

Zero Trust identity and device protection for Microsoft 365

Recommended Zero Trust capabilities for protecting identities and devices that access Microsoft 365, other SaaS services, and on-premises applications published with Azure Active Directory (Azure AD) Application Proxy

See more architecture resources like this at aka.ms/cloudarch

Three tiers of protection for data, identities, and devices

Microsoft provides many protection capabilities across our cloud services. We know it can be challenging to choose the right set of capabilities for your organization.

This document recommends the most common capabilities for Zero Trust protection to secure your data, identities, and devices.

Capabilities are recommended in three tiers — starting point protection, enterprise protection, and specialized security protection for environments with highly regulated or classified data.

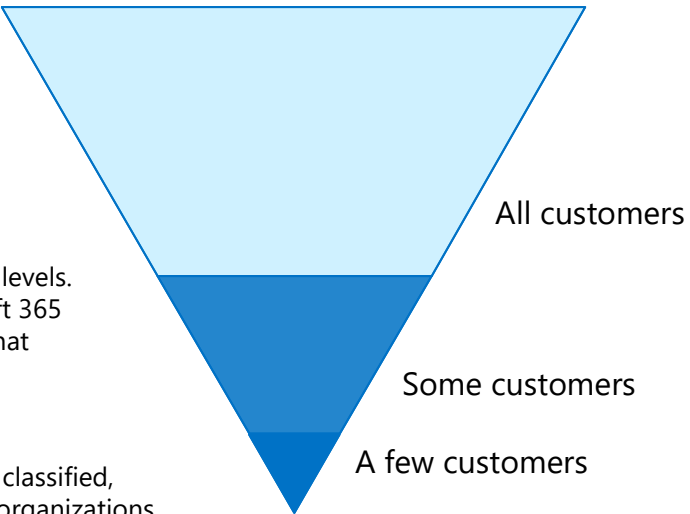
It's important to use consistent levels of protection across your data, identities, and devices. For example, if you protect sensitive data at a higher level, be sure to protect the identities and devices that access this data at a comparable level. This document shows you which capabilities are comparable.

- 1

Starting point protection
Microsoft recommends you establish a minimum standard for protecting data, as well as the identities and devices that access your data. Microsoft provides strong default protection that meets the needs of many organizations. Some organizations require additional capabilities to meet their starting point requirements.
- 2

Enterprise protection
Some customers have a subset of data that must be protected at higher levels. You can apply increased protection to specific data sets in your Microsoft 365 environment. Microsoft recommends protecting identities and devices that access sensitive data with comparable levels of security.
- 3

Specialized security protection
Some organizations may have a very small amount of data that is highly classified, trade secret, or highly regulated. Microsoft provides capabilities to help organizations meet these requirements, including added protection for identities and devices.

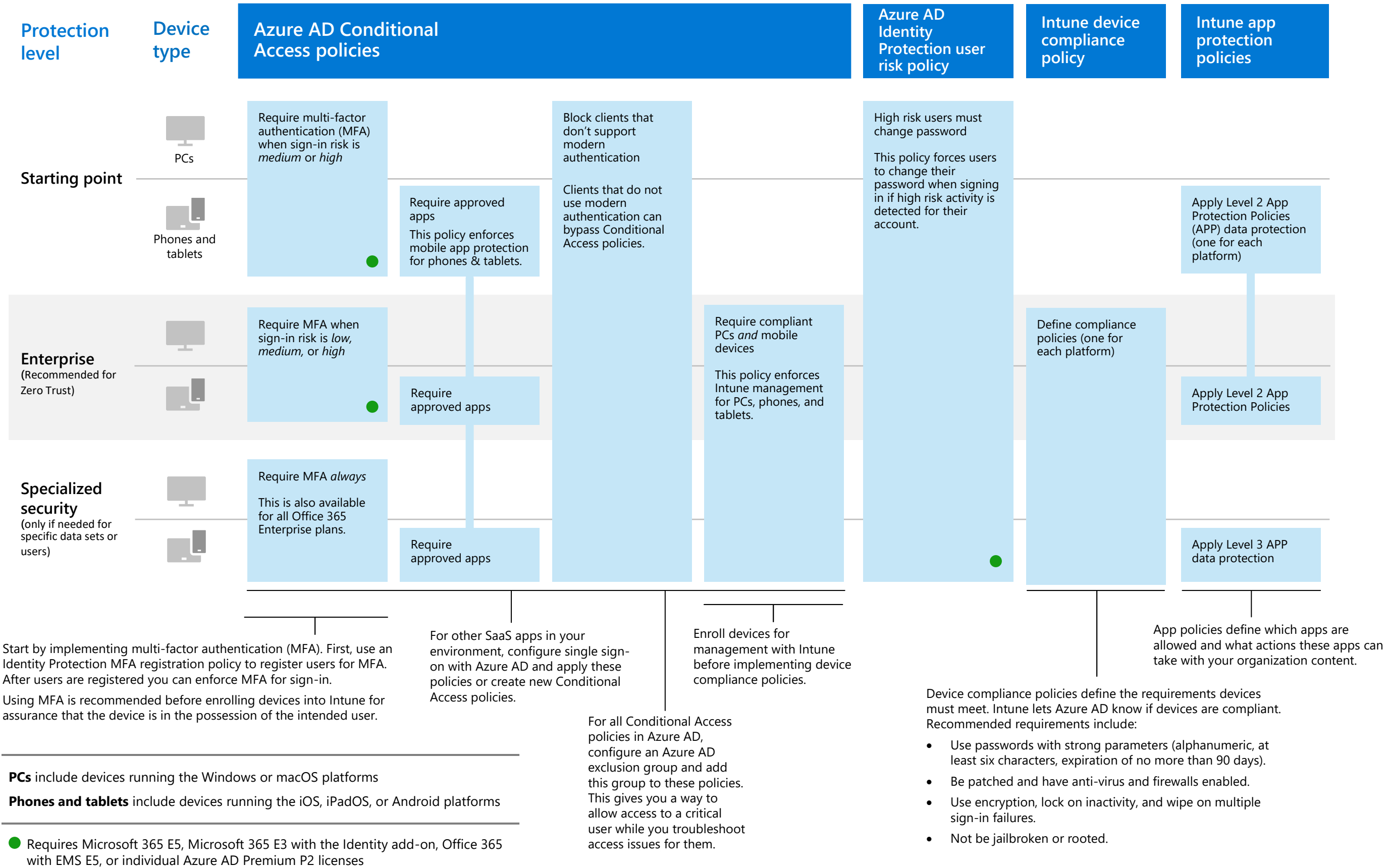


Summary of capabilities

	Starting point protection	Enterprise data protection	Specialized security data protection
Data protection See Deploy information protection for data privacy regulations for more information about these capabilities.	<div>Default file encryption</div> <div>Permissions for SharePoint and OneDrive libraries</div> <div>External sharing policies</div> <div>Device access policies for SharePoint and OneDrive</div>	<div>Classification, labeling, and protection</div> <div>Data Loss Prevention (DLP) in Microsoft 365</div> <div>Microsoft 365 service encryption with Customer Key</div> <div>Bitlocker for Windows 11 or Windows 10 and Windows Information Protection (WIP) for Windows 10</div>	<div>Bring Your Own Key (BYOK) with Azure Information Protection and SharePoint</div> <div>Hold Your Own Key (HYOK) with Active Directory Rights Management Service and SharePoint</div>
Identity and device protection Identity and device capabilities work together to secure access to your data. This document includes more information about these capabilities plus additional recommendations.	<div>Intune device management of PCs</div>	<div>Mobile apps protection</div> <div>Intune device management of PCs and phones/tablets</div> <div>Azure Multi-Factor Authentication</div> <div>Azure AD Conditional Access</div> <div>Azure AD Identity Protection</div> <div>Microsoft Cloud App Security</div> <div>Azure AD Privileged Identity Management</div>	

Recommended policies for starting point, enterprise, and specialized security protection

This page illustrates a set of policies Microsoft recommends for achieving protection at the three tiers. For help implementing these policies, including policies for protecting Teams, Exchange email, and SharePoint sites, see [Zero Trust identity and device access configurations](#).



Additional capabilities for starting point protection

These recommendations and capabilities increase the starting point level of protection across your environment.

Protect identities

<p>Follow Microsoft’s recommended guidelines for passwords</p> <p>The Microsoft Password Guidance paper provides recommendations for password management based on current research and lessons from Microsoft’s experience as one of the largest Identity Providers (IdPs) in the world.</p> <ul style="list-style-type: none">• Maintain an 8-character minimum length requirement (and longer is not necessarily better).• Eliminate character-composition requirements.• Eliminate mandatory periodic password resets for user accounts.• Ban common passwords, to keep the most vulnerable passwords out of your system.• Educate your users not to re-use their password for non-work-related purposes.• Combine these guidelines with MFA registration and risk-based challenges.	<p>Use Azure AD password protection on premises</p> <p>Eliminate weak passwords on premises by monitoring for banned passwords. Eliminate weak passwords on-premises</p> <p>Enable Azure AD Identity Protection policies for your users</p> <p>Enable Identity Protection to see the user and sign in risk of logins. Even without enabling policies, you will gain insights from the signals. Azure AD Identity Protection</p> <p>Protect admin accounts with PIM and privileged access management</p> <p>Azure AD Privileged Identity Management Privileged access management in Microsoft 365</p>	<p>Manage the user lifecycle holistically</p> <p>Remove manual steps from your employee account lifecycle everywhere you can to prevent unauthorized access:</p> <ul style="list-style-type: none">• Synchronize identities from your source of truth (HR System) to Azure AD.• Use Dynamic Groups to automatically assign users to groups based on their attributes from HR (or your source of truth), such as department, title, region, and other attributes.• Use group-based licensing to assign services to your users automatically as soon as they arrive in the cloud.• Use group-based access management/provisioning to automatically provision users for SaaS applications. <p>Manage access to resources with Azure AD groups Microsoft Azure AD licensing</p>	<p>Enable self-service password reset</p> <p>Allow your users to reset their passwords, with no administrator intervention, when and where they need to. Self-service password reset Password writeback to on-premises directories</p> <p>Migrate your external accounts to Azure AD B2B collaboration</p> <p>External accounts on premises are a threat that you can mitigate by moving the accounts to Azure AD B2B collaboration. Azure AD B2B Collaboration enables secure collaborate between business-to-business partners. Any accounts that are needed for SaaS application access or SharePoint collaboration can be moved to Azure AD B2B. Azure AD B2B collaboration</p>	<p>Implement Azure AD Connect Health</p> <p>Monitor and gain insight into your on-premises identity infrastructure and the synchronization services with Azure AD Connect Health.</p> <p>This enables you to maintain a reliable connection to Microsoft 365 by providing monitoring capabilities for your key identity components such as Azure AD Connect servers, Active Directory Domain Services (AD DS) domain controllers, and Active Directory Federation Services (AD FS) servers.</p> <p>It also makes the key data points about these components easily accessible, making it easy to get usage and other important insights to take informed decisions. Azure AD Connect Health</p>
---	---	---	---	--

Protect devices

<p>Configure basic password policies for mobile device access to Outlook Web Access (OWA)</p> <p>Configure basic password policies for Outlook Web Access (OWA).</p> <p>If you implement password policies using Intune later, these settings are disregarded. Intune password policies require device enrollment. Mobile device mailbox policies in Exchange Online</p>	<p>Use Intune to manage applications on mobile devices</p> <p>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. Intune app protection policies</p>	<p>Use Azure AD Join with Windows 11 or Windows 10 devices</p> <p>Azure AD offers a simplified joining experience, efficient device management, automatic mobile device management enrollment, and single sign-on capability for Azure AD and on-premises resources. An incremental step in this direction is to auto-Azure-AD join your on-premises joined Windows 11 or Windows 10 devices. Extending cloud capabilities to Windows devices through Azure AD Join</p>	<p>Implement Windows 11 or Windows 10 native protection capabilities</p> <p>BitLocker — Use this on all PCs to encrypt all data at rest and protect it against offline attacks.</p> <p>Credential Guard — Prevents attacks by protecting NTLM password hashes and Kerberos Ticket Granting tickets.</p> <p>Device Guard — Prevents tampering by users or malware and only allows trusted applications. AppLocker can also be used.</p>	<p>Enable Windows Hello for Business on all Windows 11 or Windows 10 PCs</p> <p>Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. Windows Hello for Business</p>
---	--	--	--	--

Windows 11 or Windows 10 PCs

Additional capabilities for enterprise and specialized security data

You can greatly increase protection with the capabilities on this page.
Choose the ones that are best for your environment.

Enterprise protection

Protect identities

Increase protection with Azure AD Identity Protection policies for user accounts

For users who access highly regulated or classified data, use more risk-averse policies. For example, require MFA when sign in risk is low. Change risk access from high to medium or low.

Azure AD Identity Protection

Enable Azure AD Privileged Identity Management

Enable just-in-time Privileged Identity Management (PIM) for your privileged administrator accounts in the cloud. With PIM, your administrator accounts are not able to perform administrative actions until they request their role to be activated. Additionally, you can set parameters for a specific action. For example, you can require MFA, require them to fill out a service request number, or just notify other admins.

Azure AD Privileged Identity Management

Use Microsoft Cloud App Security

Microsoft Cloud App Security is a Cloud Access Security Broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Requires Microsoft 365 E5.

Microsoft Defender for Cloud Apps

Protection for specialized security data

Use Microsoft Cloud App Security with advanced policies

For highly regulated or classified data, implement more advanced policies to alert you and to take action on suspicious activity or leaked data.

Microsoft Defender for Cloud Apps

Increase protection with Azure AD Privileged Identity Management

For admins who work with services that host highly regulated or classified data, increase protection by requiring MFA on activation of their role. Also activate roles for shorter time windows.

Azure AD Privileged Identity Management

For an HYOK solution, add partner accounts to your on-premises directory

If you are using a Hold Your Own Key (HYOK) solution to protect data stored in SharePoint, add necessary partner accounts to your on-premises directory.

HYOK solutions for files stored in SharePoint require federated identity integration with Microsoft 365. These solutions do not work with synchronized identities.

Protect devices

Use device health attestation features with Windows 11 or Windows 10 devices

If you choose to enable "Windows Device Health Attestation" in a device compliance policy, create a separate policy. When you create the corresponding Conditional Access policy in Azure AD, configure the policy to apply only to the Windows platform. Use caution with this policy because it will deny access to Windows devices that do not support Device Health Attestation.

Use Windows Information Protection (WIP) to protect apps on Windows 10 devices

WIP allows you to protect data within Intune-managed applications.

Create a WIP policy using Microsoft Intune

Deploy a third party, real-time threat detection solution for non-Windows devices

Windows 11 or Windows 10 PCs