METIS SECURITY

MICROSOFT 365 SECURITY ASSESSMENT

WHAT WE CHECK. WHAT WE FIND.

Control Domain	Most Common Misconfiguration	Secure Score
Conditional Access	One or more policies in report-only mode - actively enforcing nothing whilst appearing active on every dashboard.	Passes
Data Loss Protection	Policies in simulation mode across one or more workloads - monitoring activity but enforcing no controls.	Passes
Email Authentication	DMARC record present but policy set to p=none - monitoring only, no rejection or quarantine of spoofed email.	Passes
Privileged Identity Management	Standing global admin assignments present since tenant creation - no just-in-time activation, no approval requirement.	Passes
Guest Access Governance	Guest accounts with no review in 12+ months, often with access to sensitive content. No expiry policy configured.	Not flagged
Device Compliance	Compliance policies exist but coverage gaps leave a material proportion of devices unevaluated - enrolled but not assessed.	Partial
Legacy Authentication	Legacy authentication protocols active at tenant level - enabling credential-based attacks that bypass MFA entirely.	Passes
SMTP Authentication	SMTP AUTH enabled at tenant level, allowing client applications to authenticate directly and bypass modern auth controls.	Not flagged
SharePoint External Sharing	Anonymous sharing links with no expiry. Site-level overrides more permissive than tenant policy - often unreviewed.	Not flagged
Audit Logging	Default audit log retention period insufficient for meaningful incident investigation at current licence tier.	Not flagged
Sensitivity Labels	Label taxonomy exists in the tenant but labels not published to users - no classification, no DLP dependency, no protection.	Not flagged
Defender for Office 365	Default anti-phishing policy in use rather than standard or strict preset - materially lower protection against impersonation.	Passes
Cloud App Security (CASB)	CASB licensed and connected but no session or access policies configured - app discovery running, governance absent.	Not flagged

Secure Score legend: Passes = misconfiguration is invisible to Secure Score and passes all internal dashboards. **Not flagged** = not surfaced by any automated tooling. Partial = partially visible.

A healthy Secure Score is not evidence of a secure environment. It is evidence that certain features are present. These are different things, and the difference matters.

Want to know which of these apply to your environment?

The answer is one conversation away.

https://www.metis-security.co.uk
david@metis-security.co.uk

Fixed price. One week. Personally delivered