MICROSOFT CLOUD ASSESSMENT

Microsoft Cloud Security Assessment

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 07/09/2025

Prepared for: End Users

Prepared by: TEL5

07/09/2025

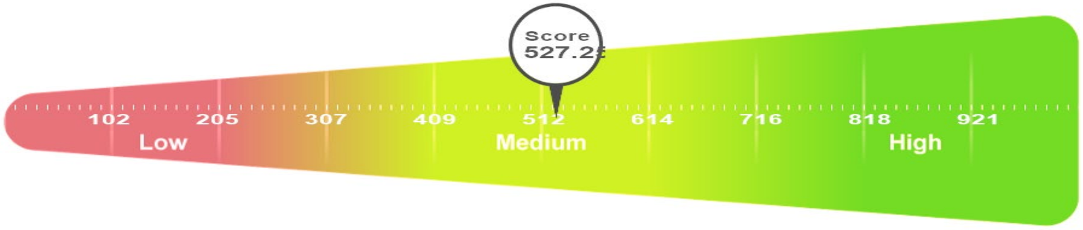
Table of Contents

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.

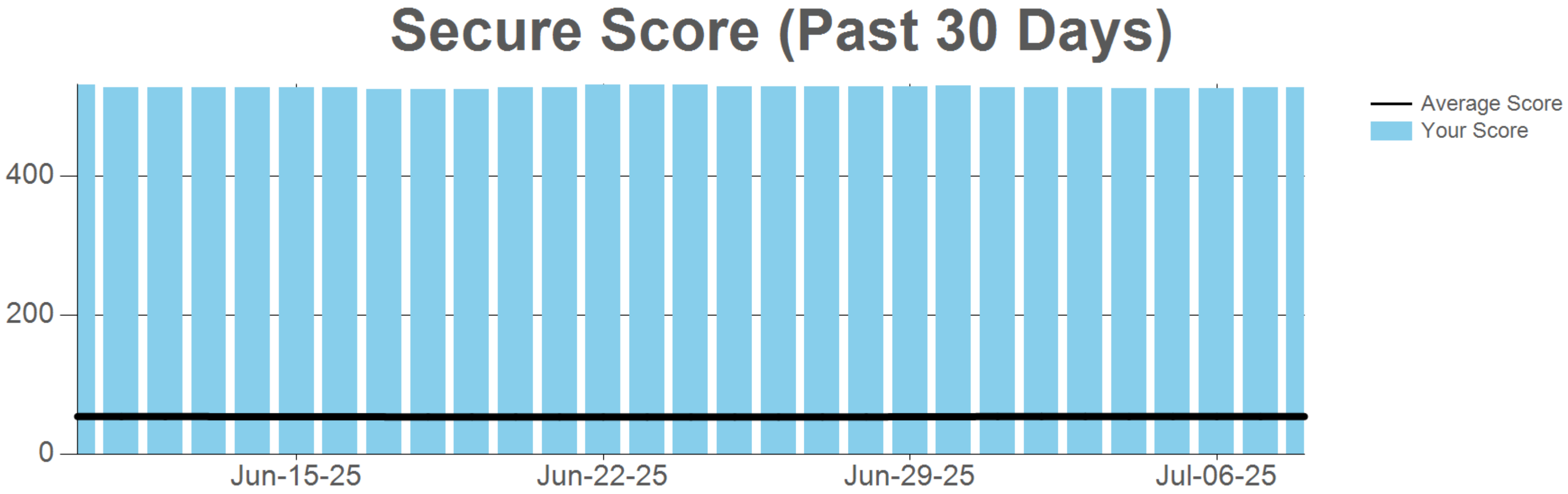
2 - Current Secure Score

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

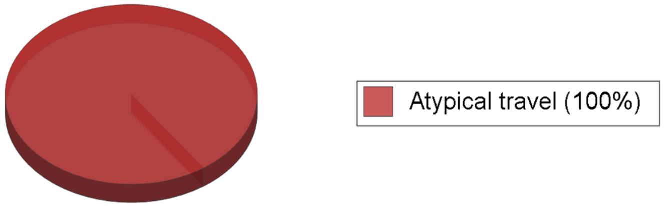
CONTROL NAME	DESCRIPTION	SCORE
Ensure the Common Attachment Types Filter is enabled (mdo_commonattachmentsfilter)	There are certain types of files that are risker to send and receive via email due to the likelihood that they contain malware (for example, executable files). To make sure these file types 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, <span style="text-decoration: underline;">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

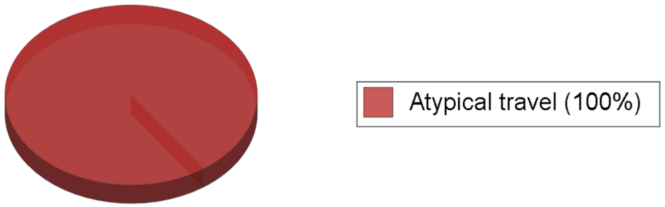
5 - Alert Analysis

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.

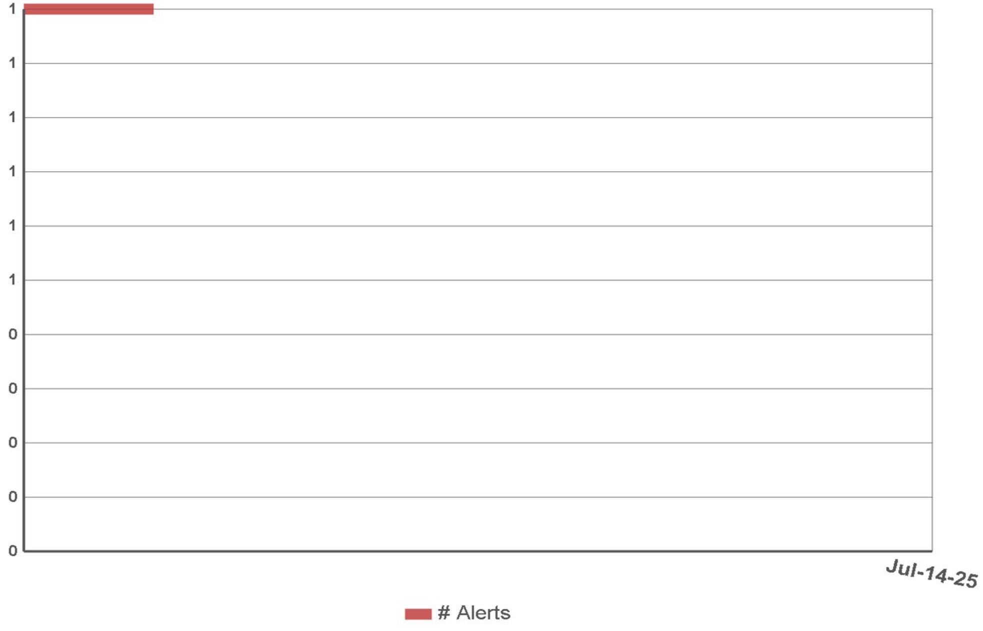
Alerts by Type (Past 30 Days)



Alerts by Type (Past 7 Days)



Alerts by Day (Past 30 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