M365 Hardening Cheat Sheet

Secure-by-Default Guidance

Contents

1, Introduction

Microsoft 365 is the backbone of most modern organisations and also one of the most targeted platforms by attackers. Misconfigurations, legacy settings, and weak identity controls are responsible for a large percentage of real-world breaches. This cheat sheet gives you the essential hardening steps that every organisation should implement to protect their M365 environment.

It focuses on practical, high-impact controls: stronger identity security, safer defaults, conditional access baselines, improved email protection, and hardened endpoint configurations. These are the exact measures BlackBox Pentesters expects to see during penetration tests and red team engagements, because they meaningfully reduce risk.

Use this as a quick reference for securing new tenants, reviewing existing environments, or strengthening internal security policies. Even small changes here can deliver major improvements to your overall security posture.

1. Identity & Access – Start Here

Mandatory MFA (for ALL users)

Enable MFA for:

- All standard users
- All privileged roles
- Service accounts where possible
- External/guest accounts (if used)

Preferred methods:

- Authenticator app
- FIDO2 key
- Temporary Access Pass (for onboarding)

Avoid:

- SMS-based MFA
- Phone call MFA

2. Conditional Access – Safe Default Policies

Create baseline, catch-all policies:

Block Legacy Authentication

- Immediately blocks old protocols like IMAP/POP/SMTP Auth
- Removes most credential-stuffing attack paths

Require MFA for All Users

- Applies organisation-wide
- Exclude break-glass accounts only (2 accounts maximum)

Admin-Level Protection

- Require MFA every login
- Require compliant or trusted device
- Block from risky locations/countries

High-Risk Sign-In Action

- Auto-block or require password reset for high-risk users/sign-ins

Geo Control

- Block login from countries you do not operate in
- Allow only named countries if appropriate

3. Privileged Accounts & Roles

Admin Accounts

- Admin accounts must *not* have email access
- Create dedicated admin identities separate from day-to-day accounts

Role Assignment

- Follow least privilege
- Avoid Global Administrator unless necessary
- Use Privileged Role Administrator + PIM (see below)

PIM (Privileged Identity Management)

Enable PIM for:

- Global Administrator
- Exchange Administrator
- SharePoint Administrator
- User Administrator

Require:

- MFA
- Justification
- Time-bound access

4. Defender for Office 365 – Safe Defaults

Anti-phishing

Enable:

- Impersonation protection for executives & high-value targets
- Domain & user impersonation protection

Set actions to:

- Quarantine (not delivery)
- Notify admins

Safe Links

Enable Safe Links for:

- Email
- Teams
- Office apps

Enable click-time URL scanning.

Safe Attachments

- Use Dynamic Delivery or Block
- Do NOT allow delivery before scanning

Zero-Hour Auto Purge (ZAP)

Turn on to remove malicious emails post-delivery.

5. Device Compliance & Endpoint Security

Intune Recommended Policies

- Require device encryption (BitLocker)

- Block jailbroken or rooted devices
- Require up-to-date OS
- Device health checks (AV, firewall, Secure Boot)

Windows Hardening (Baseline)

- Enable Defender AV with cloud protection
- Enable Controlled Folder Access
- Enable ASR (Attack Surface Reduction) rules:
    - Block Office macros
    - Block executable content from email/web
    - Block credential harvesting

MDM Enrollment Policy

- Only corporate-owned or approved devices allowed
- Block personal devices unless explicitly required

6. Email Security & Hygiene

DMARC, DKIM, SPF

- SPF configured correctly with minimal includes
- DKIM enabled for default domain
- DMARC enforcing (p=quarantine or p=reject after monitoring phase)

External Sender Warning

Enable banner or tag in subject/body:

- “External Email – Caution”

Disable Auto-Forwarding to External Domains

Huge data-loss vector, block it globally.

7. Collaboration Security

SharePoint / OneDrive

- Block anonymous sharing
- Only allow authenticated external guests
- Use expiration dates on shared links
- Restrict download for sensitive libraries

Teams

- Disable external guest chat unless required
- Restrict external meeting access
- Disable file sharing for non-corporate accounts

8. Logging, Alerts & Monitoring

Enable Auditing

Ensure:

- Unified audit log is enabled
- Mailbox audit logging enabled for all users
- Admin activity logging enabled

Alerts to Enable

- Impossible travel
- Multiple failed sign-in attempts
- Email forwarding rule creation
- High-risk user
- Malware detected
- Newly granted admin roles

Retention

- Keep logs for **at least 90–180 days**
- Higher for regulated industries

9. Break-Glass Accounts (Emergency Access)

- Create **exactly two**
- Exclude from CA policies
- Cloud-only (not synced)
- Long, complex passwords stored securely
- Alert whenever used

10. Quick Wins (High-Impact, Low-Effort)

- Block legacy authentication
- Enforce MFA for all accounts
- Enable Safe Links and Safe Attachments
- Turn on ZAP
- Enable PIM for admin roles
- Disable external auto-forwarding
- Restrict external sharing
- Configure DKIM + DMARC

These changes stop the majority of real-world attacks immediately.