MICROSOFT 365 SECURITY

Microsoft 365 security assessment.

Understand how identities, access policies and managed devices contribute to your Microsoft 365 security posture. Turn the available evidence into priorities your IT team and leadership can use.

HOW IT WORKS

1. **Scope and authorise.**
   Agree the authorised tenant, the questions that matter to your team and the read-only Microsoft consent needed to collect evidence.
2. **Collect read-only evidence.**
   Gather identity, access, policy, device and available activity signals without changing anything in the tenant.
3. **Analyse against references.**
   Review the observed conditions against CIS-aligned and NIST CSF references, and record where a feed is unavailable as a coverage gap.
4. **Prioritise with owners.**
   Turn findings into leadership priorities and technical actions, naming the affected identities, policies or devices for each one.
5. **Confirm and re-collect.**
   Authorise any change through your own process, then collect fresh evidence at the next review to check the outcome.

CONDITIONS A MICROSOFT 365 ASSESSMENT CAN SURFACE

- Stale or unused accounts, and privileged accounts that no longer need their level of access.
- MFA registration gaps across users and administrators — registration is not the same as MFA being enforced at every sign-in.
- Broad or unreviewed application (OAuth) consent grants and long-lived client secrets.
- Conditional Access coverage gaps for administrators, legacy authentication or risky sign-ins.
- Device-compliance and Intune posture inconsistencies measured against your own policy.
- External SharePoint or file-sharing exposure that has not been reviewed.
- Microsoft Secure Score movement read alongside the underlying identity, policy and device evidence.

Each item is a reason to review the affected accounts, policies or devices — not a proof of compromise. What is included depends on the agreed scope and the feeds your tenant makes available.

Framework alignment. The assessment organises Microsoft 365 findings against widely used references so a technical team and its leadership can discuss the same baseline. It draws on CIS-aligned control references and NIST Cyber Security Framework perspectives, and the results can inform a UK Cyber Essentials review of user access, multi-factor authentication and device controls.

Start with an authorised, read-only scope

Begin with your assessment questions; we agree coverage and delivery before any commitment.

threatshield@threatshield.global
Read the full page ↗

ThreatShield is part of ITS Consulting — ITS Consulting Ltd (United Kingdom) and ITS Consulting LLC (United States). This guide summarises an assessment capability; the actual scope, coverage and evidence available depend on your environment, licensing and permissions. Framework references organise findings and are not a certification or an assurance that a control is effective. © 2026 ThreatShield.