Microsoft

Protect your data in files, apps, and devices, within and across organizations

Empowering your employees to work outside the office is essential to company productivity, but it can be hard to balance security concerns with work flexibility. Most companies focus their security solutions around users, devices, and apps, but overlook invoking strong security for their most valuable asset, their data. Data needs to be protected at the time of creation. That protection should stay with the data whether it's sent internally to another employee or sent to someone outside the organization. You need visibility into what data is shared and how it's being shared, especially through third-party apps like Dropbox or Salesforce. Then you need the ability to take immediate action to limit or change access according to the current risk profile. Microsoft 365 security solutions allow users to work the way that's best for them.

My employees are using their own devices at work. How can I help ensure organizational data is safe?

Several elements are available to make sure organizational data is safe on employee-owned devices (BYOD). Microsoft 365 brings together all the elements you need into a single solution to keep your data safe.

Manage employee identities with Microsoft Azure Active Directory (Azure AD), which gives your employees the ability to sign in to business apps and access appropriate company data on their own devices. Azure AD works with iOS, Mac OS X, Android, and Windows devices.

Microsoft Intune lets you manage the apps employees use to do business through Intune App Protection. Intune App Protection policies work with Intune-managed apps and let you restrict copy-and-paste and save-as functions, configure web links to open inside the Intune Managed Browser app, and enable multi-identity use and app-level conditional access.

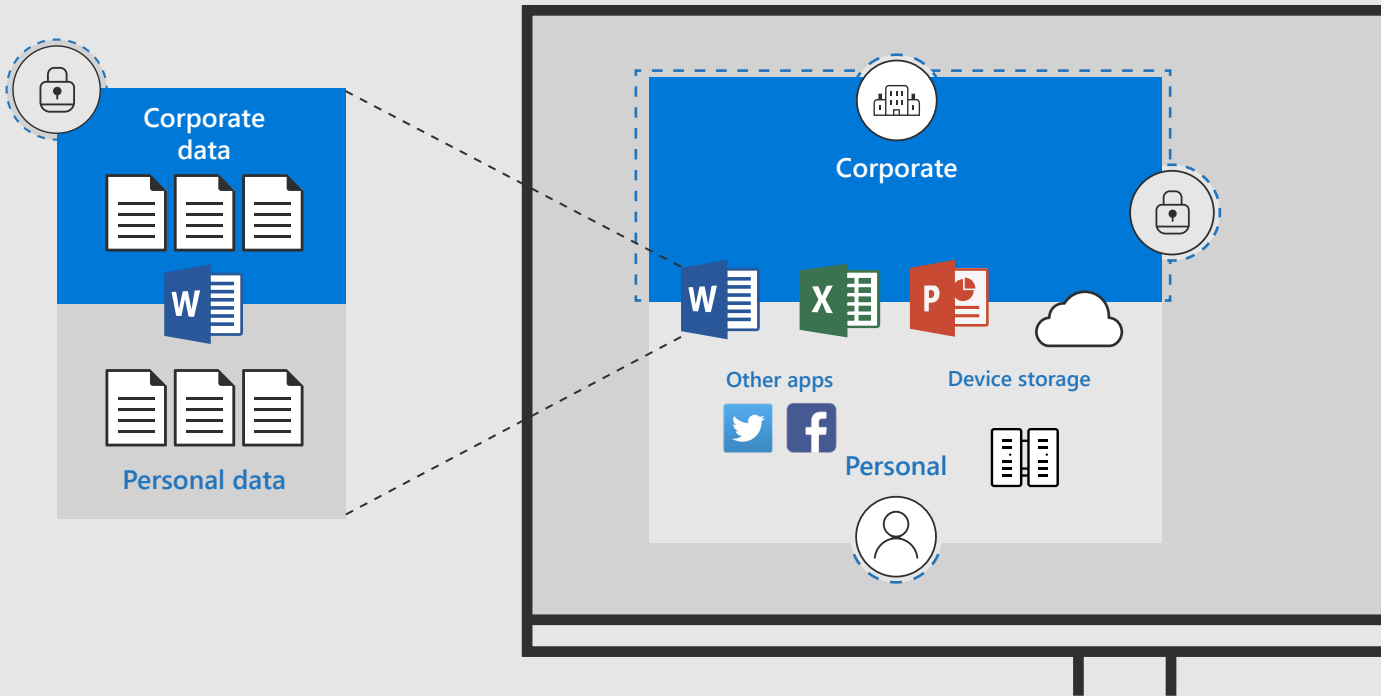

Figure 1. Manage the apps employees use to do business through Intune App Protection.

Conditional access lets you set policies to manage what users can access. You can set levels of access on employee-by-employee, device-by-device, or group-by-group basis.

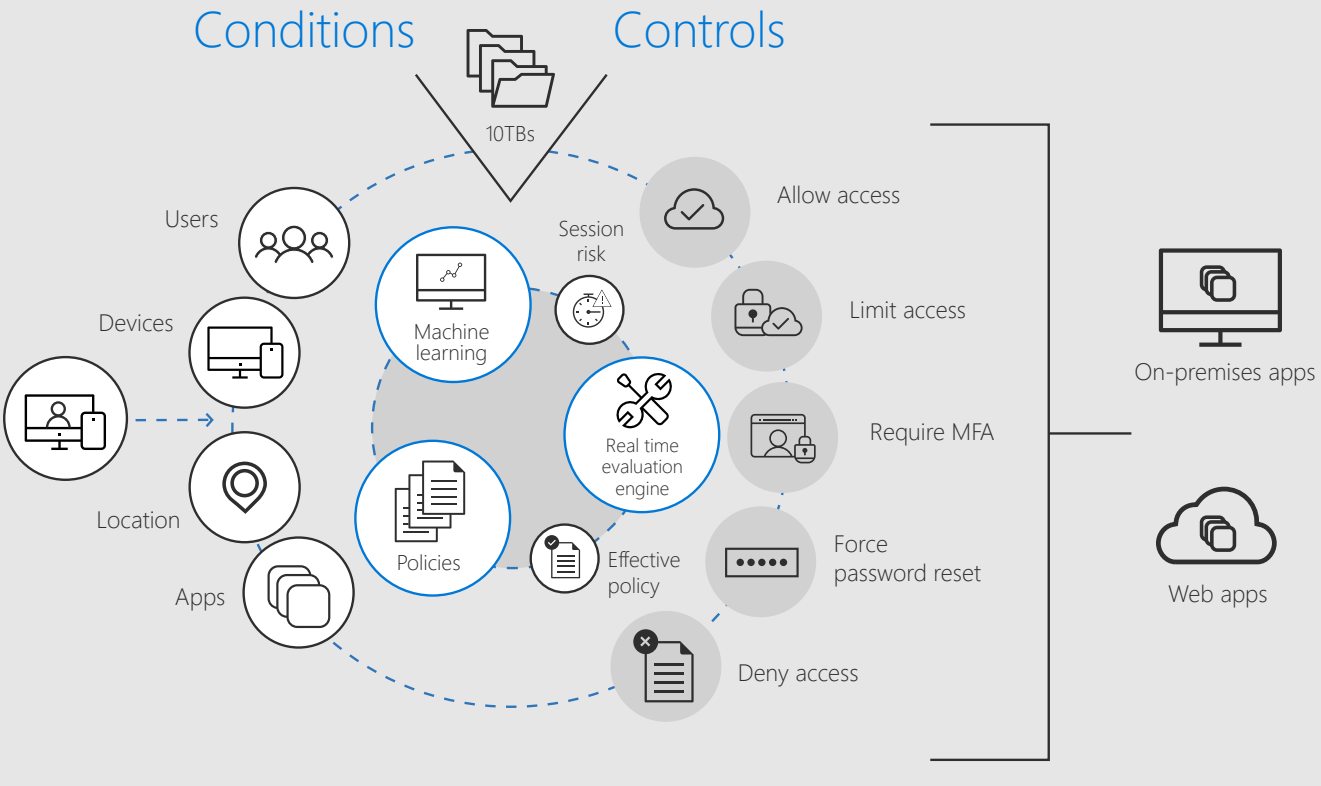

Figure 2. Conditional access lets you set policies to manage what users can access.

Through Microsoft Managed Mobile Productivity solutions, you can streamline IT efforts by empowering your employees with self-service capabilities. You can let employees reset their password or PIN, join and manage their own groups, get access to apps, and invite external partners to collaborate within corporate apps—all on their own.

Windows Information Protection is designed to help protect against accidental data leaks. It works with Microsoft Office 365 and Azure Rights Management to help protect business data when it leaves your employees' devices or when it's shared with others.

With Windows Information Protection, you can:

- Help protect data locally and on removable storage.
- Offer a common experience across all Windows 10 devices.
- Restrict copy-and-paste functions.
- Help prevent unauthorized apps from accessing business data.
- Discriminate between corporate and personal data on the device so that it can be wiped if necessary.
- Seamlessly interoperate Windows Information Protection with the platform and all apps without needing to switch modes.

Windows Information Protection can be configured through Microsoft Intune or Microsoft System Center Configuration Manager (ConfigMgr).

Help protect your computer's data using Microsoft BitLocker Drive Encryption technology. It's included in Windows 10, which uses the strongest publicly available encryption. The technology prevents others from accessing your disk drives and flash drives without authorization, even if they're lost or stolen.

How can I help protect my organization's information in the cloud?

Whether your company is totally cloud-based or a hybrid of cloud and on-premises, you can help protect your company in the cloud by managing employee identities, devices, and data.

The Azure Security Center offers you a unified view of security across all your on-premises and cloud workloads. Azure AD helps provide secure identity and access management. You can easily extend your on-premises Active Directory to Azure AD using Azure AD Connect. Azure AD allows you to provide the convenience of single sign-on access to thousands of cloud and on-premises applications with one unified identity. This includes Office 365 apps and support for Salesforce, Concur, Workday, and thousands of other popular software as a service (SaaS) apps.

Windows 10 Enterprise offers you modern management capabilities designed to work with Azure. Windows Defender, for example, will turn on automatically if any employee device lacks an active antivirus subscription.

Through Microsoft SharePoint Online, your employees can build and use a team site and a team library, which make sharing and accessing resources easy and intuitive. SharePoint Online has a number of security features to protect that collaborative environment. You can configure conditional access policies and other security features through the SharePoint Admin center to restrict access on the basis of network location.

Finally, if you choose to have Microsoft engineers help you resolve a customer issue, you can enable Microsoft Customer Lockbox and limit what they can see, without impeding their service.

My company has very strict compliance requirements for data access and sharing. How can I make sure that my employees don't try to circumvent our technology to work more effectively?

To ensure your employees remain compliant with organizational policy, it must be easy for them to do so as part of their daily routine. Otherwise, employees will find other ways to share or access data so they can complete their current task at hand.

Enable Azure Information Protection to label, classify, and encrypt documents on the basis of their level of security. Azure Information Protection gives you the flexibility to apply automatic classifications to all employee files based on existing company policy, or to empower your employees to determine how their files are classified. You can also set recommendations for classification based on company policy.

Sending and receiving email is one of the weakest spots for IT security. Azure Information Protection offers several ways to keep your employee data safe over email. With it, you can:

- Configure policies to classify, label, and protect data based on sensitivity. You can classify information automatically, let your employees decide how to classify their data, or offer recommendations for classification.
- Track activities on shared data and revoke user access if necessary. Your IT team can use powerful logging and reporting to monitor and analyze data.
- Add classification and information protection for persistent protection that follows your data, ensuring it remains protected regardless of where it's stored or with whom it's shared.

For security against malicious emails, Office 365 Advanced Threat Protection lets you set up anti-phishing protections to help prevent your employees from increasingly sophisticated phishing attacks. Office 365 comes with a wide range of compliance features that can be enabled without affecting your employees' ability to get work done.

The Office 365 Security and Compliance Center helps you protect against data loss and threats. It also lets you monitor and audit your employees' usage to determine areas of weakness or potential threats.

Make sure your employees' identities are managed through Azure AD. Attaching security to identity helps to ensure that your company policies can be enforced across devices, data, apps, and infrastructure, in the cloud, on mobile, or on-premises. Facilitating secure remote access empowers your employees to work wherever they need to, so they won't seek unsecured channels. Microsoft Cloud App Security uses traffic logs to uncover shadow IT that employees may be turning to if compliance requirements are hindering the way they work.

What can I do when my employees lose their device?

Whether your employees use a personal or company-owned devices, you can take several steps to mitigate information leaks in case of loss or theft. Microsoft has solutions that let you do either a full or selective device wipe, depending on how your employees' devices are managed.

If your employees use their own devices (BYOD), you can manage their business apps with Microsoft Intune App Protection policies. They enable you to wipe data only from managed business apps, like Microsoft Word and Microsoft SharePoint. Selective wipe is helpful if an employee leaves your company. You can wipe company data, but leave the rest of the employee device alone.

Company-owned devices can be managed through Microsoft Intune mobile device management (MDM). Intune MDM gives you the flexibility to wipe an entire device (factory reset) or just wipe company data. You can opt for either action through the Azure portal.

After you have removed sensitive data from the device, you can remove it from Azure AD so that the device will no longer be part of your company ecosystem.

Deployment tips from our experts

Keep your company data safe

Deploy Azure Information Protection and set up your data classification, labels, and automatic policies to control access. It will allow you to label, classify, and encrypt documents according to their level of security. Then use Windows Information Protection to help protect against accidental data leaks.

Keep your identities safe

Manage employee identities with Azure AD by allowing them to sign in to business apps and access appropriate company data on their devices, and enable conditional access to manage what apps employees can access.

Manage your devices in Intune

Enable Intune to be your mobile management strategy to manage the apps that employees use to do business. You can control the apps employees can access, and you have the ability to wipe a device when someone leaves the company.

Plan for success with Microsoft FastTrack

FastTrack comes with your subscription at no additional charge. Whether you're planning your initial rollout, needing to onboard your product, or driving end-user adoption, FastTrack is your benefit service that is ready to assist you.

Get started at FastTrack for Microsoft 365.

Microsoft