**Purpose**: This document captures the findings from the review of CUSTOMER instance of the Microsoft Office 365 configuration against best practice recommendations. Potential threats and observations are also recorded during the engagement, analysing configurations through various Microsoft administration portals.

**Approval:** This document contains highly sensitive information and has been classified as CONFIDENTIAL. It has been reviewed and approved for distribution to Talanos internal staff members and to the CUSTOMER (Customer's) internal staff members responsible for IT security.

A full change log should be kept to record document versions, authors of contents and the relevant changes.

| Date | Author | Version | Changes |
|---|---|---|---|
| | | V 0.1 | |
| | | | |
| | | | |
| | | | |

**Supporting Documentation:** This document should be read along with the complete control reference:
**CUSTOMER Microsoft-365 Control Reference.xlsx**

## 1. Executive Summary

Talanos Cybersecurity has been requested by CUSTOMER to perform an assessment of their Microsoft 365 Security platform instance.

This comprehensive assessment of Microsoft Office 365 (O365) was conducted to evaluate the effectiveness, security, and overall performance of the platform. The primary objective was to highlight areas of excellence, potential vulnerabilities, and avenues for optimization, ensuring that O365 aligns seamlessly with CUSTOMER strategic business objectives.

The assessment included a comprehensive review of multiple security controls across below categories:

- Identity
- Email
- Microsoft Teams
- SharePoint
- Applications
- Endpoint Manager
- Information Protection
- Microsoft Defender and E5 Security
- Microsoft Intune
- Defender for Office
- Sway
- Data Lifecycle Management

Below are some key observations about the environment's security configuration:

**1. Pilot Testing Phase Policies:** Numerous critical policies, including Conditional Access and Data Loss Prevention (DLP) policies have been created but are in Pilot /Testing phase.

**2. Stale User Accounts**: There are user accounts that have been disabled for quite some time, potentially classified as stale accounts, but they have not been removed from the EntraID directory.

**3. Identity Lifecycle Policies:** Identity lifecycle policies are not configured. These policies are essential for regulatory compliance, data security and privacy, efficient data management as well as risk management.

**4. Device Security Configuration:** Local Security Authority Subsystem Service (LSASS.exe) is currently still enabled on devices. Attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS.

**5. Cross-Tenant Access:** Cross-tenant access is currently configured for "XXX", "XXX", and "XXX".

**6. Direct Login for Shared Mailboxes:** Several shared mailboxes have direct login enabled. This poses risks such as accountability issues, data breaches, and compliance concerns.

The detailed report, provided separately, delves into specific findings and offers actionable recommendations to secure CUSTOMER Microsoft 365 Security platform. Addressing these key observations will enhance the platform's security, aligning it more effectively with CUSTOMER strategic requirements.

## 2. Microsoft Control Review

### 2.1. Summary

Microsoft Office 365 is an integral part of CUSTOMER business, providing key services such as Azure Active Directory for identity management, email services, SharePoint and OneDrive for file management, Microsoft Teams for collaboration, and device management. Given the various ways sensitive business data can be accessed, ensuring the security of CUSTOMER Microsoft Office 365 suite is imperative.

Talanos conducted a comprehensive assessment of CUSTOMER Microsoft Office 365 (O365) security. The assessment included a thorough examination of identity management, checking user authentication, and access controls. Talanos scrutinized the details of email security, Teams collaboration, and SharePoint usage, identifying strengths and areas for improvement. The assessment also covered application security, Endpoint Manager, Information Protection, Microsoft Defender with E5 Security, Microsoft Intune, Defender for Office, Sway, and Data Lifecycle Management, ensuring a holistic examination of the O365 environment.

The assessment has been conducted after reviewing multiple controls under security categories. The below table shows an overview of the status of these controls.

| | Number of Controls | Complete | Partially Complete | Not Done |
|---|---|---|---|---|
| Identity | 44 | 21 | 10 | 13 |
| Email | 23 | 11 | 9 | 3 |
| Teams | 17 | 8 | 4 | 5 |
| SharePoint | 9 | 2 | 3 | 4 |
| Applications | 5 | 3 | 2 | 0 |
| Endpoint Manager | 7 | 6 | 0 | 1 |
| Information Protection | 7 | 2 | 5 | 0 |
| Microsoft Defender and E5 Security | 138 | 42 | 36 | 60 |
| Microsoft Intune | 27 | 11 | 3 | 13 |
| Defender for Office | 37 | 17 | 15 | 5 |
| Sway | 1 | 0 | 0 | 1 |
| Data Lifecycle Management | 12 | 0 | 1 | 11 |
| | **327** | **123** | **88** | **116** |

A detailed scoring system was utilized that considered the specific requirements and best practices for each control, providing a comprehensive overview of their O365 security posture and guidelines towards areas of improvement for a more robust security posture.

| Sr. No. | | CUSTOMER Score | Target Score |
|---|---|---|---|
| 1 | Identity | 120 | 205 |
| 2 | Email | 79 | 114 |
| 3 | Teams | 38 | 59 |
| 4 | SharePoint | 16 | 33 |
| 5 | Applications | 21 | 25 |

| | | | |
|---|---|---|---|
| 6 | Endpoint Manager | 30 | 35 |
| 7 | Information Protection | 20 | 31 |
| 8 | Microsoft Defender and E5 Security | 207 | 346 |
| 9 | Microsoft Intune | 52 | 93 |
| 10 | Defender for Office | 79 | 125 |
| 11 | Sway | 0 | 3 |
| 12 | Data Lifecycle Management | 3 | 38 |

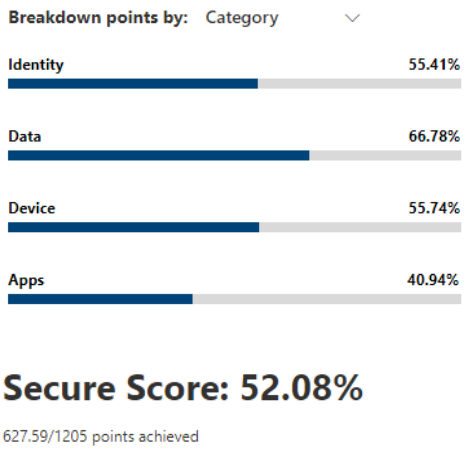
## 2.2. Out of Scope

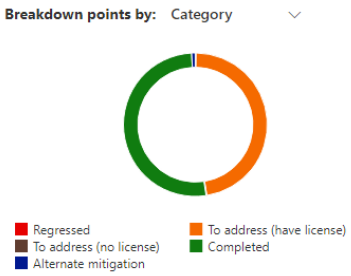
a. Microsoft 365 integration with CUSTOMER on-premises Active Directory infrastructure is out of scope of this report.
b. Analysis of current licence for Landing Zone. The analysis of licence requirement will be part of Landing Zone design.

## 2.3. Microsoft Secure Score

Microsoft Secure Score represents an overall scoring of security across five key Microsoft 365 areas: identities, data, apps, devices, and infrastructure, each with its own associated score. The higher the score, the more secure these are. It is a good check of overall system security health and by assessing each area the individual and overall scores can be raised. Microsoft Secure Score is also based on Microsoft licensing, CUSTOMER has Microsoft 365 E3 and Microsoft 365 E5 Security licence.

Microsoft Secure Score is always changing, a score of 627 today may reduce over time as new threats are found and new mitigation options are available. A continuous management through the monitoring of various logs is required and regular reviews of the current Security Score to implement ongoing improvements is required.



## 3. Security Assessments

*To assess the current Microsoft 365 environment and security configurations, dedicated accounts were used with the following assigned roles:* ***Security Reader*** *and* ***Global Reader***

Microsoft 365 security solutions are built on four pillars: identity and access management, threat protection, information protection, and security management. Microsoft 365 includes products for each pillar that work together to keep your organization safe.


Customer has the Microsoft 365 E3 product licence with the Microsoft 365 E5 Security add on licence. The Microsoft 365 E5 Security includes: Entra ID , MS Defender for Office 365, MS Defender for Identity, MS Defender for cloud Apps and MS Defender for Endpoint. The last four are also known collectively as "Microsoft 365 Defender".

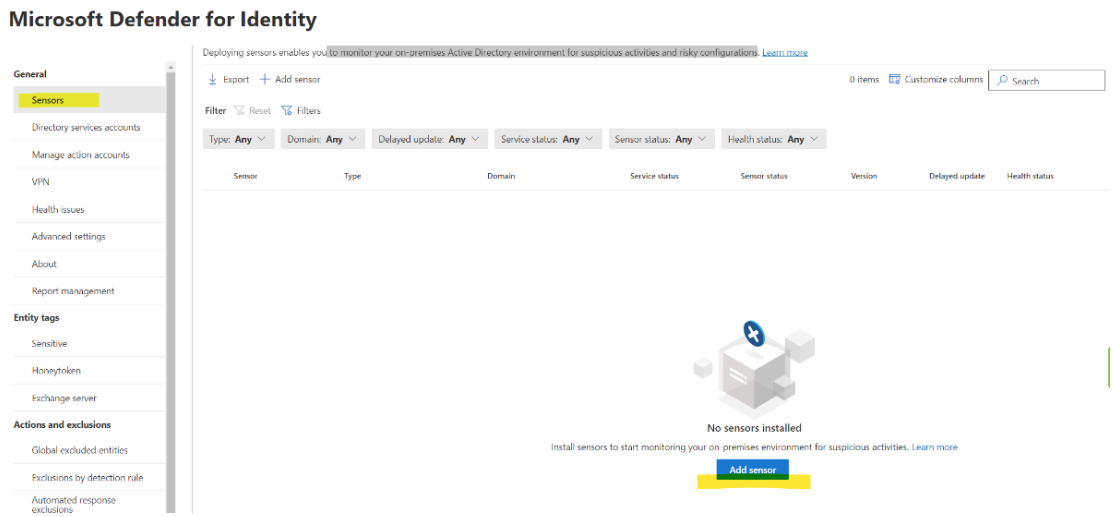
### 3.1. Identity

Identity assessments typically concentrate on evaluating the effectiveness of identity management within the organization's Microsoft 365 environment.

The current overall configuration of Identity features in the CUSTOMER instance is moderately efficient, with conditional access policies configured.

**Key Findings:**

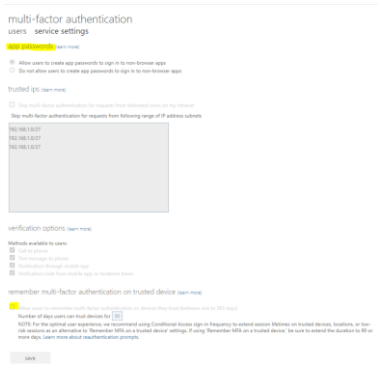
a. Audit identified an excessive number of privileged role assignments, amplifying risks such as insider threats and complicating access governance. A recommended strategy is to minimize and closely monitor privileged accounts.
b. Implementing MFA has significantly reduced the risk of identity breaches. While MFA is enabled in the tenant, there are additional settings listed below that can further enhance its effectiveness.
c. Conditional access policies have been created, but they are configured and applied to pilot groups, with some in report-only mode.
d. There are a number of disabled accounts have not been accessed recently. This may indicate a lack of a user cleanup procedure or a current security policy ensuring the review of user accounts, as well as security and distribution groups.
e. There are currently no sensors configured for the CUSTOMER instance in Microsoft Defender for Identity (previously called Azure ATP), which hinders the detection of identity-based attacks in the hybrid environment.



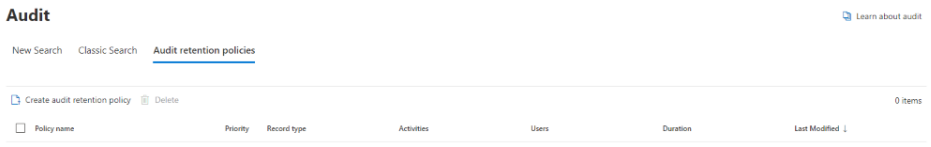

Configuring this will help capture signals from Windows Active Directory deployed on-premises and Azure Active Directory in the cloud. It processes these signals, using them to detect, investigate, and respond to threats, including malicious insiders and compromised accounts.

Recommendations:

a. Disable app passwords if possible. If there are no legacy clients that do not support MFA, this is recommended.
b. Disable text and phone call as MFA methods.
c. Enable "remember MFA on trusted devices" and to 90 days




d. Configure password-less authentication using Windows Hello and 2FA keys where possible.
e. Create break glass accounts exempted from MFA and CA policies in case of AAD MFA being down.
f. Creating a Conditional Access policy to block Geographic locations where Customer does not have offices. Current location "Customer Trusted Locations" does exist, but is only specified with certain IP ranges.
g. Create an audit retention policy for maximum retention, currently no policy configured.




h. Develop procedure for a regular user and group review and cleanup in Entra ID (AAD).

### 3.2. E-Mail Security

Email remains one of the most common attack vectors, with many high-profile breaches starting from a simple phishing email that harvested an ordinary user's credentials.

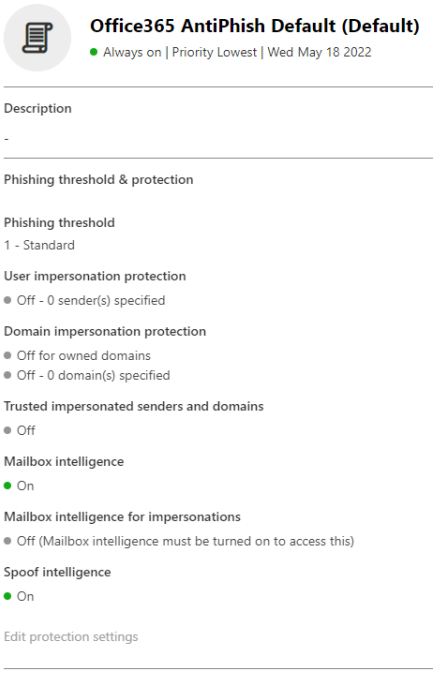
The current email security for the CUSTOMER tenant is well-established and effectively meets security requirements. However, there are opportunities for further optimization and enhancement. By exploring these areas for improvement, email system can be further refined, ensuring it remains robust, secure, and efficient in supporting evolving organizational needs.

#### Key Findings:

a. Mailbox intelligence for impersonations is currently not enabled.
b. Safety tips are not enabled. Safety Tips are a feature designed to provide users with a quick visual cue about the safety status of an email. These tips can help users make informed decisions about how to interact with their email messages.
c. There are several shared mailboxes that have direct login enabled. This poses risks such as accountability issues, data breaches, and compliance concerns. It's generally recommended to access shared mailboxes through individual user accounts with appropriate permissions.
d. Spam Confidence Level (SCL) is not configured. This is an essential component of Microsoft's email filtering technology, helping categorize emails and take appropriate action to manage spam effectively.

#### Reccomendations:

a. Enable Mailbox intelligence for impersonations setting to take action on messages that are identified as impersonation attempts.
b. Enable the remaining safety tips for user impersonation, domain impersonation and unusual characters.




c. Configure Safe links policy for all users globally. Currently applied to pilot group of 34 users.
d. There are 17 shared mailboxes that have login enabled. Review if they are required and block login where login is not required.
e. Under Safe attachments policy, "Enable Redirect" should be enabled with "Send messages that contain monitored attachments to the specified email address." to security team mailbox. This will help in monitoring action.
f. Ensure Spam confidence level (SCL) is configured in mail transport rules with specific domains.
g. DKIM for Customerholdings.com is disabled. To be revisited by business.

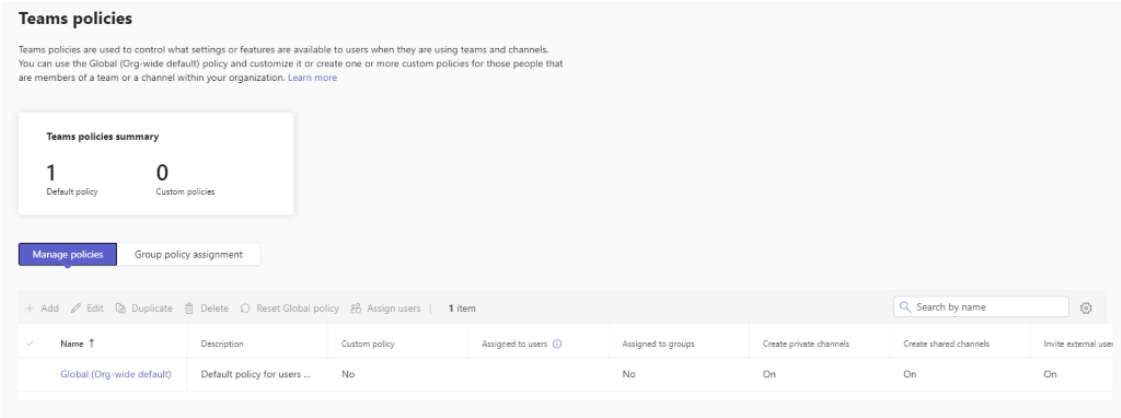
### 3.3. Microsoft Teams

Microsoft Teams is a widely used collaboration and communication platform, part of the Microsoft 365 suite, offering features like chat, video conferencing, file sharing, and integration with various Microsoft and third-party applications. While it brings significant productivity benefits, there are inherent security risks associated such as phishing and social engineering, insecure external sharing and even possible data breaches.

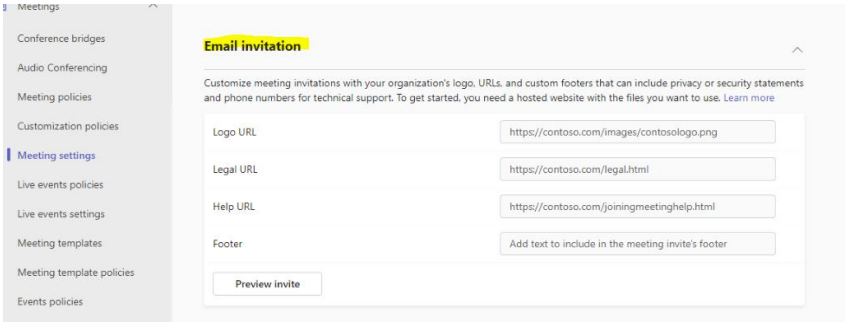
The current default security best practices are configured for the CUSTOMER Teams tenant. There are however some additional areas that can be configured to enhance the security posture withing Microsoft Teams, ensuring the platform is used safely and in compliance with organizational and regulatory standards.

**Key Findings:**

a. There are currently no Teams' policy created to limit creation of channels. It is best practise to only allow certain privileged users to create Private channels.




b. No Custom Email Invitation configured. Customized meeting invitations with your company logo, URL and contact details builds trust. Recognizable branding can make invitees more confident about the legitimacy of the invitation, reducing the risk of them dismissing it as spam or phishing.




c. Collaboration Restrictions is set to : *Allow invitations to be sent to any domain (most inclusive)*
There are some Cross-tenant access configured currently for the following organizations:
This should be reviewed by business and if no longer required, be removed from the tenant.

**Recommendations:**

a. Configure customized meeting invitation branding.
b. Configure settings so only invited users can be admitted automatically.
c. Review cross-tenant access.
d. Restrict anonymous users from joining meetings.
e. Limit private channel creation to a set of users.

### 3.4. SharePoint

Microsoft SharePoint enables organizations to store, organize, share, and access information from any device. Despite its versatility and utility, SharePoint poses certain security risks, such as unauthorized access, insecure external sharing, phishing, malware, and insider threats.

The basic security configurations, including the critical setting controlling external sharing of files, have been set for the CUSTOMER tenant. However, there are some settings that are partially completed and others that have not been set at all, requiring attention.

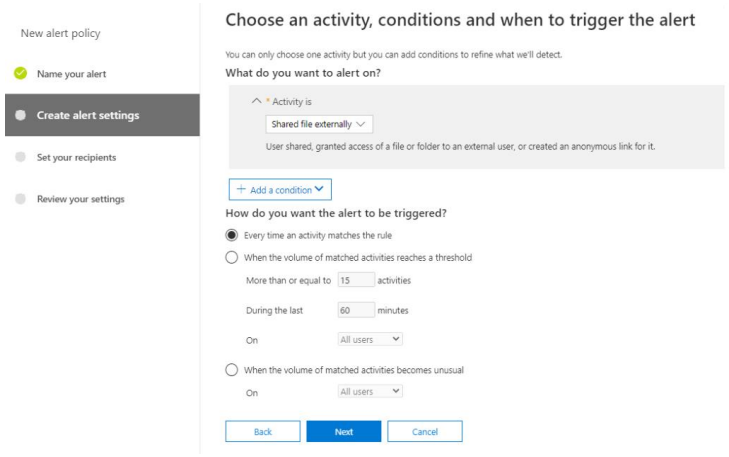
**Key Findings:**

a. Alerts are not configured to notify the appropriate security team / person when files are shared externally.
b. OneDrive for Business sync is not blocked for unmanaged devices.
c. The signing out of inactive users is not set.

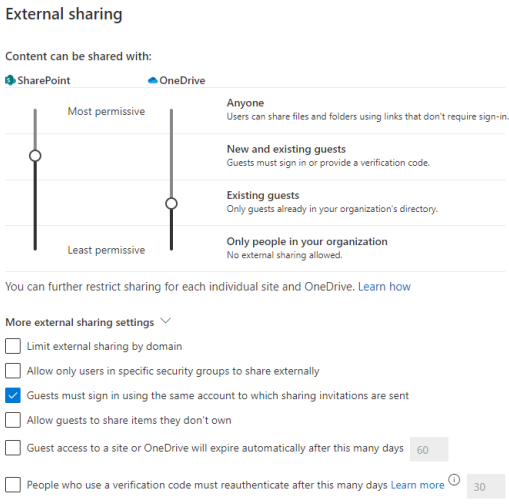
**Recommendations:**

The following additional recommendations should be considered:

a. Configure an alert policy to be informed when SharePoint folder or files are shared externally.




b. Configure External file sharing settings to "guest access to expire after 60 days or less".
c. Configure External file sharing settings to "people using verification code must reauthenticate".




d. Idle session time-out should be enabled under Access control. It is currently not enabled.

## 3.5. Applications

In the context of Microsoft 365 security, Enterprise and OAuth applications play a significant role, but also present certain security considerations.

Enterprise applications are third-party or custom-developed applications integrated with Microsoft 365 services. Granting these applications access to Microsoft 365 data can be risky if not managed properly. They could potentially access, modify, or share sensitive data.

OAuth is an open standard for access delegation commonly used as a way for users to grant websites or applications access to their information on other websites but without giving them the passwords. OAuth apps can be a vector for phishing attacks, where malicious apps masquerade as legitimate ones to gain access to users' data. There's also the risk of excessive permissions being granted to these apps.

**Key Findings:**

a. There are no key findings in this section as there no OAuths apps configured in the CUSTOMER tenant. Some recommendations are made below in terms of Enterprise applications.

**Recommendations:**

a. Although there are no suspicious applications identified from the list of enterprise applications, there are some applications with a naming convention that is not descriptive such as testapp and test as examples. They have been checked however and found that no admin or user permissions have been granted to these.

   It's crucial to regularly review and audit the permissions granted to these applications, ensure they adhere to least privilege access principles, and use secure development practices.

### 3.6. Microsoft Intune and Endpoint Manager

Microsoft Intune is a cloud-based service focused on mobile device management (MDM) and mobile application management (MAM). To optimize its usage, it is important to follow best practices that enhance both security and efficiency.

The current overall configuration of Microsoft Intune's features in CUSTOMER instance are moderately efficient. Best practises such as compliance policies, conditional access and security groups with Intune deployment rings for autopatch have been configured. These rings provides for Ring 1 for test users, Ring 2 for Pilot users and then Ring 3 for broad deployment to the majority of the user-base.

**Key Findings:**

a. There are a significant number of devices that has a compliance status of "non-compliant"
b. The "device management policies are required for email profiles" policy is not set.
c. Automatic device enrolment is not configured. This enable devices to enrol automatically when they join or register in your hybrid Microsoft Entra ID environment.
d. Device cleanup rules are not configured.

**Recommendations:**

a. Define device groups such as Company Devices, Phones, Personal Devices etc.
b. Create Company terms and conditions.
c. Create Company terms and conditions.

d. Customize Company Portal branding.
e. Configure Windows 10/11 automatic enrolment.
f. Configure device cleanup rules.
g. Configure device restrictions policy. There are a number of them shared in the Control reference document.

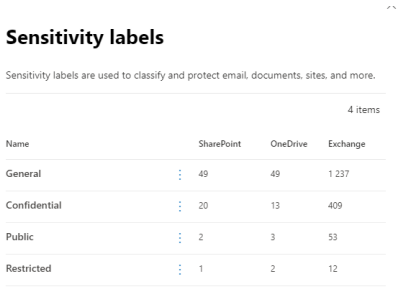
### 3.7. Information Protection

Microsoft Information Protection offers a comprehensive approach to securing sensitive data, providing tools for classification, protection, and monitoring, and is a crucial component for any organization's data security and compliance strategy.

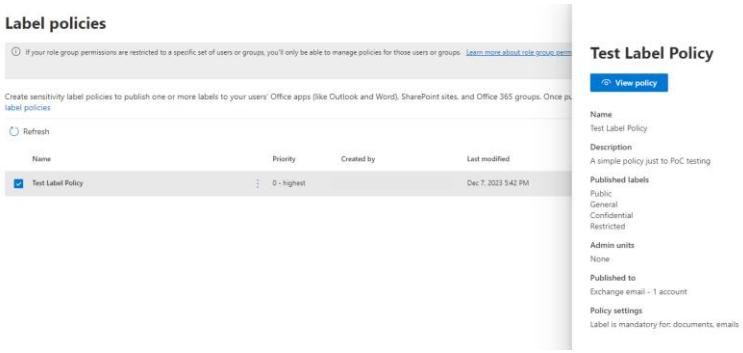
CUSTOMER has successfully started creating and implementing sensitivity labels in their tenant.

**Key Findings:**

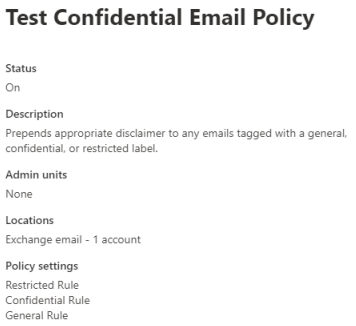
a. Labels have been created but no content marking or encryption have been configured for the labels.




b. Microsoft 365 sensitivity label data classification policies have been created, but currently in test phase




c. DLP policies created are currently in test phase




Recommendations:

a. Configure content markings and encryption for sensitivity labels where required.
b. It is recommended that the testing Label policy advance to the evaluation, refinement, and eventual deployment phases.
c. It is recommended to create more effective DLP policies that best suite the business needs for example:
    i. Regulatory Compliance Policies that align with regulatory requirement like GDPR for personal data, HIPAA for health information and PCI-DSS for payment card information.
    ii. Intellectual Property Protection policies to prevent unauthorized sharing or transfer of proprietary or confidential business information, including trade secrets, internal project documents, and research data.
    iii. Preventing Financial Data Leakage by establishing policies to protect sensitive financial information, such as bank account details, financial statements, and payroll information.
    iv. Geographical Restrictions for organizations with specific regional compliance requirements, set up policies that restrict the transfer of data across geographic boundaries.

### 3.8. Microsoft Defender

Microsoft Defender is a suite of security software products offered by Microsoft, providing comprehensive protection against various types of cyber threats. With the MS 365 Security add-on that CUSTOMER procured, the suite of products includes Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, and Microsoft Defender for Office (scored in a separate section below).

CUSTOMER has successfully implemented the majority of the essential settings for Microsoft Defender, demonstrating a solid foundation in its cybersecurity approach. However, there are some additional configurations and features of Microsoft Defender that have not yet been fully utilized or optimized.

Addressing these areas will further enhance the organization's security posture and ensure more comprehensive protection against potential cyber threats.

Key Findings:

a. No advanced audit retention policies have been configured for users.
b. Adaptive protection is currently not enabled therefore insider risk management policies cannot be configured
c. Lsass.exe is not blocked via any ASR rules for any devices. Attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS
d. No DLP polices have been configured for Microsoft Teams to prevent people from sharing sensitive information in a Microsoft Teams channel or chat session.

e. Microsoft Defender Application Guard is not configured. Employees browsing untrusted sites with malicious behaviour expose the host PC to attackers gaining access to sensitive data such as enterprise credentials.

**Recommendations:**

a. Define policies that prevent people from sharing sensitive information in a Microsoft Teams channel or chat session in MS Purview.
b. Configure Advanced Audit retention policies to 1 year for all users.
c. Enable adaptive protection and configure Insider Risk Management policies.
d. Configure Communication Compliance policies and reviewers.
e. Access reviews to be configured for Azure AD directory roles, teams and groups.
f. Turn on Microsoft Defender Application Guard managed mode. This helps prevent untrusted files from accessing trusted resources, keeping your enterprise safe from new and emerging attacks. This is a feature that can be deployed via Group Policy or manually from windows features in Windows10/11.
g. Implement the highest ranking "Recommended Actions" with the lowest User Impact under Microsoft Secure score first as this will considerably increase the overall security posture whilst also increasing the Secure Score.

### 3.9. Defender for Office

Microsoft 365 for Office 365 is a service that offers protection for organization's Office 365 services, including email, links (URLs), and collaboration tools.

It can be seen from our audit that CUSTOMER has proactively developed policies for Microsoft Defender for Office 365, which are currently in the pilot testing phase. This stage is crucial for fine-tuning the policies and ensuring they align effectively with the organization's specific security needs and operational workflows before a full-scale implementation.

**Key Findings:**

a. Exchange Online Spam Policies are not set to alert administrators. This ensures that administrators are promptly informed about potential spam incidents, allowing for quick action and analysis.
b. There are 27 allowed senders and 11 allowed domains in the policy called "Customer Spam Policy 2023".
c. There are allowed IP addresses in the connection filter policy. This is not recommended as per Microsoft.
d. Email bulk complaint level (BCL) threshold currently set to 7. This is default anti-spam threshold setting.

**Recommendations:**

a. Configure notifications to Ensure Exchange Online Spam Policies are set to notify administrators.
b. Ensure that no send domains are allowed for anti-spam policies. Remove all allowed domains and allowed senders from all your inbound anti-spam policies.
c. Microsoft recommends not adding allowed IP addresses to the connection filter policy as this can inadvertently create security loopholes. Even if an IP address is currently trusted, it can become compromised in the future, potentially allowing a bad actor to bypass email filters.
d. Set the email bulk complaint level (BCL) threshold to be 6 or lower. Threshold setting can be set from 1-9 where 1 marks most bulk email as spam, and 9 allows most bulk email to be delivered.

### 3.10. Sway

Sway is a Microsoft 365 app that helps you and your colleagues express ideas using an interactive, web-based canvas.

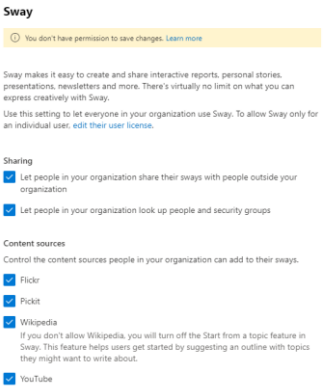
Sway benefits from the security infrastructure of Microsoft 365, which includes a range of security features and compliance standards. Since it is integrated into the Microsoft 365 suite, Sway inherits the security assurances such as data encryption, authentication and sharing controls.
There are only a few additional Sharing and Content sources settings that are controlled by administrators.

**Key Finding:**

a. The only finding for sway that can be identified is that sharing outside of the organization is enabled currently.

**Recommendation:**

a. Ensure that Sways cannot be shared with people outside of your organization by changing the Org settings in the Microsoft 365 admin centre.




### 3.11. Data Lifecycle Management

Data Lifecycle Management (DLM) in Microsoft 365 refers to the policies and processes that manage the flow of an organization's data throughout its lifecycle, from creation and initial storage to the time it becomes obsolete and is deleted.

Implementing and managing these data retention aspects within Microsoft 365 helps organizations control their data throughout its lifecycle, minimize risks, and comply with legal and regulatory requirements.

There are currently no Data Retention policies created except for the Data retention policy for Exchange Mailboxes that is set "infinite".

**Key Findings:**

a. Data retention policies for the following does not exist:
   i. SharePoint sites
   ii. OneDrive accounts
   iii. Microsoft 365 group mailboxes & sites

iv. Teams channel messages, chats and private channel messages
v. Exchange public folders
vi. Skype for business

**Recommendation:**

a. It is recommended to implement Data Retention policies for the applications mentioned above. The policies can be according to the local regulatory requirements for example GDPR in EU.

## 4. Conclusion

The Microsoft Office 365 assessment covered crucial aspects including identity management, email security, Microsoft Teams, SharePoint, Microsoft Information Protection, and Microsoft Defender.

While CUSTOMER has implemented foundational security measures across these platforms, there are opportunities for further refinement. Recommendations include enabling mailbox intelligence for impersonations, implementing safety tips, reviewing direct logins for shared mailboxes, configuring Spam Confidence Level (SCL), and optimizing Microsoft Teams and SharePoint security settings.

In addition, the review highlighted successes such as the initiation of sensitivity labels in Microsoft Information Protection and the majority implementation of essential settings in Microsoft Defender.

Addressing the identified areas for improvement will not only improve CUSTOMER security posture but also align the organization more closely with best practices and compliance standards. This ongoing security optimization ensures a resilient, efficient, and secure digital environment that will effectively support CUSTOMER evolving organizational needs.