Microsoft

Practical guide to security using Microsoft 365 Business (Basic, Standard, and Premium)

Table of Contents

Introduction

This guide summarizes Microsoft's recommendations for enabling employees at small and medium-sized businesses to securely work from anywhere- whether from home, in the office or on the go, using the features included in Microsoft 365 Business Premium.

Microsoft 365 Business Premium is a comprehensive suite of collaboration products and enterprise-grade security tools curated specifically for businesses with 1 to 300 employees. It includes Office productivity apps and services plus advanced security capabilities to help defend businesses against cyberthreats, protect company data, and secure devices. Although other licensing plans include some of these advanced security and management capabilities, for organizations with less than 300 employees, Microsoft 365 Business Premium is generally the most cost-effective package.

Because SMBs have different security needs and attitudes, the checklist includes general recommendations scenarios; however, you should evaluate each recommendation and adjust based on your customers' unique circumstances and requirements.

Many businesses will want to enable security and balance ease of use with security. Other businesses may want to maximize security protections and have higher concern for risk (for example, to adhere to regulatory requirements such as HIPAA or GLBA). This business is also willing to apply more effort and resources into maintaining security and control of the work environment.

These guidelines are intended to provide a starting point for a serious discussion around the security and compliance options available, rather than prescriptive guidance. One of the first and most important things that IT leaders and business leaders can do is talk through the possibilities.

You can download the summary checklist here. If you'd like to learn more about the checklist items, we've broken it down section by section below.

Getting Started: Preparation Checklist for Onboarding

Checklist item	***Description***	***Learn more***
Adopt a formal cybersecurity framework	Using a vendor agnostic cybersecurity framework such as NIST or CIS can help you prioritize and validate your adoption of cybersecurity technology.	NIST Cybersecurity Framework CIS Critical Security Controls
Plan for identity management	Most SMBs should move toward a cloud-only architecture, but in some cases, you may need to retain a hybrid environment.	Determine your cloud identity model
Plan for administrative accounts	Partners should set up GDAP to manage customer tenants, but customers may also want to maintain one or more admin accounts.	Set up GDAP for your customers Granular Delegated Admin Privileges Least privileged roles by task
Plan for device management	What types of devices are Company owned? Do you allow personally owned devices to access company data? If so, how will you manage those devices?	What is the difference between device and app management
Plan for licensing	We recommend Microsoft 365 Business Premium for most SMB deployments, but some organizations may want to mix-and-match licenses for different user personas.	Compare All Microsoft 365 Plans for Business
Choose technical and administrative contacts	Determine where to send billing notifications, security alerts, and more.	Manage billing notifications

Here is a brief explanation & our recommendation for each checklist item.

- **Adopt a formal cybersecurity framework:** A security framework will help guide and rationalize decision making around cybersecurity vendors, products, and features in use by your business and your customers. They are basically independent blueprints of most of the things you should consider regarding cybersecurity. If you don't already have a framework in mind, we recommend starting with CIS Controls v8, Implementation group 1 because we find it very approachable for SMB partners and customers. Additionally, the CIS Microsoft 365 Foundations Benchmark provides prescriptive guidance for establishing a secure configuration posture for Microsoft 365 Cloud offerings. Your customers may find a different cybersecurity framework more suitable based on

regional or industry vertical considerations; however, the controls between different frameworks are mostly compatible with each other so solving controls for one usually solves for controls in other frameworks. For your convenience, we have listed the applicable CIS control in the checklist below.

- **Plan for identity management:** The users in the Microsoft 365 tenant can have their identities (usernames, passwords, etc.) managed completely in the cloud, or synchronized with an on-premises Active Directory. If your customer does not have an existing Active Directory on-premises, you can set up cloud-only identity by adding users individually in the admin portal, using PowerShell, or bulk loading users using a CSV file. If your customer has Active Directory, then we recommend starting with a hybrid approach—using Azure AD Connect to synchronize the domain to Microsoft 365 and them moving from hybrid to managing identities only in the cloud as soon as reasonably possible because it's simpler to administer, reduces complexity, and it is much easier to secure a single cloud identity than identities synchronized from on-premises infrastructure. We recommend configuring Azure AD Connect with Microsoft 365 Business Premium:

Setting	***Description***	***Recommended Value***
Azure AD Connect - sign-in method	Password Hash Sync is the simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure.	Password Hash Sync
Azure AD Connect - single sign-on	SSO provides users easy access to cloud-based applications without needing any additional on-premises components.	Enabled
Azure AD Connect - On-premises attribute for Azure AD username	The userPrincipalName in AD should match the user's email address.	userPrincipalName
Azure AD Connect - Password writeback	Password writeback synchronizes password changes in Azure AD back to the on-premises AD environment. Additional configuration required.	Enabled
Azure AD Connect – Service Connection Point (SCP)	Azure AD Connect can configure the service connection point (SCP) object in AD for you. This will enable domain joined computers to	Configured using Azure AD Connect **Additional tasks –> Configure Device Options ->**

	discover Azure AD tenant information. For more information click here.	**Configure hybrid Azure AD Join**
Azure AD Connect – hybrid Azure AD join device operating systems	Select the operating systems in use. We recommend upgrading operating systems older than Windows 10.	Windows 10 and later

- **Plan for administrative accounts:** There are five rules that we recommend observing with regard to administrative accounts in Microsoft 365:
    1. ***Reduce the number of global admins:*** *We recommend 2 and no more than 5 global administrators per tenant.*
    2. ***Use separate accounts:*** *Do not assign admin privileges to standard user accounts, and do not sync existing admins from on-premises Active Directory, and assign those same accounts cloud administrative privileges. Instead, use a separate, unlicensed administrative user ID in the onmicrosoft.com domain.*
    3. ***Require strong authentication:*** *All administrative accounts should be required to use strong authentication methods. This requirement will also be addressed under Identity Protection in this checklist.*
    4. ***Partners are encouraged to implement GDAP:*** *Granular Delegated Admin Privileges or GDAP allows partners to manage least privilege access for their users within customer tenants. See this article for more information. Microsoft 365 Lighthouse has an easy to use wizard that will set up GDAP. See this article for more information on using Lighthouse to set up GDAP for your customers.*
    5. ***Customers are encouraged to implement RBAC:*** *Delegate admin roles where appropriate. For example, instead of assigning Global admin to every user, determine if lesser roles would be adequate for each user's job function: e.g., Helpdesk administrator, License administrator, Billing administrator, etc. See this article for a list of roles and permissions.*
- **Plan for device management:** We recommend enrolling Company-owned devices into Microsoft Intune in order to establish a device and software inventory and to centralize management. When it comes to personally owned devices, companies will have some additional decisions to make prior to implementation:
    - ***MAM vs. MDM for mobile devices:*** We can protect corporate data that resides on *personal* iOS and Android devices at the application layer using MAM, without needing to enroll the devices for full management (MDM). Company-owned mobile devices, however, should always be enrolled.
    - ***Block enrollment and access for other devices:*** Some organizations may want to consider blocking access to company apps and data on personally owned desktop and laptop computers (Windows, MacOS, Linux, etc.).

    - ***Enable web-only access:*** Another option that organizations have for personally owned devices is to allow a limited web access experience where data cannot be copied, printed, or downloaded to the device.
- **Plan for licensing*:*** It is essential to understand the needs of your organization and select an appropriate plan that aligns with the needs of your company. For small to medium-sized businesses we recommend using **Microsoft 365 Business Premium**, as it provides a comprehensive set of features and tools to help manage and secure your organization's data and devices. However, depending on the specific requirements of your organization, you may want to consider mixing different licenses for different user personas. It's important to note that Microsoft 365 Business Basic and Microsoft 365 Business Standard have security features but are not security solutions and require additional capabilities. If you have customers using Microsoft 365 Business Basic or Microsoft 365 Business Standard, we recommend adding Microsoft Defender for Business, Microsoft Defender for Office 365, and Azure Active Directory Premium P1 to those users.
- **Choose technical and administrative contacts:** Select individuals within your organization who will act as the primary point of contact for notifications such as billing, security alerts and service health. This will ensure that important notifications are received on time and are quickly and efficiently resolved. We recommend creating distribution groups for this purpose.

Identity Protection Checklist

Identity protection is a crucial aspect of securing sensitive information and maintaining the privacy of both employees and customers in today's digital landscape. Microsoft 365 Business Premium included Azure Active Directory Premium P1 that provides robust security features to protect the user identities from security threats such as password attacks, phishing scams, and malicious software. Microsoft 365 Lighthouse also helps partners monitor and manage their customers' identities, ensuring that only authorized personnel have access to critical information. With identity protection in Microsoft 365 Business Premium, small and medium businesses can safeguard their operations and maintain the trust of their customers while they focus on growing their business.

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Apply principles of least privilege	Use separate admin accounts & RBAC roles to limit admin privileges; grant only the minimum roles required for job function.	Partners: Set up GDAP for your customers Customers: Least privileged roles by task	5.4, 6.8, 12.2
Create emergency access account(s)	Microsoft recommends 2 or more cloud-only accounts for emergency access.	Manage emergency access admin accounts	N/A
Set up Conditional Access	Enable Multi-factor authentication, block legacy authentication, etc.	Providing a default level of security in Azure AD	6.3, 6.4, 6.5
Enable Self Service Password Reset	End users will be able to reset their own passwords from the cloud using their secure authentication methods.	Cloud-only: Enable Azure Active Directory self-service password reset Hybrid: Enable Azure Active Directory password writeback	
Configure Azure AD primary authentication method	Configure Microsoft Authenticator auth method to enhance security for sign-ins.	Passwordless sign-in with Microsoft Authenticator	N/A

- **Apply principles of least privilege:** Pay special attention to admin accounts. Use a separate named account for each Global Administrator that does not have a license assigned. Use limited admin roles whenever possible. For partner access to customer tenants, run the GDAP wizard in Lighthouse to assign technicians to appropriate roles in customer tenants.
- **Create emergency access account(s):** To prevent accidental lockout of administrative access, creating two emergency access accounts that are not synchronized to AD and are excluded from Conditional Access policies. Store the account credentials safely and protect these accounts with a FIDO2 security key. Configure Azure Log Analytics to trigger email and SMS alerts whenever these accounts sign in. For more information see Enable passwordless security key sign-in and Integrate Azure AD logs with Azure Monitor logs.
- **Set up Conditional Access:** Most common conditional access policies can be deployed using built-in templates; see Conditional Access templates for more details. We recommend deploying at least the following four policies to replace the functionality of Security Defaults:
    - Block legacy authentication
    - Require multifactor authentication for admins
    - Require multifactor authentication for all users
    - Require multifactor authentication for Azure management

- **Enable Self Service Password Reset:** Allowing end users to reset their own passwords from the cloud, without the need for IT administrator intervention. This helps to improve productivity and reduces the workload on the IT department by enabling users to reset their own passwords quickly and easily. To set up Self Service Password Reset (SSPR) in Microsoft 365, the wizard provided in the Microsoft 365 admin center should be used. The wizard will guide you through the process of configuring the authentication methods that users will use to verify their identity before resetting their password. You can choose from phone call, text message, and the Microsoft Authenticator app. Additionally, you will need to specify the users or groups that will be able to use SSPR, and set rules for password complexity, length, and how often passwords can be reset. Once you have completed the wizard, SSPR will be enabled for your tenant, and users will be able to reset their own passwords from the Microsoft 365 login page or the Azure AD self-service password reset page.
- **Configure Azure AD primary authentication method:** Configure the primary authentication method for Azure AD to use Microsoft Authenticator to enhance security for sign-ins. Users will be able to sign in to Azure AD and other Microsoft services using a one-time passcode generated by the app, or a number matching experience where the user must enter the correct number in their Authenticator app, which is being displayed to them within the sign-in prompt.

Email & Apps Protection Checklist

Email is a critical tool for communication and collaboration in today's fast-paced business environment. Unfortunately, it is also a prime target for cybercriminals looking to exploit vulnerabilities and steal sensitive information. Solving problems with Phishing and SPAM is one of the first items we recommend partners focus on because it is so important for small and medium businesses and it's hard to move on to other things if the customer is plagued with email hygiene problems. Microsoft 365 Business Premium includes Defender for Office 365 P1 which is a highly effective safeguard against threats such as phishing scams, spam, and malware. The platform employs advanced filtering techniques to identify and block malicious messages, while also providing users with tools to report suspicious emails and for your to take action to protect their accounts.

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Configure SPF record	Enter this TXT DNS record to help validate outbound email sent from your domain.	Set up SPF to help prevent spoofing	
Configure email authentication with DKIM and DMARC	Email authentication builds on SPF to build a solid foundation to reduce email spoofing. Misconfiguration can lead to false detections and outbound email going to junk mail.	Email authentication in EOP	
Enable Unified Audit Log	Record activity from Microsoft 365 services such as Exchange Online and SharePoint Online.	Turn auditing on or off	
Enable Alert Policies	With the audit log enabled, you can alert on suspicious activities such as Elevation of Exchange admin privilege and more.	Microsoft 365 alert policies	
Enable Defender for Office 365 preset policies	Quickly configures anti-spam, anti-malware, anti-phishing and zero-day protections including Safe Links and Safe Attachments.	Preset security policies	

Block auto forwarding	Prevent inbox rules or mailbox forwarding from automatically sending mail to external addresses.	Configuring and controlling external email forwarding in Microsoft 365	
Manage user Phishing reports	Allow end users to report messages suspected as phishing to Microsoft and to you as part of a managed service for email protection.	Deploy and configure the report message add-in to users	
Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams	Activate Microsoft Defender for Office 365 to secure SharePoint, OneDrive, and Microsoft Teams against potential cyber threats, and ensure the integrity of your data and files stored on these platforms.	Reduce the attack surface for Microsoft Teams	
Guest access in Teams	Allow end users to invite external guests into Teams.	Use guest access to collaborate with people outside your organization	
External chat in Teams	Allow end users to chat with people external to the organization.	Manage external access in Microsoft Teams	
Third-party cloud storage in Teams	Control which third-party cloud storage providers, if any, are allowed to be presented through Teams.	Manage Microsoft Teams settings for your organization	
Use configuration analyzer	Compare your customer's email protection settings to Microsoft recommendations	Configuration analyzer for protection policies in EOP and Microsoft Defender for Office 365	

- **Configure SPF record:** SPF is a TXT record in DNS that helps validate outbound email sent from your custom domain. Microsoft will recommend the correct value if all email originates from the Exchange Online service. If your customer has email originating from other places, consider routing it through Microsoft or customizing the SPF record.
- **Configure email authentication with DKIM & DMARC:** DomainKeys Identified Mail (DKIM) will protect your customers' domains from malicious email spoofing. It allows the system receiving the email to check that it was sent by the domain it claims to be sent from, and that it hasn't been modified in transit. To set up DKIM, you will need to

create DKIM DNS records and then configure Microsoft 365 to sign outgoing messages with the corresponding private key. See Use DKIM to validate outbound email sent from your custom domain. Adding DMARC records to your customers' domain's DNS allow you to specify what the receiving email systems should do with messages that fail the check (e.g. accept, quarantine or reject). This way you can Use DMARC to validate email and ensure the destination email systems trust messages sent from your customers' domains. The DNS records for DKIM are very specific and we recommend either copying the values directly from the M365 Admin Center or using automation such as a PowerShell script to reliably create the correct DNS records.

- **Enable Unified Audit Log:** Enterprise tenants will have this enabled by default; however, partners should verify the auditing status for their customer organizations. The audit log is required for several security scenarios in this guide.
- **Enable Alert Policies:** Microsoft provides built-in alert policies. On the Alert policies page, the names of these built-in policies are in bold, and the policy type is defined as System. Configure the policy to send email notifications to the technical or administrative contacts defined earlier in this guide.
- **Enable preset security policy:** Start with Standard protection for the entire domain. If your customer has specific users that are either sensitive to or targets for malicious email or SPAM, consider the Strict level of protection for them. For more information see Set up steps for the Standard or Strict preset security policies in Microsoft Defender for Office 365.
- **Block auto forwarding:** New tenants will have the outbound spam policy configured to block automatic forwarding. For existing tenants, this is a way to help prevent business email compromises.
- **Respond to user Phishing reports:** Enable users to report false positives (good email marked as bad) or false negatives (bad email allowed) to Microsoft for analysis. Optionally, you can set up a process to review these messages and respond to users. For more information see Enable the Microsoft Report Message or the Report Phishing add-ins and Admin review for reported messages.
- **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams**
- **Guest access in Teams:** Many businesses want to use Teams to collaborate with outside clients, suppliers, and partners beyond participating in meetings. To allow external users to fully participate in teams, enable guest access in the Teams admin center. We recommend enabling guest access even for security-conscious businesses because only specific users are allowed access and they must be explicitly added to individual teams. For more information refer to Use guest access to collaborate with people outside your organization.
- **External chat in Teams:** is different from guest access in that it only allows users outside of the business to initiate a Teams chat. This is useful when it is desirable for employees at businesses to initiate a chat just by knowing someone's email address; however, it may turn tricky in situations where uninvited chats are undesirable. By

default, external chat is allowed from any domain even if guest access is disabled and we recommend the default setting for most customers; however, you can turn it off or restrict external chat to a list of domains. For more information see Manage external access in Microsoft Teams and Disable open federation.

- **3rd party cloud storage in Teams:** Teams includes the ability for users to upload and share files from cloud storage services such as Dropbox, Box, and Google Drive. Some businesses may want to limit cloud storage to only those services they control directly in their Microsoft 365 tenant (SharePoint and OneDrive). For more information refer to Manage Microsoft Teams settings for your organization and Managing third party storage options.
- **Use configuration analyzer:** Partners can use the Configuration analyzer in the Microsoft 365 Defender portal to quickly find and fix email security policies where the settings are below the Standard protection and Strict protection profile settings in preset security policies.

Endpoint Enrollment Checklist

Enrolling devices in Microsoft 365 Business Premium is an important step partners should take to maintain the security and compliance of their customers' data and systems. Enrollment is the first step to ensure that all the devices used to access their information and applications are properly configured and managed. This helps to minimize the risk of security breaches, data loss, and other security incidents. Once enrollment is complete, additional controls can block or limit unknown devices from accessing data and applications. Microsoft 365 Business Premium included Microsoft Endpoint Manager (also known as Intune) which is a comprehensive device management solution that enables customers to enroll, monitor, and manage all the devices used in their organization, including macOS, iOS, and Android devices. Microsoft 365 Lighthouse provides partners deployment steps that make it easy to enroll devices for multiple customers.

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Choose mobility management approach	iOS and Android devices can be managed via either MAM or MDM. For personally owned devices, we recommend MAM.	What is the difference between device and app management	1.1
Configure device enrollment restrictions	For MAM deployments, block personal enrollments.	Create device platform restrictions	1.2
Deploy App protection policies (MAM)	Protects company data on mobile devices at the application layer.	Create and deploy app protection policies	

Configure device enrollment pre-reqs for supported platforms	Prepare supported device platforms for MDM enrollment, as needed. You do not need to configure platforms you do not intend to enroll or support.	Apple: Get an Apple MDM Push certificate Android: Connect your Google Play account Windows: Set up enrollment for Windows devices	
Configure default compliance policy settings	We recommend using the default compliance policy settings for most deployments.	Device compliance policies in Microsoft Intune	
Create compliance policies	For each platform you intend to support, create a basic compliance policy.	Create device compliance policies in Microsoft Intune	
Enable device-based conditional access policies	Use Conditional Access to enforce app protection and device compliance policies, and prevent unauthorized device access.	Require approved app or app protection Require compliant, hybrid join, or MFA Block unsupported platforms Require MFA for Intune Enrollment	1.2
Configure Enterprise State Roaming	Allow user settings in Windows to sync with Azure AD and follow the user.	Enable Enterprise State Roaming in Azure Active Directory	
Deploy Microsoft 365 apps	Use Intune to remotely deploy the Microsoft 365 apps to managed Windows devices.	Add Microsoft 365 Apps to Windows 10/11 devices using Microsoft Intune	2.1
Enroll devices	Company-owned devices should be Azure AD joined and enrolled.	Android iOS Linux macOS Windows	1.1

- **Choose mobility management approach:** For personally owned devices, we recommend implementing MAM (Mobile App Management). For Company-owned devices, we recommend enrolling the devices for MDM (device-based management). For more information, see What is the difference between device and app management?

- **Configure device enrollment restrictions**: Determine in advance whether you will need to block or allow enrollment of specific device types. For example, you can block personal enrollment of iOS and Android devices (MAM does not require enrollment). For more information, see Create device platform restrictions. Another reason to consider enrollment restrictions is if you intend to use MAM, you can prevent end users from inadvertently enrolling their device in MDM.
- **Deploy App protection policies (MAM):** App protection policies enable MAM on iOS and Android mobile devices. These policies include settings that help protect data on mobile devices, without requiring the device itself to become enrolled. For example, we can require a PIN or biometric to use the Outlook application, instead of requiring a passcode to open the "Home" screen of the device. We can also restrict the ability to save company data to local storage on the device and require that data always be kept within the boundaries of the Corporate-owned and managed applications. Microsoft has Microsoft has introduced a data protection configuration framework taxonomy, organized into distinct configuration scenarios. For more information see Data protection framework using app protection policies. Basic recommendations include:
    - *From **Apps** > **App protection policies**, create policies for both **iOS/iPadOS** and **Android***
    - *Target policy to **Microsoft core apps** (this includes Outlook)*
    - ***Block** backup of org data to iCloud or Google cloud*
    - *Send org data to **Policy managed apps***
    - ***Block** saving copies of org data; Allow users to save to **OneDrive** and **SharePoint***
    - *For remaining selections, accept the default values or choose your own preferences, and finish creating the policy, assigning to **All users**.*
- **Configure device enrollment pre-reqs for supported platforms:** Before you enroll any devices, it may be necessary to complete some pre-requisites for certain scenarios. You do not have to complete these steps for any device platforms you do not intend to enroll and support in your organization:
    - Get an Apple MDM Push certificate
    - Connect your Google Play account
    - Set up enrollment for Windows devices
- **Configure default compliance policy settings:** Compliance policy settings are evaluated as the "Built-in compliance policy" by Intune. The most important setting is to determine whether devices which have not yet been evaluated by a compliance policy are to be considered *Compliant* or *Not compliant*. In other words, we are telling Intune whether to treat devices as innocent until proven guilty (*Compliant*), or guilty until proven innocent (*Not compliant*). We recommend using the default settings.
- **Create compliance policies:** For every device platform that you will have enrolled, we recommend creating a compliance policy. Think of this policy as defining the "minimum bar" that devices must reach before they are extended access to company data. For example, you can require BitLocker for Windows devices. Note however that

compliance-based access will not be enforced until the corresponding Conditional Access policy is deployed.
    - *Recommended compliance policy for Windows 10 and later:*
        - *Turn on **Device Health** options including **BitLocker**, **Secure Boot**, **Require code integrity***
        - *Turn on **System Security** > **Device Security** options including **Firewall**, **TPM**, **Antivirus** and **Antispyware***
        - *Turn on **Defender** options including **Antimalware**, **Antimalware security intelligence up-to-date** and **Real-time protection***
        - *Under **Actions for noncompliance**, set **Mark device noncompliant** after **1** day*
        - *Assign the policy to **All users***
    - *For other platforms: It is generally recommended to enforce device passcode with device encryption and code integrity where available.*
- **Enable device-based conditional access policies**: We recommend the following policies which can be used to help protect the device enrollment process, and enforce device-based access controls:
    - Require multifactor authentication to register or join devices to Azure AD
    - Block unknown or unsupported device platforms
    - Require multifactor authentication for Intune device enrollment
    - Require approved app or app protection policy
    - Require compliant, hybrid joined devices, or MFA
- **Configure Enterprise State Roaming**: Certain settings in Windows 10/11 can follow users around between different devices. See this article for more information.
- **Deploy Microsoft 365 apps**: When endpoints are enrolled with Intune, assigned software such as Microsoft 365 apps for the desktop can be automatically installed on the device. See this article for more information. Using Intune to deploy apps also helps establish and maintain a software inventory as outlined in CIS Control v8 2.1.
- **Enroll devices:** Once you have laid all the groundwork and prepared your device policies, you can begin enrolling devices. See these articles for more details:
    - Enroll Android personally owned work profile
    - Enroll personally owned iOS devices
    - Enroll Linux devices
    - Enroll personally owned macOS devices
    - Enroll personally owned Windows devices

Endpoint Protection Checklist

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Set up Microsoft Defender for Business	Use the setup wizard for Microsoft Defender for Business to automatically onboard devices and create your initial policies including antivirus, firewall and EDR as well as set up email notification rules.	Use the setup wizard in Microsoft Defender for Business	10.1, 4.4, 4.5
Configure Attack Surface Reduction (ASR) rules	Enable ASR rules to reduce attack surface on devices.	Attack surface reduction capabilities in Microsoft Defender for Business	
Configure disk encryption (BitLocker) policy	We recommend the silent encryption option using the Endpoint security disk encryption policy.	Encrypt Windows devices with BitLocker in Intune	
Configure compliance policy integration with Defender for Business	Defender can report a machine risk score, which can be leveraged by Intune compliance policies.	Use Microsoft Defender for Endpoint in Microsoft Intune	
Other security policies	Import other recommended security policies (device configuration profiles)	Manage device security with endpoint security policies in Microsoft Intune	

- **Set up Microsoft Defender for Business**: To set up Microsoft Defender for Business, we recommend using the setup wizard provided in the Microsoft 365 Defender admin center. The wizard will guide you through the process of onboarding your devices and creating your initial security policies.
  First, the wizard will assist you to Assign security roles and permissions in Microsoft Defender for Business. Grant your security team access to the Microsoft 365 Defender portal, where your security team will manage the security capabilities of your organization, view alerts, and take any necessary actions on detected threats. Also, don't forget to set up email notifications for your security team to ensure that your team is informed of alerts and vulnerabilities.
  The wizard will also guide you to the process to Onboard devices to Microsoft Defender for Business. If you are already using Intune, you can continue using it to Manage

endpoint security in Microsoft Intune, otherwise you can use the Microsoft 365 Defender portal to onboard devices.
Finally, you can configure your security policies. Defender includes default security policies for next-generation protection and firewall protection that can be applied to your company's devices. These default policies use recommended settings and are designed to provide strong protection for your devices. You also have the option to create your own security policies. See View and edit security policies and settings in Microsoft Defender for Business

- **Configure Attack Surface Reduction (ASR) rules**: There are several features available in the Windows Operating System that are generally not needed by the average information worker. It is a best practice to close doors that you yourself do not intend to walk through, so we have *Attack Surface Reduction rules* to turn off some of these superfluous capabilities. The Threat and Vulnerability Management in Microsoft Defender for Business will recommend which ASR policies to turn on first. See Review remediation actions in the Action center for more information. If you'd like to test the impact of a rule before enabling it, then enable the rule in Audit mode and use the attack surface reduction report to view detections. For more information see Attack surface reduction capabilities in Microsoft Defender for Business.
- **Configure disk encryption policy**: We recommend configuring your disk encryption policy to enable BitLocker in Silent mode. That means the end user is not prompted for any inputs, and the service is configured "silently" in the background. Here are the settings to include in your policy to make this happen:
    - *BitLocker base settings*
        - *Enable full disk encryption for OS and fixed data drives*
        - *Hide prompt about third-party encryption*
            - *Allow standard users to enable encryption during autopilot*
        - *Enable rotation on Azure AD Joined devices*
    - *BitLocker fixed drive settings*
        - *Recovery key file creation: Allowed*
        - *Configure BitLocker recovery package: Password and key*
        - *Require device to back up recovery information to Azure AD*
        - *Recovery password creation: Allowed*
        - *Hide recovery options during BitLocker setup*
        - *Block the use of certificate-based data recovery agent (DRA)*
        - *Block write access to fixed data drives not protected by BitLocker*
    - *BitLocker OS drive settings*
        - *Startup authentication required*
        - *Compatible TPM required*
        - *Compatible startup PIN: Blocked*
        - *Compatible startup key: Blocked*
        - *Compatible startup key and PIN: Blocked*

        - *Disable BitLocker on devices where TPM incompatible*
        - *Recovery key file creation: Allowed*
        - *Configure BitLocker recovery package: Password and key*
        - *Require device to back up recovery information to Azure AD*
        - *Recovery password creation: Allowed*
        - *Hide recovery options during BitLocker setup*
        - *Block the use of certificate-based data recovery agent (DRA)*
- **Configure compliance policy integration with Defender for Business**: Microsoft Defender for Business integrates with Intune compliance policies and reports a "device risk score" that can be leveraged as a bar for device compliance. When you combine this with Conditional Access, it means that devices which are considered "at risk" will lose access to resources until the problem is resolved, and the risk score returns to a clear state. See this article for more information: Use Microsoft Defender for Endpoint in Microsoft Intune.
    - *Recommended Windows policy:*
        - *From **Endpoint Security > Device compliance**, create a new policy for **Windows 10 and later devices***
        - *Configure the Compliance settings for **Microsoft Defender for Endpoint**:*
        - *Set **Require the device risk score…** to **Clear***
        - *Assign to **All users***
- **Other security policies**: You may want to create additional endpoint configuration profiles to establish a secure baseline for your Company owned endpoints. See Overview of using Microsoft 365 Lighthouse baselines to deploy standard tenant configurations and Create a device profile in Microsoft Intune for more information.

Data Protection Checklist

Data protection is crucial in Microsoft 365 Business Premium as it ensures the confidentiality, integrity, and availability of sensitive business information stored within the platform. This includes personal information of employees and customers, financial data, and other critical business records. By implementing robust data protection measures for your customers, you can help safeguard their data against cyber-attacks, unauthorized access, and accidental loss, thus maintaining the trust of their stakeholders and complying with relevant data protection regulations.

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Create and publish Sensitivity labels	Provides the ability to classify documents according to sensitivity, including encryption for confidential information.	Create and publish sensitivity labels	
Create DLP policies	Monitor or block external sharing of sensitive information.	Create a DLP policy from a template	
Create a retention policy for Exchange mailboxes, and other locations as needed	This allows you to retain mailbox data when employees leave the organization.	Get started with data lifecycle management	

- ***Create and publish Sensitivity labels***: Sensitivity labels help end users to classify and protect sensitive or proprietary information, including company files, emails, and sites or groups (such as Teams). A common deployment might contain the following labels:

Label name	***Description***	***Files & emails***	***Groups & sites***
Personal	Non-business data that is intended for personal use only.	No restrictions	Not defined
Public	Business data intended for public consumption.	No restrictions	Not defined
General	Business data that can be shared as needed for business purposes.	No restrictions	Allow external guests and sharing with Anyone
Confidential	Business data that is sensitive and	Apply encryption for Any authenticated user	Allow external guests and sharing

	should be shared discreetly.		with New and Existing guests
Highly Confidential	Business data that should never be shared externally.	Apply encryption for internal users only	Block external guests and sharing

- **Create DLP policies**: Microsoft 365 Business Premium tenants come with a default DLP policy, and you can modify this for customers based on potentially sensitive data discovered in the tenant. For more information see Get started with the default DLP policy.
- **Create retention policies**: We recommend defining at minimum a retention policy for Exchange email. Once you have a mailbox retention policy in place, you can take advantage of Inactive mailboxes, which means that within the retention timeframe, you can still recover or restore the mailboxes of departed employees who have left the organization. You can also deploy retention policies for other locations in Microsoft 365 such as OneDrive and SharePoint. Always be sure that your retention policy parameters follow organizational as well as State and Federal requirements.

Advanced Security and Additional Recommendations

In the previous sections we have covered the essential steps required to quickly secure your customers' Microsoft 365 environment. However, implementing the steps outlined in this section will provide an extra layer of security and help you protect your organization's sensitive information even better. These steps are not mandatory but are highly recommended for optimal security and you should review them for additional considerations that may apply to your customer.

Advanced Identity Protection Checklist

By taking extra steps to implement advanced identity protection features in Azure AD Premium P1 (Included in M365 Business Premium), partners can help safeguard their customer's business and maintain the trust of their stakeholders by providing extra layers of security to protect identities and sensitive information from malicious actors.

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Use FIDO2 keys for passwordless authentication	Consider using strong authentication for global admins as well as access to highly sensitive apps and data.	Enable passwordless security key sign-in	6.6, 12.7, 16.11
Secure MFA and self-service password reset registration	Restrict when and how users register for Azure AD multifactor Authentication and self-service password reset with a Conditional Access policy	Common Conditional Access policy: Securing security info registration	6.6
Manage customer consent to applications & permissions requests	Reduce the risk of threat actors using malicious applications to trick users into granting them access to your customers' data by managing user consent requests.	Configure how users consent to applications	3.3
Configure granular control of Azure AD external identities	Manage how your customer collaborates with other Azure AD tenants with B2B direct connect.	Overview: Cross-tenant access with Azure AD External Identities	6.3

- ***Use FIDO2 keys for passwordless authentication:*** Enable passwordless security key sign-in by using a FIDO2 security key. This provides more security for your organization

and is also phishing resistant. With this method, users can authenticate to web-based applications using their Azure AD account without the need for a username or password.

- **Secure MFA and self-service password reset registration** by only allowing users to register for MFA and configure self-service password reset from trusted locations. You can provide your customers a Temporary Access Pass if they need to register from a different location after verifying their identity.
- **Manage customer consent to applications & permissions requests -** By default, all users are allowed to consent to applications for permissions that don't require administrator consent. You can provide additional security value by managing this for your customer and routing user consent requests to you for approval. See Configure the admin consent workflow for more information.
- **Configure granular control of Azure AD external identities** - Control how external Azure AD organizations collaborate with your customer. For example, your customer may want to require MFA for guest access to their tenant or specify who can invite guests to Teams.

Advanced Email & Apps Protection

Phishing and malware attacks are among the most common threats faced by SMB organizations, and they can result in data breaches and significant financial losses. Configuration is key to using Microsoft 365 Defender for Office 365 successfully. False positives are disruptive to your customer's business and a top cause for concern with email security. Implementing advanced phishing and malware protection in Defender for Office 365 P1 (Included in M365 Business Premium) is crucial for ensuring the security of a customer's sensitive information and digital assets. Defender for Office 365 P1 provides advanced phishing and malware protection features, such as threat intelligence, advanced threat protection, and email security, to help prevent these types of attacks.

Checklist item	***Description***	***Learn more***	***CIS Ref.***
Configure defense in depth for email security	Review the latest guidance for Microsoft 365 Defender for Office 365 paying special attention if you're using any kind of 3rd party filtering service.	Getting the best security value from Microsoft Defender for Office 365 when you have third party email filtering	
Configure skip listing if using a third-party email filtering device or service	Customers will have erroneous SPAM and Phishing detections if using	Manage mail flow using a third-party cloud service with Exchange Online	

	3rd party filtering without skip listing or bypass.		
Block all executable email attachments	Enforce a strict policy that prohibits the receipt and execution of email attachments with executable file extensions to safeguard against potential malicious software and viruses that could compromise security.	Use mail flow rules to block messages with executable attachments in Exchange Online	
Customize quarantine permissions and policies	Allow users to request release of lower risk quarantined messages.	Creating Custom quarantine policies with Request release flow	
Customize Defender for Office 365 Anti-phishing Policies	Configure additional impersonation protection for email addresses that might be impersonated by attackers, such as top-level executives, board members, and other people in key roles.	Impersonation settings in anti-phishing policies in Microsoft Defender for Office 365	
Extend DMARC protection to domains not used for email	Attackers may leverage seldom used domains in your customer tenant if left unprotected, including the onmicrosoft.com domain.	How to enable DMARC Reporting for Microsoft Online Email Routing Address (MOERA) and parked Domains	
Configure additional email encryption	Microsoft 365 delivers multiple encryption options to help you meet your customers' needs for email security.	Email encryption	
Restrict external domains that can send email messages to Teams channels	Specify the domains that can send email to Teams channels.	Reduce the attack surface for Microsoft Teams	
Disable 3rd party & custom apps in Teams	Applications are a very useful part of Microsoft Teams; however, we recommend only enabling a	Disabling Third-party & custom apps	

	specific list of allowed apps rather than allowing all apps by default.		
Customize Teams meeting settings	Consider controls on the ability of guests to request access to control presenter's screens and how to handle anonymous participants.	Reduce the attack surface for Microsoft Teams	
Set up digest notifications			

- **Configure skip listing if using a third-party email filtering device or service** – Microsoft Defender for Office 365, included in M365 Business Premium, has excellent Phish and SPAM protection and we recommend configuring your MX records to point to Office 365 so the algorithms work optimally. If a 3rd party receives mail before Office 365 and/or modifies the content of the inbound email it will cause problems with false positives, false negatives, and email authentication errors. If you're using a 3rd party filter that scans email before M365 then you must either configure skip listing (recommended) or bypass SPAM filtering. See Enhanced Filtering for Connectors in Exchange Online for more information.
- **Block all executable email attachments** - If you enabled the Standard or Strict pre-set email policy it will have enabled the Common Attachments filter to block several executable attachment types. Many small and medium businesses to do need to send executable attachments of any type via email. You can enhance protection to block all executable attachments via transport rules. See Use mail flow rules to block messages with executable attachments in Exchange Online and Configure anti-malware policies in EOP.
- **Customize quarantine permissions and policies:** You can enable your customers to triage false positives for specific verdicts (bulk, spam, phish, high confidence phish, or malware) and request release of those items. For more information see this.
- **Customize Defender for Office 365 Anti-phishing Policies:** Enabling Standard or Strict pre-set policies enables protection from phishing email threats in real-time by using intelligent systems that inspect attachments and links for malicious content. Safety tips can inform users when receiving email from a sender for the first time or when the sender does not pass email authentication, which are common in phishing scenarios. You may also want to configure policies to help prevent impersonation of key individuals, also known as spear-phishing, or impersonation of domains that belong to key suppliers and partners. For more information see Anti-phishing policies in Microsoft 365 and Configure anti-phishing policies in Microsoft Defender for Office 365.

- **Extend DMARC protection to other domains not used for email:** Best practice for domain email security protection is to enable DMARC for all domains even if they parked or not currently used for email.
- **Configure additional email encryption:** If you configure sensitivity labels for your customer they will be able to send encrypted email. Your customer may have additional requirements for email encryption such as S/MIME.
- **Restrict external domains that can send email messages to Teams channels:** By default, any channel in a team can receive email from any sender. You may limit the domains allowed to send to Teams channels. For more information see Manage and monitor Teams.
- **Disable 3rd party & custom apps in Teams:** You can use app permission policies to control the apps that are available to your customers. For more information see Use app permission policies to control user access to apps.