vijilan
IT Security: Enabled

M365 SECURITY BEST PRACTICES

Essential Hardening for Microsoft 365

Strengthening the Security of Your Microsoft 365 Environment

Microsoft 365 has become a critical platform for modern organizations, enabling collaboration, communication, and productivity across distributed teams. However, its widespread adoption also makes it a prime target for cyberattacks such as account compromise, phishing, data exfiltration, and privilege abuse.

Without proper security configurations and continuous monitoring, attackers can exploit weak authentication controls, misconfigured permissions, and unmonitored user activity.
This guide outlines essential best practices to help organizations secure, monitor, and harden their Microsoft 365 environment.

Enforce Strong Identity Protection

Identity is the primary security perimeter in Microsoft 365. Strengthening authentication and access controls is one of the most effective ways to prevent account compromise.

Enable Multi-Factor Authentication (MFA)
Require MFA for all users, especially administrators and privileged accounts.

Implement Conditional Access Policies
Restrict access based on user location, device compliance, and risk level.

Use Identity Risk Detection
Monitor sign-in risk events such as impossible travel, unfamiliar sign-ins, and credential abuse.

Adopt Least Privilege Access
Limit administrative roles and grant only the permissions necessary for job functions.

Secure Email and Collaboration

Email remains one of the most common entry points for cyberattacks. Proper protection can significantly reduce phishing and malware risks.

Enable Anti-Phishing and Anti-Malware Protections
Use advanced email filtering and phishing detection capabilities.

Protect Against Business Email Compromise (BEC)
Monitor for suspicious forwarding rules, impersonation attempts, and unusual email behavior.

Secure File Sharing and Collaboration
Control external sharing in OneDrive and SharePoint to prevent unauthorized access.

Implement Safe Links and Safe Attachments
Protect users from malicious links and files in emails and documents.

Monitor User and Administrative Activity

Continuous monitoring is critical for detecting suspicious behavior and responding quickly to threats.

Track Administrative Changes
Monitor role assignments, permission modifications, and policy changes.

Review Sign-In Activity
Identify unusual login patterns or geographic anomalies.

Audit Mailbox Activity
Detect unauthorized mailbox access, data downloads, or forwarding rules.

Monitor Data Access
Track sensitive file access within SharePoint, OneDrive, and Teams.

Protect Data and Prevent Leakage

Organizations must ensure sensitive information remains protected across cloud environments.

Implement Data Loss Prevention (DLP)
Prevent unauthorized sharing of sensitive data such as financial records or personal information.

Enable Sensitivity Labels
Classify and protect important data with encryption and access restrictions.

Control External Access
Limit guest access and enforce strict sharing policies.

Monitor Data Exfiltration Risks
Detect unusual downloads or large data transfers.

Strengthen Your Microsoft 365 Security Posture

Microsoft 365 provides powerful collaboration capabilities, but it must be configured and monitored properly to prevent misuse and cyber threats.

Organizations that implement strong authentication controls, secure collaboration policies, and continuous monitoring can significantly reduce the risk of compromise and protect sensitive data.

HELPING ORGANIZATIONS MONITOR, DETECT, AND RESPOND TO CYBERSECURITY THREATS.

vijilan.com
info@vijilan.com
+1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN