Microsoft 365

Security Assessment

Prepared for

CUSTOMER

Table of Contents

1 Document Control

1.1 Document Details

Property	Detail
Document Name	CNNECT-Microsoft 365 Security Assessment EXAMPLE v1.0.docx
Document Version Date	19/09/2023
Date of Assessment	TBC
Author	Aaron Bhatti
Quality Reviewed by	

1.2 Revision History

Version	Date	Author	Description
1.0	19/09/2023	Aaron Bhatti	Initial Creation

1.3 Key Contacts

Name	Company	Title	Contact Details
Aaron Bhatti	CNNECT	Technology Director	aaron@cnnect.uk
Adnan Iqbal	CNNECT	Senior Cloud Consultant	adnan@cnnect.uk

2 Introduction

2.1 Overview

CUSTOMER COMPANY OVERVIEW.

To conduct the assessment, CNNECT has utilised CIS benchmarks, internationally recognised security standards for defending IT systems and data against cyberattacks. Used by thousands of businesses, they offer prescriptive guidance for establishing a secure baseline configuration. The CIS Benchmarks are designed to focus on the technical configuration settings used to maintain or increase the security of your Microsoft 365 tenant, which includes Exchange Online, SharePoint Online, OneDrive for Business, Teams, and Azure Active Directory.

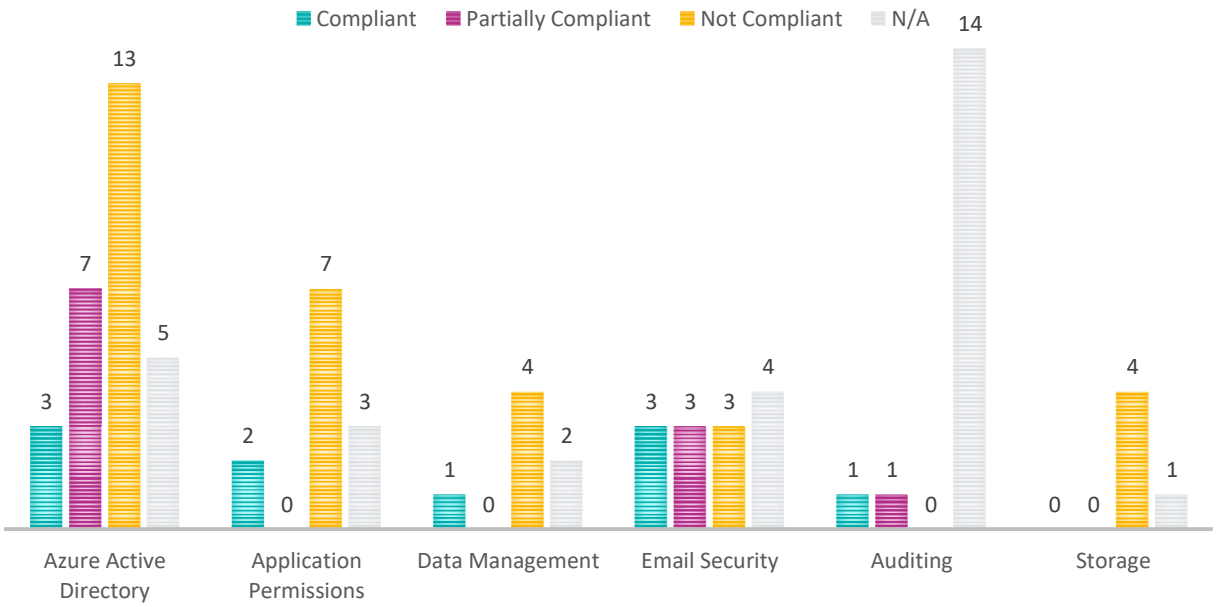
This report covers 81 Security Controls split into Account Authentication (Azure Active Directory), Application Permissions, Data Management, Email Security, Auditing and Storage providing a comprehensive review of your overall Microsoft 365 security.

Following the audit, the Microsoft 365 environment achieved a 20% compliance rating against the 54 applicable controls. It is worth noting that some controls have been marked as 'Not Applicable'—these are recommendations that should be reviewed and integrated as part of ongoing processes.

Compliant	Partially Compliant	Not Compliant	Not Applicable
11	12	31	27

We strongly advise reviewing this report and strategically implementing the recommended measures. In the short term, we suggest prioritising controls with an "E3 Level 1" profile, as these will not impede the functionality of Microsoft 365 beyond acceptable thresholds. For the longer term, we recommend a thorough evaluation of the "E3 Level 2" items following successful testing.

The following graph provides an overview of the compliance rating across the six areas reviewed.



2.2 Key Recommendations

A full list is included in Section 4 of this report, however, key recommendations can be summarised as:

- Review, test and deploy Microsoft Conditional Access templates along with the Azure Active Directory recommendations to provide increased security for the overall tenant, including enforcing Modern Authentication for all services and users.
- Restrict application permissions to restrict users from installing third-party applications and plugins and utilise the admin workflow for centralised approval and deployment.
- Review the data management section to restrict users from sharing files external to the organisation, including implementing basic Data Leakage Prevention (DLP) measures.
- Ensure email security authentication settings and anti-spam/anti-phishing policies are implemented for all domains authorised within the tenant.
- Review auditing recommendations and incorporate them into monthly or quarterly checks and reports, where applicable.
- Implement the recommendations to restrict storage providers. Educate users to utilise OneDrive and SharePoint across all services within Microsoft 365. Furthermore, restrict synchronisation from unmanaged devices and implement a link expiration policy.

2.3 Key Findings

A full list is included in Section 5 of this report however, the key findings can be

summarised as:

- There are a low number of administrative accounts, however for auditing and accountability administrators should utilise named accounts with Role Based Access Control, reducing the number of Global Administrator accounts.
- Multifactor Authentication is enabled for all users, however, 550 out of 600 users are not registered with MFA.
- Users can install and share data with third-party plugins and applications that are not sanctioned by IT, which may result in a user inadvertently sharing data external to the organisation.
- It is possible for files to be inadvertently shared outside of the organisation with the current tenant settings.
- Email security settings follow recommended practice. However, it is recommended to ensure this is in place for all domains authorised within the Microsoft 365 tenant.
- Auditing settings are configured within the constraints of the licensing limitation. However, two accounts should be reviewed. In addition to this, several Not Applicable items relate to process recommendations that should be reviewed and incorporated into monthly or quarterly checks.
- The tenant currently allows all third-party storage providers which can result in data leakage. Furthermore, storage is accessible on unmanaged devices and indefinitely restricts the ability to secure the organisation's data.

3 Report Overview

3.1 Report Structure

This section explains the key definitions used within the results for each control assessed throughout this report.

Title

A concise description of the recommendation's intended configuration.

Assessment Status

An assessment status is included for each control tested. The assessment status indicates whether the given control has been:

- **Compliant** – the control has been implemented to a satisfactory standard and no action is required.
- **Partially Compliant** – the control has been implemented but requires further attention.
- **Not Compliant** – the control has not been implemented and requires attention.
- **Not Applicable** – the control is not applicable due to a licensing limitation or is a recommendation only.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile.

The following configuration profiles are defined by this Benchmark:

Profile	Description
E3 Level 1	Items in this profile apply to customer deployments of Microsoft M365 with an E3 license and intend to: • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means.
E3 Level 2	This profile extends the "E3 Level 1" profile. Items in this profile exhibit one or more of the following characteristics and are focused on customer deployments of Microsoft M365 E3: • are intended for environments or use cases where security is paramount. • acts as a defence in depth measure. • may negatively inhibit the utility or performance of the technology.
E5 Level 1	Items in this profile extend what is provided by the "E3 Level 1" profile for customer deployments of Microsoft M365 with an E5 license and intend to: • be practical and prudent. • provide a clear security benefit. • not inhibit the utility of the technology beyond acceptable means.
E5 Level 2	This profile extends the "E3 Level 1" and "E5 Level 1" profiles. Items in this profile exhibit one or more of the following characteristics and are focused on customer deployments of Microsoft M365 E5: • are intended for environments or use cases where security is paramount. • acts as a defence in depth measure. • may negatively inhibit the utility or performance of the technology.

Description

Detailed information about the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user with a clear and concise understanding of the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

This section includes systematic instructions for determining if the target system complies with the recommendation.

Impact Rating

The impact rating is used within the Risk & Recommendations section to categorise the impact of the control not being implemented as:

- **Low** – implementing this recommendation **will not** impact the functionality or performance of the technology beyond acceptable means.
- **High** – implementing this recommendation may negatively impact the functionality or performance of the technology.

3.2 Microsoft 365 CIS Benchmark

The Center for Internet Security (CIS) has published benchmarks for Microsoft products and services including the Microsoft Azure and Microsoft 365 Foundations Benchmarks, the Windows 10 Benchmark, and the Windows Server 2016 Benchmark. CIS benchmarks are internationally recognised as security standards for defending IT systems and data against cyberattacks. Used by thousands of businesses, they offer prescriptive guidance for establishing a secure baseline configuration.

The CIS Benchmarks are designed to focus on the technical configuration settings used to maintain or increase the security of your Microsoft 365 tenant. The benchmark is designed as a key component of a comprehensive cybersecurity program and should be used in conjunction with other essential cybersecurity governance.

This document provides the results from our review of your secure configuration posture for Microsoft 365 and includes recommendations for Exchange Online, SharePoint Online, OneDrive for Business, Teams, and Azure Active Directory.

The report has been separated into the following areas:

1. **Account Authentication / Azure Active Directory** – this section contains recommendations for Azure Active Directory (AAD), a cloud-based identity management service that underpins Microsoft 365.
2. **Application Permissions** – focuses on the usage and installation of third-party applications, including the sharing of applications used within Microsoft 365 with external organisations.
3. **Data Management** –focuses on securing your organisation's data and minimising the potential for data leakage.
4. **Email Security** – focuses on ensuring you effectively secure email within your organisation, including email authentication methods and advanced custom security features to prevent business email compromise.
5. **Auditing** – focuses on ensuring there is clear accountability and auditing capabilities enabled within the tenant. This also includes several recommended reports to review regularly to maintain a good security posture.
6. **Storage** – focuses on restricting the storage services available to access and share documents within your Microsoft 365 tenant.

4 Summary Report & Recommendations

4.1 Account Authentication / Azure Active Directory

Benchmark Recommendation	Assessment Status	Impact Rating	Recommendation
1.1.1 Ensure Security Defaults is disabled on Azure Active Directory	Compliant	Low	This setting is configured correctly.
1.1.2 Ensure multifactor authentication is enabled for all users in administrative roles	Partially Compliant	Low	MFA is enabled for all users, however, several accounts including an admin account have not been enabled. A break glass account is required but should not be used for day-to-day administration, only in the event of an emergency.
1.1.3 Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	Not Compliant	Low	There is currently once Conditional Access Policy, we would strongly recommend reviewing the Microsoft templates to increase the current security posture.

4.2 Application Permissions

Benchmark Recommendation	Assessment Status	Impact Rating	Recommendation
2.1 Ensure the admin consent workflow is enabled	Not Compliant	Low	It is recommended to enable the admin consent workflow to ensure Administrators are sent an email to review and approve applications that require admin approval. As the administrator acts on the request, the user is notified of the action and decision to approve or deny access.
2.2 Ensure third-party integrated applications are not allowed	Not Compliant	High	It is recommended to disable third-party integrated apps and force users to request access with approval by an Administrator to ensure the app is for legitimate business use.
2.3 Ensure 'External sharing' of calendars is not available	Not Compliant	High	"Let your users share their calendars with people outside of your organisation who have Office 365 or Exchange" is currently set to "yes" the control requires this to be set to "No" to meet the control. This functionality is not widely used so is unlikely to impact most users, however, it will impact anyone sharing calendars outside the organisation.

4.3 Data Management

Benchmark Recommendation	Assessment Status	Impact Rating	Recommendation
3.1 Ensure the customer lockbox feature is enabled	N/A	High	Microsoft 365 E5 licensing is required.
3.2 Ensure SharePoint Online Information Protection policies are set up and used	Not Compliant	High	SharePoint Online Data Classification Policies enable organisations to classify and label content in SharePoint Online based on its sensitivity and business impact. The creation of data classification policies is unlikely to have a significant impact on an organisation. However, maintaining long-term adherence to policies may require ongoing training and compliance efforts across the organisation. Therefore, organisations should include training and compliance planning as part of the data classification policy creation process.
3.3 Ensure 'external access' is restricted in the Teams Admin Center	Not Compliant	High	The impact of disabling external access to Teams and Skype for an organisation is highly dependent on current usage practices. If users infrequently communicate with external parties using these channels, the impact is likely to be minimal. However, if users regularly use Teams and Skype for client communication, the impact could be significant. This should be discussed and agreed with the business.

4.4 Email Security

Benchmark Recommendation	Assessment Status	Impact Rating	Recommendation
4.1 Ensure the Common Attachment Types Filter is enabled	Compliant	Low	This setting is configured correctly.
4.2 Ensure Exchange Online Spam Policies are set to notify administrators	Not Compliant	Low	It is recommended to set a notification to alert the Service Desk if an account has been blocked due to spam as it is a good indicator the account may have been compromised.
4.3 Ensure all forms of mail forwarding are blocked and/or disabled	Not Compliant	Low	The default policy is set to 'System Controlled' and a custom policy is defined with forwarding enabled for 4 users.

4.5 Auditing

Benchmark Recommendation	Assessment Status	Impact Rating	Recommendation
5.1.1 Ensure 'Access reviews' for Guest Users are configured	N/A	Low	Microsoft 365 E5 Licensing is required.
5.1.2 Ensure 'Access reviews' for high privileged Azure AD roles are configured	N/A	Low	Microsoft 365 E5 Licensing required.
5.2 Ensure Microsoft 365 audit log search is Enabled	Compliant	Low	This setting is set correctly.

4.6 Storage

Benchmark Recommendation	Assessment Status	Impact Rating	Recommendation
6.1 Ensure SharePoint external sharing is managed through domain whitelist/blacklists	Not Compliant	High	It is strongly recommended to restrict users from sharing files external to your organisation directly from SharePoint unless the domain is whitelisted. User training should be provided, and files should be shared externally from a specific location.
6.2 Block OneDrive for Business sync from unmanaged devices	Not Applicable	High	This setting is only applicable to Active Directory Domains. For Azure AD Joined devices, a Conditional Access policy should be set to restrict access.
6.3 Ensure expiration time for external sharing links is set	Not Compliant	Low	The setting is currently not set "RequireAnonymousLinksExpireInDays : -1" the required setting should be 30 days or less to meet the control.

5 Security Audit

5.1 Account Authentication / Azure Active Directory

1.1.1 Ensure Security Defaults is disabled on Azure Active Directory

Profile Applicability: E3 Level 1

Assessment Status: Compliant

Impact Rating: Low

Description:

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect the organisation. Security defaults contain preconfigured security settings for common attacks.

By default, Microsoft enables security defaults. The goal is to ensure that all organisations have a basic level of security enabled. The security default setting is manipulated in the Azure Portal.

The use of security defaults, however, will prohibit custom settings which are being set with more advanced settings from this benchmark.

Rationale:

Security defaults provide secure default settings that are managed on behalf of organisations to keep customers safe until they are ready to manage their own identity security settings.

For example, doing the following:

Requiring all users and admins to register for MFA.

- Challenging users with MFA - mostly when they show up on a new device or app, but more often for critical roles and tasks.
- Disabling authentication from legacy authentication clients, which can't do MFA.

Impact:

The potential impact associated with disabling Security Defaults is dependent upon the security controls implemented in the environment. Most organisations disabling Security Defaults likely plan to implement equivalent controls to replace Security Defaults.

It may be necessary to check settings in other Microsoft products, such as Azure, to ensure settings and functionality are as expected when disabling security defaults for MS365.

Audit:

Ensure security defaults are disabled:

1. Navigate to Microsoft Entra Admin Center https://entra.microsoft.com.
2. Click to expand Azure Active Directory and select Overview.
3. Click Properties.
4. Click Manage security defaults.
5. Verify the Security defaults dropdown is set to Disabled.

1.1.2 Ensure multifactor authentication is enabled for all users in administrative roles

Profile Applicability: E3 Level 1

Assessment Status: Partially Compliant

Impact Rating: Low

Description:

Multi-factor authentication is a process that requires an additional form of identification during the sign-in process, such as a code from a mobile device or a fingerprint scan, to enhance security.

Ensure users in administrator roles have MFA capabilities enabled.

Rationale:

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Implementation of multifactor authentication for all users in administrative roles will necessitate a change to user routine. All users in administrative roles will be required to enrol in multifactor authentication using phone, SMS, or an authentication application. After enrolment, the use of multifactor authentication will be required for future access to the environment.

Audit:

Ensure the multifactor authentication configuration for administrators:

1. Navigate to the Microsoft Entra Admin Center https://entra.microsoft.com.
2. Click Expand Azure Active Directory > Applications and select Enterprise Applications.
3. Under Security, select Conditional Access.
4. Review the list of policies and ensure that there is a policy that requires the Grant access control with Require multi-factor authentication for the appropriate Directory roles under Users and groups.
5. The minimum list of Directory roles can be found in the Remediation section.

1.1.3 Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users

Profile Applicability: E3 Level 1

Assessment Status: Not Compliant

Impact Rating: Low

Description:

In complex deployments, organisations might need to restrict authentication sessions. Conditional Access policies allow for the targeting of specific user accounts. Some scenarios might include:

- Resource access from an unmanaged or shared device
- Access to sensitive information from an external network
- High-privileged users
- Business-critical applications

Ensure Sign-in frequency does not exceed 4 hours for E3 tenants, or 24 hours for E5 tenants using Privileged Identity Management.

Ensure Persistent browser session is set to Never persist.

Note: This CA policy can be added to the previous CA policy in this benchmark "Ensure multifactor authentication is enabled for all users in administrative roles"

Rationale:

Forcing a time out for MFA will help ensure that sessions are not kept alive for an indefinite period of time and ensuring that browser sessions are not persistent will help in the prevention of drive-by attacks in web browsers, this also prevents the creation and saving of session cookies leaving nothing for an attacker to take.

Impact:

Users with Administrative roles will be prompted at the frequency set for MFA.

Audit:

Ensure Sign-in frequency is enabled, and browser sessions are not persistent for Administrative users:

1. Navigate to Microsoft Entra Admin Center https://entra.microsoft.com.
2. Click to expand Azure Active Directory > Applications Select Enterprise applications.
3. Under Security, select Conditional Access.
4. Review the list of policies and ensure that there is a policy that has Sign-in frequency set to the time determined by your organisation and that the Persistent browser session is set to Never persistent.
5. Ensure Sign-in frequency does not exceed 4 hours for E3 tenants. E5 tenants using PIM may be set to a maximum of 24 hours.

5.2 Application Permissions

2.1 Ensure the admin consent workflow is enabled

Profile Applicability: E3 Level 1

Assessment Status: Not Compliant

Impact Rating: Low

Description:

The admin consent workflow gives admins a secure way to grant access to applications that require admin approval. When a user tries to access an application but is unable to provide consent, they can send a request for admin approval. The request is sent via email to admins who have been designated as reviewers. A reviewer takes action on the request, and the user is notified of the action.

Rationale:

The admin consent workflow (Preview) gives admins a secure way to grant access to applications that require admin approval. When a user tries to access an application but is unable to provide consent, they can send a request for admin approval. The request is sent via email to admins who have been designated as reviewers. A reviewer acts on the request, and the user is notified of the action.

Impact:

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.

Audit:

Ensure the admin consent workflow is enabled:

1. Navigate to Microsoft Entra Admin Center https://entra.microsoft.com.
2. Click to expand Azure Active Directory > Applications and select Enterprise applications.
3. Under Security select Consent and Permissions.
4. Under Manage select Admin consent settings.
5. Verify that Users can request admin consent to apps they are unable to consent to is set to Yes.

2.2 Ensure third-party integrated applications are not allowed

Profile Applicability: E3 Level 2

Assessment Status: Not Compliant

Impact Rating: High

Description:

App registrations allow users to register custom-developed applications for use within the directory.

Rationale:

Third-party integrated applications connection to services should be disabled unless there is a very clear value and robust security controls are in place. While there are legitimate uses, attackers can grant access from breached accounts to third-party applications to exfiltrate data from your tenancy without having to maintain the breached account.

Impact:

Implementation of this change will impact both end users and administrators. End users will not be able to integrate third-party applications that they may wish to use.

Administrators are likely to receive requests from end users to grant them permission to necessary third-party applications.

Audit:

Ensure third-party integrated applications are not allowed:

1. Navigate to Microsoft Entra Admin Center https://entra.microsoft.com.
2. Click to expand Azure Active Directory > Users select Users settings.
3. Verify Users can register applications is set to No.

2.3 Ensure 'External sharing' of calendars is not available

Profile Applicability: E3 Level 1

Assessment Status: Not Compliant

Impact Rating: Low

Description:

External calendar sharing allows an administrator to enable the ability for users to share calendars with anyone outside of the organisation. Outside users will be sent a URL that can be used to view the calendar.

Rationale:

Attackers often spend time learning about organisations before launching an attack. Publicly available calendars can help attackers understand organisational relationships and determine when specific users may be more vulnerable to an attack, such as when they are travelling.

Impact:

This functionality is not widely used. As a result, it is unlikely that the implementation of this setting will cause an impact to most users. Users who do utilise this functionality are likely to experience a minor inconvenience when scheduling meetings or synchronising calendars with people outside the tenant.

Audit:

Ensure calendar details sharing with external users is disabled:

1. Navigate to the Microsoft 365 Admin Center https://admin.microsoft.com.
2. Click to expand Settings and select Org settings.
3. In the Services section click Calendar.
4. Verify Let your users share their calendars with people outside of your organisation who have Office 365 or Exchange is unchecked.

5.3 Data Management

3.1 Ensure the customer lockbox feature is enabled

Profile Applicability: E5 Level 2

Assessment Status: Not Applicable

Impact Rating: High

Description:

Customer Lockbox is a security feature that provides an additional layer of control and transparency to customer data in Microsoft 365. It offers an approval process for Microsoft support personnel to access organisation data and creates an audited trail to meet compliance requirements.

Rationale:

Enabling this feature protects organisational data against data spillage and exfiltration.

Impact:

Administrators will need to grant Microsoft access to the tenant environment prior to a Microsoft engineer accessing the environment for support or troubleshooting.

Audit:

Ensure the customer lockbox feature is enabled:

1. Navigate to the Microsoft 365 Admin Center https://admin.microsoft.com.
2. Click to expand Settings then select Org settings.
3. Select the Security & Privacy tab.
4. Click Customer lockbox.
5. Ensure the box labelled Require approval for all data access requests is checked.

3.2 Ensure SharePoint Online Information Protection policies are set up and used

Profile Applicability: E3 Level 2

Assessment Status: Not Compliant

Impact Rating: High

Description:

SharePoint Online Data Classification Policies enables organisations to classify and label content in SharePoint Online based on its sensitivity and business impact. This setting helps organisations to manage and protect sensitive data by automatically applying labels to content, which can then be used to apply policy-based protection and governance controls.

Rationale:

By categorising and applying policy-based protection, SharePoint Online Data Classification Policies can help reduce the risk of data loss or exposure and enable more effective incident response if a breach does occur.

Impact:

The creation of data classification policies is unlikely to cause a significant impact on an organisation. However, maintaining long-term adherence to policies may require ongoing training and compliance efforts across the organisation. Therefore, organisations should include training and compliance planning as part of the data classification policy creation process.

Audit:

Ensure SharePoint Online Information Protection policies are set up and used:

1. Navigate to the Microsoft Purview compliance portal https://compliance.microsoft.com.
2. Under Solutions select Information Protection.
3. Click on the Label Policies tab.
4. Ensure that a Label policy exists and is published accordingly.

3.3 Ensure 'external access' is restricted in the Teams Admin Center

Profile Applicability: E3 Level 2

Assessment Status: Not Compliant

Impact Rating: High

Description:

As of December 2021 the default for Teams external communication is set to 'People in my organisation can communicate with Teams users whose accounts aren't managed by an organisation.' This means that users can communicate with personal Microsoft accounts (e.g. Hotmail, Outlook etc.), which presents data loss/phishing / social engineering risks.

Note: Skype for business is deprecated as of July 31, 2021, although these settings may still be valid for a period of time.

Rationale:

Allowing users to communicate with Skype or Teams users outside of an organisation presents a potential security threat as external users can interact with organisation users over Skype for Business or Teams. While legitimate, productivity-improving scenarios exist, they are outweighed by the risk of data loss, phishing, and social engineering attacks against organisation users via Teams. Therefore, it is recommended to restrict external communications to minimise the risk of security incidents.

Impact:

The impact of disabling external access to Teams and Skype for an organisation is highly dependent on current usage practices. If users infrequently communicate with external parties using these channels, the impact is likely to be minimal. However, if users regularly use Teams and Skype for client communication, the impact could be significant. Therefore, before disabling external access, users should be notified, and alternate communication mechanisms should be identified to ensure continuity of communication.

Audit:

Ensure external access is not allowed in Skype or Teams:

1. Navigate to the Microsoft Teams Admin Center https://admin.teams.microsoft.com.
2. Click to expand Users select External access.
3. Under Teams and Skype for Business users in external organisations ensure Block all external domains
   Note: If the organisation's policy allows select Allow only specific external domains and add the allowed domains.
4. Under Teams accounts not managed by an organisation ensure the slider is set to Off.
5. Under Skype users ensure the slider is set to Off.

5.4 Email Security

4.1 Ensure the Common Attachment Types Filter is enabled

Profile Applicability: E3 Level 1

Assessment Status: Compliant

Impact Rating: Low

Description:

The Common Attachment Types Filter lets a user block known and custom malicious file types from being attached to emails.

Rationale:

Blocking known malicious file types can help prevent malware-infested files from infecting a host.

Impact:

Blocking common malicious file types should not cause an impact in modern computing environments.

Audit:

Ensure the Common Attachment Types Filter is enabled:

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand Email & collaboration select Policies & rules.
3. On the Policies & rules page select Threat policies.
4. Under policies select Anti-malware and click on the Default (Default) policy.
5. On the policy page that appears on the righthand pane, under Protection settings, verify that the Enable the common attachments filter has the value of On.

4.2 Ensure Exchange Online Spam Policies are set to notify administrators

Profile Applicability: E3 Level 1

Assessment Status: Not Compliant

Impact Rating: Low

Description:

In Microsoft 365 organisations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organisations without Exchange Online mailboxes, email messages are automatically protected against spam (junk email) by EOP.

Configure Exchange Online Spam Policies to copy emails and notify someone when a sender in the organisation has been blocked for sending spam emails.

Rationale:

A blocked account is a good indication that the account in question has been breached and an attacker is using it to send spam emails to other people.

Impact:

Notification of users that have been blocked should not cause an impact to the user.

Audit:

Ensure Exchange Online Spam Policies are set to notify administrators:

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand Email & collaboration select Policies & rules.
3. On the Policies & rules page, under Policies select Anti-spam.
4. Click on the Anti-spam outbound policy (default).
5. Verify that Send a copy of outbound messages that exceed these limits to these users and groups is set to On and ensure the email address is correct.

4.3 Ensure all forms of mail forwarding are blocked and/or disabled

Profile Applicability: E3 Level 1

Assessment Status: Not Compliant

Impact Rating: Low

Description:

Exchange Online offers several methods of managing the flow of email messages. These are Remote domain, Transport Rules, and Anti-spam outbound policies. These methods work together to provide comprehensive coverage for potential automatic forwarding channels:

- Outlook forwarding using Inbox rules
- Outlook forwarding is configured using the OOF rule
- OWA forwarding setting (ForwardingSmtpAddress)
- Forwarding set by the admin using EAC (ForwardingAddress)
- Forwarding using Power Automate / Flow

Ensure a Transport rule and Anti-spam outbound policy are used to block mail forwarding.

Note: Any exclusions should be implemented based on organisational policy.

Rationale:

Attackers often create these rules to exfiltrate data from your tenancy, this could be accomplished via access to an end-user account or otherwise. An insider could also use one of these methods as a secondary channel to exfiltrate sensitive data.

Impact:

Care should be taken before implementation to ensure there is no business need for case-by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users in an organisation. Any exclusions should be implemented based on organisational policy.

Audit:

STEP 1 - Transport rules

To verify the mail transport rules do not forward emails to external domains, use the Microsoft 365 Admin Center:

1. Select Exchange to open the Exchange Admin Center.
2. Select Mail Flow then Rules.
3. Review the rules and verify that none of them forwards or redirects e-mail to external domains.

STEP 2 - Anti-spam outbound policy

Ensure an anti-spam outbound policy is properly configured:

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Expand E-mail & collaboration then select Policies & rules.
3. Select Threat policies > Anti-spam.
4. Inspect Anti-spam outbound policy (default) and ensure Automatic forwarding is set to Off - Forwarding is disabled
5. Inspect any additional custom outbound policies and ensure Automatic forwarding is set to Off - Forwarding is disabled, in accordance with the organisation's exclusion policies.

Note: According to Microsoft if a recipient is defined in multiple policies of the same type (anti-spam, anti-phishing, etc.), only the policy with the highest priority is applied to the recipient. Any remaining policies of that type are not evaluated for the recipient (including the default policy).

5.5 Auditing

5.1.1 Ensure 'Access reviews' for Guest Users are configured

Profile Applicability: E5 Level 1

Assessment Status: Not Applicable

Impact Rating: Low

Description:

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organisation.

Ensure Access reviews for Guest Users are configured to be performed no less frequently than monthly.

Rationale:

Access to groups and applications for guests can change over time. If a guest user's access to a particular folder goes unnoticed, they may unintentionally gain access to sensitive data if a member adds new files or data to the folder or application. Access reviews can help reduce the risks associated with outdated assignments by requiring a member of the organisation to conduct the reviews. Furthermore, these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

Impact:

Access reviews that are ignored may cause guest users to lose access to resources temporarily.

Audit:

Verify an access review for Guest Users is in place:

1. Navigate to Microsoft Entra Admin Center https://entra.microsoft.com.
2. Expand Azure Active Directory > Identity Governance and select Access reviews
3. Inspect the access reviews, and ensure an access review is created with the following criteria:
    a. Overview: Scope is set to Guest users only and the status is Active
    b. Reviewers: Ensure appropriate reviewer(s) are designated.
    c. Settings > General: Mail notifications and Reminders are set to Enable
    d. Reviewers: Require reason on approval is set to Enable
    e. Scheduling: Frequency is Monthly or more frequent.
    f. When completed: Auto apply results to resource is set to Enable
    g. When completed: If reviewers don't respond is set to Remove access

5.1.2 Ensure 'Access reviews' for high privileged Azure AD roles are configured

Profile Applicability: E5 Level 1

Assessment Status: Not Applicable

Impact Rating: Low

Description:

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organisation.

Ensure Access reviews for high privileged Azure AD roles are done no less frequently than weekly. These reviews should include at a minimum the roles listed below:

- Global Administrator
- Exchange Administrator
- SharePoint Administrator
- Teams Administrator
- Security Administrator

Note: An access review is created for each role selected after completing the process.

Rationale:

Regular review of critical high privileged roles in Azure AD will help identify role drift or potential malicious activity. This will enable the practice and application of "separation of duties" where even non-privileged users like security auditors can be assigned to review assigned roles in an organisation. Furthermore, if configured these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

Audit:

Verify access reviews for high privileged roles is in place:

1. Navigate to Microsoft Entra Admin Center https://entra.microsoft.com.
2. Expand Azure Active Directory > Identity Governance and select Privileged Identity Management
3. Select Azure AD Roles under Manage
4. Select Access reviews
5. Ensure there are access reviews configured for each high privileged roles and each meets the criteria laid out below:

    a. Scope – Everyone
    b. Status – Active
    c. Reviewers - Role reviewers should be designated personnel. Preferably not a self-review.
    d. Mail notifications - Enable
    e. Reminders - Enable
    f. Require reason on approval - Enable
    g. Frequency - Monthly or more frequent
    h. Duration (in days) - 4 at most
    i. Auto-apply results to resource - Enable
    j. If reviewers don't respond - No change

Any remaining settings are discretionary.

Note: Reviewers will have the ability to revoke roles should be trusted individuals who understand the impact of the access reviews. The principle of separation of duties should be considered so that no one administrator is reviewing their own access levels.

Note 2: The setting If reviewers don't respond is recommended to be set to Remove access due to the potential of all Global Administrators being unassigned if the review is not addressed.

5.2 Ensure Microsoft 365 audit log search is Enabled

Profile Applicability: E3 Level 1

Assessment Status: Compliant

Impact Rating: Low

Description:

When audit log search is enabled in the Microsoft Purview compliance portal, user and admin activity within the organisation is recorded in the audit log and retained for 90 days. However, some organisations may prefer to use a third-party security information and event management (SIEM) application to access their auditing data. In this scenario, a global admin can choose to turn off audit log search in Microsoft 365.

Rationale:

Enabling audit log search in the Microsoft Purview compliance portal can help organisations improve their security posture, meet regulatory compliance requirements, respond to security incidents, and gain valuable operational insights.

Audit:

Ensure Microsoft 365 audit log search is Enabled:

1. Navigate to Microsoft Purview https://compliance.microsoft.com.
2. Select Audit to open the audit search.
3. Choose a date and time frame in the past 30 days.
4. Verify search capabilities (e.g. try searching for Activities as Accessed files and results should be displayed).

To verify audit log search is enabled using PowerShell:

1. Connect to Exchange Online using Connect-ExchangeOnline.
2. Run the following PowerShell command:

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

3. Verify the resulting value is UnifiedAuditLogIngestionEnabled : True.

5.6 Storage

6.1 Ensure SharePoint external sharing is managed through domain whitelist/blacklists

Profile Applicability: E3 Level 2

Assessment Status: Not Compliant

Impact Rating: High

Description:

Control sharing of documents to external domains by either blocking domains or only allowing sharing with specific named domains.

Rationale:

Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the domains that users can share documents with will reduce that surface area.

Impact:

Enabling this feature will prevent users from sharing documents with domains outside of the organisation unless allowed.

Audit:

Ensure document sharing is being controlled by domains with whitelist or blacklist:

1. Navigate to the SharePoint Admin Center https://admin.microsoft.com/sharepoint.
2. Expand Policies then click Sharing.
3. Expand More external sharing settings and confirm that Limit external sharing by domain is checked.
4. Verify that an accurate list of allowed domains is listed.

6.2 Block OneDrive for Business sync from unmanaged devices

Profile Applicability: E3 Level 2

Assessment Status: Not Applicable

Impact Rating: High

Description:

Microsoft OneDrive allows users to sign into their cloud tenant account and begin syncing select folders or the entire contents of OneDrive to a local computer. By default, this includes any computer with OneDrive already installed, whether or not it is Azure Domain Joined or Active Directory Domain joined.

Rationale:

Unmanaged devices pose a risk since their security cannot be verified through existing security policies, brokers or endpoint protection. Allowing users to sync data to these devices takes that data out of the control of the organisation. This increases the risk of the data either being intentionally or accidentally leaked.

Note: This setting is only applicable to Active Directory domains when operating in a hybrid configuration. It does not apply to Azure AD domains. If there are devices which are only Azure AD joined, consider using a Conditional Access Policy instead.

Impact:

Enabling this feature will prevent users from using the OneDrive for Business Sync client on devices that are not joined to the domains that were defined.

Audit:

To ensure sync settings on unmanaged devices:

1. Navigate to the SharePoint Admin Center https://admin.microsoft.com/sharepoint.
2. Click Settings followed by OneDrive – Sync
3. Verify that Allow syncing only on computers joined to specific domains is checked
4. Verify that the Active Directory domain GUIDS are listed in the box.
5. Use the Get-ADDomain PowerShell command to obtain the GUID for each on-premises domain

6.3 Ensure expiration time for external sharing links is set

Profile Applicability: E3 Level 1

Assessment Status: Not Compliant

Impact Rating: Low

Description:

The external sharing features of Microsoft SharePoint let users in the organisation share content with people outside the organisation (such as partners, vendors, clients, or customers). External sharing in SharePoint is part of secure collaboration with Microsoft 365.

Rationale:

An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, and then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared. Restricting how long the links are valid can reduce the window of opportunity for attackers.

Impact:

Enabling this feature will ensure links expire within the defined number of days. This will have an effect on links that were previously not set with an expiration.

Audit:

Ensure the expiration time for external sharing links is set:

1. Navigate to the SharePoint Admin Center https://admin.microsoft.com/sharepoint.
2. Click to expand Polices then select Sharing.
3. Under Choose expiration and permissions options for Anyone links check These links must expire within this many days.
4. Confirm the number of days is set to the desired value, such as 30.

Note: The UI settings will not appear if the External sharing slider for SharePoint is set to New and existing guests or anything less permissive.

End of Document