Microsoft

Quick start guide to secure remote work with Azure Active Directory

A business's ability to engage in remote work capabilities has gone from a benefit to a necessity, taking center stage in an organization's digital transformation plan. Enabling employees to work remotely has become the only way for many businesses to keep their workforce, partners, and communities safe and running smoothly.

However, while enabling remote work is a priority, the security of devices, users, and applications remains important. As more employees access apps via their home networks, the corporate network perimeter has truly disappeared, making identity the control plane for effective and secure access across all users and resources.

Azure Active Directory (Azure AD) has rapidly become the identity control plane of choice for secure remote work managing more than 345 million monthly active users, with 200,000 customers and 30 billion daily authentication requests. By enabling secure access to cloud apps, as well as on-premises apps, from personal devices and remote locations, Azure AD supports your organization's journey to productive remote work.

Here are five steps you can take today to secure your remote workforce while helping them stay productive.

- □ Connect your apps to one identity solution ›
- □ Simplify end-user experiences with single sign-on (SSO) ›
- □ Securely collaborate with external partners ›
- □ Stay secure by enabling strong authentication ›
- □ Save time by empowering your end users ›

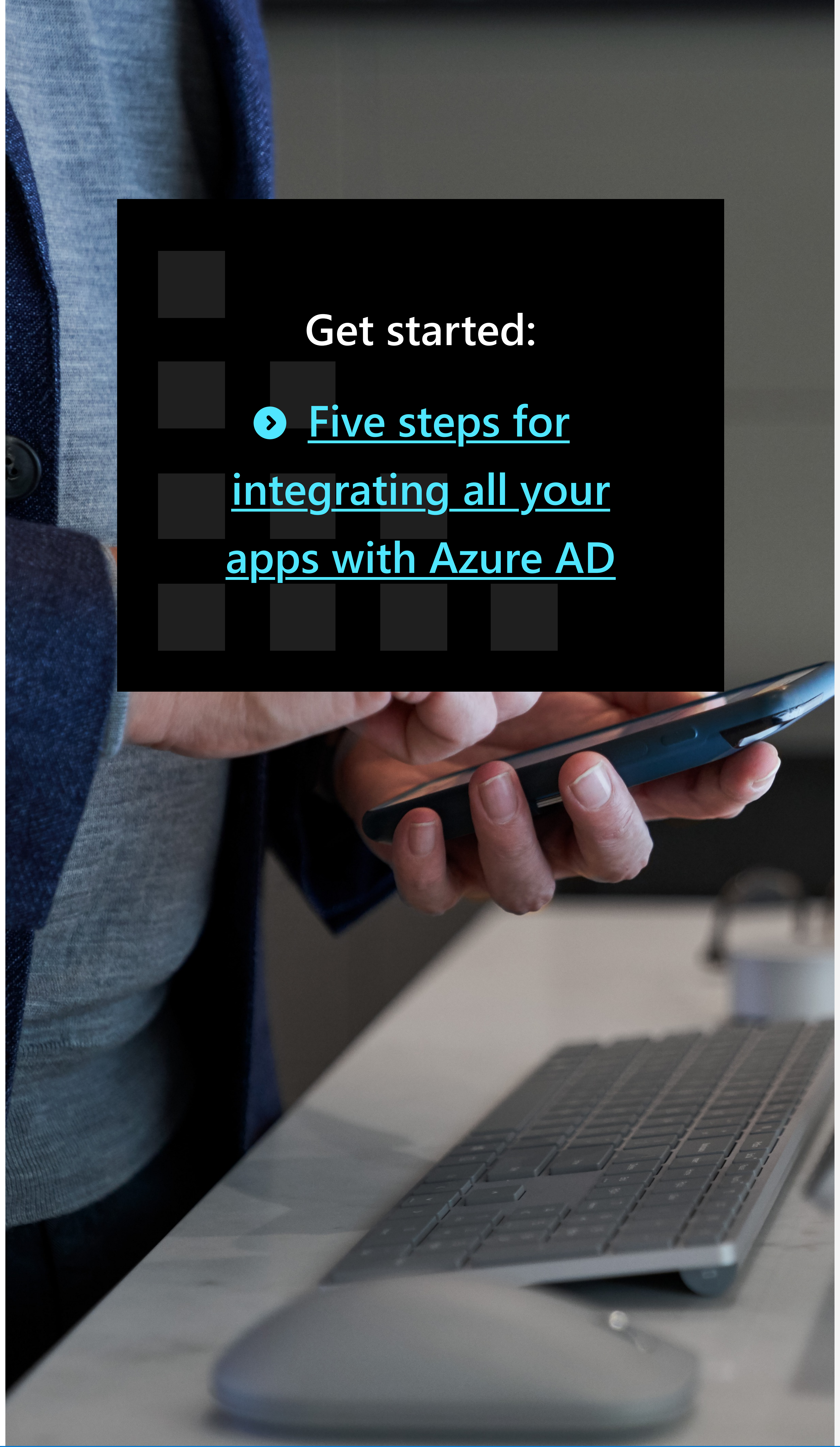
The #1 challenge reported by security leaders is providing secure remote access to resources, apps, and data.

Microsoft Security

#1 Connect your apps to one identity solution

One of the challenges of remote work is ensuring that employees can access all the applications they need to do their best work. That means employees need secure access to collaboration apps, productivity apps, and mission-critical apps on-premises.

By connecting all applications with Azure AD, you can streamline application management and ensure your workforce can seamlessly access the apps they need. You can also reduce costs by centralizing application management to a single identity solution.



Get started:

[Five steps for integrating all your apps with Azure AD](#)

Get started with the following apps available in the:

[Azure AD App Gallery](#)

Communication

Cisco Webex Workplace zoom

Document Collaboration:

box DocuSign

Security:

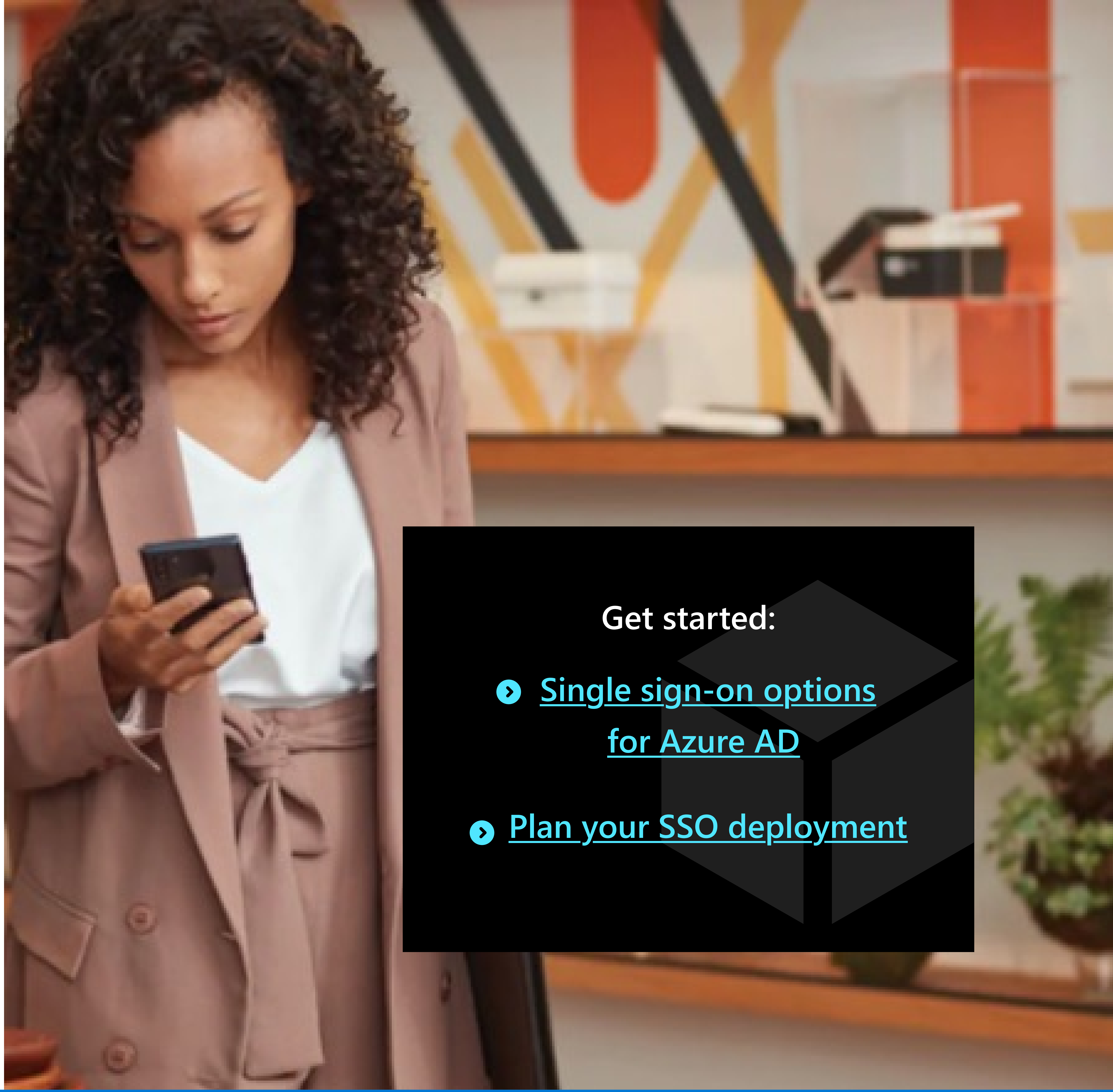
f5

#2 Simplify end-user experiences with single sign-on (SSO)

Having different identity systems, logins and passwords for every application can hurt employee productivity. Employees need to be able to seamlessly access all the apps they need quickly and securely.

With single sign on, employees gain access to all their critical apps without the complexity of multiple passwords or verifications for each application.

Single sign-on can help save people’s valuable time. *Forrester estimates that consolidating to a single identity and access management solution and providing one set of credentials can save each employee 10 minutes a week on average.



Get started:

- Single sign-on options for Azure AD
- Plan your SSO deployment

* *The Total Economic Impact™ Of Securing Apps With Microsoft Azure Active Directory, a commissioned study conducted by Forrester Consulting, August 2020*

#3 Securely collaborate with external partners

Today organizations must be able to collaborate across the boundaries of their business. As organizations increasingly rely on collaboration with external teams, they need an identity approach that enables experiences that protect the organization’s assets.

With Azure AD, simplify collaboration with external parties, such as distributors and suppliers, enabling employees to grant external access to resources and allowing business partners to submit access requests.

Set up external access:

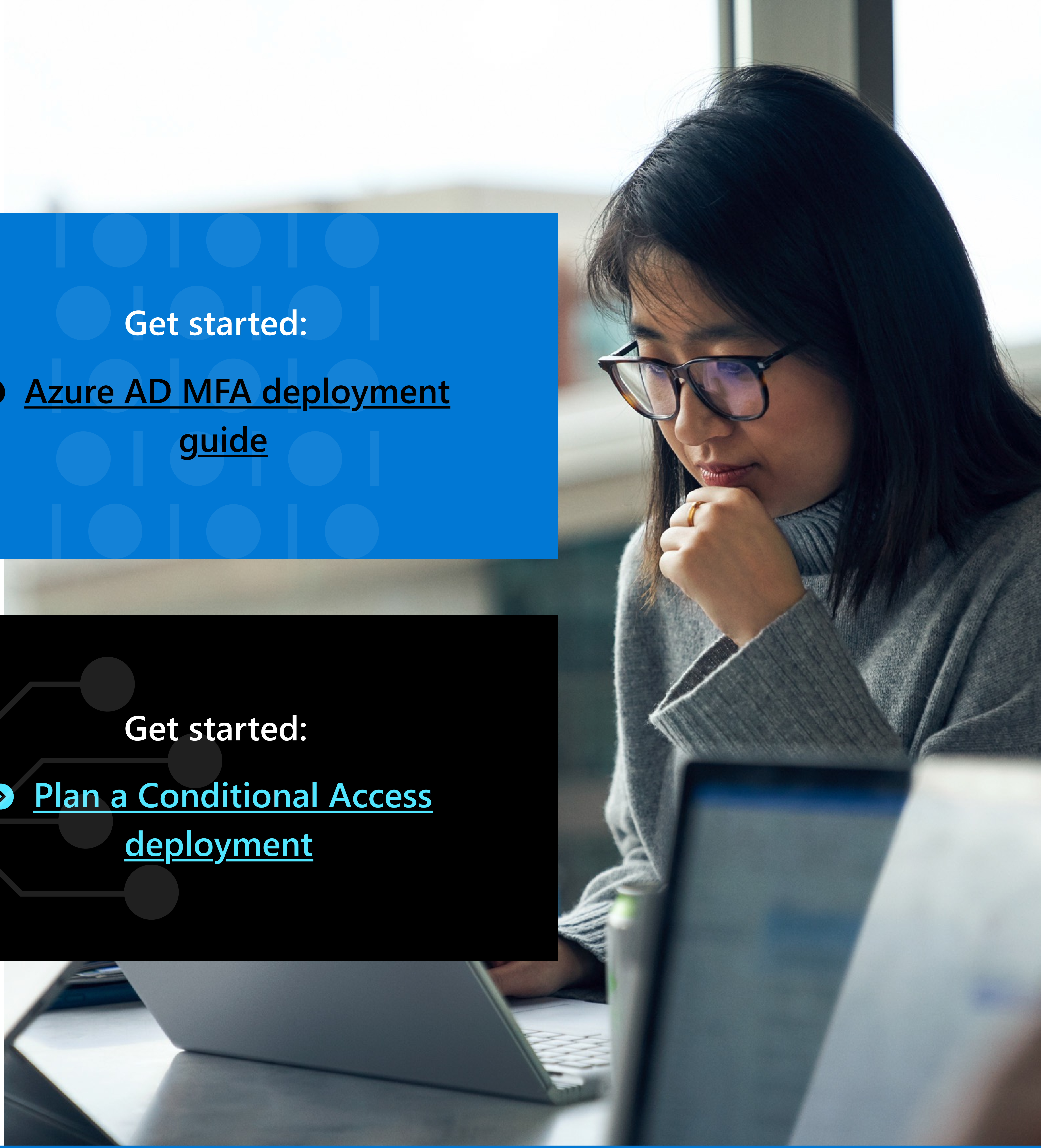
- B2B collaboration in Azure AD

#4 Stay secure by enabling strong authentication

If your business only uses passwords to authenticate employees, it can leave your organization vulnerable to bad actors. To keep your business secure, you'll want to turn on Multi-Factor Authentication (MFA). MFA can block over 99.9 percent of account compromise attacks.

MFA increases account security by requiring multiple verification methods to prove one's identity when signing into an application. Enabling MFA can help ensure your accounts are less likely to be compromised.

To further strengthen your security posture, Azure AD Conditional Access can provide adaptive access policies based on user context, device, location, and session risk information. With Conditional Access, you can define the specific conditions for how employees authenticate and gain access to your apps and data.

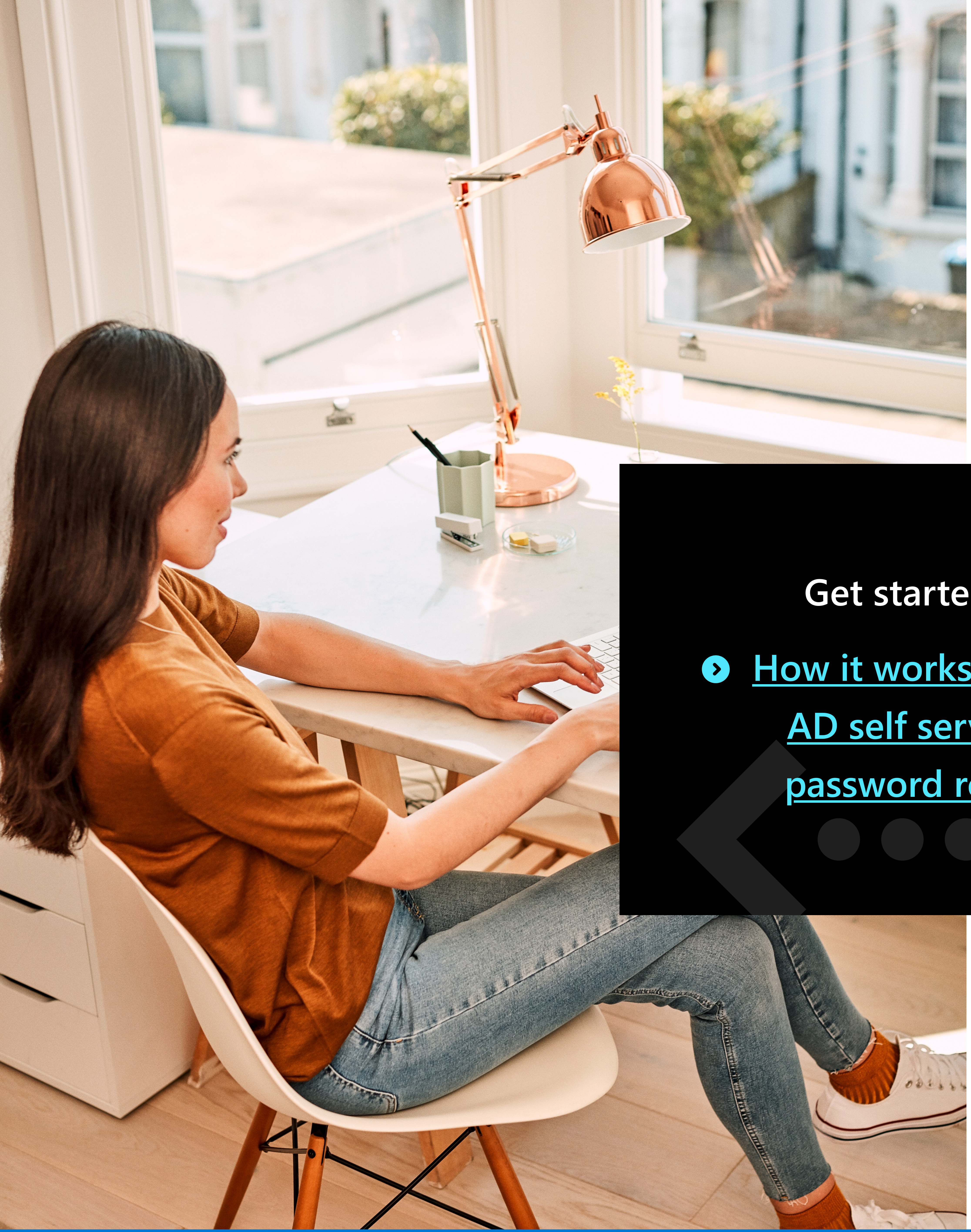


Get started:

- Azure AD MFA deployment guide

Get started:

- Plan a Conditional Access deployment



#5 Save time by empowering your end users

If you have an IT help desk, your employees likely make thousands of password reset requests per month. Locked out users can't be productive, and help desk tickets take valuable time that could be spent on other priorities.

With self-service password reset, organizations can empower users to reset their passwords, reducing the number of password reset requests submitted to the help-desk.

In the Forrester study, The Total Economic Impact™ Of Securing Apps With Microsoft Azure Active Directory, participating organizations reduced their password reset calls by 75% by enabling self-service.

Get started:

- How it works: Azure AD self service password reset

Secure access to the apps you use today and the apps you'll need tomorrow with Azure Active Directory

Learn more at Microsoft.com/AzureAD

Microsoft