

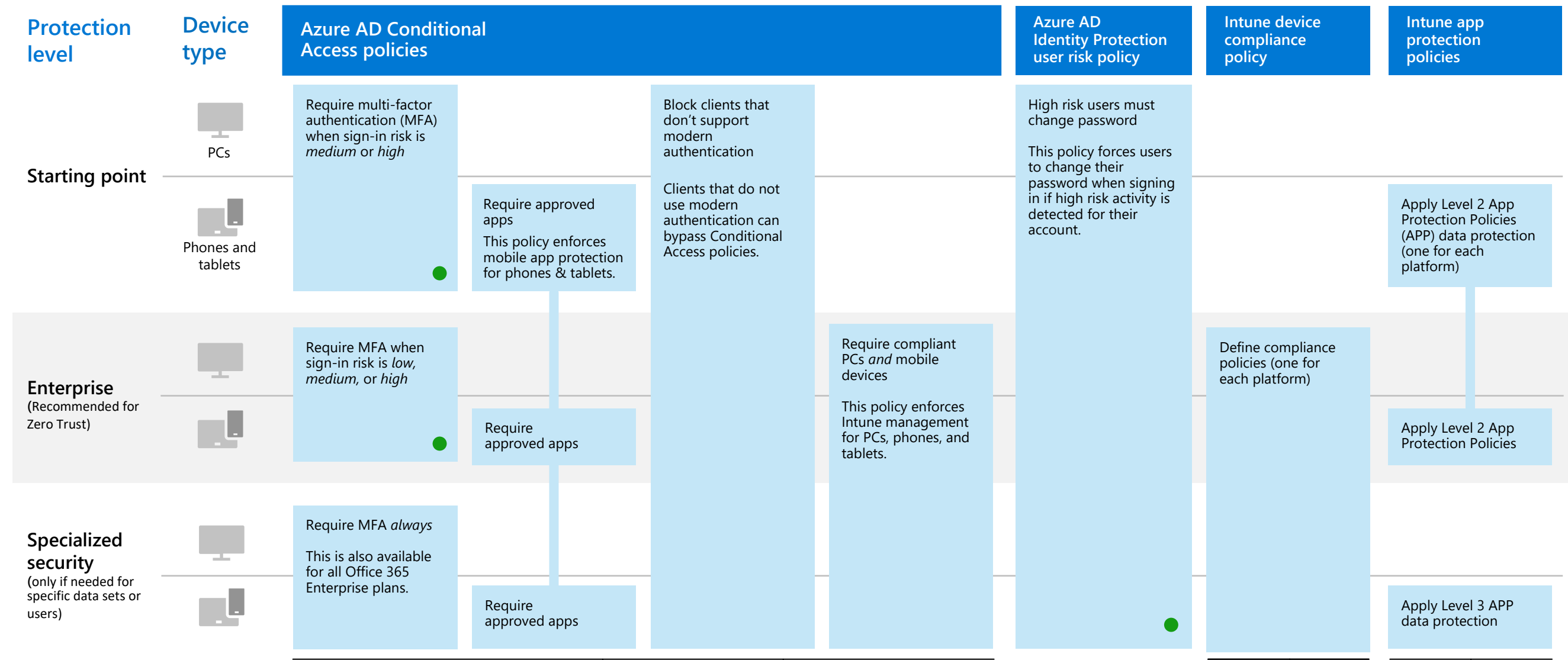
Zero Trust identity and device access policies for starting point, enterprise, and specialized security protection

Identity and device access policies ensure that only approved users and devices can access your critical apps and data.

Starting point protection is a minimum level of security for your identities and devices that access your apps and data.

Enterprise protection provides additional security for specific data. Identities and devices are subject to higher levels of security and device health requirements.

Specialized protection is for typically small amounts of data that is highly classified, contain trade secrets, or is subject to data regulations. Identities and devices are subject to much higher levels of security and device health requirements.



For help implementing these policies, including policies for protecting Teams, Exchange email, and SharePoint sites, see [Zero Trust identity and device access configurations](#).

Start by implementing multi-factor authentication (MFA). First, use an Identity Protection MFA registration policy to register users for MFA. After users are registered you can enforce MFA for sign-in.

Using MFA is recommended before enrolling devices into Intune for assurance that the device is in the possession of the intended user.

PCs include devices running the Windows or macOS platforms

Phones and tablets include devices running the iOS, iPadOS, or Android platforms

● Requires Microsoft 365 E5, Microsoft 365 E3 with the Identity add-on, Office 365 with EMS E5, or individual Azure AD Premium P2 licenses

For other SaaS apps in your environment, configure single sign-on with Azure AD and apply these policies or create new Conditional Access policies.

For all Conditional Access policies in Azure AD, configure an Azure AD exclusion group and add this group to these policies. This gives you a way to allow access to a critical user while you troubleshoot access issues for them.

Enroll devices for management with Intune before implementing device compliance policies.

Device compliance policies define the requirements devices must meet. Intune lets Azure AD know if devices are compliant. Recommended requirements include:

- Use passwords with strong parameters (alphanumeric, at least six characters, expiration of no more than 90 days).
- Be patched and have anti-virus and firewalls enabled.
- Use encryption, lock on inactivity, and wipe on multiple sign-in failures.
- Not be jailbroken or rooted.

App policies define which apps are allowed and what actions these apps can take with your organization content.