarizations