Microsoft 365 Best Practices

With an increase in the number of cybersecurity compromises as a result of phishing attacks, companies using Microsoft 365™ should take steps to prevent or mitigate the damage from these incidents.

Microsoft has several tools available that can help an enterprise manage its Microsoft 365 environment. While many of these are freely available, some tools may require a subscription. Unit 42 recommends enabling as many of these tools as needed.

Table 1: Microsoft 365 Management Tools	
Enable MFA and Disable Legacy Authentication	In conjunction with a strong password policy (password complexity enabled, password rotation, etc.) multi-factor authentication (MFA) adds an extra layer of protection by requiring users to pass an additional challenge to access their account. This lessens the likelihood of a compromise even if a password has been stolen or compromised. **Refer to Microsoft's documentation for details on MFA and an implementation guide.** Legacy authentication protocols should be disabled in order to ensure that MFA cannot be easily circumvented by attackers. **Learn how to disable legacy protocol.** Microsoft 365 environments using a premium level of Azure® Active Directory (AD), can accomplish this through conditional access policies, and non-premium environments can create an authentication policy through PowerShell that blocks all basic authentication.
Enable the Unified Audit Log	The Microsoft 365 unified audit log provides a centralized logging facility that includes activities from Azure AD, Exchange Online, SharePoint Online, OneDrive for Business, and other applications. Note that the unified audit log is not currently enabled by default and needs to be manually enabled. *Note that mailbox auditing has been enabled by default since January 2019.* **Refer to Microsoft's documentation for details and an implementation guide on enabling the unified audit log.**
Configure and Enable DLP	Data loss prevention (DLP) allows an administrator to identify and create policies to prevent users from accidentally or intentionally sharing sensitive information. DLP can be implemented across all Microsoft 365 applications, SharePoint, and OneDrive. **Refer to Microsoft's documentation for details on DLP and an implementation guide.**
Enable Microsoft 365 Cloud Application Security	Microsoft's Cloud Application Security enables an administrator to investigate suspicious activities. Microsoft 365 consists of multiple tools that enable an organization to track a number of suspicious activities from unauthorized users, track ransomware activity, and much more. *Note: Microsoft 365 Cloud Application Security is only available to Enterprises Licensees.* **Refer to Microsoft's documentation for details on Cloud Application Security.**
Enable Microsoft Secure Score	Microsoft's Secure Score is a security analytics score that analyzes Microsoft 365 settings and activities and compares them to a baseline. A score is calculated that shows whether an organization is aligned with security best practices. **Refer to Microsoft's documentation for details on obtaining and enabling Microsoft Secure Store, as well as an implementation guide.**

Figure 1: Cybercriminals can target business email accounts for financial gain

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com