

MICROSOFT CLOUD ASSESSMENT

Risk Report



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.

Prepared for: HQ

Prepared by: Indusflow Systems

02/21/2025

Scan Date: 02/21/2025

Table of Contents

01		Overview
02		Risk Score
03		Issues Summary

1 - Overview

The Microsoft Cloud is composed of various components and applications including Azure Active Directory, Microsoft Teams, OneDrive, Outlook and SharePoint. Risks associated with using the Microsoft Cloud are grouped into operational and misconfiguration. Some issues represent improvement in configuration desired to improve the Microsoft Secure Score. Not all changes are necessary for every type of business. A qualified IT professional should always evaluate the benefits of implementing any particular control or recommendation, balancing it with business needs and cost.

2 - Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score reflects the risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

Issue: 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.

Recommendation: Microsoft services provide step-by-step guidance to select and enable the right MFA method for your organization in the Microsoft 365 admin center. Go to the Microsoft 365 MFA wizard (<https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/securty/ConditionalAccess>), If you would like to perform the implementation yourself, first check what Microsoft Entra ID license you have under "Prerequisites" in Microsoft Secure Score or see your license type under "Basic information" in the Microsoft Entra ID Overview (https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview). If you've invested in Microsoft Entra ID Premium P1 or P2 licenses, you can create a Conditional Access policy from scratch or by using a template. Follow these steps to create a Conditional Access policy from scratch or by using a template (<https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-registration>), If you would like to perform the implementation yourself and you're using Microsoft Entra ID Free, turn on security defaults. Note: Security defaults and Conditional Access can't be used side by side. Enable security defaults (<https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>), Keep track of your user's progress of registering authentication methods by going to Microsoft Entra ID > Security > Authentication methods > User registration details (requires Microsoft Entra ID Premium P1 or P2 licenses). Go to User registration details (https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/UserRegistrationDetails),

5580

Unimplemented Microsoft Control: Ensure that Auto-labeling data classification policies are set up and used (90 pts each)

Current Score: 90 pts x 62 = 5580: 2.2%

Issue: 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.

Recommendation: Open Microsoft Purview compliance portal, Under Solutions, click Information protection, Click on Auto-Labeling tab, Ensure that an Auto-Labeling policy exists and is published accordingly, Make sure Auto-Labeling policies are published on all of your licensed users and group,

5580

Unimplemented Microsoft Control: Ensure all forms of mail forwarding are blocked and/or disabled (90 pts each)

Current Score: 90 pts x 62 = 5580: 2.2%

Issue: 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 end-user account or otherwise. An insider could also use one of these methods as a secondary channel to exfiltrate sensitive data.

Recommendation: 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: STEP 1: Transport rules To alter the mail transport rules so they do not forward email to external domains, use the Microsoft 365 Admin Center: Select Exchange to open the Exchange admin center. Select Mail Flow then Rules. For each rule that redirects email to external domains, select the rule and click the 'Delete' icon. To perform remediation you may also use the Exchange Online PowerShell Module: Connect to Exchange Online user Connect-ExchangeOnline. Run the following PowerShell command: Remove-TransportRule {RuleName}, To verify this worked you may re-run the audit command as follows: Get-TransportRule | Where-Object {\$_.RedirectMessageTo -ne \$null} | ft Name,RedirectMessageTo, STEP 2: Anti-spam outbound policy Configure an anti-spam outbound policy: Navigate to Microsoft 365 Defender <https://security.microsoft.com/>, Expand E-mail & collaboration then select Policies & rules. Select Threat policies > Anti-spam. Select Anti-spam outbound policy (default), Click Edit protection settings, Set Automatic forwarding rules dropdown to Off - Forwarding is disabled and click Save, Repeat steps 4-6 for any additional higher priority, custom policies.

5580

Unimplemented Microsoft Control: Block users who reached the message limit (90 pts each)

Current Score: 90 pts x 62 = 5580: 2.2%

Issue: 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 (<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide#eop-outbound-spam-policy-settings>) can reduce the impact.

Recommendation: Ensure that all users have an assigned outbound anti-spam policy with the 'Over limit action' option set to recommended values (<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide#eop-outbound-spam-policy-settings>) which is "Restrict the user from sending mail", by either updating your existing policies or creating new ones.

5580

Automatic email forwarding is enabled (90 pts each)

Current Score: 90 pts x 62 = 5580: 2.2%

Issue: A misalignment between Microsoft best practices based on Microsoft Secure Score was detected related to Automatic email forwarding is enabled. The control may not be implemented or partially implemented.

Recommendation:

5580

Unimplemented Microsoft Control: Ensure that no sender domains are allowed for anti-spam policies (90 pts each)

Current Score: 90 pts x 62 = 5580: 2.2%

Issue: 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.

Recommendation: Remove all allowed domains and allowed senders from all your inbound anti-spam policies.

5310

Unimplemented Microsoft Control: Publish M365 sensitivity label data classification policies (90 pts each)

Current Score: 90 pts x 59 = 5310: 2.09%

Issue: 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).

Recommendation: Open Microsoft Purview compliance portal, Under Solutions click Information protection, Ensure Labels exist, Click on Label policies tab, Ensure that a Label policy exists and is published accordingly, Make sure Labels are published on all of your licensed users and groups,

720

Unimplemented Microsoft Control: Ensure multifactor authentication is enabled for all users in administrative roles (90 pts each)

Current Score: 90 pts x 8 = 720: 0.28%

Issue: 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

Recommendation: Microsoft services provide step-by-step guidance to select and enable the right MFA method for your organization in the Microsoft 365 admin center. Go to the Microsoft 365 MFA (<https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess>) wizard, If you would like to perform the implementation yourself, first check what Microsoft Entra ID license you have under "Prerequisites" in Microsoft Secure Score or see your license type under "Basic information" in the Microsoft Entra ID Overview (https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview). If you've invested in Microsoft Entra ID Premium P1 or P2 licenses, you can create a Conditional Access policy from scratch or by using a template. Follow these steps to create a Conditional Access policy from scratch or by using a template (<https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa>), If you would like to perform the implementation yourself and you're using Microsoft Entra ID Free, turn on security defaults. Note: Security defaults and Conditional Access can't be used side by side. Enable security defaults (<https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>), Keep track of your admin's progress of registering authentication methods by going to Microsoft Entra ID > Security > Authentication methods > User registration details (requires Microsoft Entra ID Premium P1 or P2 licenses). Go to User registration details (https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~~/UserRegistrationDetails)

630

Unimplemented Microsoft Control: Disable JavaScript on Adobe DC (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines whether to globally disable and lock JavaScript execution in Adobe DC JavaScript could potentially be used by attackers to manipulate users or to execute undesired code locally.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630

Unimplemented Microsoft Control: Enable 'Microsoft network client: Digitally sign communications (always)' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management

> Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable the local storage of passwords and credentials (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable Anonymous enumeration of shares (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines whether anonymous logon users (null session connections) are allowed to list all account names and enumerate all shared resources. Allowing this can provide a map of potential points to attack the system.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable Solicited Remote Assistance (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable IP source routing (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines whether IP source routing is enabled. Configuring the system to disable IP source routing protects against spoofing.

Recommendation: Within Microsoft 365 security, go to Vulnerability management

> Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set IPv6 source routing to highest protection (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines whether IPv6 source routing is enabled. Configuring the system to disable IP source routing protects against spoofing.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Allow Basic authentication' for WinRM Service (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Allow Basic authentication' for WinRM Client (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Autoplay' for all drives (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 immediately. An attacker could use this feature to launch a malicious program to damage a client computer or data on the computer.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Autoplay for non-volume devices' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set 'Minimum PIN length for startup' to '6 or more characters' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Prohibit use of Internet Connection Sharing on your DNS domain network (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Enable 'Require domain users to elevate when setting a network's location' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Installation and configuration of Network Bridge on your DNS domain network' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Enable 'Block third party cookies' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Password Manager' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Disable 'Continue running background apps when Google Chrome is closed' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 is closed.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Enable 'Hide Option to Enable or Disable Updates' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Controls whether to hide the user interface (UI) options to enable or disable Office automatic updates from users.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Enable 'Apply UAC restrictions to local accounts on network logons' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 administration and support. A compromised local administrator account can provide means for an attacker to move laterally between domain systems.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set 'Minimum password age' to '1 or more day(s)' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines the number of days that you must use a password before you can change it.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set 'Enforce password history' to '24 or more password(s)' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines the number of unique new passwords that are required before an old password can be reused in association with a user account.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set 'Minimum password length' to '14 or more characters' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: Determines the minimum password length

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630

Unimplemented Microsoft Control: Disable 'Enumerate administrator accounts on elevation' (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630

Unimplemented Microsoft Control: Block abuse of exploited vulnerable signed drivers (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630

Unimplemented Microsoft Control: Block persistence through WMI event subscription (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 gain periodic execution control. Some threats can abuse the WMI repository and event model to stay hidden.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Block process creations originating from PSEXEC and WMI commands (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-process-creations-originating-from-psexec-and-wmi-commands>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Use advanced protection against ransomware (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?use-advanced-protection-against-ransomware>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Block executable files from running unless they meet a prevalence, age, or trusted list criterion (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-executable-files-from-running-unless-they-meet-a-prevalence-age-or-trusted-list-criterion>) 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 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

630 Unimplemented Microsoft Control: Set User Account Control (UAC) to automatically deny elevation requests (90 pts each)

Current Score: 90 pts x 7 = 630: 0.25%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

450 Unimplemented Microsoft Control: Enable 'Local Security Authority (LSA) protection' (90 pts each)

Current Score: 90 pts x 5 = 450: 0.18%

Issue: Forces LSA to run as Protected Process Light (PPL). If LSA isn't running as a protected process, attackers could easily abuse the low process integrity for attacks (such as Pass-the-Hash).

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

450 Unimplemented Microsoft Control: Set controlled folder access to enabled or audit mode (90 pts each)

Current Score: 90 pts x 5 = 450: 0.18%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

450 Unimplemented Microsoft Control: Turn on PUA protection in block mode (90 pts each)

Current Score: 90 pts x 5 = 450: 0.18%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

360 Unimplemented Microsoft Control: Turn on Microsoft Defender Credential Guard (90 pts each)

Current Score: 90 pts x 4 = 360: 0.14%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Enable 'Network Protection' (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: Network protection (<https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Enable Microsoft Defender Antivirus email scanning (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block Office applications from creating executable content (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-office-applications-from-creating-executable-content>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block all Office applications from creating child processes (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-all-office-applications-from-creating-child-processes>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose

remediation or exception options.

180 Unimplemented Microsoft Control: Block executable content from email client and webmail (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-executable-content-from-email-client-and-webmail>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block Office applications from injecting code into other processes (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-office-applications-from-injecting-code-into-other-processes>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Enable Automatic Updates (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management

> Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block JavaScript or VBScript from launching downloaded executable content (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-javascript-or-vbscript-from-launching-downloaded-executable-content>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block Win32 API calls from Office macros (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-win32-api-calls-from-office-macros>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the Public profile (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: Controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. Users with administrative privileges might create firewall rules that expose the system to remote attack. Local connection rules should not be merged with

Group Policy settings on a public network to prevent Group Policy settings from being changed and weakened.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180

Unimplemented Microsoft Control: Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180

Unimplemented Microsoft Control: Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180

Unimplemented Microsoft Control: Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block execution of potentially obfuscated scripts (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-execution-of-potentially-obfuscated-scripts>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block Adobe Reader from creating child processes (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-adobe-reader-from-creating-child-processes>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180 Unimplemented Microsoft Control: Block Office communication application from creating child processes (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-office-communication-application-from-creating-child-processes>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180

Unimplemented Microsoft Control: Block untrusted and unsigned processes that run from USB (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-untrusted-and-unsigned-processes-that-run-from-usb>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

180

Unimplemented Microsoft Control: Block credential stealing from the Windows local security authority subsystem (lsass.exe) (90 pts each)

Current Score: 90 pts x 2 = 180: 0.07%

Issue: 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 (<https://learn.microsoft.com/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?block-credential-stealing-from-the-windows-local-security-authority-subsystem-lsassexe>) 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90

Unimplemented Microsoft Control: Disable JavaScript on Adobe Reader DC (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Determines whether to globally disable and lock JavaScript execution in Adobe Reader

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose

remediation or exception options.

90 Unimplemented Microsoft Control: Disable Flash on Adobe Reader DC (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Determines whether Adobe Reader will render Flash content.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Unimplemented Microsoft Control: Enable 'Require additional authentication at startup' (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Unimplemented Microsoft Control: Limit external participants from having control in a Teams meeting (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Log into Microsoft Teams admin center (<https://admin.teams.microsoft.com/>), In the left navigation, go to Meetings > Meeting Policies, Under Manage Policies, select a group/direct policy, Under the Content Sharing section, toggle "Allow an external participant to give or request control" to Off, You'll need to change this setting for each group/direct policy,

90 Unimplemented Microsoft Control: Ensure 'External sharing' of calendars is not available (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Microsofters should not be allowed to share the full details of their calendars with external users.

Recommendation: In the Microsoft 365 Exchange admin center (<https://admin.exchange.microsoft.com/>), go to Organization > Sharing. Under Individual Sharing, make sure all policies are unticked.

90

Block OneDrive for Business sync from unmanaged devices (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Microsoft OneDrive allows users to sign in their cloud tenant account, and begin syncing select folders or the entire contents of OneDrive to a local computer. By default this includes any computer with OneDrive already installed, whether or not it is Azure Domain Joined or Active Directory Domain joined. Unmanaged devices pose a risk, since their security cannot be verified through existing security policies, brokers or endpoint protection. Allowing users to sync data to these devices takes that data out of the control of the organization. This increases the risk of the data either being intentionally or accidentally leaked. Note: This setting is only applicable to Active Directory domains when operating in a hybrid configuration. It does not apply to Microsoft Entra ID domains. If you have devices which are only Microsoft Entra ID joined, consider using a Conditional Access Policy instead.

Recommendation: To block the sync client on unmanaged devices, use the Microsoft 365 Admin Center: Navigate to Microsoft 365 administration portal (<https://admin.microsoft.com>), Click on All Admin Centers and then Show All, then SharePoint. Now click Settings followed by OneDrive - Sync, Check the Allow syncing only on computers joined to specific domains, Use the Get-ADDomain PowerShell command to obtain the GUID from each domain then add them to the box. Click Save

90

Set user authentication for remote connections by using Network Level Authentication to 'Enabled' (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Determines whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90

Set 'Interactive logon: Machine inactivity limit' to '1-900 seconds' (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: You should require your users to use encryption on their mobile devices. Unencrypted devices can be stolen and their data extracted by an attacker very easily. Note: To comply, there should be at least one device configuration for Android with device password encryption. User impact: This setting should have no user impact, provided the device supports the feature.

Recommendation: To set mobile device management profiles, use the Microsoft Intune admin center (<https://intune.microsoft.com/#home>): Select Devices, then under Policy select Configuration profiles, If there are no policies, select Create Policy. Set a Name for the policy, choose the appropriate Platform and select Device restrictions. In the Password section, ensure that Encryption is set to Require. If there are existing policies, per each policy - Select the policy by clicking on it. Select Edit next to Configuration settings. In the Password section, ensure that Encryption is set to Require. Note: To comply, there should be at least one device configuration for Android with device password encryption.

90 Ensure mobile device management policies are set to require advanced security configurations (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Managing mobile devices in your organization, helps provide a basic level of security to protect against attacks from these platforms. For example ensure that the device is up to date on patches or is not rooted. These configurations open those devices to vulnerabilities that are addressed in patched versions of the mobile OS. You should configure your mobile device management policies to require advanced security configurations. If you do not require this, users will be able to connect from devices that are vulnerable to basic exploits, leading to potential breaches of accounts and data. Note: To comply, only mobile devices must be configured (Windows or MacOS is not required). User impact: The impact associated with this change is dependent upon the settings specified in the mobile device configuration profile.

Recommendation: To set mobile device management profiles, use the Microsoft Intune admin center (<https://intune.microsoft.com/#home>): Select Devices and then under Policy select Configuration profiles, Select Create profile to create a new profile. Select the appropriate Platform (iOS or Android). Choose, based on your organization's needs, the desired settings from the configuration screens. Note that the condition to comply is the mere existence of such profile, the specific settings should be decided according to your organization's needs. To comply, there should be at least one configuration policy for mobile devices. It is suggested to create two policies for both iOS and Android.

90 Ensure 'User owned apps and services' is restricted (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: By default, users can install add-ins in their Microsoft Word, Excel, and PowerPoint applications, allowing data access within the application. Do not allow users to install add-ins in Word, Excel, or PowerPoint. Rationale: Attackers commonly use vulnerable and custom-built add-ins to access data in user applications. While allowing users to install add-ins by themselves does allow them to easily acquire useful add-ins that integrate with Microsoft applications, it can represent a risk if not used and monitored carefully. Disable future user's ability to install add-ins in Microsoft Word, Excel, or PowerPoint helps reduce your threat-surface and mitigate this risk. Impact: Implementation of this change will impact both end users and administrators. End users will not be able to install add-ins that they may want to install.

Recommendation: To prohibit users installing Office Store add-ins and starting 365 trials: Navigate to Microsoft 365 admin center <https://admin.microsoft.com>. Click to expand Settings Select Org settings. 3. Under Services select User owned apps and services. 4. Uncheck Let users access the Office Store and Let users start trials on behalf of your organization. 5. Click Save. Note - Due to temporary limitations, only "Let users access the Office Store" will be taken into account in scoring this control. It is suggested to uncheck both settings for the sake of better posture.

90 Ensure third party integrated applications are not allowed (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Do not allow third party integrated applications to connect to your services. You should not allow third party integrated applications to connect to your services unless there is a very clear value and you have robust security controls in place. While there are legitimate uses, attackers can grant access from breached accounts to third party applications to exfiltrate data from your tenancy without having to maintain the breached account

Recommendation: In the Microsoft 365 Admin Center Select Admin Centers and Microsoft Entra ID. Select Users from the Azure navigation pane, Select Users settings. Set App registrations is set to No. Click Save.

90 Ensure 'Phishing-resistant MFA strength' is required for Administrators (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Authentication strength is a Conditional Access control that allows administrators to specify which combination of authentication methods can be used to access a resource. For example, they can make only phishing-resistant authentication methods available to access a sensitive resource. But to access a non-sensitive resource, they can allow less secure multifactor authentication (MFA) combinations, such as password + SMS. Microsoft has 3 built-in authentication strengths. MFA strength, Passwordless MFA strength, and Phishing-resistant MFA strength. Ensure administrator roles are using a CA policy with Phishing-resistant MFA strength. Administrators can then enroll using one of 3 methods: FIDO2

Security Key, Windows Hello for Business, Certificate-based authentication (Multi-Factor), NOTE: Additional steps to configure methods such as FIDO2 keys are not covered here but can be found in related MS articles in the references section. The Conditional Access policy only ensures 1 of the 3 methods is used. WARNING: Administrators must be pre-registered for a strong authentication mechanism before this Conditional Access Policy is enforced. Additionally, as stated elsewhere in the CIS Benchmark a break-glass administrator account should be excluded from this policy to ensure unfettered access in the case of an emergency. Rationale: Sophisticated attacks targeting MFA are more prevalent as the use of it becomes more widespread. These 3 methods are considered phishing-resistant as they remove passwords from the login workflow. It also ensures that public/private key exchange can only happen between the devices and a registered provider which prevents login to fake or phishing websites. References: FIDO2 security keys (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys>), Enable passwordless security key sign-in (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key>), Conditional Access authentication strength (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths>), How To: Configure the Microsoft Entra ID multifactor authentication registration policy (<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>),

Recommendation: To create a phishing-resistant MFA CA policy for users in administrative roles: Navigate to the Microsoft Entra ID admin center <https://entra.microsoft.com>. Click to expand Microsoft Entra ID > Applications select Enterprise Applications. Under Security, select Conditional Access. Click New policy. Go to Users > Users and groups > Include > Select users and groups > Directory roles, Add at least the Directory roles listed after these steps. Select Cloud apps or actions > All cloud apps (and don't exclude any apps). Grant > Grant Access with Require authentication strength (Preview): Phishing-resistant MFA, Click 'Select', Set Enable policy to Report-only and click Create, At minimum these directory roles should be included for the policy: Application administrator, Authentication administrator, Billing administrator, Cloud application administrator, Conditional Access administrator, Exchange administrator, Global administrator, Global reader, Helpdesk administrator, Password administrator, Privileged authentication administrator, Privileged role administrator, Security administrator, SharePoint administrator, User administrator, WARNING: Ensure administrators are pre-registered with strong authentication before enforcing the policy. After which the policy must be set to "On".

90

Ensure password protection is enabled for on-prem Active Directory (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Enable Microsoft Entra ID Password Protection to Active Directory to protect against the use of common passwords. Note: This recommendation applies to Hybrid deployments only, and will have no impact unless working with on-premises Active Directory.

Recommendation: To setup Microsoft Entra ID Password Protection, use the following steps: Download and install the Microsoft Entra ID Password Proxies and DC Agents from the following location: <https://www.microsoft.com/download/details.aspx?id=57071>, After the installation is complete, login to <https://admin.microsoft.com> as a Global Administrator. Go to

Admin centers and click on Microsoft Entra ID. Select Microsoft Entra ID then Security on the left side navigation followed by Authentication methods. Select Password protection and toggle Enable password protection on Windows Server Active Directory to Yes and Mode to Enforced, Click Save at the top of the right pane.

90 Ensure 'Microsoft Azure Management' is limited to administrative roles (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: The Microsoft Azure Management application governs various Azure services and can be secured through the implementation of a Conditional Access policy. This policy can restrict specific user accounts from accessing the related portals and applications. When Conditional Access policy is targeted to the Microsoft Azure Management application, within the Conditional Access policy app picker the policy will be enforced for tokens issued to application IDs of a set of services closely bound to the portal. Azure Resource Manager, Azure portal, which also covers the Microsoft Entra ID admin center, Azure Data Lake, Application Insights API, Log Analytics API, Microsoft Azure Management should be restricted to specific pre-determined administrative roles. NOTE: Blocking Microsoft Azure Management will prevent non-privileged users from signing into most portals other than Microsoft 365 Defender and Microsoft Purview. Rationale: Blocking sign-in to Azure Management applications and portals enhances security of sensitive data by restricting access to privileged users. This mitigates potential exposure due to administrative errors or software vulnerabilities, as well as acting as a defense in depth measure against security breaches.

Recommendation: To enable Microsoft Azure Management restrictions: Navigate to the Microsoft Entra ID admin center <https://entra.microsoft.com>. Click expand Protection > Conditional Access select Policies. Click New Policy and then name the policy. Select Users > Include > All Users, Select Users > Exclude > Directory roles and select only administrative roles (See below). Select Cloud apps or actions > Select apps > Select then click the box next to Microsoft Azure Management. Click Select. Select Grant > Block access and click Select. Ensure Enable Policy is On then click Create. WARNING: Exclude Global Administrator at a minimum to avoid being locked out. Report-only is a good option to use when testing any Conditional Access policy for the first time. Below is an example list of Administrator roles that could be excluded: Application administrator, Authentication administrator, Billing administrator, Cloud application administrator, Conditional Access administrator, Exchange administrator, Global administrator, Global reader, Helpdesk administrator, Password administrator, Privileged authentication administrator, Privileged role administrator, Security administrator, SharePoint administrator, User administrator, Default Value: No - Non-administrators can access the Microsoft Entra ID administration portal.

90 Unimplemented Microsoft Control: Ensure modern authentication for SharePoint applications is required (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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).

Recommendation: In the Microsoft 365 Admin Center: 1. Go to SharePoint Admin Center. 2. Expand the Policies section then select Access control. 3. Select Apps that don't use modern authentication. 4. Select the radio button for Block access. 5. Click Save.

90 Unimplemented Microsoft Control: Ensure additional storage providers are restricted in Outlook on the web (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Restrict additional storage providers are restricted using PowerShell: Connect to Exchange Online using Connect-ExchangeOnline. Run the following PowerShell command: Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -AdditionalStorageProvidersAvailable \$false, Run the following Powershell command to verify that the value is now False: Get-OwaMailboxPolicy | Format-Table Name, AdditionalStorageProvidersAvailable,

90 Unimplemented Microsoft Control: Ensure MailTips are enabled for end users (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: MailTips assist end users with identifying strange patterns to emails they send.

Recommendation: To enable MailTips, use the Exchange Online PowerShell Module: Run Microsoft Exchange Online PowerShell Module, Connect using "Connect-ExchangeOnline", Run the following PowerShell command: Set-OrganizationConfig -MailTipsAllTipsEnabled \$true - MailTipsExternalRecipientsTipsEnabled \$true -MailTipsGroupMetricsEnabled \$true - MailTipsLargeAudienceThreshold '25'

90 Unimplemented Microsoft Control: Ensure mailbox auditing for all users is Enabled (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: To enable mailbox auditing for all users: Connect to Exchange Online using Connect-ExchangeOnline. Run the following PowerShell command: Set-OrganizationConfig -AuditDisabled \$false, For each unconfigured MailBox of type Resource Mailboxes, Public Folder Mailboxes or DiscoverySearch Mailbox run: Get-Mailbox -Filter "Name -eq 'MailBox name'" | Set-Mailbox -AuditEnabled \$true,

90

Unimplemented Microsoft Control: Start your Defender for Identity deployment, installing Sensors on Domain Controllers and other eligible servers. (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Go to the sensor page in Settings, you can view the already installed sensors in your environment and download the install package to deploy them on your remaining domain controllers. You will be scored as a percentage of your deployment progress.

90

Ensure Administrative accounts are separate and cloud-only (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. Regular user accounts should never be utilized for Administrative tasks and care should be taken, in the case of a hybrid environment, to keep Administrative accounts separated from on-prem accounts. Administrative accounts should not have applications assigned so that they have no access to potentially vulnerable services (EX. email, Teams,

SharePoint, etc.) and only access to perform tasks as needed for Administrative purposes.

Recommendation: 1. Navigate to Microsoft 365 admin center 2. Click to expand Users select Active users. 3. Sort by the Licenses column. 4. For each user account in an administrative role verify the following: The account is Cloud only (not synced) The account is assigned a license that is not associated with applications i.e. (Microsoft Entra ID P1, Microsoft Entra ID P2)

90 Unimplemented Microsoft Control: Disable SMBv1 client driver (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Unimplemented Microsoft Control: Fix Microsoft Defender for Endpoint impaired communications (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Unimplemented Microsoft Control: Turn on Microsoft Defender for Endpoint sensor (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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 Endpoint The Microsoft Defender for Endpoint service will not be able to determine the security state of machines that are not sending sensor data.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Unimplemented Microsoft Control: Restrict anonymous users from joining meetings (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: 1. Log into Microsoft Teams admin center 2. In the left navigation, go to Meetings > Meeting Settings 3. Under the Participants section, toggle "Anonymous users can join a meeting" to Off

90 Unimplemented Microsoft Control: Deploy a log collector to discover shadow IT activity (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: In the Defender for Cloud Apps portal, go to the Automatic log upload page. In the Data sources tab, select Add data source to create a data source for your appliance. In the Log collector tab, select Add log collector to add a new one. Follow the instructions provided to deploy Docker (<https://docs.microsoft.com/cloud-app-security/discovery-docker>) and the log collector container.

90 Unimplemented Microsoft Control: Fix Microsoft Defender for Endpoint sensor data collection (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: 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.

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Ensure SharePoint external sharing is managed through domain whitelist/blacklists (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Control sharing of documents to external domains by either blocking domains or only allowing sharing with specific named domains. Note - this control's mandatory compliance requirement is to set allow list domains.

Recommendation: To configure document sharing restrictions: Navigate to SharePoint admin center - <https://admin.microsoft.com/sharepoint>. Expand Policies then click Sharing. Expand More external sharing settings and check Limit external sharing by domain. Select Add domains to add a list of approved domains. Click Save at the bottom of the page. To configure document sharing restrictions using PowerShell: Connect to SharePoint Online using Connect-SPOService. Run the following PowerShell command: `Set-SPOTenant -SharingDomainRestrictionMode AllowList - SharingAllowedDomainList "domain1.com domain2.com"`

90 Unimplemented Microsoft Control: Disable the built-in Administrator account (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Determines whether the built-in Administrator account is disabled

Recommendation: Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.

90 Ensure that Sways cannot be shared with people outside of your organization (90 pts each)

Current Score: 90 pts x 1 = 90: 0.04%

Issue: Sway is a new app from Microsoft Office that allows users to create and share interactive reports, personal stories, presentations, and more. This setting controls user Sway sharing capability, both within and outside of the organization. By default, Sway is enabled for everyone in the organization. Rationale: Disable external sharing of Sway documents that can contain sensitive information to prevent accidental or arbitrary data leak.

Recommendation: To ensure Sways cannot be viewed outside of your organization: Navigate to Microsoft 365 admin center <https://admin.microsoft.com>. Click to expand Settings then select Org settings. Under Services select Sway and block Let people in your organization share their sways with people outside your organization. Click Save.

75 Teams guests allowed to create and remove channels (25 pts each)

Current Score: 25 pts x 3 = 75: 0.03%

Issue: Team settings allows guests to create and remove channels. This could cause loss of data as guests add and remove channels.

Recommendation: Verify if guest creation and removal of channels is desired on the specified Teams. When not necessary, disable the ability of Team guests to create and remove channels to avoid potential data loss and channel proliferation.