Microsoft

Work securely from anywhere, anytime, across all your devices

Your employees expect technology to help them be productive; you need to keep your organization's data safe. These desires need not be incompatible. Microsoft 365 has the solutions to help you ensure that your users, devices, apps, and data are secure wherever they are accessed or used. Empower your employees to work whenever and wherever they want with solutions for identity and access management, information protection, threat protection, and security management.

How can I make sure my employees are working securely when they are working remotely?

Digital technology is changing how people work. Your employees expect to have access to everything they need to be productive on a variety of devices, both company-provided and employee-owned (BYOD) devices. You must be able to enable secure collaboration and safeguard corporate data. The vital foundation to your in-depth security strategy is strong, integrated identity protection.

Security across devices, cloud, and on-premises apps

Identity management in Azure Active Directory (Azure AD) is your first step. Azure AD Single Sign-On (SSO), lets you manage authentication across devices, cloud apps, and on-premises apps. Once you enable SSO, your employees can access resources in real time on any device while working remote, including to confidential or sensitive work documents. Next, layer multi-factor authentication (MFA) with Azure AD Conditional Access by setting user policies (see Figure 1). These security tools work together to reauthenticate high-risk users and to take automated action to secure your network.

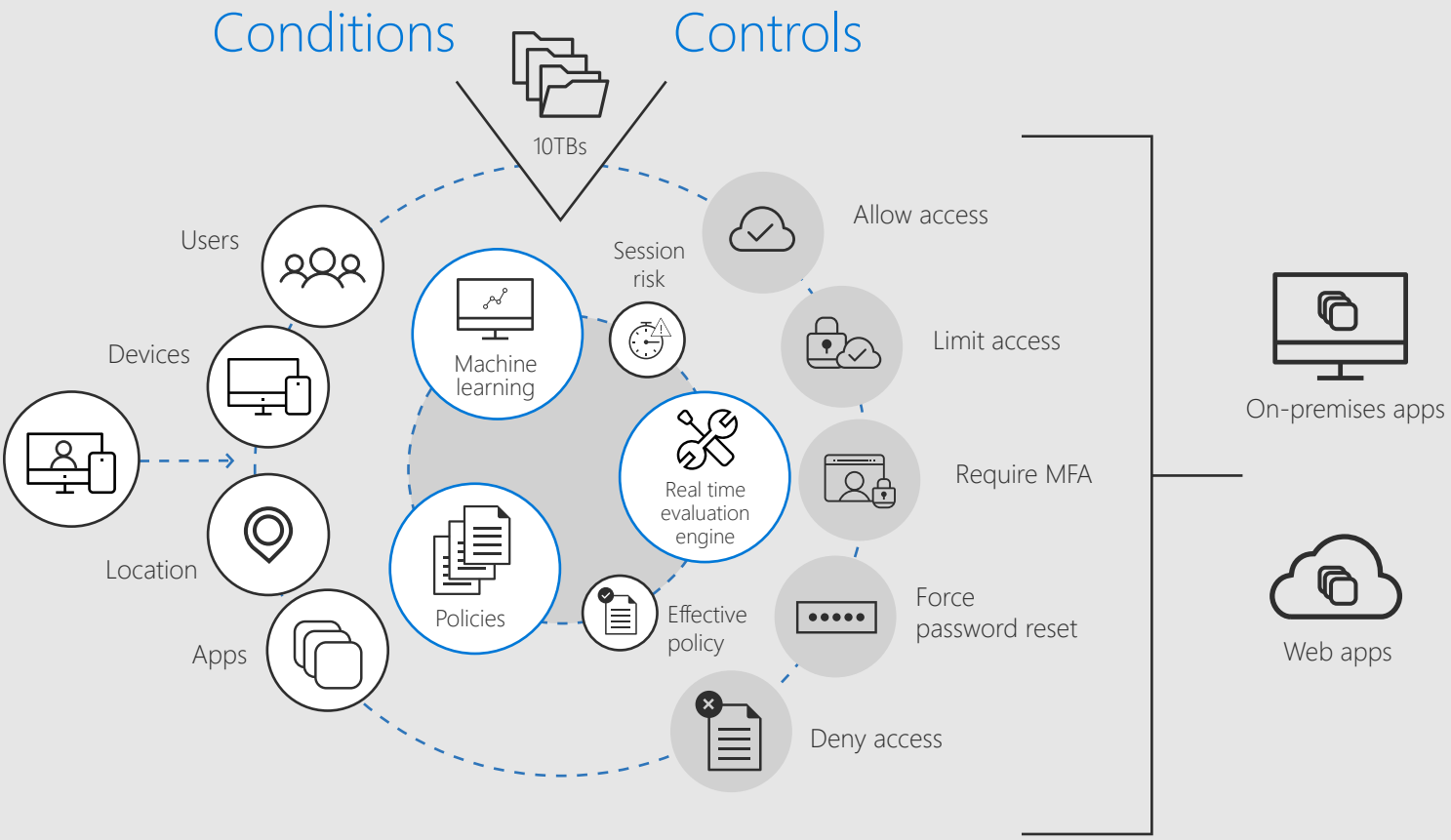

Figure 1. Set user policies using Azure AD Conditional Access.

Security across devices

Microsoft Intune lets you manage both company-owned and employee-owned devices from the cloud. It allows you to manage across devices (laptop, tablet, smartphone) and operating systems (iOS, Windows, Android). Once you set up your Intune subscription, you can add users and groups of users, assign licenses, deploy and protect apps, and set up device enrollment.

Azure AD Conditional Access is Microsoft's identity security policy hub. Through Azure AD, you can create conditional access policies according to user, device, application, and risk. For example, with Intune and Azure AD Conditional Access, you can enforce controls that allow a device trying to access a specific resource only if it's compliant. With device-based conditional access policies, you can:

- Require employees to use MFA before they can access data on a device.
- Enable location-based policies on a device that restrict or permit access depending on the device's location.
- Require a device to be registered with Azure AD and to be marked as compliant through Intune or third-party mobile device management (MDM).

Remote employees on Windows 10 company-owned devices can be enrolled through Windows Autopilot, which lets you automatically join devices to Azure AD and auto-enroll devices into MDM services like Microsoft Intune. Non–Windows 10 devices can be manually configured into Intune. Employees can securely enroll new mobile devices to the corporate ecosystem with the ability to install corporate apps from a self-service portal. Intune automatically discovers rogue devices when these devices attempt to connect to the network and prompts users to register their device and sign in using their SSO credentials.

To strengthen employee sign-in from Windows 10 PCs, deploy Windows Hello for Business, which replaces passwords with strong two-factor authentication on PCs. This authentication consists of a user credential that is tied to a device and uses a biometric or PIN. Windows Hello for Business lets users authenticate to an on-premises Active Directory or an Azure AD account.

Security across apps

Through Microsoft 365, you'll have access to mobile Microsoft business apps such as Microsoft Outlook, Word, and OneDrive for Business. Once you provision identities through Azure AD, you can manage these mobile apps through Intune App Protection, which allows you to protect and manage just the apps your employees use for work on both company-owned devices and BYOD.

Microsoft Cloud App Security gives you visibility and control over the cloud apps that your employees are using. You can see the overall picture of cloud apps across your network, including any unsanctioned apps your employees may be using. Discovering these shadow IT apps can help you prevent unmonitored avenues into or out of your network. Microsoft Cloud App Security can also help you manage and limit cloud app access using factors like user identity, device health, and physical location.

Microsoft Office 365 Cloud App Security (CAS), a subset of Microsoft Cloud App Security, provides visibility into Office 365. With Office 365 CAS, you can detect threats through user activity logs, discover shadow IT for apps similar to Office 365 apps, and control app permissions to Office 365. Providing your employees with rich productivity apps that you can manage and safeguard will ensure they can work effectively and securely.

Security across email

Once you have secured your organization's devices and applications, it's equally important to safeguard your organization's flow of information. 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 Azure Information Protection, 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 (ATP) lets you set up anti-phishing protections to help protect your employees from increasingly sophisticated phishing attacks.

Security across data

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.

Windows Information Protection is designed to help protect against accidental data leaks. It works with 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 into 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).

How can I proactively monitor for compliance and threats?

In addition to empowering your employees to work securely on any device, Azure AD and Intune offer additional solutions that help you proactively monitor for noncompliance and threats.

Monitor your identities

Azure AD Identity Protection provides an overview of risk and vulnerabilities that may be affecting your organization's identities. Azure AD Identity Protection uses existing Azure AD anomaly detection capabilities available through Azure AD anomalous activity reports. You can enable Azure AD Identity Protection through the Azure portal.

Azure AD Identity Protection helps you identify the risk level of a particular employee or user. You can set up risk-based conditional access policies to automatically mitigate threats and secure corporate or organizational resources and data. Risk-based conditional access gets rich signals from the Microsoft Intelligent Security Graph and then converts them to actionable risk-based policies you can apply to your organization.

Monitor your devices

Microsoft Intune device compliance reports allow you to analyze enrolled device compliance within your organization and quickly troubleshoot compliance-related issues encountered by your employees. You can view information about the overall compliance states of devices, for an individual setting, and for an individual policy, and drill down into individual devices to view specific settings and policies that affect the device. To reach the Intune Device compliance dashboard (see Figure 2), sign in to the Azure portal with your Intune credentials. From there, you can see all the specific compliance policies and settings on each device and if and how each device is compliant.

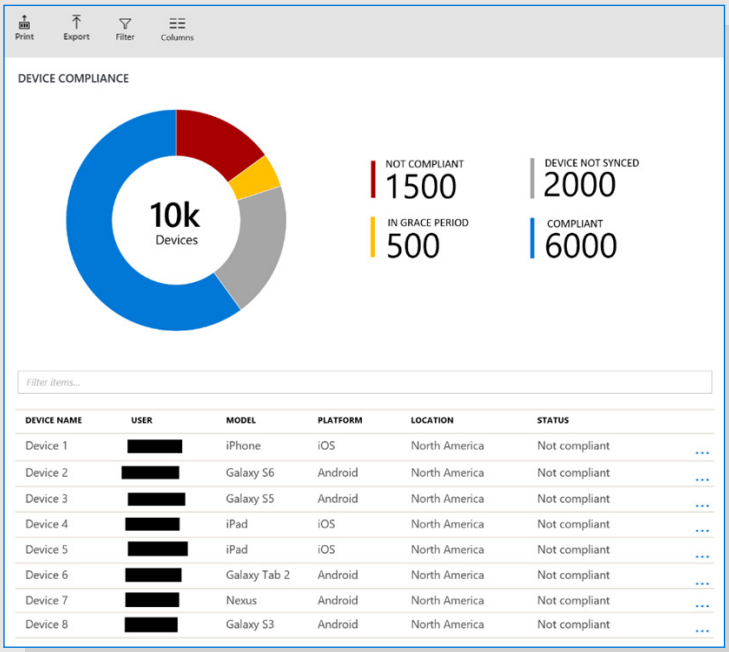

Figure 2. Intune Device compliance dashboard can be accessed by signing in to the Azure portal.

Setting up conditional access policies for mobile devices is a crucial step for preventing threats and leaks. With actions for noncompliance, you can set up an Intune Device compliance policy with conditional access so that when Intune detects a device that isn't compliant, it immediately marks the device as noncompliant; then Azure AD blocks it through conditional access. That way, noncompliant devices can't access corporate data until they are brought into compliance. Actions for noncompliance also offer the flexibility to decide what to do about the noncompliant device. For example, you may opt not to block the device immediately and give your employees a grace period to conform to compliance requirements. Either way, you can enforce compliance policies that protect your company's data.

Monitor for threats

There are three main attack vectors through which threats emerge: identity, device, and email. Microsoft 365 offers comprehensive threat protection for each of the three vectors.

Azure Advanced Threat Protection (ATP) detects dozens of types of malicious attacks, security risks, and suspicious behaviors by focusing on several phases of the cyber attack kill chain, including:

- Reconnaissance, during which attackers gather information on how the environment is built, what the different assets are, and which entities exist. They are generally building their plan for the next phases of the attack.
- Lateral movement cycle, during which attackers invest time and effort in spreading their attack surface inside your network.
- Domain dominance (persistence), during which attackers capture the information allowing them to resume their campaign by using various sets of entry points, credentials, and techniques.

For threat protection across your productivity and business apps, Office 365 Advanced Threat Protection (ATP) offers quick detection of potential threats, including phishing and ransomware, to your Office 365 environment across email, Office 365 client applications, and Office collaboration applications.

Microsoft Cloud App Security then provides alerts if it detects anomalous user behavior or anomalous behavior in your cloud apps ecosystem.

For intelligence-driven protection, detection, and response, Windows Defender Advanced Threat Protection (ATP) offers Windows 10 threat protection built in to the operating system. It's a key component of the Microsoft Secure stack, amplifying security across Windows, Office, and Azure (see Figure 3). Windows Defender ATP uses a variety of built-in technologies to detect and protect against threats, such as:

- Endpoint behavioral sensors that collect and process behavioral signals from the operating system (for example, process, registry, file, and network communications). This sensor data is then sent to your private, isolated, cloud instance of Windows Defender ATP.
- Cloud security analytics that leverage big data, machine learning, and unique Microsoft optics across the Windows ecosystem. Behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- Threat intelligence that enables Windows Defender ATP to identify attacker tools, techniques, and procedures, and to generate alerts when these are observed in collected sensor data.

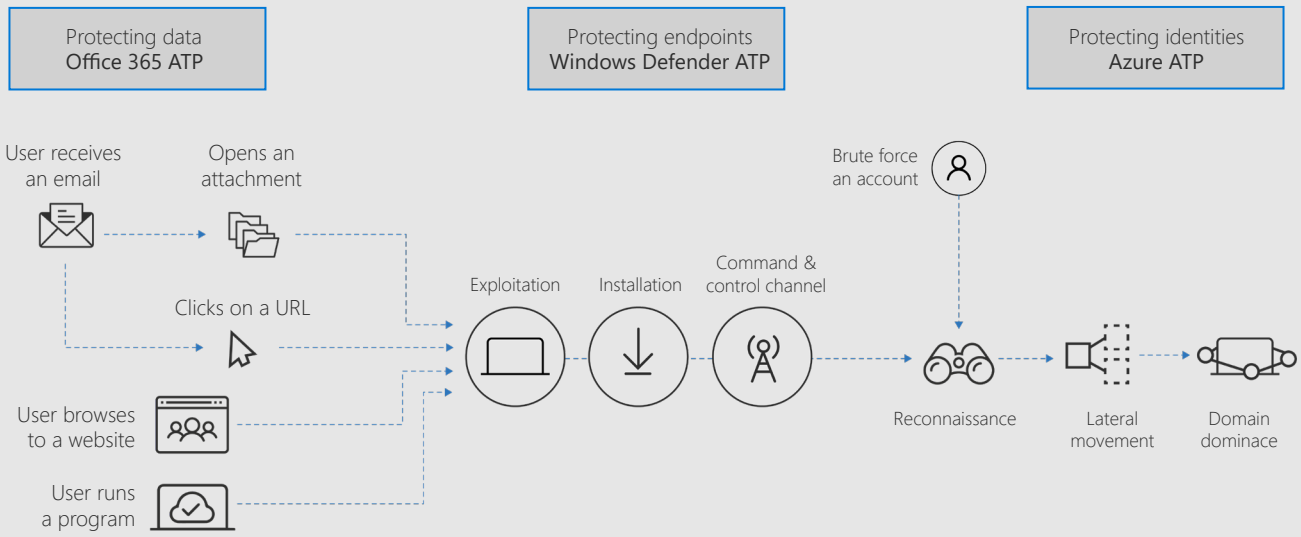

Figure 3. Integrated threat detection across Microsoft 365.

Deployment tips from our experts

Be proactive, not reactive

Proactively provisioning identities through Azure AD, enrolling devices through Intune, and setting up Intune App Protection for unenrolled devices can help keep your company's data safe by preventing threats or data breaches before they happen.

Keep your company data safe

Managing employee identities is a fundamental part of information security. Enable single sign-on and multifactor authentication, and set up conditional access policies. Then deploy Azure Information Protection for classification and protection of sensitive data.

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

ATSG