nettko



# M365 Security Health Check

An independent review of your Microsoft 365 security posture

## Purpose

Most organisations run Microsoft 365 with a mix of default, inherited and inconsistently applied security settings. Each gap is a potential entry point for phishing, account takeover, business email compromise or data leakage, and most go unnoticed until something goes wrong.

The **M365 Security Health Check** is a quick, structured review of how your Microsoft 365 tenant is configured against Microsoft's recommended security baseline. We assess 81 controls from the Microsoft Security Framework, identify what needs remediation and in what order, and provide a clear quote to fix it.

### At a Glance

| Item | Detail |
|---|---|
| **Framework** | Microsoft Security Framework – 81 baseline controls. |
| **Scope** | Microsoft 365 tenant security configuration: Entra ID, Exchange Online, SharePoint, Teams, Defender for Office 365 and Purview. |
| **Approach** | Read-only assessment. No changes are made to your environment. |
| **Your time** | Approximately 45 minutes in total. |
| **Turnaround** | Findings and quote delivered within five business days of access being approved. |
| **Outcome** | A remediation report and a fixed quote to resolve the findings. |

### How It Works

- **Connect** – Your Global Administrator approves access to your Microsoft 365 tenant. This takes around 10 minutes and we guide you through it.

- **Assess** – We assess 81 controls against the Microsoft Security Framework. Controls that depend on licences you do not hold are identified separately.
- **Analyse** – A Nettko security consultant reviews the results, ranks the risks and scopes the work required to remediate them.
- **Report & Quote** – We walk you through the findings in a 30-minute session and provide a remediation report with a quote for the fixes. Our access is then removed.

## What We Assess

| Area | Controls | Examples of what we check |
|---|---|---|
| **Microsoft Entra ID** | 19 | MFA coverage, legacy authentication, administrator roles, sign-in and password policies, guest and application access. |
| **Exchange Online** | 9 | Mailbox auditing, automatic external forwarding, modern authentication and mail flow. |
| **SharePoint & OneDrive** | 5 | External sharing levels, default sharing links and guest access to files. |
| **Microsoft Teams** | 6 | External and guest access, anonymous meeting participation and unmanaged accounts. |
| **Defender – Anti-Phishing** | 12 | Impersonation protection, spoof intelligence and mailbox intelligence. |
| **Defender – Anti-Spam** | 17 | Inbound and outbound spam policies, quarantine and user notifications. |
| **Defender – Anti-Malware** | 2 | Blocking of risky attachment types and malware notifications. |
| **Defender – Safe Attachments** | 4 | Sandbox detonation of attachments before delivery. |
| **Defender – Safe Links** | 2 | Time-of-click scanning of links in email and Office apps. |
| **Microsoft Purview** | 5 | Unified audit logging and data protection settings. |
| **Total** | **81** | |

## What You Receive

- **Executive summary** – Your overall alignment with the Microsoft Security Framework, in plain business language.
- **Results by area** – Passed and failed controls for each product area, showing where exposure is concentrated.

- **Remediation priorities** – The items that need fixing, ranked by risk and the likely impact on your users, including quick wins.
- **Full control checklist** – The status of all 81 controls assessed.
- **Remediation proposal** – A fixed proposal for Nettko to implement the recommended changes in a phased, controlled manner with minimal disruption.

## Scope and Limitations

- A point-in-time, read-only review of Microsoft 365 configuration settings. It does not access the content of email, files or chats.
- It is not a penetration test, vulnerability scan or formal compliance audit, and does not certify alignment with the Essential Eight, ISO 27001 or any other standard.
- Devices, servers, on-premises infrastructure, Azure workloads and third-party applications are outside scope.
- Your report is confidential and shared only with your nominated contacts. Nettko access is removed once the review is complete.