METIS SECURITY

MICROSOFT 365 SECURITY ASSESSMENT

INDEPENDENT CONTROL VERIFICATION

THE PROBLEM

Your firm pays Microsoft every month for security capabilities that came with your licence.

Your IT provider configured those capabilities and told you they are working. Your Secure Score looks healthy.

None of that tells you whether your security controls are actually working.

Secure Score measures the presence of features, not whether those features are correctly configured or actively enforcing. A Conditional Access policy in report-only mode - blocking nothing - passes Secure Score. A DLP policy in simulation mode - enforcing nothing - passes Secure Score. The dashboard that reassures you every morning is measuring the wrong thing.

Your managed service provider cannot tell you either. Not because they are dishonest - but because they configured the environment, they manage it, and they invoice for it. The structural conflict of interest is irresolvable. Their assessment of their own work is not independence. It is reassurance.

THE STAKES

For a professional services firm, the consequences of this gap being exploited are not abstract.

For Partners

- Client confidential data exposed
- Professional indemnity exposure
- Regulatory censure - SRA, FCA, ICO
- Reputational damage to the firm

A breach does not stay in the IT department

For IT Directors

- Career exposure if a gap was knowable
- No independent validation on record
- MSP findings cannot be independently trusted
- Secure Score gives false confidence

Knowing is better than assuming.

For Operations

- Insurance renewal requires evidence of effectiveness
- Client ask harder questions every year
- Copilot deployment amplifies gaps
- Due diligence must be documentable

Evidence, not assertion.

SECURE SCORE

What Secure Score sees
Score: Healthy

- Conditional Access policy - present
- DLP policy - present
- DMARC record - present
- MFA enabled - present

What is actually happening
Reality: Exposed

- Policy in report-only mode - enforcing nothing
- Policy in simulation mode - blocking nothing
- DMARC at p=none - rejecting nothing
- MFA enabled but not enforced via Conditional Access

METIS SECURITY

THE SOLUTION

The Metis Security M365 assessment is an independent, fixed-price configuration review of your Microsoft 365 security controls — personally delivered by a practitioner with 27 years of relevant experience.

What is assessed

Identity and access management, Conditional Access policy configuration and coverage, Privileged Identity Management, device compliance, email security (SPF, DKIM, DMARC, anti-phishing, Safe Links, Safe Attachments), data loss prevention, sensitivity labels, guest and external access governance, cloud app security where deployed, audit logging and sign-in log retention.

What is delivered

A complete written report: executive summary for partners and directors in plain language; technical findings by control domain; remediation guidance for every finding. Everything needed to act, in one document.

What is not included

Remediation delivery. Attack simulation. Per-file or per-site content audits. Deep DLP logic review. Microsoft Sentinel architecture assessment. These are available as separate, properly scoped engagements.

Timeline

Standard engagements complete within one working week. Larger estates (700+ users) typically require a second week. Start date agreed within one week of engagement confirmation.

THE PROOF POINTS

Independence

We do not configure environments, nor sell Microsoft licences, and do not manage ongoing services. No stake in any outcome other than an accurate picture.

Fixed Price

The fee is agreed at scoping and does not change. No day-rate negotiations. No supplementary invoices for overruns within agreed scope. No ambiguity about what the engagement will cost.

Personal Delivery

The person who scopes your engagement, conducts the assessment, writes the report, and presents the findings is the same person. No briefing chain. No handoff. No dilution.

Complete Deliverable

Executive summary for leadership. Technical findings for the IT team. Remediation guidance for every finding. One document that contains everything needed to understand the posture and act on it.

27 Years of Experience

CISSP since 2002. ISSAP since 2004. Microsoft Security certifications across the full stack. Career spanning NCC Group, BT, IBM ISS X-Force, Security Alliance, and NGS Software.

A Fraction of Licensing Spend

For any firm with 200 or more licensed M365 users, the assessment fee is less than half of what you pay Microsoft in a single month. For larger estates, the proportion falls further still.

HOW IT WORKS

01 SCOPING CONVERSATION

Five questions. User count, primary licence type, deployed workloads, any specific concerns, preferred timing. Fixed-price proposal the same day.

02 ASSESSMENT

One working week. Full review of every material control domain. Read-only access. No data leaves your environment. Interim reporting for larger estates.

03 REPORT AND DEBRIEF

Written report with executive summary and technical findings. Remediation guidance for every finding. Debrief call with David Morgan.

PRICING

For any firm with 200 or more licensed users, the assessment fee is less than half of your monthly Microsoft 365 licensing spend. Pricing is confirmed in the scoping conversation based on your specific environment and licensing profile.

Start with a conversation.

Five questions. Fixed-price proposal the same day. David Morgan will speak with you directly.

david@metis-security.co.uk