rasotec

FREE CHECKLIST

Microsoft 365 and Entra ID Hardening Checklist

The settings attackers look for first: identities, admin roles, app consent, sharing and email

Most Microsoft 365 compromises start with a stolen password, a malicious app consent or an over-privileged account, not with a software vulnerability. Use this checklist to review the most important settings of your tenant. Items marked P1, P2 or MDO require Entra ID P1, Entra ID P2 or Microsoft Defender for Office 365 licenses. For a complete baseline, see the CIS Microsoft 365 Foundations Benchmark.

1 Sign-in and authentication

- [ ] **MFA for all users,** enforced with Conditional Access (P1) or, without P1 licenses, with security defaults.
- [ ] **Phishing-resistant MFA for administrators:** FIDO2 security keys, passkeys or Windows Hello for Business.
- [ ] **Legacy authentication blocked** with Conditional Access, and SMTP AUTH disabled for mailboxes that do not need it.
- [ ] **Entra ID Password Protection** with a custom banned-password list (company name, products, locations).
- [ ] **Sign-in risk and user risk policies** that require MFA or a password change (P2).

2 Privileged access

- [ ] **Fewer than five Global Administrators;** everyone else uses the least-privileged role that fits the task.
- [ ] **Separate cloud-only admin accounts** without a mailbox, not used for daily work.
- [ ] **Just-in-time admin roles** with Privileged Identity Management, including approval for the most critical roles (P2).
- [ ] **Two emergency access (break-glass) accounts** with strong credentials, excluded from Conditional Access, and every sign-in alerted.
- [ ] **Regular access reviews** of admin roles, guest accounts and inactive users.

3 Applications and consent

- [ ] **User consent restricted** to verified publishers and low-risk permissions, with the admin consent workflow enabled for everything else.
- [ ] **Enterprise apps and app registrations reviewed** for high-privilege permissions such as Mail.ReadWrite or Directory.ReadWrite.All.
- [ ] **Unused apps and expired or unused client secrets removed;** certificates or managed identities preferred over secrets.
- [ ] **Owners of app registrations reviewed,** since an owner can add new credentials to the app.

4 Guests and external sharing

- [ ] **Guest invitations restricted** to specific roles, and guest access to directory information limited.
- [ ] **SharePoint and OneDrive sharing** set to the most restrictive level that still works for your business, with "specific people" as the default link type.
- [ ] **Expiration for "Anyone" links,** or "Anyone" links disabled entirely.

- [ ] **Teams external access** limited to the domains you work with.

5 Exchange Online and email

- [ ] **Automatic forwarding to external addresses blocked** in the outbound spam policy.
- [ ] **SPF, DKIM and DMARC** configured for every domain, including domains that do not send email. Check yours for free: www.rasotec.com/emailcheck
- [ ] **Preset security policies** applied, including Safe Links and Safe Attachments (MDO).
- [ ] **Inbox rules and mailbox delegations** reviewed for signs of compromise.

6 Devices and Conditional Access

- [ ] **Compliant or hybrid-joined devices required** for admin portals and sensitive applications (P1, with Intune or hybrid join).
- [ ] **Exclusions from Conditional Access policies** reviewed: every excluded user, group or location is a potential gap.
- [ ] **Sign-in frequency and session controls** for admins and unmanaged devices.

7 Monitoring

- [ ] **Unified audit log enabled** and retained long enough for incident investigations.
- [ ] **Alerts** for new admin role assignments, new app consents, risky sign-ins and new forwarding rules.
- [ ] **Microsoft Secure Score** reviewed regularly, with open recommendations tracked.

Get an independent review of your tenant

Our cloud security assessments cover Entra ID, Microsoft 365, Azure, AWS and Google Cloud. Details: **www.rasotec.com/tests/cloud**

Book a free 30-minute consultation · **contact@rasotec.com** · **www.rasotec.com**