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.

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, and Exchange Online Advanced Threat Protection increase protection and substantially raise the minimum standard for protecting devices, accounts, 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 Rights Management (RMS) and Data Loss Protection (DLP) across Office 365 can be used to enforce permissions and other policies that protect sensitive data.	Strongest protection and separation You can achieve the highest levels of protection with capabilities such as Customer Lockbox for Office 365, eDiscovery features in Office 365, and SQL Server Always Encrypted for partner solutions that interact with Office 365. Use auditing features to ensure compliance to policies and prescribed configurations. 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)
  - Azure AD Premium
  - Intune
  - Azure Rights Management

1 Simplify and protect access

Disable identities in Azure Active Directory that are not active	Enable self-service password reset in Azure Active Directory	Configure Multi-Factor Authentication (MFA)	Use MDM features in Office 365 to protect data on mobile devices	Use Intune to protect data on mobile devices, desktop computers, and in applications	Enable Microsoft Passport for Work	Configure single sign-on to other SaaS apps in your environment	Configure Azure AD conditional access to configure rules for access to applications	Use device health attestation features with Windows 10 devices
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	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	Use the Mobile Device Management (MDM) features in Office 365 to allow access to corporate email and documents only from devices that are managed and compliant. Wipe company data from a device without affecting personal data. Basic conditional access controls apply to Exchange Online and SharePoint Online. Manage mobile devices in Office 365	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	Use Passport for Work to authenticate identities without passwords. Passport can provide private/public key or certificate-based authentication. Manage identity verification using Microsoft Passport Authenticating identities without passwords through Microsoft Passport	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	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	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

2 Allow collaboration and prevent leaks

Configure Office encryption settings	Use Azure Rights Management (RMS) with Office 365 to protect data from unauthorized access	Train users to protect sensitive documents by using the RMS sharing application	Configure Data Loss Prevention (DLP) across Office 365 services and applications	Control e-mail attachment handling in Outlook Web App	Use Intune to manage applications on mobile devices	Use the Intune App Wrapping Tool to apply policies to line-of-business applications	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
Control the way data is encrypted when Office applications are used: Access, Excel, OneNote, PowerPoint, Project, and Word. Encryption in Office 365	Apply encryption, identity, and authorization policies. Configure templates to make it easy for users to apply policies. Track and revoke access to documents. Azure Rights Management Activate Rights Management (RMS) in the Office 365 admin center Blog: Collaborate confidently using Rights Management	Through the web, document owners can track activities such as recipients who open files, unauthorized users who are denied access, and the latest state of files. You can also view the geographical locations where files were accessed, and revoke access to a shared file. Track and revoke your documents when you use the RMS sharing application Blog: Welcome to Azure RMS Document Tracking	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	Set policies that determine how attachments are handled. For example, restrict access to documents from public networks. Or, block attachments from being synchronized to mobile devices. Public attachment handling 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	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	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	Start using Office 365 Advanced Security Management	Use Azure AD access and usage reports and Audit Events	Use Exchange Online auditing capabilities	Audit the Azure RMS logs to identify potential leaks or account theft	Ensure only trusted software is run on Windows 10 Enterprise	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)	Set up policies to alert you about anomalous and suspicious activity. Admins can disable an account directly from an alert, or you can configure alerts to automatically disable an account. Built-in alerts scan user activities and evaluate risk against over 70 different indicators, including sign-in failures, administrator activity and inactive accounts. Overview of Advanced Security Management in Office 365 Blog and video	Audit all account actions and use Azure AD reports to identify potential fraudulent activities. Use Azure AD Audit Events to identify privileged actions. Automate monitoring by consuming the security audit feed. Office 365 includes basic reports. Azure Active Directory Premium includes advanced reports. View your access and usage reports Azure Active Directory Audit Report Events	Audit administrator, user, application, and external user access. Determine who has accessed mailboxes and what they have done. Detect non-owner mailbox access, privileged Administrator changes, and regularly review configuration changes. Exchange auditing reports	Use RMS logs as a definitive source of information for forensic analysis when you protect your data by using RMS. For example, identify if an account is used to access data from two different geographic locations within the same timeframe. Or, detect a spike in the use of RMS-protected data at an unexpected time. Logging and Analyzing Azure Rights Management Usage	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?	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

Monitor and manage external sharing in Office 365	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	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
Monitor or restrict sharing in SharePoint, OneDrive for Business, and Skype for Business. Setup External Sharing Policies with partners. Manage external sharing for your SharePoint Online environment	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	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 accounts	Secure privileged access	Use dedicated workstations for administration of cloud services	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. 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	Protect administrative identities and credentials by using workstations that are hardened for this purpose. Securing privileged access	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

Microsoft