ManageEngine
M365 Manager Plus

The

US Department of Homeland Security's

best practices for Microsoft 365 security, and how to expand on them

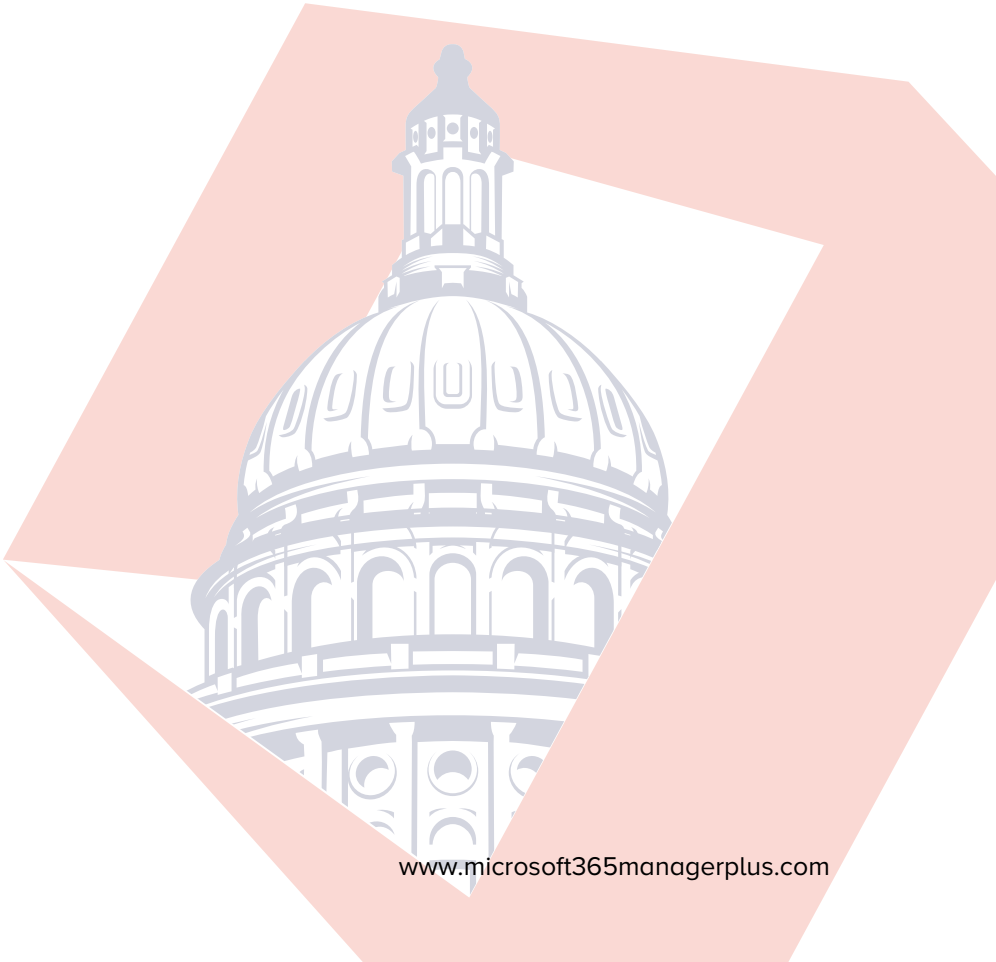
www.microsoft365managerplus.com

Introduction

As more organizations around the world adopt Microsoft 365, it's important to know the risks involved in this transition. The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) engaged with several Microsoft 365 customers who used third-party agencies to migrate to Microsoft 365 to gain a better understanding of the security posture of those customers along with the vulnerabilities they're facing post-migration.

In this analysis report, AR19-133A, the CISA discusses the cloud services configuration vulnerabilities found in the surveyed organizations. The report also recommends steps to mitigate these risks and vulnerabilities.

Microsoft 365's native tools have a number of shortcomings, which means implementing some of these best practices can be a challenge. In this guide, we'll take a closer look at these challenges and how M365 Manager Plus—ManageEngine's comprehensive Microsoft 365 reporting, monitoring, auditing, managing, and alerting solution—makes it easy to implement these best practices. We'll also discuss how to go beyond CISA recommendations to enhance the security of Microsoft 365 environments.



Configuration vulnerabilities highlighted by the CISA

According to the CISA, organizations that used a third party for Microsoft 365 migration suffered from a weakened security posture at some point post-migration. On top of this, the majority of these organizations didn't have dedicated security teams for their cloud services, which led to user accounts and mailboxes being compromised.

The configuration vulnerabilities highlighted in the report include:how to go beyond CISA recommendations to enhance the security of Microsoft 365 environments.

- **Admin accounts do not have multi-factor authentication (MFA) enabled by default:**

  The Global Administrator role possesses the highest administrator privileges for an Microsoft 365 tenant. This is the most powerful role as they are the only admin role that can assign other admin roles. By default, MFA is disabled for these crucial accounts. As Microsoft 365 platforms increase in popularity among hackers, this vulnerability could be an opening for attackers.

- **Mailbox auditing and unified audit logging is disabled:**

  Mailbox auditing is an important aspect of securing an Microsoft 365 environment as it helps in tracking the actions performed by mailbox owners, delegates, and admins. Organizations that migrated to Microsoft 365 before January 2019 won't have this feature enabled by default in their Microsoft 365 environment.

  Unified audit logging is also disabled by default, which means that an admin has to enable this before running queries about events in Exchange Online, Azure Active Directory (AD), OneDrive for Business, and other Microsoft 365 services.

- **Password sync is enabled:**

  With Azure AD Connect, admins can create identities in Azure AD from on-premises AD, or match previously created Azure AD identities with their on-premises AD identities. One method of authentication in Azure AD is password sync.

  By enabling this option, the on-premises AD account's password overwrites the password in Azure AD. This practice can be dangerous, because if an on-premises AD account is compromised, the hacker will also have access to any synced cloud services.

- **The latest authentication methods aren't compatible with legacy protocols:**

  Microsoft 365 uses Azure AD as the authentication method for Exchange Online. However, some of the protocols associated with Exchange Online, including POP3, IMAP, and SMTP, do not support modern authentication methods like MFA.

  Though these older protocols can be disabled at the tenant or user level, organizations using older email clients often have to stick with them. This means the only thing standing in a cyberattacker's way is the account's username and password.

Microsoft 365 security best practices

The CISA's report suggests five best practices to mitigate the vulnerabilities discussed above:

- **Enable MFA:**

  Setting up MFA is a crucial step in fortifying the security of all administrator accounts. Organizations need to decide on various aspects of MFA, including which second factor should be used and which accounts should be MFA-enabled, before implementing it.

  Microsoft 365 provides the option to configure MFA, but its UI is not very user-friendly. To enable MFA, admins need to move between different tabs to select users and configure settings. M365 Manager Plus, on the other hand, simplifies this task by allowing admins to configure MFA for multiple users from a single console in just a few clicks. Admins can configure multiple tenants and configure MFA for users belonging to any of the tenants from the same console.

  Learn how to configure MFA for Microsoft 365 using M365 Manager Plus.

- **Enable unified audit logging:**

  Using unified audit logs, admins can search for events occurring in all of the services within their Microsoft 365 environment.

  Even after enabling unified audit logs, Microsoft 365's native tools are insufficient for performing security audits and investigations. The 90-day log storage limitation forces admins to export and save audit logs in external locations. Aside from increasing admins' workloads, this takes up a large amount of storage space in organizations' databases.

M365 Manager Plus overcomes this limitation with:

- **Indefinite log storage:** Audit logs are not only stored indefinitely, but are also easy to access during compliance audits and security investigations.

- **Audit log archival:** Audit logs are placed in an archive at the admin's convenience, and admins can restore deleted audit logs in a single click.

Learn more about M365 Manager Plus' auditing feature, and see how to create custom audit views.

- **Enable mailbox auditing for every user:**

Starting in 2019, Microsoft has changed the default mailbox auditing status to enabled. Most securityconscious organizations that migrated to Microsoft 365 before 2019 will have enabled mailbox auditing for all accounts using PowerShell.

For those organizations that migrated before 2019 and haven't enabled mailbox auditing yet, this is where M365 Manager Plus' management feature comes in handy. In just a few clicks, administrators can easily enable auditing for any number of mailboxes.

Learn how to enable Exchange Online auditing using M365 Manager Plus.

- **Ensure proper planning and correct configuration of Azure AD password sync:**

In hybrid environments, admins need to be careful when configuring Azure AD Connect to synchronize onpremises user identities with the cloud. Though Microsoft has disabled the capability to sync certain admin accounts since October 2018, the CISA is concerned that some privileged accounts may have been synced before this.

- **Limit the number of legacy email protocols or disable them completely:**

The CISA report suggests that many users still use email clients that work on old protocols such as POP3, IMAP4, and SMTP. Admins can block these clients from connecting by using Azure AD conditional policies or Exchange Online authentication policies. This will persuade users to switch to more secure clients that support modern authentication.

Securing Microsoft 365: Going beyond CISA recommendations

The CISA recommendations above are only basic steps for securing organizations moving to Microsoft 365. Admins need to implement measures beyond these recommendations to ensure comprehensive security for their Microsoft 365 environment.

- **Enable spam and malware detection**

  Of all the messages sent to Microsoft 365 inboxes in a single month, on average about 55 billion are spam or bulk emails, and 20 million contain some form of malware. detection can help admins stop threats before they get a foothold in their Microsoft 365 environment.

  Using M365 Manager Plus, admins can comprehensively monitor all inbound and outbound traffic in their Exchange Online environment, and get scheduled reports on spam and malware detections. Admins can also set alert notifications for early detection so they can take immediate steps to remediate any issues that arise.

- **Remove suspicious auto-mail forwarding**

  Auto-mail forwarding is potentially dangerous as it can result in sensitive information leaving the organization— whether that was the intention or not. If hackers gain access to an Microsoft 365 account, they can set up forwarding rules to learn how an organization works before executing an attack. Forwarding rules are immune to the usual threat response measures, like password resets, and if left unchecked, they allow hackers to continue collecting confidential data for as long as they want.

  Using M365 Manager Plus' Mailboxes with External Mail Forwarding report, admins can view the list of user accounts with mail forwarding in place, along with the address emails are being forwarded to. Admins can also perform management actions from within the report itself, allowing them to easily view and disable external email forwarding for all users who have enabled this capability.

- **Track mobile devices connected to Microsoft 365**

  Hackers often connect their mobile devices to compromised accounts in order to send and receive emails from them. Admins should regularly evaluate their Microsoft 365 setup to look for any unauthorized devices connected to users' Outlook Web App.

  M365 Manager Plus' Mobile Devices report displays all the mobile devices that are configured to synchronize with users' Microsoft 365 mailboxes. It provides information including username, device name, device type, device ID, first sync, and device IMEI number.

- **Tracking sensitive information in emails**

  Admins need to track sensitive information leaving the tenant via emails. M365 Manager Plus' Microsoft 365 content search feature helps admins keep an eye on all the emails sent and received by their organization. Using this feature, admins can label profiles for sensitive information and receive notification about emails containing information corresponding to these profiles. The tool will still notify admins about these emails even if they're deleted or moved.

- **Implementing Microsoft Secure Score recommendations**

  An organization's Secure Score in Microsoft 365 is an indicator of how secure its Microsoft 365 environment currently is. The Secure Score is assigned based on the security configurations and activities enabled in an Microsoft 365 environment. When an admin logs in to the Secure Score dashboard, it displays their current score compared to the maximum score they can attain. Though a perfect Secure Score doesn't provide an absolute guarantee that an organization won't be breached, it does ensure that admins have taken additional steps towards mitigating the risk of security breaches.