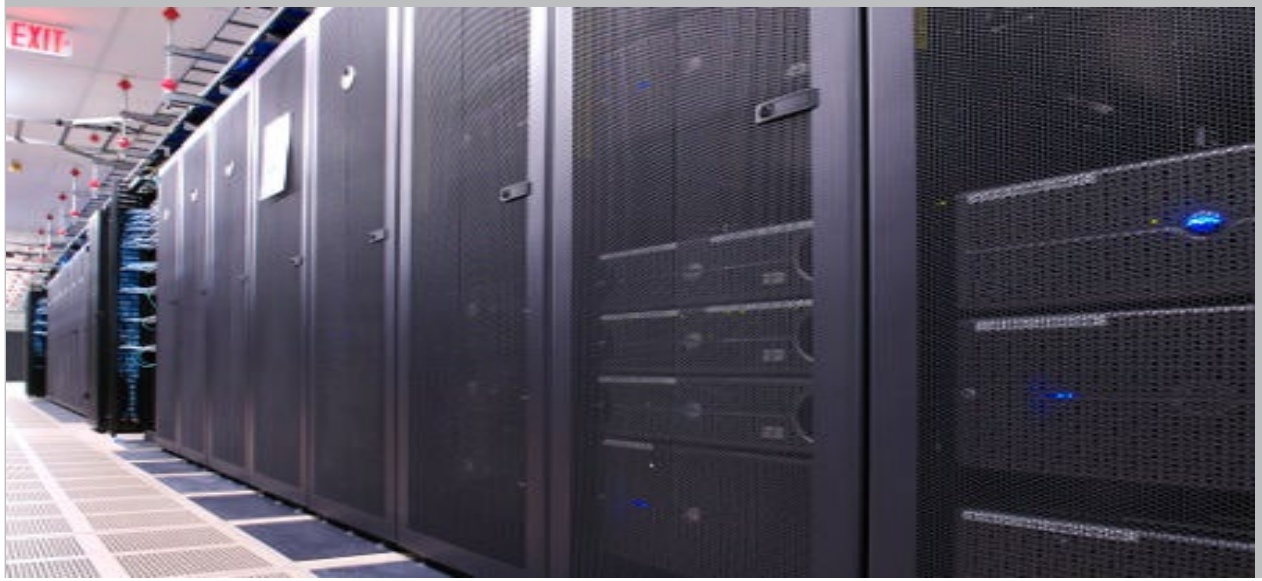
MICROSOFT CLOUD ASSESSMENT

Microsoft Cloud Security Assessment



Scan Date: 07/09/2025

Prepared for: TEL5

Prepared by: TEL5

07/09/2025

TEL5 PTY LTD
WWW.TEL5.COM.AU
0881005255
INFO@TEL5.COM.AU

Prepared for:
TEL5
Scan Date:
07/09/2025

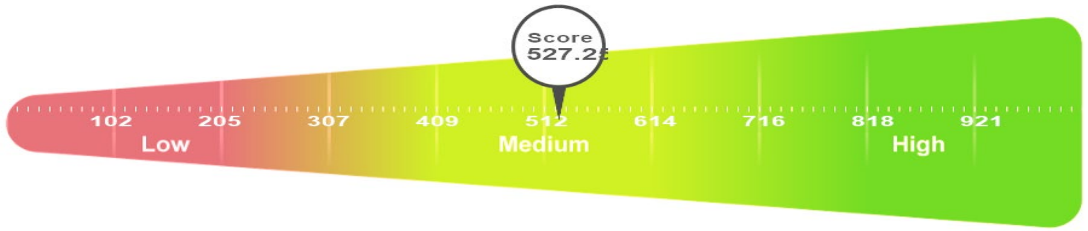
Table of Contents

1 - Overview

This report presents a consolidated view of the security of the Microsoft Cloud environment. The assessment consists of a view of your current Microsoft Secure Score and shows trends over time. The Microsoft Secure Score is a proprietary security score provided by Microsoft. It is an aggregate of scores provided by implementing various security controls and best practices. The score is a relative measure and while there is a theoretical maximum, it may not always be possible or desirable to the business to obtain the maximum score possible. This report further breaks down the various Microsoft Controls and their associated Control Scores. A trained IT professional should review the controls and assist in identifying and prioritizing which controls should be implemented. The final aspect of this security assessment is a review of alerts which have recently occurred.

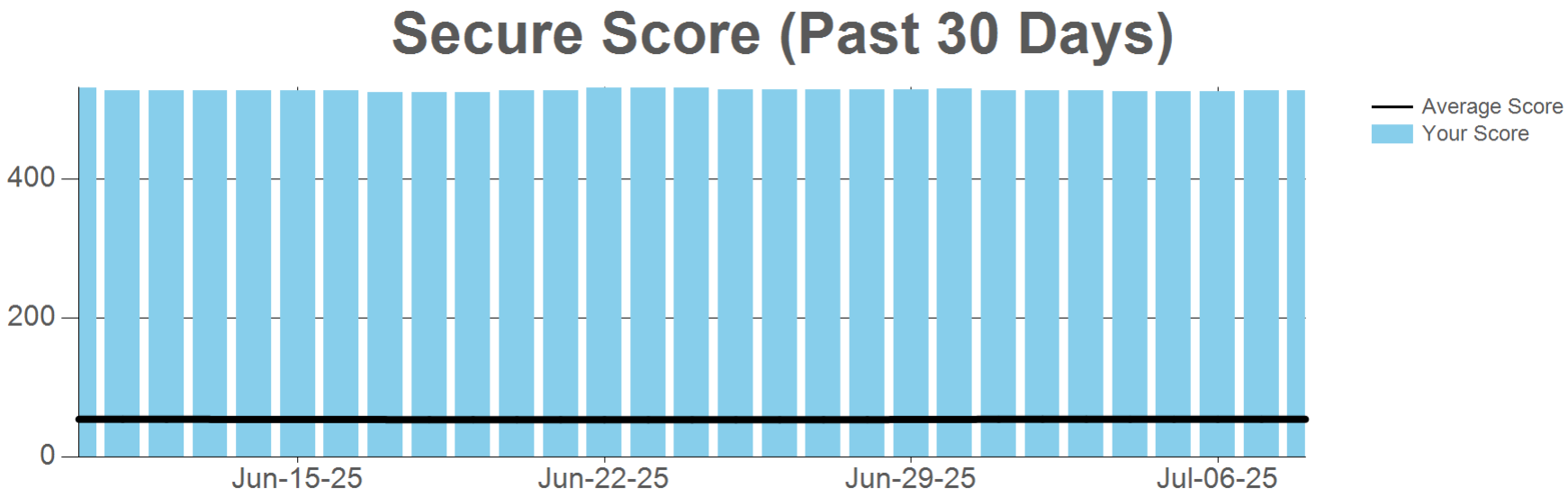
2 - Current Secure Score

Your current Microsoft Secure Score is **527.25** and is shown compared to your theoretical maximum. The more improvement actions you take, the higher your Secure Score will be. The theoretical maximum changes based on the number of users, devices, groups, and subscriptions. Your current theoretical maximum is **1023**.



3 - Secure Score Trend

The following chart shows changes to your Secure Score over time. It also shows the average score of your peer group as a reference. The secure score should be used as a relative measure of security. A qualified IT professional can assess and prioritize which security controls are appropriate for your organization.



4 - Control Scores

Implementing best practice controls can result in a more secure environment. Microsoft assigns a control score based on the organization's progress in implementing these measures. Below is a table showing the individual controls and your specific scores. Scores of 0 indicate controls that should be evaluated and implemented if possible.

CONTROL NAME	DESCRIPTION	SCORE
Apps		
Create Safe Links policies for email messages (mdo_safelinksforemail)	MDO Built-in protection policy will provide base level safe links protection for everyone by default. You could also create additional Safe Links policies for enhanced or customized Safe Links operations.	9
Ensure that mailbox intelligence is enabled (mdo_enablemailboxintelligence)	Turns on artificial intelligence (AI) that identifies users' email patterns with their frequent contacts to spot potential phishing attempts.	8
Turn on Safe Attachments in block mode (mdo_safeattachments)	Safe Attachments in block mode prevents messages with detected malware attachments from being delivered. These messages are quarantined and only admins (not regular users) can review, release, or delete them. This will also automatically block future malware attachments. MDO Built-in protection policy provides safe attachments protection for everyone by default. You could also create additional Safe Attachment policies for customized Safe Attachment operations.	8
Create zero-hour auto purge policies for malware (mdo_zapmalware)	Zero-hour auto purge (ZAP) quarantines the message that contains malware attachment for both read, as well as unread, messages that are found to contain malware after delivery. Only admins can view and manage messages that have been quarantined. For additional information, see https://docs.microsoft.com/microsoft-365/security/office-365-security/zero-hour-auto-purge Zero-hour auto purge (ZAP) in Exchange Online.	6
Ensure 'External sharing' of calendars is not available (exo_individualsharing)	Users should not be allowed to share the full details of their calendars with external users.	5
Ensure Safe Attachments policy is enabled (mdo_safeattachmentpolicy)	The Safe Attachments policy helps protect users from malware in email attachments by scanning attachments for viruses, malware, and other malicious content. When an email attachment is received by a user, Safe Attachments will scan the attachment in a secure environment and provide a verdict on whether the attachment is safe or not. Rationale: Enabling Safe Attachments policy helps protect against malware threats in email attachments by analyzing suspicious attachments in a secure, cloud-based environment before they are delivered to the user's inbox. This provides an additional layer of security and can prevent new or unseen types of malware from infiltrating the organization's network.	5

CONTROL NAME	DESCRIPTION	SCORE
Ensure the Common Attachment Types Filter is enabled (mdo_commonattachmentsfilter)	There are certain types of files that are risker to send and receive via email due to the likelihood that they contain malware (for example, executable files). To make sure these file types don't get through, enable the common attachment filter. You can use the default list of file types or customize it. The default file types are: .ace, .ani, .app, .docm, .exe, .jar, .reg, .scr, .vbe, .vbs. Messages with the specified attachments types are treated as malware and are automatically quarantined.	5
Set action to take on high confidence phishing detection (mdo_highconfidencephishaction)	Set the action that will be taken on high confidence phishing detection.	5
Set action to take on high confidence spam detection (mdo_highconfidencespamaction)	Set the action that will be taken on high confidence spam detection.	5
Set action to take on phishing detection (mdo_phisspamacation)	Set the action that will be taken on phishing detection.	5
Set action to take on spam detection (mdo_spamaction)	Set the action that will be taken on spam detection.	5
Turn on Microsoft Defender for Office 365 in SharePoint, OneDrive, and Microsoft Teams (mdo_atpprotection)	Microsoft Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams protects your organization from inadvertently sharing malicious files.	5
Turn on Safe Documents for Office Clients (mdo_safedocuments)	Safe Documents uses Microsoft Defender for Endpoint to scan documents and files for malicious content. To keep you protected, Safe Documents sends files to the Defender for Endpoint cloud for analysis. Files sent by Safe Documents are not retained in Defender for Endpoint beyond the time needed for analysis (typically, less than 24 hours).	5
Create zero-hour auto purge policies for phishing messages (mdo_zapphish)	For read or unread messages that are identified as phishing after delivery, the ZAP outcome depends on the action that's configured for a Phishing email filtering verdict in the applicable anti-phishing policy. For additional information, see https://docs.microsoft.com/microsoft-365/security/office-365-security/zero-hour-auto-purge Zero-hour auto purge (ZAP) in Exchange Online.	3
Ensure Exchange Online Spam Policies are set to notify administrators (mdo_spam_notifications_only_for_admins)	In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations 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 organization has been blocked for sending spam emails. Note: Audit and Remediation guidance may focus on the Default policy however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.	3

CONTROL NAME	DESCRIPTION	SCORE
Ensure Microsoft 365 audit log search is Enabled (mip_search_auditlog)	When audit log search in the Microsoft Purview compliance portal is enabled, user and admin activity from your organization is recorded in the audit log and retained for 90 days. However, your organization might be using a third-party security information and event management (SIEM) application to access your auditing data. In that case, a global admin can turn off audit log search in Microsoft 365.	3
Ensure modern authentication for Exchange Online is enabled (exo_oauth2clientprofileenabled)	Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. When you enable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use modern authentication to log in 'to Microsoft 365 mailboxes. When you disable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use basic authentication to log in to Microsoft 365 mailboxes. When users initially configure certain email clients, like Outlook 2013 and Outlook 2016, they may be required to authenticate using enhanced authentication mechanisms, such as multifactor authentication. Other Outlook clients that are available in Microsoft 365 (for example, Outlook Mobile and Outlook for Mac 2016) always use modern uthentication to log in to Microsoft 365 mailboxes	3
Ensure Safe Links for Office Applications is Enabled (mdo_safelinksforOfficeApps)	Enabling Safe Links policy for Office applications allows URL's that exist inside of Office documents and email applications opened by Office, Office Online and Office mobile to be processed against Defender for Office time-of-click verification and rewritten if required.	3
Ensure Spam confidence level (SCL) is configured in mail transport rules with specific domains (exo_transportrulesallowlistdomains)	You should set Spam confidence level (SCL) in your Exchange Online mail transport rules with specific domains. Allow-listing domains in transport rules bypasses regular malware and phishing scanning, which can enable an attacker to launch attacks against your users from a safe haven domain. Note: In order to get a score for this security control, all the active transport rule that applies to specific domains must have a Spam Confidence Level (SCL) of 0 or higher.	3
Ensure users installing Outlook add-ins is not allowed (exo_outlookaddins)	Specify the administrators and users who can install and manage add-ins for Outlook in Exchange Online By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application. Rationale: Attackers exploit vulnerable or custom add-ins to access user data. Disabling user installed add-ins in Microsoft Outlook reduces this threat surface.	3
Set action to take on bulk spam detection (mdo_bulkspamaction)	Set the action that will be taken on bulk spam detection.	3
Ensure that no sender domains are allowed for anti-spam policies (mdo_allowedsenderscombined)	Never add your own accepted domains or common domains (for example, microsoft.com or office.com) to the allowed domains list. If these domains are allowed to bypass spam filtering, attackers can easily send messages that spoof these trusted domains to your organization. In addition, avoid adding specific senders that can bypass spam filtering.	2
Create zero-hour auto purge policies for spam messages (mdo_zapspam)	For unread messages that are identified as spam after delivery, the ZAP outcome depends on the action that's configured for the Spam filtering verdict in the applicable anti-spam policy. For additional information, see https://docs.microsoft.com/microsoft-365/security/office-365-security/zero-hour-auto-purge Zero-hour auto purge (ZAP) in Exchange Online.	1

CONTROL NAME	DESCRIPTION	SCORE
Don't add allowed IP addresses in the connection filter policy (mdo_connectionfilter)	If you're a Microsoft 365 customer with mailboxes in Exchange Online or a standalone Exchange Online Protection (EOP) customer without Exchange Online mailboxes, EOP offers multiple ways of ensuring that users will receive email from trusted senders. These options include Exchange mail flow rules (also known as transport rules), Outlook Safe Senders, the IP Allow List (connection filtering), and allowed sender lists or allowed domain lists in anti-spam policies. Collectively, you can think of these options as safe sender lists. The available safe sender lists are described in the following list in order from most recommended to least recommended: 1. Mail flow rules 2. Outlook Safe Senders 3. IP Allow List (connection filtering) 4. Allowed sender lists or allowed domain lists (anti-spam policies) Without additional verification like mail flow rules, email from sources in the IP Allow List skips spam filtering and sender authentication (SPF, DKIM, DMARC) checks. Since the IP Allow List doesn't prevent malware or high confidence phishing messages from being filtered, this creates a high risk of attackers successfully delivering email to an inbox that would otherwise be filtered.	1
Ensure modern authentication for SharePoint applications is required (spo_legacy_auth)	Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by SharePoint applications. Requiring modern authentication for SharePoint applications ensures strong authentication mechanisms are used when establishing sessions between these applications, SharePoint, and connecting users. This information was taken from Center for Internet Security (CIS).	1
Limit external participants from having control in a Teams meeting (meeting_externalrequestcontrol_v1)	External participants are users that are outside your organization. Limiting their permission to share content, add new users, and more protects your organization’s information from data leaks, inappropriate content being shared, or malicious actors joining the meeting.	1
Only invited users should be automatically admitted to Teams meetings (meeting_autoadmitusers_v1)	Users who aren’t invited to a meeting shouldn’t be let in automatically, because it increases the risk of data leaks, inappropriate content being shared, or malicious actors joining. If only invited users are automatically admitted, then users who weren’t invited will be sent to a meeting lobby. The host can then decide whether or not to let them in.	1
Restrict anonymous users from joining meetings (meeting_restrictanonymousjoin_v1)	By restricting anonymous users from joining Microsoft Teams meetings, you have full control over meeting access. Anonymous users may not be from your organization and could have joined for malicious purposes, such as gaining information about your organization through conversations.	1
Restrict anonymous users from starting Teams meetings (meeting_anonymousstartmeeting_v1)	If anonymous users are allowed to start meetings, they can admit any users from the lobbies, authenticated or otherwise. Anonymous users haven’t been authenticated, which can increase the risk of data leakage.	1
Restrict dial-in users from bypassing a meeting lobby (meeting_pstnusersbypasslobby_v1)	Dial-in users aren’t authenticated though the Teams app. Increase the security of your meetings by preventing these unknown users from bypassing the lobby and immediately joining the meeting.	1
Retain spam in quarantine for 30 days (mdo_quarantineretentionperiod)	Specifies how long to keep the message in quarantine if you selected "Quarantine message" as the action for a spam filtering verdict. After the time period expires, the message is deleted, and is not recoverable.	1

CONTROL NAME	DESCRIPTION	SCORE
Set a daily message limit (mdo_recipientlimitperday)	Configure the maximum number of recipients that a user can send to within a day. After an account is compromised, attackers commonly use the account to generate spam and phish. Configuring recommended values can reduce the amount of spam and phishing emails, while also allowing you to be notified when these thresholds have been reached.	1
Set maximum number of external recipients that a user can email per hour (mdo_recipientexternallimitperhour)	Configure the maximum number of external recipients that a user can email per hour. After an account is compromised, attackers commonly use the account to generate spam and phish. Configuring recommended values can reduce the amount of spam and phishing emails, while also allowing you to be notified when these thresholds have been reached.	1
Set maximum number of internal recipients that a user can send to within an hour (mdo_recipientinternallimitperhour)	Configure the maximum number of recipients that a user can send to per hour for internal recipients. After an account is compromised, attackers commonly use the account to generate spam and phish. Configuring recommended values can reduce the amount of spam and phishing emails, while also allowing you to be notified when these thresholds have been reached.	1
Set the email bulk complaint level (BCL) threshold to be 6 or lower (mdo_bulkthreshold)	Specifies the bulk complaint level (BCL) of a message that triggers the specified action for the bulk spam filtering verdict that you configure on the next page. A higher value indicates that the message is less desirable (more likely to resemble spam). While the default value is 7, 6 or lower is the recommended value.	1
Sign out inactive users in SharePoint Online (spo_idle_session_timeout)	Idle session sign-out lets you specify a time at which users are warned and are later signed out of Microsoft 365 after a period of browser inactivity in SharePoint and OneDrive. This policy is one of several you can use with SharePoint and OneDrive to balance security and user productivity and help keep your data safe, regardless of where users access the data from, what device they're working on, and how secure their network connection is.	1
Block users who reached the message limit (mdo_thresholdreachedaction)	Configure action to take when any of the limits specified in the outbound anti-spam policy are reached. It is common, after an account compromise incident, for an attacker to use the account to generate spam and phish. Configuring the recommended values can reduce the impact.	0
Configure which users are allowed to present in Teams meetings (meeting_designatedpresenter_v1)	Only allow users with presenter rights to share content during meetings. Restricting who can present limits meeting disruptions and reduces the risk of unwanted or inappropriate content being shared.	0
Deploy a log collector to discover shadow IT activity (McasFirewallLogUpload)	Log collectors provide visibility into cloud app usage so you can identify if there are any apps that run without official approval, or if there is anomalous behavior. Log collectors automatically upload reports and parse the firewall/ proxy traffic logs to see if there is a match with your services in the Cloud App Catalog.	0
Enable impersonated domain protection (mdo_enabledomainstoprotect)	Prevents specified domains from being impersonated by the message sender's domain. When you add domains to the 'Enable domains to protect' list, messages from senders in those domains are subject to impersonation protection checks. The message is checked for impersonation if it's sent to a recipient that the policy applies to. If impersonation is detected in the sender's domain, the impersonation protection actions for domains are applied to the message. By default, no sender domains are covered by impersonation protection, either in the default policy	0

CONTROL NAME	DESCRIPTION	SCORE
	or in custom policies.	
Enable impersonated user protection (mdo_targetedusersprotection)	Prevents specified internal or external email addresses from being impersonated as message senders in phishing attempts. By default, impersonated user protection is disabled, and no sender email addresses are covered by impersonation protection, whether in the default policy or in custom policies. We highly recommend adding users (message senders) in key roles. Internally, protected senders might be your CEO, CFO, and other senior leaders. Externally, protected senders could include council members or your board of directors.	0
Enable the domain impersonation safety tip (mdo_similardomainssafetytips)	This setting specifies whether to enable the safety tip that is shown to recipients for domain impersonation detections. When the 'Show domain impersonation safety tip' is enabled, the tip " This sender might be impersonating a domain that's associated with your organization" is shown to recipients in messages where the sender's email domain is included in domain impersonation protection. This setting is available only if the 'Enable impersonated domain protection' setting is configured properly.	0
Enable the user impersonation safety tip (mdo_similaruserssafetytips)	This setting specifies whether to enable the safety tip that is shown to recipients for user impersonation detections. When the 'Show user impersonation safety tip' is enabled, the tip " This sender appears to be similar to someone who previously sent you email but may not be that person" is shown to recipients in messages where the sender's email address is included in user impersonation protection. This setting is available only if the 'Enable impersonated user protection' setting is configured properly.	0
Enable the user impersonation unusual characters safety tip (mdo_unusualcharacterssafetytips)	This setting specifies whether to enable the safety tip that is shown to recipients for unusual characters in domain and user impersonation detections. When the 'Show user impersonation unusual safety tip' is enabled, the tip is shown to recipients in messages where the sender's name or email address contains characters that are not typically used together, such as a mix of mathematical symbols and plain text or a mix of uppercase and lowercase letters. Example tip: 'The email address MARY@CoNToSO.CoM includes unexpected letters or numbers. We recommend you do not interact with this message.' This setting is available only if the 'Enable impersonated user protection' setting is configured properly.	0
Ensure additional storage providers are restricted in Outlook on the web (exo_storageproviderrestricted)	This setting allows users to open certain external files while working in Outlook on the web. If allowed, keep in mind that Microsoft doesn't control the use terms or privacy policies of those third-party services. Ensure AdditionalStorageProvidersAvailable is restricted. Rationale: By default additional storage providers are allowed in Office on the Web (such as Box, Dropbox, Facebook, Google Drive, OneDrive Personal, etc.). This could lead to information leakage and additional risk of infection from organizational non-trusted storage providers. Restricting this will inherently reduce risk as it will narrow opportunities for infection and data leakage.	0
Ensure all forms of mail forwarding are blocked and/or disabled (mdo_blockmailforward)	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 configured using OOF rule, OWA forwarding setting (ForwardingSmtpAddress), Forwarding set by the admin using EAC (ForwardingAddress), Forwarding using Power Automate / Flow, . NOTE: In this control, remediation is carried out in two stages - Step 1 is manual and will not be monitored automatically by secure score, whereas Step 2 is monitored automatically. Any exclusions should be implemented based on organizational policy. Rationale: Attackers often create these rules to exfiltrate data from your tenancy, this could be accomplished via access to an	0

CONTROL NAME	DESCRIPTION	SCORE
	end-user account or otherwise. An insider could also use one of these methods as an secondary channel to exfiltrate sensitive data.	
Ensure mailbox auditing for all users is Enabled (exo_mailboxaudit)	By turning on mailbox auditing, Microsoft 365 back office teams can track logons to a mailbox as well as what actions are taken while the user is logged on. After you turn on mailbox audit logging for a mailbox, you can search the audit log for mailbox activity. Additionally, when mailbox audit logging is turned on, some actions performed by administrators, delegates, and owners are logged by default. Rationale: Starting in January 2019, Microsoft is turning on mailbox audit logging by default for all organizations. This means that certain actions performed by mailbox owners, delegates, and admins are automatically logged, and the corresponding mailbox audit records will be available when you search for them in the mailbox audit log. When mailbox auditing on by default is turned on for the organization, the AuditEnabled property for affected mailboxes won't be changed from False to True. In other words, mailbox auditing on by default ignores the AuditEnabled property on mailboxes. However, only certain mailbox types support default auditing setting 'On': User Mailboxes, Shared Mailboxes, and Microsoft 365 Group Mailboxes. The remaining mailbox types require auditing to be turned on at the mailbox level: Resource Mailboxes, Public Folder Mailboxes, and DiscoverySearch Mailbox. Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing allows for Microsoft 365 back office teams to run security operations, forensics or general investigations on mailbox activities. NOTE: Without advanced auditing (E5 function) the logs are limited to 90 days.	0
Ensure MailTips are enabled for end users (exo_mailtipsenabled)	MailTips assist end users with identifying strange patterns to emails they send.	0
Ensure that an anti-phishing policy has been created (mdo_antiphishingpolicies)	By default, Office 365 includes built-in features that help protect users from phishing attacks. Set up anti-phishing polices to increase this protection, for example by refining settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization, and is a single view to fine-tune anti-phishing protection. Custom policies can be created and configured for specific users, groups or domains within the organization and will take precedence over the default policy for the scoped users. Rationale: Protects users from phishing attacks (like impersonation and spoofing), and uses safety tips to warn users about potentially harmful messages.	0
Ensure that intelligence for impersonation protection is enabled (mdo_mailboxintelligenceprotection)	Enables enhanced impersonation results based on each user's individual sender map and allows you to define specific actions for impersonated messages. This setting is available only if 'Enable mailbox intelligence' is selected.	0
Ensure the customer lockbox feature is enabled (CustomerLockBoxEnabled)	Turning on the customer lockbox feature requires that approval is obtained for datacenter operations that grants a Microsoft employee direct access to your content. Access may be needed by Microsoft support engineers if an issue arises. There's an expiration time on the request and content access is removed after the support engineer has fixed the issue.	0
Move messages that are detected as impersonated users by mailbox intelligence	This setting specifies what to do with messages for impersonation detections from mailbox intelligence results. If a message is detected to be an impersonated user by mailbox intelligence, no action will be applied by default. We recommend moving the message to the recipients' junk email folder and strongly recommend quarantining it. This setting is available only if the 'Ensure that intelligence for impersonation protection is enabled' setting is properly	0

CONTROL NAME	DESCRIPTION	SCORE
(mdo_mailboxintelligenceprotectionaction)	configured.	
Quarantine messages that are detected from impersonated domains (mdo_targeteddomainprotectionaction)	This setting specifies the action to take on detected domain impersonation messages. If a message is detected from an impersonated domain, no action is taken by default. We recommend quarantining the message. This setting is available only if 'Enable impersonated domain protection' setting is configured properly.	0
Quarantine messages that are detected from impersonated users (mdo_targeteduserprotectionaction)	This setting specifies the action to take on detected user impersonation messages. If a message is detected from an impersonated user, no default action will be taken. We recommend quarantining the message. Whenever you select 'Quarantine the message' , a 'Select quarantine policy' box is available. Quarantine policies define who is allowed to do to quarantined messages. This setting is available only if 'Enable impersonated user protection' setting is configured properly.	0
Set automatic email forwarding rules to be system controlled (mdo_autoforwardingmode)		0
Set the phishing email level threshold at 2 or higher (mdo_phishthresholdlevel)	The threshold controls the sensitivity with which machine learning models are applied to email messages to determine whether a phishing attempt has occurred. A higher value indicates greater sensitivity. The default value is 1, but 2 or 3 are the recommended values.	0
Data		
Ensure DLP policies are enabled (dlp_datalossprevention)	Data Loss Prevention (DLP) policies allows content in multiple locations, such as, devices, Exchange online and Teams chats to be scanned for specific types of data like social security numbers, credit card numbers, or passwords.	0
Ensure that Auto-labeling data classification policies are set up and used (mip_autosensitivitylabelspolicies)	Create auto-labeling policies to automatically apply sensitivity labels to email messages or OneDrive and SharePoint files that contain sensitive info. This ability to apply sensitivity labels to content automatically is important because: You don't need to train your users on the appropriate way to use each of your classifications. You don't need to rely on users to classify all content correctly. Users no longer need to know about your policies—they can instead focus on their work.	0
Extend M365 sensitivity labeling to assets in Microsoft Purview data map (mip_purviewlabelconsent)	To get work done, people in your organization collaborate with others both inside and outside the organization. Data doesn't always stay in your cloud, and often roams everywhere—across devices, apps, and services. When your data roams, you still want it to be secure in a way that meets your organization's business and compliance policies. Applying sensitivity labels to your content helps you keep your data secure by stating how sensitive certain data is in your organization. It also abstracts the data itself, letting you track the type of data without exposing sensitive data on other platforms. For example, applying the sensitivity label 'highly confidential' to a document that contains social security numbers and credit card numbers helps you identify the sensitivity of the document without knowing the actual data in the document. The sensitivity labels created in Microsoft Purview Information Protection can also be extended to the Microsoft Purview data map. When you apply a label on an office document and then scan it into the Microsoft Purview data map, the label will be applied to the data asset.	0

CONTROL NAME	DESCRIPTION	SCORE
Publish M365 sensitivity label data classification policies (mip_sensitivitylabelspolicies)	Set up and use data classification policies on data stored in your users' Office apps (like Outlook and Word), SharePoint sites, and Office 365 groups. The policies will help categorize your most important data so you can effectively protect it from illicit access and will help make it easier to investigate discovered breaches. Creation of data classification policies will not cause a significant impact to an organization. However, ensuring long term adherence with policies can potentially be a significant training and ongoing compliance effort across an organization. Organizations should ensure that training and compliance planning is part of the classification policy creation process. This information was taken from Center for Internet Security (CIS).	0
Device		
Enable Microsoft Defender Antivirus scanning of downloaded files and attachments (scid_92)	Determines whether Microsoft Defender Antivirus scans all downloaded files and attachments for malicious code.Not scanning downloaded files and attachments leaves devices vulnerable to malicious code penetration into the organization.	10
Turn on Microsoft Defender Antivirus (scid_2010)	Determines whether Microsoft Defender Antivirus is configured to run and scan for malware and other potentially unwanted software. This feature is available for machines on Windows 10, version 1607 or later.Not having a current, updated antivirus product scanning each computer for malicious file activity exposes the organization to malware or other potentially unwanted software.	10
Turn on Microsoft Defender Firewall (scid_2070)	Microsoft Defender Firewall is designed to keep hackers and malicious software from gaining access to your device through a network or the Internet. This security control is only assessed for machines with Windows 10, version 1709 or later.If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.	10
Turn on real-time protection (scid_2012)	This status indicates that Microsoft Defender Antivirus real-time protection is disabled. This feature is available for machines on Windows 10, version 1607 or later.Not having real-time protection enabled will cause important AV functionalities to not work.	10
Resume BitLocker protection on all drives (scid_2091)	BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. This security control is only assessed for machines with Windows 10, version 1803 or later.Drives that aren't encrypted are exposed to unauthorized access to user data and to data tampering while the system is offline.	9
Secure Microsoft Defender Firewall domain profile (scid_2071)	Determines whether Microsoft Defender Firewall uses the settings for this profile to filter network traffic for the Domain Network profile. This security control is only assessed for machines with Windows 10, version 1709 or later.If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.	9
Secure Microsoft Defender firewall private profile (scid_2072)	Microsoft Defender Firewall is designed to keep hackers and malicious software from gaining access to your device through a network or the Internet. Turn on to have Microsoft Defender Firewall use the settings for the Private Network profile to filter network traffic. This security control is only assessed for machines with Windows 10, version 1709 or later.If the firewall is turned off all traffic will be able to access the system and an attacker may	9

CONTROL NAME	DESCRIPTION	SCORE
	be more easily able to remotely exploit a weakness in a network service.	
Secure Microsoft Defender Firewall public profile (scid_2073)	Microsoft Defender Firewall is designed to keep hackers and malicious software from gaining access to your device through a network or the Internet. This security control is only assessed for machines with Windows 10, version 1709 or later.If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.	9
Set Microsoft Defender SmartScreen app and file checking to block or warn (scid_2060)	SmartScreen helps protect PCs by warning users before running potentially malicious programs downloaded from the Internet. This security control is only applicable for machines with Windows 10, version 1703 or later.	9
Set Microsoft Defender SmartScreen Microsoft Edge site and download checking to block or warn (scid_2061)	Microsoft Defender SmartScreen provides warning messages to help protect your employees from potential phishing scams and malicious software. This security control is only applicable for machines with Windows 10, version 1703 or later.	9
Update Microsoft Defender Antivirus definitions (scid_2011)	This status indicates that Microsoft Defender Antivirus definitions are not up to date.Not having the latest antivirus definitions could potentially expose you to recently discovered viruses.	9
Fix Microsoft Defender for Endpoint impaired communications (scid_2002)	This status indicates that there's limited communication between the machine and the Microsoft Defender for Endpoint service.Limited communication between the machine and the Microsoft Defender for Endpoint service can lead to the service not being able to determine the security state of machine.	8.33
Fix Microsoft Defender for Endpoint sensor data collection (scid_2001)	The Microsoft Defender for Endpoint service relies on sensor data collection to determine the security state of a machine.The Microsoft Defender for Endpoint service will not be able to determine the security state of machines that are not reporting sensor data properly.	8.33
Turn on Microsoft Defender for Endpoint sensor (scid_2000)	Determines whether the Microsoft Defender for Endpoint sensor embedded in Windows collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender for EndpointThe Microsoft Defender for Endpoint service will not be able to determine the security state of machines that are not sending sensor data.	8.33
Change service account to avoid cached password in windows registry (scid_3003)	Determines the existence on the machine of one or more services, which are configured to run with account that stores its password in reversible encryption in the registry.	8
Disable 'Always install with elevated privileges' (scid_66)	Determines whether Windows Installer always elevates privileges when installing applications.Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.	8
Disable 'Anonymous enumeration of SAM accounts' (scid_68)	Controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account usernames on the systems in your environment.Anonymous enumeration of SAM accounts allows anonymous log on users (null session connections) to list all accounts names, thus providing a list of potential points to attack the	8

CONTROL NAME	DESCRIPTION	SCORE
	system.	
Disable 'Insecure guest logons' in SMB (scid_30)	Determines whether insecure guest logons are used by file servers to allow unauthenticated access to shared folders.Insecure guest logons allow unauthenticated access to shared folders and retrieve sensitive data, as well as place malicious files. Shared resources on a system must require authentication to establish proper access.	8
Disable SMBv1 client driver (scid_53)	Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1.SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.	8
Disable SMBv1 server (scid_54)	Disabling SMBv1 support may prevent access to file or print sharing resources with systems or devices that only support SMBv1.SMBv1 is a legacy protocol that uses the MD5 algorithm as part of SMB. MD5 is known to be vulnerable to a number of attacks such as collision and preimage attacks as well as not being FIPS compliant.	8
Disable 'Store LAN Manager hash value on next password change' (scid_65)	Controls whether or not a LAN Manager hash of the password is stored in the SAM the next time the password is changed.The LAN Manager hash uses a weak encryption algorithm and there are several tools available that use this hash to retrieve account passwords.	8
Disable the built-in Guest account (scid_3011)	Determines whether the built-in Guest account is disabled	8
Enable cloud-delivered protection (scid_2016)	Indicates that Microsoft Defender Antivirus cloud-delivered protection is not enabled. Cloud-delivered protection service provides very important protection against malware on your endpoints and across your network.Not having cloud-delivered protection enabled leaves your endpoint and your network vulnerable to malware.	8
Enable 'Network Protection' (scid_96)	Network protection helps reduce the attack surface of your devices from Internet-based events. It prevents employees from using any application to access dangerous domains that may host phishing scams, exploits, and other malicious content on the Internet. It expands the scope of Windows Defender SmartScreen to block all outbound HTTP(s) traffic that attempts to connect to low-reputation sources (based on the domain or hostname) This security control is only applicable for machines with Windows 10, version 1709 or later.Not enabling Network Protection in block mode exposes your users and machines to phishing scams, as well as to internet delivered exploits and malicious content.	8
Enable 'Safe DLL Search Mode' (scid_26)	Determines whether an application searches for DLLs in the system path before searching the current working directory.An unauthorized DLL inserted by an attacker into an applications working directory could allow malicious code to be run on the system.	8
Enable scanning of removable drives during a full scan (scid_89)	This setting controls whether or not to scan for malicious software and unwanted software in the contents of removable drives, such as USB flash drives, when running a full scan.This security control is only applicable for machines with Windows 10, version 1709 or later.	8
Ensure BitLocker drive compatibility	BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the	8

CONTROL NAME	DESCRIPTION	SCORE
(scid_2093)	threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. This security control is only assessed for machines with Windows 10, version 1803 or later.Drives that aren't compatible with BitLocker remain not encrypted. Drives that aren't encrypted are exposed to unauthorized access to user data and to data tampering while the system was offline.	
Fix Windows Defender Antivirus cloud service connectivity (scid_2014)	Indicates that Microsoft Defender Antivirus is not properly configured to report its health state.Status reports that are not properly sent prevent you from being able to monitor your antivirus health state.	8
Restrict anonymous access to named pipes and Shares (scid_64)	Determines whether anonymous access is restricted to only shares and pipes that are named.Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment in order to gain unauthorized system access. Network shares can be accessed by any network user. This could lead to the exposure or corruption of sensitive data. This setting configures Windows to restrict anonymous access to only those shares and pipes listed in Network Access: named pipes that can be accessed anonymously.	8
Set 'Remote Desktop security level' to 'TLS' (scid_24)	Determines the method used by the server and client for authentication prior to a remote desktop connection being established.If the authentication level isn't secure enough, an attacker could gain remote access to the machine	8
Turn on Tamper Protection (scid_2003)	Tamper Protection essentially locks Microsoft Defender for Endpoint and prevents your security settings from being changed through apps and methods such as editing registry values, changing settings through PowerShell cmdlets and editing or removing security settings through group policies. Without enabling Tamper Protection, malicious apps can potentially change important Microsoft Defender for Endpoint settings, for example disable virus and threat protection, turn off real-time protection or disable cloud-delivered protection.	8
Change service executable path to a common protected location (scid_3002)	Determines the existence on the machine of one or more services, which are configured with a path to executable that is stored in an uncommon/unprotected folder location.	7.33
Disable the built-in Administrator account (scid_3010)	Determines whether the built-in Administrator account is disabled	7.33
Encrypt all BitLocker-supported drives (scid_2090)	BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. This security control is only assessed for machines with Windows 10, version 1803 or later.Drives that aren't encrypted are exposed to unauthorized access to user data and to data tampering while the system is offline.	6.75
Turn on PUA protection in block mode (scid_2013)	Enabling Potentially Unwanted Application (PUA) protection will block and automatically quarantine potentially unwanted applications. PUA protection blocking takes effect on endpoint clients after the next signature update or computer restart. This feature is available for machines on Windows 10, version 1607 or later.Not having PUA enabled leaves your machines vulnerable to unwanted applications with potentially malicious behavior.	6.75
Fix unquoted service path for Windows services (scid_3001)	Determines the existence on the machine of one or more services, which are configured with a path to executable that contains spaces and also isn't surrounded by quotation marks.	6

CONTROL NAME	DESCRIPTION	SCORE
Set 'Account lockout threshold' to 1-10 invalid login attempts (scid_44)	Determines the number of failed logon attempts before the account is locked. The number of failed logon attempts should be reasonably small to minimize the possibility of a successful password attack, while still allowing for honest errors made during a legitimate user logon. This security control is only assessed for machines with Windows 10, version 1709 or later.	5.5
Block Flash activation in Office documents (scid_80)	Determines whether Flash can be used in office documents.	5
Disable 'Configure Offer Remote Assistance' (scid_63)	Determines whether unsolicited offers of help to this computer via Remote Assistance are allowed. Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.	5
Disable 'Network access: Let Everyone permissions apply to anonymous users' (scid_55)	Determines whether anonymous network users have the same rights and permissions as the built-in 'Everyone' group.. This security control is only assessed for machines on Windows 10, version 1709 or later.	5
Disable sending unencrypted password to third-party SMB servers (scid_94)	Determines whether the SMB redirector will send unencrypted (plain text) passwords when authenticating to third-party SMB servers that do not support password encryption.Sending plain text passwords across the network, when authenticating to an SMB server, reduces the overall security of the environment and introduces a significant security risk. Check with the vendor of the SMB server to see if there is a way to support encrypted password authentication.	5
Disable 'WDigest Authentication' (scid_57)	When the WDigest Authentication protocol is enabled, plain text passwords are stored in the Local Security Authority Subsystem Service (LSASS) exposing them to theft.Disabling this setting will prevent WDigest from storing credentials in memory.	5
Enable 'Domain member: Digitally encrypt or sign secure channel data (always)' (scid_37)	Determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted.When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the Domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted but the channel is not integrity-checked, and not all information is encrypted.	5
Enable 'Domain member: Digitally sign secure channel data (when possible)' (scid_39)	Determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted but the channel is not integrity-checked, and not all information is encrypted.	5
Enable 'Domain member: Require strong (Windows 2000 or later) session key'	When this policy setting is enabled, a secure channel can only be established with Domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.Session keys that are used to	5

CONTROL NAME	DESCRIPTION	SCORE
(scid_36)	establish secure channel communications between Domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping.	
Enable Explorer Data Execution Prevention (DEP) (scid_83)	Determines whether Data Execution Prevention can be turned off for File Explorer.DEP provides additional protection by performing checks on memory to help prevent malicious code from running.	5
Enable 'Limit local account use of blank passwords to console logon only' (scid_71)	Determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. By enabling this configuration, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer.An account without a password can allow unauthorized access to a system as only the username would be required. Password policies should prevent accounts with blank passwords from existing on a system. However, if a local account with a blank password did exist, enabling this setting will prevent network access, limiting the account to local console logon only.	5
Enable Microsoft Defender Antivirus real-time behavior monitoring (scid_91)	Determines whether Microsoft Defender Antivirus monitors file processes, file and registry changes, and other events on your endpoints for suspicious and known malicious activity.Disabling behavior monitoring will reduce your ability to detect suspicious activity that could indicate a breach.	5
Enable Set 'Domain member: Digitally encrypt secure channel data (when possible)' (scid_38)	Determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates.When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted but the channel is not integrity-checked, and not all information is encrypted.	5
Set 'Maximum password age' to '60 or fewer days, but not 0' (scid_34)	Determines the period of time (in days) that a password can be used before the system requires the user to change it.	5
Disable 'Domain member: Disable machine account password changes' (scid_40)	Determines whether automatic password changes are enforced on computer accounts.Disabling automatic password changes can make the system more vulnerable to malicious access. Frequent password changes can be a significant safeguard for your system.	2
Turn on Microsoft Defender Credential Guard (scid_2080)	Microsoft Defender Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. This security control is only assessed for machines with Windows 10, version 1709 or later.If disabled, malicious attackers could potentially gain access to user credentials stored in memory and expose the machine to various types of attacks, such as pass-the-hash.	0.73
Set 'Account lockout duration' to 15 minutes or more (scid_41)	Determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. If configured to 0, accounts will remain locked out until an administrator manually unlocks them. This security control is only assessed for machines with Windows 10, version 1709 or later.	0.5

CONTROL NAME	DESCRIPTION	SCORE
Set 'Reset account lockout counter after' to 15 minutes or more (scid_42)	Determines the length of time before the 'Account lockout threshold' counter resets to zero after a failed logon attempt. This reset time must be less than or equal to the value of the 'Account lockout duration' setting. This security control is only assessed for machines with Windows 10, version 1709 or later.	0.5
Enable Automatic Updates (scid_15)	Controls whether the Office automatic updates are enabled or disabled for all Office products installed by using Click-to-Run. This policy has no effect on Office products installed via Windows Installer.	0.42
Block abuse of exploited vulnerable signed drivers (scid_2515)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents an application from writing a vulnerable signed driver to disk. This security control is only applicable for machines with Windows 10, version 1709 or later, and Windows Server 2019.	0
Block Adobe Reader from creating child processes (scid_2513)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents Adobe Reader from creating additional child processes. This security control is only applicable for machines with Windows 10, version 1903 or later.Through social engineering or exploits, malware can download and launch additional payloads and break out of Adobe Reader.	0
Block all Office applications from creating child processes (scid_2501)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule blocks Office apps from creating child processes. This includes Word, Excel, PowerPoint, OneNote, and Access. Note: Some legitimate line-of-business applications might also use behaviors like this, including spawning a command prompt or using PowerShell to configure registry settings. This security control is only applicable for machines with Windows 10, version 1709 or later.Creating child processes is a typical malware behavior that can be exploited in various ways, especially for attacks that abuse Office as a vector, using VBA macros and exploit code to download and attempt to run additional malicious payload.	0
Block credential stealing from the Windows local security authority subsystem (lsass.exe) (scid_2509)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule locks down LSASS. This security control is only applicable for machines with Windows 10, version 1803 or later.Attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS.	0
Block executable content from email client and webmail (scid_2500)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule blocks executable and script files (such as .exe, .dll, .scr, .ps, .vbs, .js) from launching from email in Microsoft Outlook or Outlook.com and other popular webmail providers. This security control is only applicable for machines with Windows 10, version 1709 or later.Email attachments are the most common method that attackers use for transmitting malicious software and viruses into computers and organizations.	0
Block executable files from running unless they meet a prevalence, age, or trusted list criterion (scid_2507)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule blocks executable files (such as .exe, .dll, .scr) from launching unless they either meet prevalence or age criteria, or they're in a trusted list or	0

CONTROL NAME	DESCRIPTION	SCORE
	exclusion list. This security control is only applicable for machines with Windows 10, version 1803 or later.Allowing executables that have not yet established sufficient trust and validation to be executed, increases your exposure to potentially malicious applications.	
Block execution of potentially obfuscated scripts (scid_2505)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents scripts that appear to be obfuscated from running. It uses the AntiMalwareScanInterface (AMSI) to determine if a script is potentially obfuscated, and then blocks such a script, or blocks scripts when an attempt is made to access them. This security control is only applicable for machines with Windows 10, version 1709 or later.Malware and other threats can attempt to obfuscate or hide their malicious code in script files.	0
Block JavaScript or VBScript from launching downloaded executable content (scid_2504)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents JavaScript and VBScript from being allowed to launch apps. Note: This isn't a common line-of-business use, but line-of-business applications sometimes use scripts to download and launch installers. This security control is only applicable for machines with Windows 10, version 1709 or later.Malware written in JavaScript or VBS often acts as a downloader to fetch and launch additional native payload from the Internet.	0
Block Office applications from creating executable content (scid_2502)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents Office apps, including Word, Excel, and PowerPoint, from creating executable content. This security control is only applicable for machines with Windows 10, version 1709 or later.Creating executable content is a typical behavior where malware uses Office as a vector to break out of Office and save malicious code components to disk, where they persist and survive a computer reboot.	0
Block Office applications from injecting code into other processes (scid_2503)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule blocks code injection attempts from Office apps into other processes. There are no known legitimate business purposes for using code injection This security control is only applicable for machines with Windows 10, version 1709 or later.Attackers might attempt to use Office apps to migrate malicious code into other processes through code injection, so the code can masquerade as a clean process and hide the activity from antivirus scanning engines.	0
Block Office communication application from creating child processes (scid_2512)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents Outlook from creating child processes, while still allowing legitimate Outlook functions. This security control is only applicable for machines with Windows 10, version 1903 or later.Provides protection against social engineering attacks and prevents exploit code from abusing a vulnerability in Outlook, by blocking the launch of additional payload. It also protects against Outlook rules and forms exploits that attackers can use when a user's credentials are compromised.	0
Block persistence through WMI event subscription (scid_2514)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule allows admins to have more control over WMI repository persistence. This security control is only applicable for machines with Windows 10, version 1903 or later. Fileless threats employ various tactics to stay hidden, to avoid being seen in the file system, and to	0

CONTROL NAME	DESCRIPTION	SCORE
	gain periodic execution control. Some threats can abuse the WMI repository and event model to stay hidden.	
Block process creations originating from PSExec and WMI commands (scid_2510)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule blocks processes through PsExec and WMI commands from running. Warning: This rule is incompatible with management through System Center Configuration Manager because this rule blocks WMI commands the SCCM client uses to function correctly. This security control is only applicable for machines with Windows 10, version 1803 or later.Attackers often use remote code execution for spreading malware attacks.	0
Block untrusted and unsigned processes that run from USB (scid_2511)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule allows admins to prevent unsigned or untrusted executable and script files (such as .exe, .dll, .scr, .ps, .vbs, .js) from running from USB removable drives, including SD cards. This security control is only applicable for machines with Windows 10, version 1803 or later.Attackers often use removable devices for executing malicious code, even without the knowledge of the device owner.	0
Block Win32 API calls from Office macros (scid_2506)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule prevents using Win32 APIs in VBA macros. Note: Most organizations don't use this functionality, but might still rely on using other macro capabilities. This security control is only applicable for machines with Windows 10, version 1709 or later.Malicious code can abuse the ability to execute routines in the Win 32 dynamic link library from macros.	0
Disable 'Allow Basic authentication' for WinRM Client (scid_73)	Determines whether the Windows Remote Management (WinRM) client uses Basic authentication.Basic authentication uses plain text passwords that could be used by an attacker to compromise a system.	0
Disable 'Allow Basic authentication' for WinRM Service (scid_74)	Determines whether the Windows Remote Management (WinRM) service accepts Basic authentication.Basic authentication uses plain text passwords that could be used by an attacker to compromise a system.	0
Disable Anonymous enumeration of shares (scid_88)	Determines whether anonymous logon users (null session connections) are allowed to list all account names and enumerate all shared resourcesAllowing this can provide a map of potential points to attack the system.	0
Disable 'Autoplay' for all drives (scid_69)	Determines whether Autoplay is enabled on the device. Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediatelyAn attacker could use this feature to launch a malicious program to damage a client computer or data on the computer.	0
Disable 'Autoplay for non-volume devices' (scid_67)	Determines whether autoplay for non-volume devices (such as Media Transfer Protocol (MTP) devices) is enabled or disabled.An attacker could use this feature to launch a program to damage a client computer or data on the computer.	0
Disable 'Continue running background apps when Google Chrome is closed' (scid_19)	Chrome allows for processes started while the browser is open to remain running once the browser has been closed. It also allows for background apps and the current browsing session to remain active after the browser has been closed. Disabling this feature will stop all processes and background applications when the browser window	0

CONTROL NAME	DESCRIPTION	SCORE
	is closed.	
Disable 'Enumerate administrator accounts on elevation' (scid_29)	Determines whether the user needs to provide both the administrator username and password to elevate a running application, or if the system displays a list of administrator accounts to choose from.Enumeration of administrator accounts when elevating can provide part of the logon information to an unauthorized user, making attacks easier.	0
Disable 'Installation and configuration of Network Bridge on your DNS domain network' (scid_58)	Determines whether a user can install and configure the Network Bridge. The Network Bridge allows users to create a layer 2 MAC bridge, enabling them to connect two or more network segments together.A Network Bridge can connect two or more network segments, allowing unauthorized access or exposure of sensitive data in another network segment.	0
Disable IP source routing (scid_82)	Determines whether IP source routing is enabled.Configuring the system to disable IP source routing protects against spoofing.	0
Disable JavaScript on Adobe DC (scid_97)	Determines whether to globally disable and lock JavaScript execution in Adobe DCJavaScript could potentially be used by attackers to manipulate users or to execute undesired code locally.	0
Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile (scid_43)	Determines whether Microsoft Defender Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.	0
Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile (scid_46)	Determines whether Microsoft Defender Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.	0
Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile (scid_49)	Determines whether Microsoft Defender Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.	0
Disable 'Password Manager' (scid_22)	Chrome will memorize passwords and automatically provide them when a user logs into a site. By disabling this feature the user will be prompted to enter their password each time they visit a website.	0
Disable Solicited Remote Assistance (scid_87)	Remote assistance allows another user to view or take control of the local session of a user. Solicited assistance is help that is specifically requested by the local user.This may allow unauthorized parties access to the resources on the computer	0
Disable the local storage of passwords and credentials (scid_93)	Determines whether Credential Manager saves passwords or credentials locally for later use when it gains domain authentication.Locally cached passwords or credentials can be accessed by malicious code or unauthorized users.	0
Enable 'Apply UAC restrictions to local accounts on network logons' (scid_52)	With User Account Control enabled, filtering the privileged token for built-in administrator accounts will prevent the elevated privileges of these accounts from being used over the network. This recommendation is not applicable for organizations which use local password management solution (like LAPS) to protect local accounts for remote	0

CONTROL NAME	DESCRIPTION	SCORE
	administration and support.A compromised local administrator account can provide means for an attacker to move laterally between domain systems.	
Enable 'Block third party cookies' (scid_23)	Chrome allows cookies to be set by web page elements that are not from the domain in the user's address bar. Enabling this feature prevents third party cookies from being set.	0
Enable 'Hide Option to Enable or Disable Updates' (scid_16)	Controls whether to hide the user interface (UI) options to enable or disable Office automatic updates from users.	0
Enable Microsoft Defender Antivirus email scanning (scid_90)	Determines whether Microsoft Defender Antivirus analyze the mail bodies and attachments and scans them for malicious content.Not scanning incoming emails and attachments could potentially enable attackers to deliver malicious content and attachments into the organization	0
Enable 'Microsoft network client: Digitally sign communications (always)' (scid_95)	Determines whether packet signing is required by the SMB client component. If this is enabled, the SMB client will only communicate with an SMB server that performs SMB packet signing.Unsigned traffic exposes you to man-in-the-middle attacks. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.	0
Enable 'Require additional authentication at startup' (scid_62)	Determines whether BitLocker requires additional authentication each time the computer starts, and whether you are using BitLocker with or without a Trusted Platform Module (TPM).TPM without use of a PIN will only validate early boot components and does not require a user to enter any additional authentication information. If a computer is lost or stolen in this configuration, BitLocker will not provide any additional measure of protection beyond what is provided by native Windows authentication unless the early boot components are tampered with or the encrypted drive is removed from the machine.	0
Enable 'Require domain users to elevate when setting a network's location' (scid_59)	Determines whether to require domain users to elevate when setting a network's location.Selecting an incorrect network location may allow greater exposure of a system	0
Prohibit use of Internet Connection Sharing on your DNS domain network (scid_60)	Determines whether an existing internet connection, such as through wireless, can be shared and used by other systems essentially creating a mobile hotspot.This exposes the system sharing the connection to others with potentially malicious purpose.	0
Set controlled folder access to enabled or audit mode (scid_2021)	This status indicated that controlled folder access is disabled. Controlled folder access helps protect files in key system folders from changes made by malicious and suspicious apps, including file-encrypting ransomware malware. Requires Microsoft Defender Antivirus Real-time protection. This security control is only applicable for machines with Windows 10, version 1709 or later.Not enabling controlled folder access leaves you exposed to various attack vectors. Audit mode allows you to see audit events in the Microsoft Defender for Endpoint Machine timeline however it does not block suspicious applications. Consider enabling Controlled Folder Access for better protection.	0

CONTROL NAME	DESCRIPTION	SCORE
Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands' (scid_70)	Determines whether Autorun commands are allowed to execute. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.Allowing autorun commands to execute may introduce malicious code to a system without user intervention or awareness. Configuring this setting prevents autorun commands from executing.	0
Set 'Enforce password history' to '24 or more password(s)' (scid_33)	Determines the number of unique new passwords that are required before an old password can be reused in association with a user account.	0
Set 'Interactive logon: Machine inactivity limit' to '1-900 seconds' (scid_28)	Determines the amount of inactivity time (in seconds) of a logon session, beyond which the screen saver will run, locking the session. This security control is only applicable for machines with Windows 10, version 1709 or later.	0
Set IPv6 source routing to highest protection (scid_81)	Determines whether IPv6 source routing is enabled.Configuring the system to disable IP source routing protects against spoofing.	0
Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM' (scid_72)	Determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers.Using older/weaker authentication levels (LM & NTLM) make it potentially possible for attackers to sniff that traffic to more easily reproduce the user's password.	0
Set 'Minimum password age' to '1 or more day(s)' (scid_35)	Determines the number of days that you must use a password before you can change it.	0
Set 'Minimum password length' to '14 or more characters' (scid_32)	Determines the minimum password length	0
Set 'Minimum PIN length for startup' to '6 or more characters' (scid_61)	Determines the minimum PIN length for authentication without sending a password to a network where it could be compromised.BitLocker requires the use of the function keys [F1-F10] for PIN entry since the PIN is entered in the pre-OS environment before localization support is available. This limits each PIN digit to one of ten possibilities. The TPM has an anti-hammering feature that includes a mechanism to exponentially increase the delay for PIN retry attempts; however, using a PIN that is short in length improves an attacker's chances of guessing the correct PIN.	0
Set User Account Control (UAC) to automatically deny elevation requests (scid_27)	Determines the behavior of the elevation prompt for standard users.Denying elevation requests from standard user accounts requires tasks that need elevation to be initiated by accounts with administrative privileges. This prevents privileged account credentials from being cached with standard user profile information to help mitigate credential theft.	0
Set user authentication for remote connections by using Network Level Authentication to 'Enabled' (scid_45)	Determines whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.	0

CONTROL NAME	DESCRIPTION	SCORE
Use advanced protection against ransomware (scid_2508)	Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyberattacks and malicious software. This ASR rule scans executable files entering the system to determine whether they're trustworthy. This security control is only applicable for machines with Windows 10, version 1803 or later.This provides an extra layer of protection against files that closely resemble ransomware, by blocking them from running, unless they're in a trusted list or exclusion list.	0
Identity		
Ensure multifactor authentication is enabled for all users in administrative roles (AdminMFAV2)	Requiring multifactor authentication (MFA) for administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, your entire organization is exposed. At a minimum, protect the following roles: Global administrator, Authentication administrator, Billing administrator, Conditional Access administrator, Exchange administrator, Helpdesk administrator, Security administrator, SharePoint administrator, User administrator.	10
Enable Conditional Access policies to block legacy authentication (BlockLegacyAuthentication)	Today, most compromising sign-in attempts come from legacy authentication. Older office clients such as Office 2010 don’t support modern authentication and use legacy protocols such as IMAP, SMTP, and POP3. Legacy authentication does not support multifactor authentication (MFA). Even if an MFA policy is configured in your environment, bad actors can bypass these enforcements through legacy protocols.	8
Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' (PWAgePolicyNew)	Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in the future as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason, and recommends that cloud-only tenants set the password policy to never expire.	8
Ensure multifactor authentication is enabled for all users (MFARegistrationV2)	Multifactor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.	6.35
Ensure user consent to apps accessing company data on their behalf is not allowed (IntegratedApps)	To reduce the risk of malicious applications attempting to trick users into granting them access to your organization's data, we recommend that you allow user consent only for applications that have been published by a verified publisher.	4
Designate more than one global admin (OneAdmin)	Having more than one global administrator helps if you are unable to fulfill the needs or obligations of your organization. It's important to have a delegate or an emergency account someone from your team can access if necessary. It also allows admins the ability to monitor each other for signs of a breach. Note: According to CIS O365 Benchmark 2.0.0, the suggestion is to have between two to four global admins. Currently, the condition to comply is to have more than one global administrator - This security recommendation will be updated accordingly to CIS benchmark in the future. Rationale: If there is only one global tenant administrator, he or she can perform malicious activity without the possibility of being discovered by another admin. If there are numerous global tenant administrators, the more likely it is that one of their accounts will be successfully breached by an external attacker.	1

CONTROL NAME	DESCRIPTION	SCORE
Use least privileged administrative roles (RoleOverlap)	Ensure that your administrators can accomplish their work with the least amount of privilege assigned to their account. Assigning users roles like Password Administrator or Exchange Online Administrator, instead of Global Administrator, reduces the likelihood of a global administrative privileged account being breached.	1
Ensure 'Self service password reset enabled' is set to 'All' (SelfServicePasswordReset)	With self-service password reset in Microsoft Entra ID, users no longer need to engage help desk to reset passwords. This feature works well with Microsoft Entra ID dynamically banned passwords, which prevents easily guessable passwords from being used.	0.1
Enable Microsoft Entra ID Identity Protection sign-in risk policies (SigninRiskPolicy)	Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multifactor authentication (MFA).	0
Enable Microsoft Entra ID Identity Protection user risk policies (UserRiskPolicy)	With the user risk policy turned on, Microsoft Entra ID detects the probability that a user account has been compromised. As an administrator, you can configure a user risk Conditional Access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.	0
Start your Defender for Identity deployment, installing Sensors on Domain Controllers and other eligible servers. (AATP_DefenderForIdentityIsNotInstalled)	Installing Microsoft Defender for Identity sensors provides you with the ability to detect advanced threats in your entire identity infrastructure. Actionable security alerts are generated through the analysis of network traffic and security events.	0

5 - Alert Analysis

Alerts are generated automatically and can be configured in your Microsoft Cloud environment. If no alerts are found, it may be that alerting and auditing are turned off in your particular environment. A review of alerts should be performed on a periodic basis to identify underlying issues and potential security events.

Alerts by Type (Past 30 Days)

Alerts by Type (Past 7 Days)

EVENT DATE	TITLE	PROVIDER
07/08/2025 3:31:49 PM +00:00	Atypical travel	Microsoft IPC
07/07/2025 5:51:50 PM +00:00	Atypical travel	Microsoft IPC
06/08/2025 8:40:01 PM +00:00	Atypical travel	Microsoft IPC

EVENT DATE	TITLE	PROVIDER
06/08/2025 8:40:00 PM +00:00	Atypical travel	Microsoft IPC