Information Protection for Office 365

Capabilities for enterprise organizations to protect corporate assets

Empower users and enable collaboration while protecting your corporate assets

Microsoft provides the most complete set of capabilities to protect your corporate assets. This model helps organizations take a methodical approach to information protection.

A	Establish information protection priorities	The first step of protecting information is identifying what to protect. Develop clear, simple, and well-communicated guidelines to identify, protect, and monitor the most important data assets anywhere they reside.
B	Set organization minimum standards	Establish minimum standards for devices and accounts accessing any data assets belonging to the organization. This can include device configuration compliance, device wipe, enterprise data protection capabilities, user authentication strength, and user identity.
C	Find and protect sensitive data	Identify and classify sensitive assets. Define the technologies and processes to automatically apply security controls.
D	Protect high value assets (HVAs)	Establish the strongest protection for assets that have a disproportionate impact on the organizations mission or profitability. Perform stringent analysis of HVA lifecycle and security dependencies, establish appropriate security controls and conditions.

Many organizations classify data sensitivity by level

Three levels is a good starting point if your organization doesn't already have defined standards.

Mapping service capabilities to data sensitivity levels

Some information protection capabilities apply broadly and can be used to set a higher minimum standard for protecting all data. Other capabilities can be targeted to specific data sets for protecting sensitive data and HVAs.

Using Office 365 Secure Score

You can use Secure Score to learn more about capabilities recommended for your Office 365 environment.

Introducing the Office 365 Secure Score

Example

Level 1		Level 2	Level 3
Data is encrypted and available only to authenticated users This level of protection is provided by default for data stored in Office 365 services. Data is encrypted while it resides in the service and in transit between the service and client devices. For some organizations, this level of protection meets the minimum standard.	Additional data and identity protection applied broadly Capabilities such as multi-factor authentication (MFA), mobile device management, Exchange Online Advanced Threat Protection, and Microsoft Cloud App Security increase protection and substantially raise the minimum standard for protecting devices, identities, and data. Many organizations will require one or more of these features to meet a minimum standard.	Sophisticated protection applied to specific data sets Capabilities such as Azure Information Protection and Office 365 Data Loss Prevention (DLP) can be used to enforce permissions and other policies that protect sensitive data. You can also implement Azure AD Identity Protection policies to protect identities with access to sensitive data.	Strongest protection and separation You can achieve the highest levels of protection with encryption key solutions, Advanced Data Governance, and more protective policies using Azure AD Identity Protection. Also consider using SQL Server Always Encrypted for partner solutions that interact with Office 365. Not all organizations require the highest level of protection.

Capability grid

Use this grid of information protection capabilities to plan your strategy for protecting data. Capabilities are categorized by protect scenario (row). Capabilities increase in control and protection as you move to the right.

Start here → Capabilities increase in control and protection as you move to the right. → More control & protection

Product key

- All Office 365 Enterprise plans
- Office 365 Enterprise E3 Plan
- Office 365 Enterprise E5 Plan or standalone add-on
- Windows 10
- Enterprise Mobility + Security (EMS) E3 Plan
- Enterprise Mobility + Security (EMS) E5 Plan

EMS plans include Azure AD Premium, Intune, and Azure Rights Management

Test lab environments

You can create your own dev/test environment with Office 365 Enterprise E5, EMS, and Azure trial subscriptions.

Look for the test lab guide (TLG) icon in the grid for capabilities that can be tested within these environments. Here's the current set:

- Base configuration dev/test environment — Simplified intranet in Azure IaaS to simulate an enterprise configuration
- Office 365 dev/test environment — Create and Office 365 E5 trial subscription
- Multi-factor authentication for your Office 365 dev/test environment — Demonstrate MFA with a verification code sent to your smart phone
- Advanced Security Management for your Office 365 dev/test environment — Create policies and monitor your environment
- Advanced Threat Protection for your Office 365 dev/test environment — Keep malware out of your email
- Advanced eDiscovery for your Office 365 dev/test environment — Add example data and demonstrate these capabilities
- Office 365 and EMS dev/test environment — Add an EMS trial subscription to your Office 365 trial environment
- MAM policies for your Office 365 and EMS dev/test environment — Create MAM policies for iOS and Android devices
- Enroll iOS and Android devices in your Office 365 and EMS dev/test environment — Enroll and manage these devices remotely
- Data classification and labeling in the Office 365 dev/test environment — Classify files with the Azure Information Protection client

1 Simplify and protect access

Disable identities in Azure Active Directory that are not active	Enable self-service password reset in Azure Active Directory	Use Group-based Licensing to assign licenses to users	Configure Multi-Factor Authentication (MFA)	Configure single sign-on to other SaaS apps in your environment	Use Intune to protect data on mobile devices, desktop computers, and in applications	Configure Azure AD risk-based conditional access for greater protection	Configure Azure AD conditional access to configure rules for access to applications	Enable Windows Hello for Business on all Windows 10 PCs	Use device health attestation features with Windows 10 devices	Enable Azure AD Identity Protection Policies for your users	Migrate your external accounts to Azure AD B2B collaboration
Reduce the number of active identities to reduce licensing costs and the identity attack surface. Periodically check for inactive users and disable accounts that are not active. For example, you can identify Exchange Online mailboxes that have not been accessed for at least the last 30 days and then disable these accounts in Azure Active Directory. Manage inactive mailboxes in Exchange Online Blog: Office 365 – How to Handle Departed Users	Deploy Password Management and train users. Azure Active Directory Premium password management includes on-premises write-back. Enable users to reset their Azure AD passwords Whitepaper: Microsoft Password Guidance	Define a "license template" and assign it to a security group in Azure AD. Azure AD will automatically assign and remove licenses as users join and leave the group. Group-based licensing basics in Azure Active Directory Big Updates to Office 365 Identity (licensing and how to try group-based licensing)	Add a second-layer of security to user sign-ins and transactions by using multi-factor authentication (MFA). Multi-Factor Authentication documentation Compare MFA features: Office 365 vs. Azure AD Premium	Many SaaS apps are pre-integrated with Azure Active Directory. Configure your environment to use single-sign on with these apps. Office 365 plans include up to 10 SaaS apps per user. Azure Active Directory Premium is not limited. Configure your favorite SaaS cloud application on Azure Active Directory for single sign-on and easier user account management	Ensure device policy compliance using configurable conditional access policies for Office 365 to apply to Exchange Online, SharePoint Online, OneDrive for Business, and Skype for Business. Configure secure access with certificates, Wi-Fi, VPN and email profiles. Microsoft Intune Overview	Risk level is calculated for every user and every sign-in attempt. Risk-based conditional access policies can be applied to all apps protected by Azure Active Directory. Administrators can set policies that trigger specific controls based on various levels of risk. Actions can include block, enforce MFA, or password reset for the user. Azure Active Directory risk events	Create access policies that evaluate the context of a user's login to make real-time decisions about which applications they should be allowed to access. For example you can require multi-factor authentication per application or only when users are not at work. Or you can block access to specific applications when users are not at work. Working with conditional access	Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. Windows Hello for Business	Configure a MDM product to allow or deny access to secure resources based on device health attestation. The Health Attestation Service is a trusted cloud service operated by Microsoft that reports what security features are enabled on the device. Control the health of Windows 10-based devices	Enable Identity Protection (even in trial mode) to see the user and sign in risk of logins. Even without enabling policies, you will gain insights from the signals. After you have enabled it for some time, we recommend you activate Identity Protection policies. For example, require MFA on sign in when the risk of a login is medium or higher. Or, reset a user's password if the user's risk is marked as high. Azure Active Directory Identity Protection	External accounts on premises are a threat that you can mitigate by moving the accounts to Azure AD B2B collaboration. Azure AD B2B Collaboration enables secure collaborate between business-to-business partners. Any accounts that are needed for SaaS application access or SharePoint Online collaboration can be moved to Azure AD B2B. Azure Active Directory B2B collaboration

2 Allow collaboration and prevent leaks

Configure permissions for SharePoint and OneDrive for Business libraries and documents	Configure external sharing policies to support your collaboration and file protection objectives	Configure device access policies for SharePoint Online and OneDrive for Business	Use labels to implement classification-based protection	Configure Data Loss Prevention (DLP) across Office 365 services and applications	Use Intune to manage applications on mobile devices	Use Windows 10 BitLocker and Windows Information Protection (WIP)	Use the Intune App Wrapping Tool to apply policies to line-of-business applications	Configure Office 365 service-level encryption with Customer Key (coming soon)	For trade-secret or classified files, implement BYOK or HYOK encryption and protection	Use Azure Key Vault for line of business solutions that interact with Office 365	Use SQL Server Always Encrypted for partner solutions using a SQL database
Use permissions in SharePoint to provide or restrict user access to a site or its contents. SharePoint sites come with several default groups that you can use to manage permissions. These are not related to Office 365 groups. Encourage users to apply permissions to documents in their OneDrive for Business libraries. Understanding permission levels in SharePoint Understanding SharePoint groups	An external user is someone outside of your organization who is invited to access your SharePoint Online sites and documents but does not have a license for your SharePoint Online or Microsoft Office 365 subscription. External sharing policies apply to both SharePoint Online and OneDrive for Business. Manage external sharing for your SharePoint Online environment Share sites or documents with people outside your organization	Conditional access and network location policies in SharePoint admin let you determine whether access to data is limited to a browser-only experience or blocked. Control access from unmanaged devices	Use Office 365 labels and Azure Information Protection labels to classify and protect your data. Classification can be fully automatic, user-driven, or both. Once data is classified and labeled, protection can be applied automatically on that basis. File Protection Solutions in Office 365 (coming soon) What is Azure Information Protection? Blog	Enforce policies and analyze how users adhere. Use built-in templates and customizable policies. Policies include transport rules, actions, and exceptions that you create. Inform mail senders that they are about to violate a policy. Set up policies for SharePoint Online and OneDrive for Business that automatically apply to Word, Excel, and PowerPoint 2016 applications. Overview of data loss prevention policies Data loss prevention in Exchange Online	**Manage applications on mobile devices regardless of whether the devices are enrolled for mobile device management.** Deploy apps, including LOB apps. Restrict actions like copy, cut, paste, and save as, to only apps managed by Intune. Enable secure web browsing using the Intune Managed Browser App. Enforce PIN and encryption requirements, offline access time, and other policy settings. Configure and deploy mobile application management policies Intune application partners	BitLocker Drive Encryption protects data when devices are lost or stolen. WIP protects business content on devices with file level encryption that helps prevent accidental data leaks to non-business documents, unauthorized apps, and unapproved locations. Bitlocker overview Protect your enterprise data using Windows Information Protection (WIP)	Use this tool to manage your own applications on mobile devices with the Mobile Application Management policies. Configure and deploy mobile application management policies in the Microsoft Intune console	To help customers meet their compliance requirements, customers have the option to manage and control their own encryption keys for Office 365. Encrypting at the service level offers an added layer of protection for files in SharePoint Online and OneDrive for Business and for Exchange Online mailboxes. Customer Key is applied tenant-wide for all files in SharePoint Online and OneDrive for Business.	You can protect a sub-set of your files at a very high level by using Azure Information Protection together with a Bring Your Own Key (BYOK) or Hold Your Own Key (HYOK) encryption solution. File Protection Solutions in Office 365 (coming soon)	Encrypt keys and passwords using keys stored in hardware security modules (HSMs). Import or generate your keys in HSMs that are validated to FIPS 140-2 Level 2 standards—so that your keys stay within the HSM boundary. Microsoft does not see or extract your keys. Monitor and audit key use. Use Azure Key Vault for workloads both on premises and cloud hosted. Azure Key Vault	Protect sensitive data, such as credit card numbers or identification numbers, stored in Azure SQL Database or SQL Server databases. Clients encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine (SQL Database or SQL Server). This provides separation between those who own the data (and can view it) and those who manage the data (but should have no access). Always Encrypted (Database Engine) Blog: SQL Server 2016 includes new advances that keep data safer

3 Stop external threats

Add Exchange Online Advanced Threat Protection for your organization	Use Office 365 Advanced Security Management or Microsoft Cloud App Security	Use Microsoft Edge for browsing	Keep Windows Defender enabled on Windows 10 computers	Use Device Guard to ensure only trusted software is run on Windows 10 Enterprise	Use Windows Defender Advanced Threat Protection (ATP) to protect your network	Implement Azure AD Connect Health	Implement Advanced Threat Analytics (ATA) on premises to monitor your network.	Use Intune to keep client software up to date
Protect your environment against advanced threats, including malicious links, unsafe attachments, and malware campaigns. Gain insights with reporting and URL trace capabilities. Configure settings for your organization's objectives. Exchange Online Advanced Threat Protection (Features) Service Description (TechNet) How it works (TechNet)	Use Office 365 Advanced Security Management to evaluate risk, to alert on suspicious activity, and to automatically take action. Requires Office 365 E5 plan. Or, use Microsoft Cloud App Security to obtain deeper visibility even after access is granted, comprehensive controls, and improved protection for all your cloud applications, including Office 365. Requires EMS E5 plan. Overview of Advanced Security Management in Office 365 Microsoft Cloud App Security	**Use Microsoft Edge when browsing the Internet. It helps block known support scam sites using Windows Defender SmartScreen. Microsoft Edge also helps stop pop-up dialogue loops used by these sites.** Microsoft Edge Deployment Guide for IT Pros (TechNet) Blog: Evolving Microsoft SmartScreen to protect you from drive-by attacks Blog: Mitigating arbitrary native code execution in Microsoft Edge	Ask Cortana or type "Windows Defender" in the task bar search box. If you see a "PC status: Protected" message, you're good to go. If Windows Defender is turned off, uninstall other antivirus solutions and check again. Windows 10 will enable Windows Defender automatically. Windows Defender in Windows 10 (TechNet) Keep your PC safe with Windows Defender	Device Guard is a combination of enterprise-related hardware and software security features that, when configured together, will lock a device down so that it can only run trusted applications. Device Guard prevents tampering by users or malware that are running with administrative privileges. Device Guard overview (TechNet) Blog: What is Windows 10 Device Guard?	Use Windows Defender ATP service to help detect, investigate, and respond to advanced and targeted attacks on your networks. Windows Defender ATP User Guide (TechNet)	Monitor and gain insights into your on-premises identity infrastructure with the Azure AD Connect tool used with Office 365. Monitor your on-premises identity infrastructure and synchronization services in the cloud	Identify suspicious user and device activity. Build an Organizational Security Graph and detect advanced attacks in near real time. Microsoft Advanced Threat Analytics (TechNet) Blog: Microsoft Advanced Threat Analytics	Keep managed computers secure by ensuring the latest patches and software updates are quickly installed. Keep Windows PCs up to date with software updates in Microsoft Intune

4 Stay compliant

Use Message records management (MRM) in Exchange Online to manage email lifecycle and reduce legal risk	Use retention policies in SharePoint and OneDrive for sites and documents	Apply security restrictions in Exchange Online to protect messages	Use Office 365 Advanced Data Governance to classify, retain, and take action on your data	Conduct eDiscovery in Office 365	Use Advanced eDiscovery to speed up the document review process	Use data spillage features in Office 365	Audit user and administrator actions in Office 365 for compliance	Retain inactive mailboxes in Exchange Online
Keep messages needed to comply with company policy, government regulations, or legal needs, and remove content that has no legal or business value. Message records management	Compliance officers can apply policies that define when sites or documents are retained, expire, close, or are deleted. Retention in the Office 365 Compliance Center	Require encryption, digitally sign messages, and monitor or restrict forwarding. Create partner connectors to apply a set of restrictions to messages exchanged with a partner organization or service provider. Encryption in Office 365 Set up connectors for secure mail flow with a partner organization Set-RemoteDomain	Meet your organizational compliance requirements by leveraging machine assisted insights to help you import, find, classify, set policies, and take action on the data that is most important to your organization. High-value content across Exchange Online, SharePoint Online, OneDrive for Business, and Skype for Business is efficiently protected for as long as you need it to be. Blog: New Office 365 capabilities to manage security and compliance risk Capabilities vary by plan	Identify, preserve, search, analyze, and export email, documents, messages, and other types of content to investigate and meet legal obligations. Compliance Search in the Office 365 Compliance Center	Perform analysis on discovered data by applying the text analytics, machine learning, and Relevance/predictive coding capabilities of Advanced eDiscovery. These capabilities help organizations quickly reduce the data set of items that are most likely relevant to a specific case. Office 365 Advanced eDiscovery	Search and remove leaked data in mailboxes, SharePoint Online sites, and OneDrive for Business. eDiscovery in Office 365	Use the Office 365 Security & Compliance Center to search the unified audit log to view user and administrator activity in your Office 365 organization. Search the audit log in the Office 365 Security & Compliance Center	Preserve former employees' email after they leave your organization. A mailbox becomes inactive when a Litigation Hold or an In-Place Hold is placed on the mailbox before the corresponding Office 365 user account is deleted. The contents of an inactive mailbox are preserved for the duration of the hold that was placed on the mailbox before it was made inactive. Manage inactive mailboxes in Exchange Online

5 Secure admin access

Use dedicated administrative workstations and accounts for managing cloud services	Secure privileged access	Validate and monitor your security configuration	Create pure online administration accounts	Separate duties of administrators by role — SharePoint Online, Exchange Online, and Skype for Business Online	Use Azure AD Privileged Identity Management to control and monitor your privileged identities	Review the Office 365 administrator audit logs	Use Exchange Online auditing capabilities to search administrator audit logs	Use Customer Lockbox for Office 365 to require mandatory approval for service engineer work
Use dedicated administrative accounts for administrators. Use a naming convention to make them discoverable. Protect administrative identities and credentials by using workstations that are hardened for this purpose. Securing privileged access	Take a prescribed approach to securing privileged access. Cyber-attackers are targeting these accounts and other elements of privileged access to rapidly gain access to targeted data and systems using credential theft attacks like Pass-the-Hash and Pass-the-Ticket Securing Privileged Access	Validate the configuration of your Office 365 tenant against your organization's policy. Regularly monitor critical settings for unauthorized changes. Focus first on administrative control of the tenant and controls that allow broad access to data in the Office 365 tenant.	In case of a problem with federated authentication, create online administrator accounts that can be used in scenarios where federated access is not possible.	Designate several admins who serve different functions. This segments permissions to ensure that a single administrator doesn't have greater access than necessary. Assigning admin roles in Office 365	Manage, control, and monitor your privileged identities and their access to resources in Azure AD and in other Microsoft services such as Office 365 or Microsoft Intune. Implement just in time elevation for privileged actions. Azure AD Privileged Identity Management	Track the cause of unexpected behavior, identify a malicious administrator, investigate leaks, or verify that compliance requirements are being met. View the administrator audit log	Find out which accounts were used for administrative actions that cause unexpected behavior or to verify that compliance requirements are met. Exchange auditing reports	Customer Lockbox requires approval from you before a service engineer can access your SharePoint Online, OneDrive for Business, or Exchange Online information. It gives you explicit control over access to your content. In a rare event where you need Microsoft support to resolve an issue, customer lockbox lets you control whether an engineer can access your data and for how long. Office 365 Customer Lockbox Requests

March 2017

Microsoft