Protect your users and their identities

Introduction

Microsoft 365 security solutions help you protect users and corporate accounts. By making identity the control plane, the Microsoft 365 offerings manage identities as the first step to providing access to corporate resources and restricting users who are high risk. Help secure access with tools like single sign-on (SSO), multi-factor authentication (MFA), and the security built into Windows 10. Additionally, there are actions you can take if an identity is compromised and ways to lock down or wipe devices to protect sensitive data in case of loss or theft. With the right security features you can empower your employees to work securely on different devices without infringing on their productivity.

How do I provide secure access for my users?

Microsoft Azure Active Directory (Azure AD)

Managing identities is the first step in protecting your environment. Provisioning user identities through Azure AD and connecting to your on-premises Active Directory allow you to centralize identities for each user across apps, groups, and devices. Azure AD allows you to set conditional access policies (see Figure 1) for users in your organization. Your conditional access policies can control how users access your cloud apps; for example, you can restrict access according to location.

Your first step is to implement recommended identity access policies to help you secure your hybrid or cloud environment.

Azure AD SSO and MFA

Managing access in Azure AD is the next step. Azure AD SSO lets you manage authentication across devices, cloud apps, and on-premises apps with one user sign-in. Once you enable SSO, your employees can access resources in real time on any device in addition to confidential or sensitive work documents away from the office. Next, deploy MFA in Azure AD to reauthenticate high-risk users, and take automated action to secure your network. Configuring password synchronization and self-service password reset allows your users to reset their passwords when they need to and takes the burden off IT.

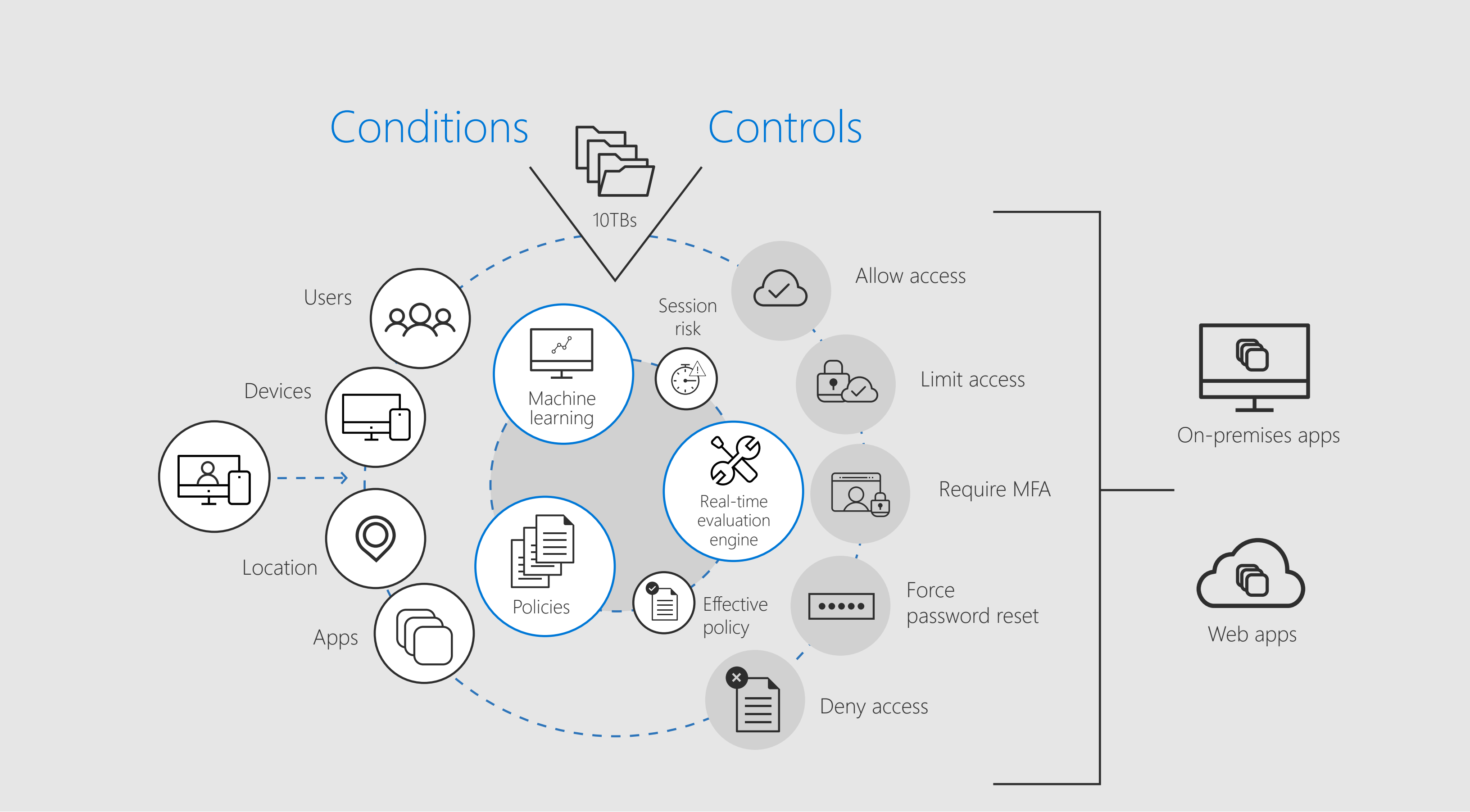

Figure 1. Set user policies using Azure AD Conditional Access.

Windows Hello for Business

Windows Hello for Business is a security feature that allows your employees to use the camera, a PIN, or their fingerprint to unlock their device. Enabling Windows Hello makes signing in faster and safer, and it works with numerous compatible apps. To deploy Windows Hello for Business, you must have:

- A well-connected, working network.
- Multi-factor Authentication Service, such as Azure MFA, to support MFA during Windows Hello for Business provisioning.
- Proper name resolution for both internal and external names.
- On-premises Active Directory and an adequate number of domain controllers per site to support authentication.
- On-premises Active Directory Certificate Services 2012 or later.
- One or more workstation computers running Windows 10, version 1703, or later.

Windows Hello for Business can be deployed in a hybrid or on-premises environment, and operates under the following trust models: hybrid Key trust or hybrid certificate trust; on-premises key trust or on-premises certificate trust.

How do I ensure that my employees' credentials are not compromised?

Azure AD Identity Protection

Managing identities is the first step toward protecting your employees' credentials. 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. Azure AD Identity Protection helps you identify the risk level of a user. Through Azure AD Identity Protection, 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 that you can apply to your organization. You can enable Azure AD Identity Protection through the Azure portal.

Windows Defender Credential Guard

Windows Defender Credential Guard helps protect against attackers by invoking the highest level of operating system privilege, so they are unable to steal Azure AD SSO credentials Windows Defender Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Windows Defender Credential Guard prevents these attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials. You must have Secure Boot enabled on any Windows 10 device to configure Windows Defender Credential Guard. You can enable Windows Defender Credential Guard on every device using a group policy a mobile device manager, such as Microsoft Intune.

Azure AD Privileged Identity Management (Azure AD PIM)

Azure AD PIM lets you monitor access to resources within your organization and recommends mitigation strategies so that you can minimize and manage the number of people who have access to secure information or resources. Continuously monitoring these high access points limits vulnerabilities. You can configure Azure AD PIM in the Azure portal to generate alerts when there's suspicious or unsafe activity in your environment and then recommend mitigation strategies.

Vulnerabilities identified and reported by Azure AD Identity Protection include risks such as multi-factor authentication registration not configured, unmanaged cloud apps, security alerts from Azure AD PIM, roles that are assigned outside of Azure AD PIM or that are activated too frequently. Address these vulnerabilities to improve the security posture of your organization and prevent attackers from exploiting them.

How can I protect my employees' information if they lose their device?

Whether your employees use a personal or company-owned device, you can take steps to mitigate information leaks in case of loss or theft. Microsoft 365 offers you the opportunity to do either a full or selective device wipe, depending on how your employees' devices are managed.

Microsoft Intune

Microsoft Intune lets you manage company-owned and employee-owned devices, regardless of the operating system, from the cloud through Azure AD. Intune allows you to designate user groups and apply appropriate settings and policies for each group according to device or application. When settings are applied to a group of devices, users are affected when they access a device from that group. Likewise, if a setting is applied to a group of users, the device settings apply to all devices in that group. When settings aren't configured, users can define the settings on their devices themselves.

With Intune mobile device management (MDM), you can add users to groups, apply different settings to each group, deploy and add apps to enrolled or unenrolled devices, apply device restrictions, manage device settings, and configure app protection policies. Through device group mapping, you can use Intune device categories to automatically add devices to groups, using categories that you define, to make it easier for you to manage those devices.

If your employees bring their own devices (BYOD) to work, you can manage your business apps on their devices with Intune App Protection policies.

You can set up Intune in the Azure portal in the Monitoring + Management section. After you've added users to your Intune subscription, you can designate a variety of admin permissions. You must assign an Intune license to each user. Once your employees are added, they can enroll their devices.

Intune App Protection

Intune App Protection enables you to selectively wipe data from managed apps. Selective wipe is helpful if an employee leaves your company; you can wipe company data but leave the rest of the employee device intact. To selectively wipe a device under Intune management, sign in to the Azure portal, search for Intune, select mobile apps from the Intune blade, and then choose App selective wipe. You can then select the user whose data needs to be wiped.

If your employee uses a company-owned device, you can manage that device with mobile device management (MDM) in Intune or through Microsoft Office 365. 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.

You may need to remove a device from Azure AD if that device will no longer be part of your company ecosystem.

Intune offers you the choice of managing corporate data for mobile devices on the app level through Intune App Protection; managing devices with a third-party management solution plus Intune App Protection; or managing devices fully from Intune using MDM and Intune App Protection policies.

Deployment tips from the experts

Start by managing user identities as your control plane

Provision your user identities through Azure AD and use Azure AD Connect to integrate identities across Azure AD and your on-premises Active Directory. Enable Multi-Factor Identification for all administrators, set conditional access policies, and initiate SSO.

Manage your devices from the cloud

Managing employee devices remotely engenders productivity and bolsters security. Deploy Intune as your mobile device manager for company and employee-owned devices.

Protect your operating system

Enable Windows Hello on your Windows 10 devices to protect your users' accounts.

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