Trusted Information Protection

On-premises. On devices. In the cloud. At all times.

Microsoft

> We must build trust directly into our technology. We must infuse technology with protections for privacy, transparency, and security.

Satya Nadella
CEO, Microsoft

Table of contents

Building trust

Today, customers, employees, and communities trust that organizations will safeguard their sensitive information. Compliance standards such as the EU's General Data Protection Regulation (GDPR) and ISO/IEC 27000 family even require information protection and proper data management. Thus, the question is no longer whether Information Protection needs to happen, but what is the best way to get it done?

Using capabilities built into Microsoft Office 365 and Windows 10, plus solutions provided in Microsoft Enterprise Mobility + Security , you can manage and secure your organization's digital information in the cloud, across devices, and on-premises, just as you manage and secure other critical entities such as identities, devices, applications, and networks. You can detect sensitive information wherever it resides, protect and manage it throughout its lifecycle, and respond to incidents when they arise.

Microsoft Information Protection

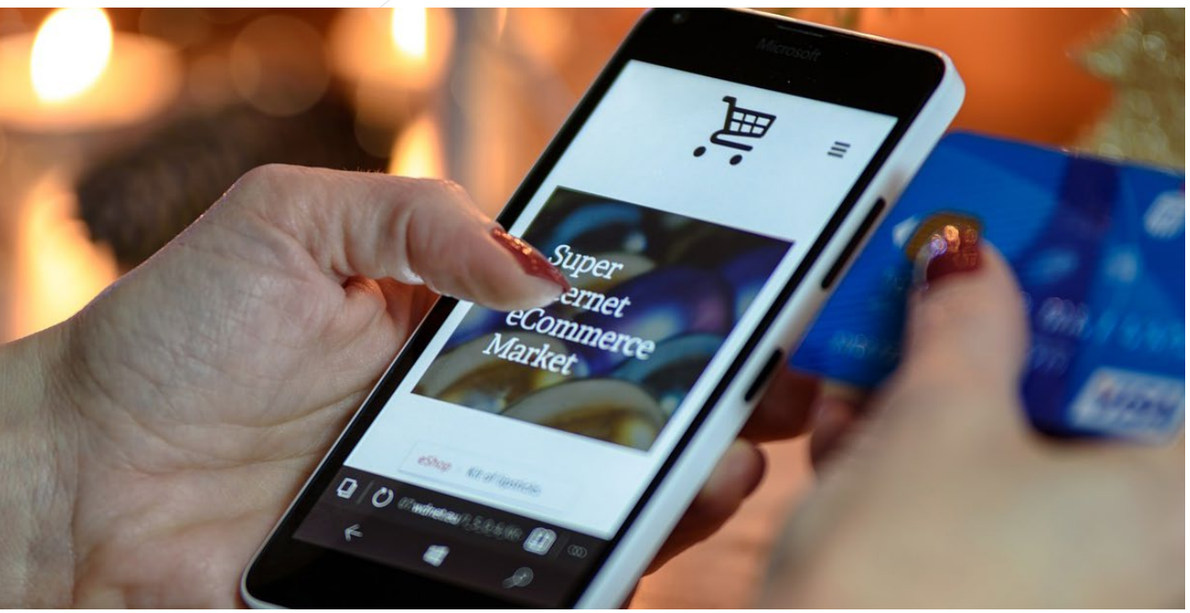
- **Protects information from leakage, blocking undesired actions and access by untrusted and/or malicious actors.**
- **Lets you "know" when information is accessed by whom and what they did.**
- **Enables users to be more productive and collaborate confidently, since they know where their documents are and how they are being used.**
- **Balances user productivity with security needs, including the flexibility to automatically apply protection or to guide users to apply the appropriate protection themselves.**
- **Gives users control of their shared files and informs them when something is wrong.**
- **Keeps management aware of information, enabling it to discover patterns and understand how information flows.**

Together, these Information Protection capabilities combine with threat protection, identity and access management, and security management to help you create a comprehensive cyber resilience strategy to secure corporate data and manage risk.

With our approach to Information Protection (refer to the list above), you can secure your sensitive information, maintain compliance with key information security standards, and decrease risk.

Our capabilities let you **discover** information as it appears, no matter where it is created or lives. You can **classify** it into distinct categories and apply sensitivity labels that persist with a document so that custom controls can be applied, such as enforcing policies and restricting access. You can **protect** it appropriately, applying policy-based actions to sensitive information. You can **monitor** the information properly to identify potential misuse of sensitive data, as well as to investigate issues and respond appropriately.

In the following pages, we provide you with an overview of capabilities you can apply to your Information Protection strategy, so you can be confident your most sensitive and confidential information is protected.



The Information Protection lifecycle

We use a four-stage lifecycle approach to Information Protection in which you discover, classify, protect, and monitor sensitive information. We provide capabilities that you can use in each of the stages (see table on pages 34–36 of this paper).

Our Information Protection capabilities are closely aligned functionally and architecturally. They share common features and implementations, use the same mechanisms, are configured in a common way, and work together across varying scenarios. Our capabilities provide what you need to build a trusted environment by following all four stages of the Information Protection lifecycle.

Journey through the Information Protection lifecycle

Here is a hypothetical example of how Information Protection can work.

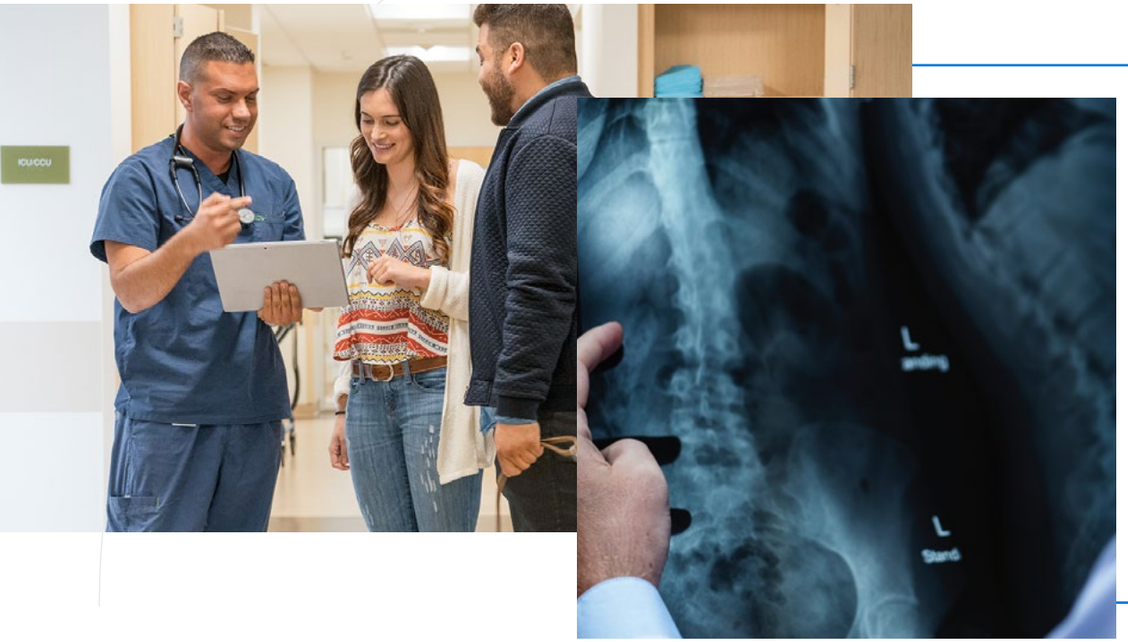
Jan works in the human resources department of a global manufacturing company with offices in the U.S., Europe, and Asia. Within Microsoft Office 365, Jan creates an Excel file that has a column for worldwide employee phone numbers. How can this information be protected appropriately, and how can the organization maintain compliance with privacy standards such as GDPR?

Discover: If the IT security administrator for Azure Information Protection (AIP) has configured rules to detect sensitive data (e.g., phone numbers and credit card numbers), AIP automatic classification will recognize that the file contains a phone number. AIP knows there are policies regarding the use of phone numbers requiring them to be kept confidential.

Classify: AIP applies a sensitivity label to classify the file based on the policy. In this case, the Excel file will be classified as confidential. If Jan's spreadsheet moves to different people, devices, and locations, its classification will travel with it, ensuring that proper protection is applied.

Protect: The organization uses AIP to automatically apply protection to the confidential spreadsheet. Access rights will be applied to limit access to only authorized recipients. Unauthorized users will not be able to open or view the file.

Monitor: Users and administrators can use a document tracking site to monitor who is accessing the Excel file and when. If they suspect misuse, they can revoke access to it. Whether the file stays in one place or moves around, AIP can monitor file access, sharing, and usage, and can respond quickly to potential abuse or threats. Response could be in the form of real-time alerts, email messages, or a reporting dashboard.



Discover

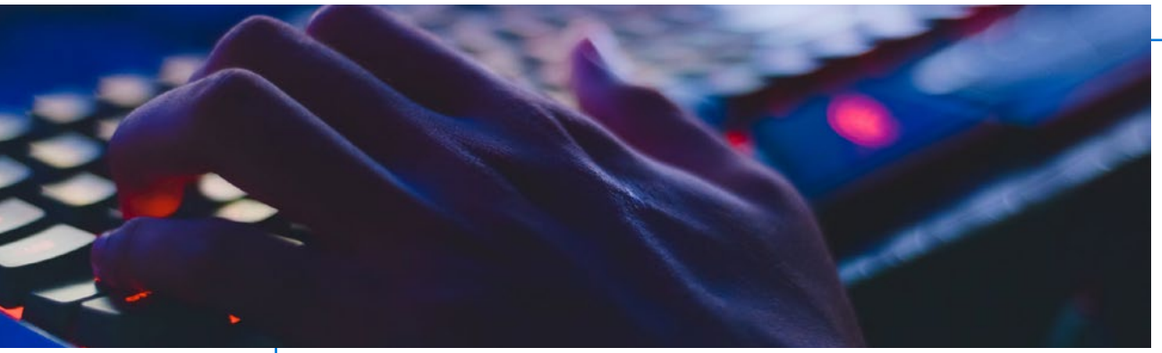
To protect sensitive information, you need to know when and where it is created—in an email or on a server, in on-premises file shares or datacenters, on individual devices, across cloud services, or within software as a service (SaaS) applications.

Azure Information Protection (AIP), Microsoft Cloud App Security (MCAS), and Office 365 data loss prevention (DLP) use discovery capabilities to find sensitive information. For example, AIP can discover sensitive data in on-premises file servers, and MCAS can discover sensitive data in third-party SaaS services. Office 365 DLP can be used to discover sensitive data within your Office 365 environment (e.g., Exchange Online, OneDrive for Business, and SharePoint Online).

Classify

Once you have discovered information, classify it into distinct categories reflecting its sensitivity using a customized classification and labeling template based on your needs. Even if the information is considered sensitive, there are typically different levels of sensitivity, and you may want different actions to be applied based on the level.

Office 365 Advanced Data Governance enables you to classify and automatically label sensitive files—in particular for the purpose of applying data retention and deletion policies across your Office 365 environment. AIP enables you to automatically classify and label sensitive files beyond Office 365 and even on-premises. AIP also works with MCAS to enable you to classify and label sensitive documents that live in third-party SaaS services.



For example, you can use AIP to classify documents and email messages. The classification results in a label being applied to the data. The label enables custom controls to be applied, such as for policy enforcement and data governance. The label is also represented as metadata written into the file that travels with it as it moves.

When you do this, the label persists with the file, regardless of where the information is stored or with whom it is shared. Metadata is added to files and email headers in clear text. The clear text ensures other services, such as data loss prevention solutions, can identify the classification and take appropriate action.

Once the information has been stamped with a sensitivity label, your company can automatically apply the desired policy to the document.

Based on the policy defined by your organization, any number of protective actions can be taken, such as applying encryption, restricting access rights, applying visual markings or a watermark, executing a retention or deletion policy, or performing a DLP action such as blocking file sharing.

A critical step in the overall information protection strategy is defining the policies and actions to take, while also ensuring users can perform their jobs.

We help customers define policies and roles for governing information. For example, we provide a default recommended set of classification and sensitivity labels to apply to documents.

Protection is built-in

We have built data encryption into our services (Office 365) and platforms (Windows 10) for both data at rest and data in transit. Encryption at rest protects your data on our servers. Encryption in transit (using SSL/TLS) protects your data when it's transmitted.

To protect individual files, you can apply rights-based permissions so that only intended recipients can access and view the information. You can also apply data loss prevention actions, such as blocking the sharing of a file with sensitive information like credit card information or personal identification numbers. You can limit or block access to cloud apps present in your environment or revoke app access among specific individuals.

To help users make more informed decisions, you can enable on-screen policy tips that notify users that the document they are working with contains sensitive information. You can even automatically apply a visual marking to a document, such as on the header or footer.

To help prevent sensitive information from remaining longer than necessary and potentially posing a risk, you can automatically retain, expire, or delete documents based on information governance policies defined by your company. These capabilities are also fundamental for meeting compliance standards (e.g., GDPR).

Protect

Once you have classified information, you move to perhaps the most important phase of information protection—applying policy-based actions to sensitive information.

The organization defines the policy-based actions to apply to sensitive information, while also ensuring users can do their jobs. These policies and their related actions determine how information can be used and shared. This approach ensures information is protected at the right level based on sensitivity.

Traditionally, protection has primarily meant controlling access to information. With Microsoft capabilities and the policies defined by your company, including those for compliance, you can take a range of protective actions depending on the sensitivity of the information.

For example, you can use MCAS to scan cloud apps for sensitive data and automatically apply AIP labels through policies, including encryption and rights management capabilities to block forwarding, printing, copying, and more.

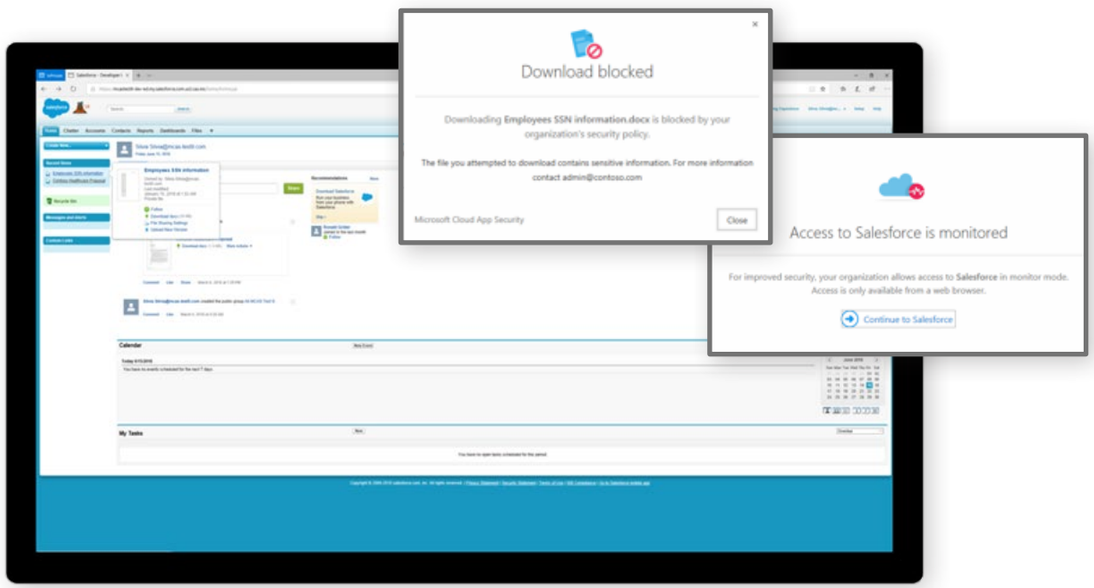
AIP and Office 365 allow for adding encryption protection as a policy action. The protection feature in AIP uses encryption, identity, and authorization policies that stay with the protected document and email to help you maintain control of your data, even when it is shared with other people.

Office 365 Message Encryption combines email encryption and rights management capabilities. Rights management capabilities are powered by AIP. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Organizations also have the option to provide and control their own encryption keys for Office 365 Message Encryption. This is offered through Bring Your Own Key (BYOK) for AIP.

With Office 365, data is encrypted both at rest and in transit by default. For data in transit, Office 365 uses industry standard secure transport protocols. For data at rest, Office 365 uses various technologies, including BitLocker, to encrypt the disk drives containing customer data at the volume level.

Customer Key in Office 365 enhances the ability for organizations to meet compliance requirements that specify key arrangements with the cloud service provider. With Customer Key, organizations can provide and control their encryption keys for their Office 365 data at rest at the application level. As a result, customers may exercise their control and revoke their keys, should they decide to exit the service. By revoking the keys, the data is unreadable to the service and will put the customer on path toward data deletion. Lastly, managing and protecting keys are crucial but can be difficult. Customer Key includes an availability key to protect against data loss.

But protection is much more than encryption. Protection can also apply rights-based permissions using AIP so that only intended recipients can access and view the information. You can use MCAS, for example, to prevent data loss of files that are classified as confidential (or some other sensitive classification) outside your organization. MCAS can detect files in your cloud apps that are classified as confidential but have the incorrect access levels, allowing unauthorized users to access them. Then it can apply automatic governance actions, such as "quarantine file," to prevent data losses from your organization.



To help users make more informed decisions, you can enable policy tips in Office 365 Data Loss Prevention (DLP) that notify them that the document they are working with contains sensitive information. Or, with AIP, you can even automatically apply a visual marking to a document, such as on the header or footer. You can also use DLP to apply data loss prevention actions, such as blocking the sharing of a file that is detected to have sensitive information like credit card information or personal identification numbers.

We can also help prevent sensitive information from remaining longer than necessary and potentially posing a risk if discovered or compromised. Office 365 Advanced Data Governance (ADG) can automatically retain, expire, or delete documents based on information governance policies defined by your company.

Organizations often have to meet compliance measures requiring certain procedures be in place before access is granted. Microsoft Customer Lockbox provides help with compliance and allows added control by injecting the customer into the approval workflow. With Office 365, you can use Customer Lockbox to control how a Microsoft support engineer accesses your data during a help session. In cases where the engineer requires access to your data to troubleshoot and fix an issue, Customer Lockbox allows you to approve or reject the access request. If you approve it, the engineer can access the data. Each request has an expiration time, and once the issue is resolved, the request is closed and access is revoked.

Compliance

To help you comply with national, regional, and industry-specific requirements governing the collection and use of individuals' information, we offer the most comprehensive set of compliance offerings of any cloud service provider. The Microsoft Cloud helps support multiple compliance initiatives, including GDPR, HIPAA, and PCI DSS.

Also, because achieving organizational compliance can be incredibly challenging, we suggest organizations periodically perform risk assessments to understand their compliance posture. Compliance Manager is a tool that works across Microsoft cloud services to help organizations meet complex compliance obligations like GDPR.

You can learn more about what Microsoft is doing to comply with regulations and also how we are helping organizations do so here.

Monitor

The last stage of the Information Protection lifecycle is the ability to monitor and respond to events. This means gaining visibility into how users are using or distributing sensitive information. For instance, you can use MCAS to find policy violations, understand cloud app usage, and create alerts when new apps are discovered on the network.

You can also investigate issues further, and then respond quickly and accurately. For example, you can use MCAS to discover inappropriate sharing, immediately revoke app access, and quarantine a file or user.

With Office 365 DLP, you can protect information to the level you desire or are required to per policy and governance requirements.

With AIP, you can see the state of the information, revoke access to a file, change what people can do to a file, control who may use the file, and apply numerous other controls.

Monitoring can be in the form of real-time alerts, email messages, or a reporting dashboard. In the Office 365 Security & Compliance Center, you have a centralized view of Office 365 data loss prevention and data governance events and activity. From here, you can email incident reports when a policy is violated. These reports can be sent to IT so that IT can find out in real time who violated a policy, what policy was violated, what exact information caused the violation, and the number of times sensitive information appeared in the content.

You can also see your policies over time within DLP reports. You can see historical information like how many times a policy was violated, when policy violations happened, who requested overrides for a policy, and what workloads the violation took place in.

Protect information. Build trust. Start now.

Capabilities built into Office 365 and Windows 10, plus Microsoft Enterprise Mobility + Security, will help you care for your organization's digital information across devices, inside or outside of Office 365, whether in the cloud, in SaaS apps, or on-premises.

Various components work together to provide end-to-end protection of sensitive information across your environment. You can also add capabilities over time as your Information Protection strategy becomes more sophisticated and mature.

But which capabilities are right for you?

Begin by assessing your needs

We recommend that you begin your Information Protection strategy by determining what you need to protect. Is it for compliance or a regulatory issue? Perhaps it meets a business need, or your organization just wants to do it. Once you know what you are protecting and why, then you can turn to identifying Information Protection capabilities—those you may already have and those you may still need.

One place to begin is the Service Trust Portal. There, you can access the Compliance Manager, a workflow-based risk assessment tool that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft cloud services, such as Office 365, Dynamics 365, and Microsoft Azure. You can also learn more about what's available to you through your Microsoft partner and/or account executive and the Microsoft product/service administrative portal.

The table of Microsoft Information Protection Capabilities in this paper helps you find what you need based on the stage of the Information Protection lifecycle and areas where you may need Information Protection—across devices, in Office 365, in cloud apps, or on-premises.

Devices

One of the most challenging places for protecting information is on devices. BitLocker is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Windows Information Protection (WIP) helps to protect against potential data leakage without otherwise interfering with the employee experience on Windows 10 devices.

Beyond Windows devices, Intune mobile device management and mobile application management provide similar protection capabilities for other platforms, such as Apple iOS and Google Android. In adopting these solutions, it is imperative to maintain a positive user experience without compromising on security of the information shared and created using mobile devices.

For example, Calvert County Public Schools uses Intune for Education to protect devices on its network from outside intrusion and general student mischief without bogging down students with cumbersome sign-in procedures. Before deploying Intune, Calvert had a generic login, and sometimes students would sign in and see each other's settings. With Intune, students sign in as themselves, even on a shared device, and it's beneficial because then they get affinity on that machine. Since both Office 365 and Intune for Education are supported by Azure Active Directory, sensitive student information, student identities, and school data benefit from enhanced privacy.

To learn more, check out this video featuring users sharing their viewpoints on productivity and user experience when it comes to information access on devices.

Office 365

Many organizations use Office 365 as their main productivity service. Information Protection capabilities in Office 365 help protect sensitive information across Exchange Online, SharePoint Online, and OneDrive for Business.

One way you can use Office 365's protection capabilities is to help meet the requirements of GDPR. For example, Office 365 Advanced Data Governance enables you to classify and label documents for applying retention, expiration, and deletion policies to important information. This is complemented by Office 365 DLP, which enables you to prevent sensitive information in Office 365 from getting into the wrong hands or being accidentally shared.

With these capabilities, you can use Office 365 to guard against leaks of personal data—one of the central components of GDPR. You can start with Office 365 DLP reports for monitoring personal data in SharePoint Online, OneDrive for Business, and email in transit. These provide the greatest level of detail for monitoring personal data.

Next, you can use alert policies and the Office 365 audit log to monitor activity across Office 365 services. Set up ongoing monitoring or search the audit log to investigate an incident. The Office 365 audit log works across Office 365 services—Sway, Power BI, eDiscovery, Dynamics 365, Microsoft Flow, Microsoft Teams, admin activity, OneDrive for Business, SharePoint Online, mail in transit, and mailboxes at rest. Skype conversations are included in mailboxes at rest.

Cloud services, SaaS apps, and on-premises

Beyond Office 365, organizations are increasingly using Azure and/or a combination of cloud services and cloud apps, often in conjunction with legacy on-premises data centers and file shares. AIP helps protect sensitive information across cloud services and on-premises environments. MCAS provides visibility and control across cloud apps and services.

You can use MCAS to monitor files with sensitive data in non-Microsoft cloud services such as Box, Salesforce, or AWS. You can use Office 365 sensitive information types and unified labels across AIP and Office 365 with MCAS. You can set up policies that apply to all your SaaS apps or specific apps (like Box).

For example, Yara is a global fertilizer company that uses Microsoft AIP. As a result, Yara employees can collaborate effectively, retain control over potentially sensitive files, and comply with security policies—all while continuing to lead their industry into the future.

In another example, Qatari shipping and maritime company Nakilat has one of the world's largest fleets of liquefied natural gas (LNG) carriers, transporting LNG from Qatar to global markets. To increase its competitive advantage, Nakilat wanted to improve employee productivity and mobility without compromising data security. It uses Office 365 and MCAS to deliver highly secure cloud-first workplaces—shipboard and in the office. Nakilat also adopted the Microsoft Azure platform to optimize operations and improve business continuity, reducing operating costs by 50 percent.

Similarly, First American Equipment Finance, a leasing company, uses Microsoft Cloud App Security to monitor and track all SaaS activity to constantly learn how each person uses SaaS to identify dangerous activities. It achieves all of this transparently without requiring agents, so there's no impact on usage of SaaS or the user experience.

And, in our own cloud-first, mobile-first environment, the use of cloud apps is on the rise. To help protect corporate data, Microsoft Core Services Engineering uses Microsoft Cloud App Security to discover and identify cloud applications in use on our network, assessing security risks for any app. With the Cloud App Security Portal, we monitor suspicious behavior patterns and unusual activity and detect threats. Cloud App Security provides protection for our network and greater visibility into our environment.

Steps you can take now

Here are some specific steps you can take to start protecting your organization's information:

Devices

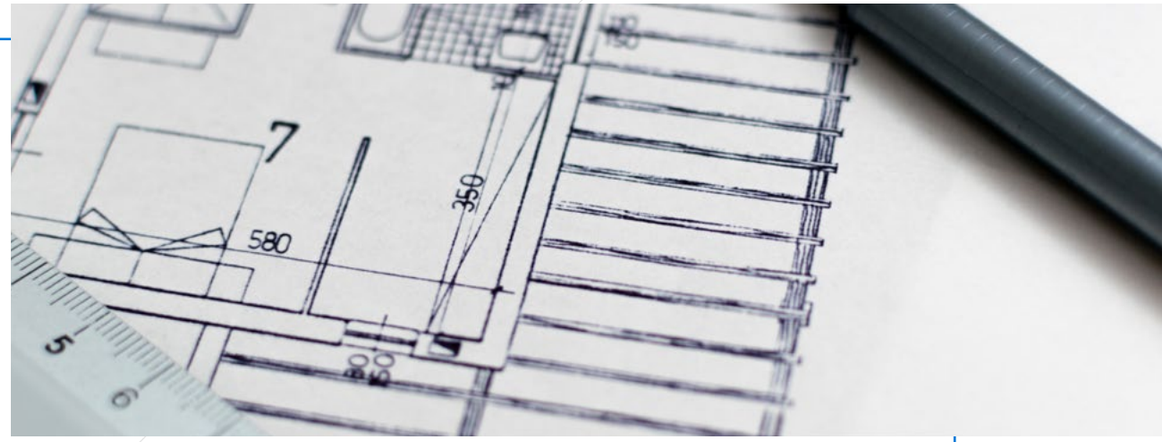
- Protect business information on your Windows 10 devices with Windows Information Protection (WIP).
- Protect business information on your Apple iOS and Google Android devices with Intune mobile device management and mobile application management.

Office 365

- Use Office 365 data loss prevention to protect your Office 365 email and documents.
- Use Office 365 Advanced Data Governance for data governance, retention, and expiration.

Cloud, on-premises

- Use Azure Information Protection (AIP) to protect beyond Office 365—on the supported versions of Office, Windows, and mobile devices.



Explore a variety of Information Protection capabilities and access free trials from the following links:

Azure Information Protection (AIP)

Cloud App Security

Office 365 Advanced Data Governance and Office 365 data loss prevention (via Office 365 Enterprise E5)

We understand that Information Protection is just part of your organization-wide security effort. For even as you protect information, you also aim to provide threat protection, identity and access management, and security management. We are committed to working with you across all of these security needs.

Our capabilities provide what you need to protect your organization's information. But they only work if you turn them on. Now is the time to make it happen.

Information Protection capabilities

The table of Microsoft Information Protection capabilities demonstrates how we help you protect information across devices, applications, and locations.

What to Protect	Product	Description	Information Protection Lifecycle Phase			
			Discover	Classify	Protect	Monitor
Devices (PCs, Tablets, and Mobile)	**BitLocker Drive Encryption**	BitLocker Drive Encryption is an information protection feature that integrates with the Windows operating system and addresses the threats of information theft or exposure from lost, stolen, or inappropriately decommissioned computers.			✓	
	Windows Information Protection (WIP)	Windows Information Protection helps to protect against potential information leakage without otherwise interfering with the user experience. WIP also helps to protect enterprise apps and information against accidental information leakage on enterprise-owned, corporate-owned, and employee-owned devices (BYOD) without requiring changes to your environment or other apps.			✓	
	Intune	Microsoft Intune is a cloud service that provides mobile device management, mobile application management, and PC management capabilities. Intune's mobile productivity management capabilities help organizations provide their employees access to corporate information, applications, and resources, while helping to protect their corporate information.			✓	
Office 365 (Exchange Online, SharePoint Online, OneDrive for Business)	**Office 365 data loss prevention (DLP)**	Office 365 data loss prevention enables you to prevent sensitive information in Office 365 from getting into the wrong hands or being accidentally shared. You can identify, monitor, and automatically protect sensitive information across Office 365 services.	✓		✓	✓
	Office 365 Advanced Data Governance (ADG)	Office 365 Advanced Data Governance applies machine learning to help customers find and retain important information while eliminating trivial, redundant, and obsolete information that could cause risk if compromised. ADG enables you to classify and label documents for applying retention, expiration, and deletion policies to sensitive information.	✓	✓		
	Office 365 Message Encryption	With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Email message encryption helps ensure that only intended recipients can view message content.			✓	
	Office 365 Service Encryption with Customer Key	With Customer Key, organizations can provide and control their own encryption keys that are used to encrypt their Office 365 data at rest at the application layer. Customer Key helps customers meet their compliance obligations that require certain key arrangements with their cloud service provider.			✓	
	Office 365 Customer Lockbox	Office 365 Customer Lockbox can help a customer control how a Microsoft support engineer accesses customer data during a scenario where a customer has raised a support request to investigate some service issues related to that customer's Office 365 tenant. If the customer gives access by approving the request, Microsoft support engineers can access the data to help the customer resolve issues.			✓	

What to Protect	Product	Description	Information Protection Lifecycle Phase			
			Discover	Classify	Protect	Monitor
Cloud services, SaaS apps, and on-premises (Azure, third-party SaaS apps, datacenters, and file shares)	**Azure Information Protection (AIP)**	Azure Information Protection helps protect sensitive information across cloud services and for on-premises environments. With AIP, you can classify and label information based on sensitivity and create different levels of protection and visual markings (such as encryption and watermarking). AIP provides enhanced protection in the form of client-side protection and other advanced capabilities.				
	Microsoft Cloud App Security (CAS)	Microsoft's Cloud App Security is a Cloud Access Security Broker (CASB) solution that gives you visibility into your cloud apps and services, provides sophisticated analytics to identify and combat cyberthreats, and enables you to control how your data travels: • Cloud discovery: Discover shadow IT and assess the risk to your organization. • Data protection: Protect your data when it travels outside your organization and monitor and control the access to your data in real time across all of your cloud apps. • Threat protection: Detect threats and anomalies and configure automatic remediation.				

Credits

Many subject-matter experts from various groups contributed to the conceptualization and articulation of the story contained in this document.

Adam Jung
Sr. Product Marketing Manager, Security Product Marketing, Microsoft

Caroline Shin
Sr. Product Marketing Manager, M365 Suite Product Marketing, Microsoft

Debraj Ghosh
Sr. Product Marketing Manager, Security Product Marketing, Microsoft

Diana Kelley
Cybersecurity Field CTO, Cybersecurity Solutions Group, Microsoft

Enrique Saggese
Principal Program Manager, Security Customer Experience and Platform COGS, Microsoft

Kim Kischel
Product Marketing Manager, Security Product Marketing, Microsoft

Mark Simos
Chief Security Advisor, Cybersecurity Solutions Group, Microsoft

Nick Robinson
Sr. Product Marketing Manager, M365 Suite Product Marketing, Microsoft

Pieter Wigleven
Sr. Product Marketing Manager, Windows Commercial Marketing, Microsoft

Raman Kalyan
Sr. Product Marketing Manager, M365 Suite Product Marketing, Microsoft

Seema Kathuria
Sr. Product Marketing Manager, Cybersecurity Solutions Group, Microsoft

Shawn Anderson
Chief Security Advisor, Cybersecurity Solutions Group, Microsoft

James Watson
Creative Director, Revel Consulting

Steven Silverman
Market Strategist, Revel Consulting

Joe Ehrbar
Copy Editor, Revel Consulting

Protect your sensitive information, no matter where it lives or travels.

microsoft.com/security/information-protection