METIS SECURITY

MICROSOFT 365 SECURITY

FIVE QUESTIONS WORTH ANSWERING

Can you confirm that every Conditional Access policy in your Microsoft 365 tenant is actively enforcing?

1

The honest answer usually is...

"I believe so, but I haven't checked recently. The policies are all enabled in the portal. " Enabled is not the same as enforcing. Report-only mode is enabled. It blocks nothing.

What good looks like

Every policy in scope is in Enabled state - not Report-only. Coverage has been reviewed to confirm no users, applications, or sign-in locations fall outside all active policies.

Can you confirm that your Data Loss Prevention policies are in enforcement mode — not simulation?

2

The honest answer usually is...

"We have DLP policies configured." Configured is not enforcing. Simulation mode policies observe and report. They block nothing and stop nothing. Both pass Secure Score

What good looks like

Policies are in Enforce mode, not Simulate, across all relevant workloads - Exchange, SharePoint, OneDrive, Teams, and Endpoint. Coverage gaps have been reviewed.

When were your guest and external accounts last reviewed - and how many have you got?

3

The honest answer usually is...

"I'm not sure of the exact number. They were reviewed at some point." Guest accounts accumulate silently. In most tenants assessed, a significant proportion have not been reviewed in over 12 months.

What good looks like

Guest account population is known, reviewed within the last 90 days, access expiry policies are configured, and access reviews are running in Entra ID.

Does your DMARC record have a policy of p=quarantine or p=reject - or is it set to p=none?

4

The honest answer usually is...

"We have a DMARC record." A DMARC record at p=none monitors email. It does not reject spoofed messages, does not quarantine them, and does not protect recipients. Most records assessed are at p=none.

What good looks like

DMARC is at p=quarantine or p=reject. SPF and DKIM are aligned. The DMARC reporting address is monitored. Subdomain policy is explicitly defined.

Has your M365 security configuration been independently assessed in the last 12 months?

5

The honest answer usually is...

"Our IT provider reviews it regularly." Your IT provider cannot independently verify their own configuration. Independent means no commercial interest in the outcome - not your MSP's opinion of their own work.

What good looks like

An independent, documented assessment has been conducted within the last 12 months by a practitioner with no commercial relationship with your IT provider. A written report exists and findings have been actioned.

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