

Hybrid Identity

The First Step for Secure Digital Transformation

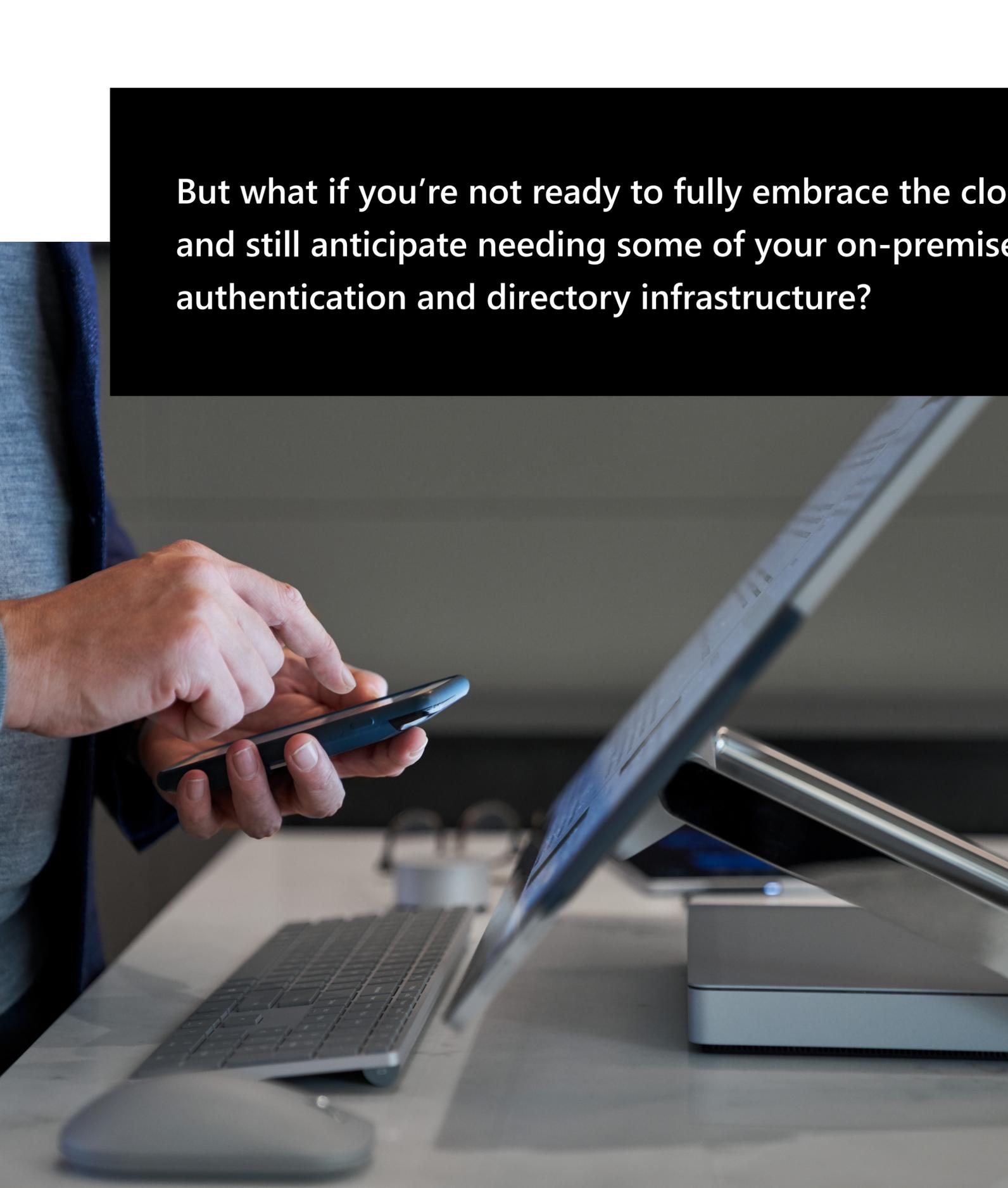


As **businesses** continue to scale their operations to meet the new challenges created by increased users and remote work, security remains a top priority. These modern organizations are finding their digital transformation journey starts with their identity and access management systems.

The mix of business users may include employees, partners, and contractors, all accessing more applications requiring seamless access from multiple devices. These days, the average large enterprise uses over 180 unique apps, many of them business critical. Add in the business need for users to work from anywhere, anytime, and it's easy to see why more companies are seeking to modernize the scalability of their identity solutions and, in turn, the security of their cloud, with identity as the new control plain and single source of truth for their business.

Moving to the cloud allows you to scale your identity management, but the ultimate payoff of modernizing is security for those identities, granting you connectivity across other security tools that work behind the scenes. Modernized security through the cloud by provides information protection, threat protection, and cloud app security with the bonus of cloud-driven machine learning to apply behavioral and risk-based analysis to adaptive access and authentication actions.



A person wearing a blue suit jacket is holding a smartphone in their hands. They are standing in front of a desk with a computer monitor and keyboard. The background is slightly blurred, showing a modern office environment.

But what if you're not ready to fully embrace the cloud and still anticipate needing some of your on-premises authentication and directory infrastructure?

Although many organizations are still making the transition from on-premises IT solutions to the cloud, leveraging your cloud IAM capabilities and reaping all the benefits of a cloud-based identity solution doesn't have to wait until you've fully transitioned. Today, you can begin the process of digital transformation by pursuing a hybrid identity, taking the first and most crucial step towards modernization, while still embracing a cloud-driven approach.

When using your apps in the cloud, you are using identity to authenticate and access them. From cloud apps, the public cloud, and IaaS, you need to make sure your authentication and access control to those endpoints are secure. Adopting an identity-first mindset and making identity the control plane in a modern world of multiple, inter-connected parameters gives you a single point of management cloud IAM can offer.



Digital Transformation through Hybrid Identity

A cloud approach is bridging a heterogeneous IT solution between public and private clouds. In an IAM context, hybrid identity in this scenario means that on-premise directories and cloud identity directories are working in harmony to ensure a common identity is provided to users to access the apps and data people use to get their work done, no matter where they are, anytime, anywhere. This identity data is synchronized between the hybrid directory infrastructure.

This emphasis on a hybrid identity allows you to reach a harmonious state with your directories and apps. Hybrid identity means you are seamlessly and consistently applying security protocols and decisions, supplying your user with a great experience that's easy to administer.



Why Hybrid Identity?



On-premises networks and onboarding to a coexistent (on-premises and cloud-based) approach. A single identity combined with single sign-on means that users only need to remember one password, and passwords your greatest weakness. 87% of security attacks exploit weak or reused passwords.

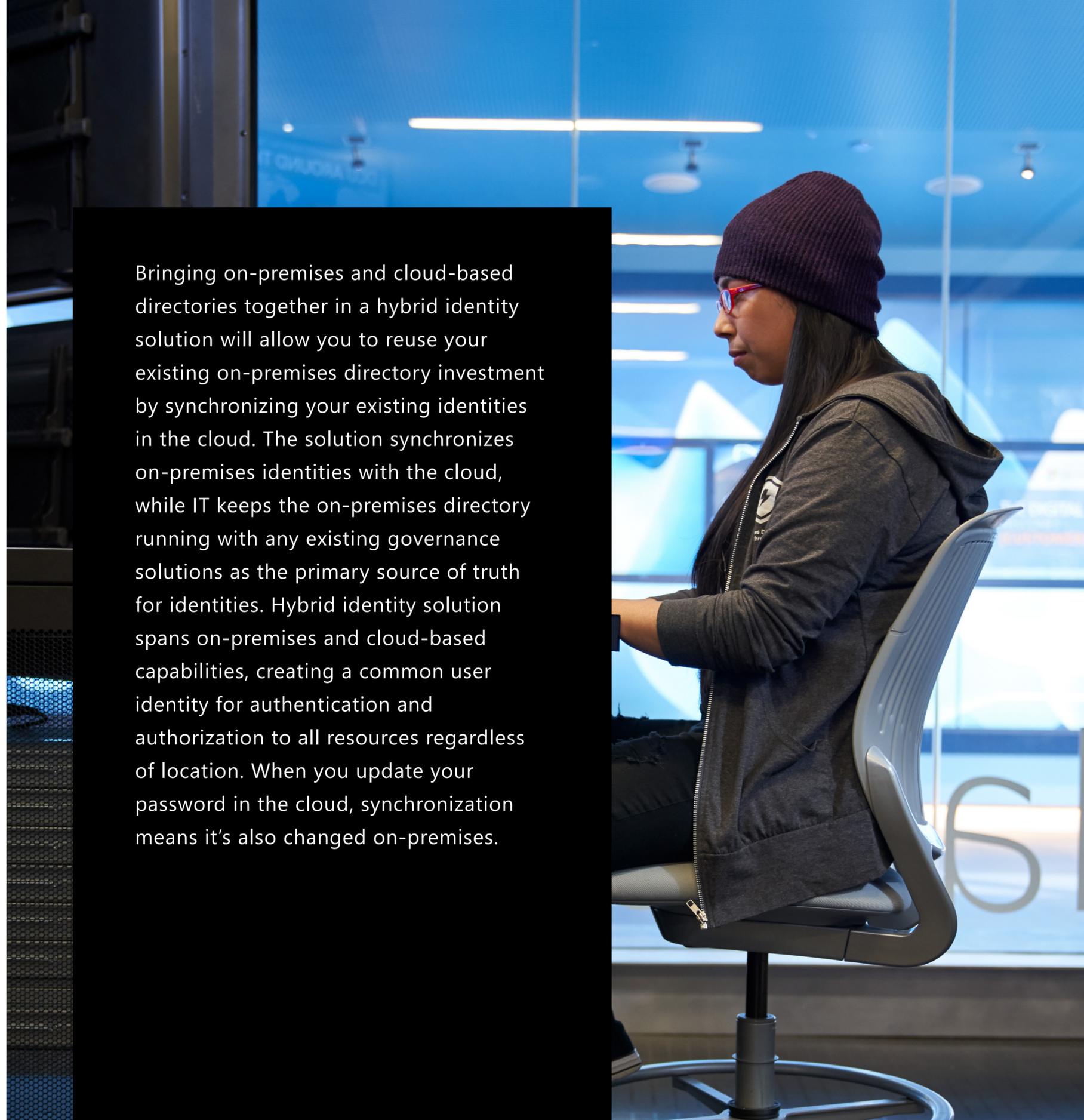


A hybrid approach allows for an accelerated transition to a more agile and efficient organization, enabling you to expand your on-premises IT systems to use more scalable, so if your on-premise system goes down, your cloud can be your reliable and secure source of authentication while keeping risks and costs down.



When an organization moves to the cloud using a hybrid approach, you can gradually de-commission your on-premise platform to match your modernization plan.

Bringing on-premises and cloud-based directories together in a hybrid identity solution will allow you to reuse your existing on-premises directory investment by synchronizing your existing identities in the cloud. The solution synchronizes on-premises identities with the cloud, while IT keeps the on-premises directory running with any existing governance solutions as the primary source of truth for identities. Hybrid identity solution spans on-premises and cloud-based capabilities, creating a common user identity for authentication and authorization to all resources regardless of location. When you update your password in the cloud, synchronization means it's also changed on-premises.

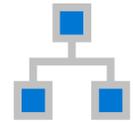


Why Microsoft Identity?

**> 95% of Fortune
500 companies**

are already using Microsoft on-premises Active Directory as their legacy identity data store and many of these organizations have started to embrace Azure Active Directory (Azure AD), Microsoft's cloud-based identity & access management solution in their hybrid identity journey. If you already have modernized your productivity solutions to Azure or Microsoft Office online services, you're already using Azure AD as your cloud identity solution.

With Azure AD, you can achieve a holistic and unified management of your identity & access management needs from the cloud through:



Connecting your entire workforce to all their apps and resources



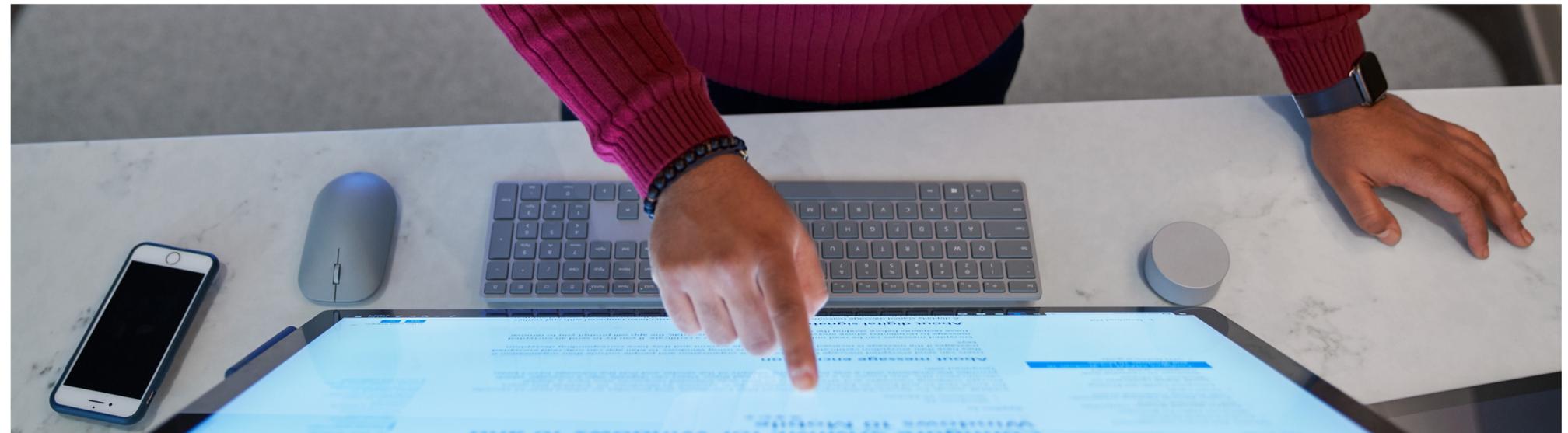
Protecting your users from identity attacks and governing their access



Collaborating with your entire identity ecosystem, including your business partners and customers



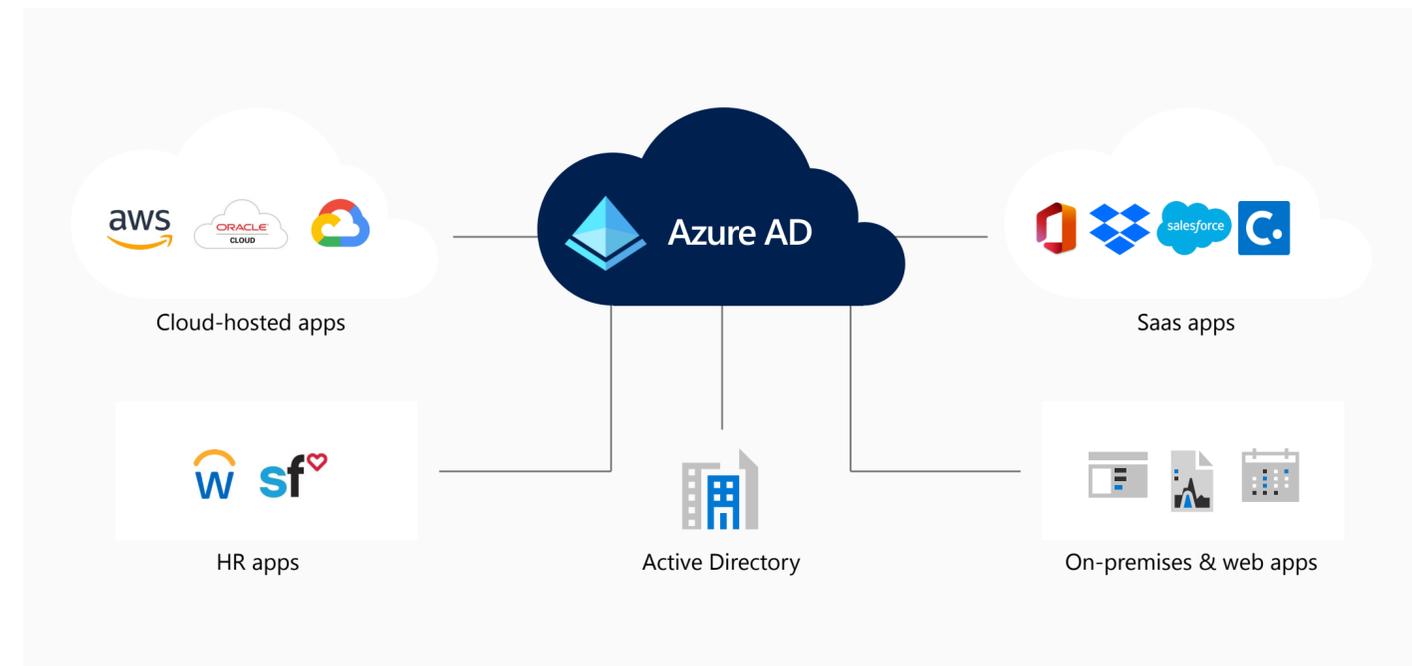
Developing applications to embrace strong authentication and open identity standards





Why Microsoft Identity?

Adopting an Azure Active Directory (AD) hybrid identity solution allows organizations to gain access to premium features that protect their users against cyberattacks and make them more productive through self-service features. Azure AD helps create and maintain the delicate balance between productivity and security with robust internal policies dictated by the level of depth to which you need your security settings applied. It will allow your workers to access company resources from wherever they need to do their work while allowing your team to govern that access and protect critical data and sensitive resources.



These measures ultimately help organizations be more agile and reduce their security risks when implementing the right Azure AD hybrid identity solution by providing centralized management-through multiple platforms.

A man with a beard and a bun, wearing a black hoodie, is standing at a desk in a modern office. He is looking at a computer monitor. The office is decorated with colorful bunting (red and yellow triangles) hanging from the ceiling. There are other people working at desks in the background. The lighting is warm and modern.

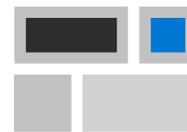
Benefits to a Hybrid Identity

Synchronize on-premises identity data to the cloud

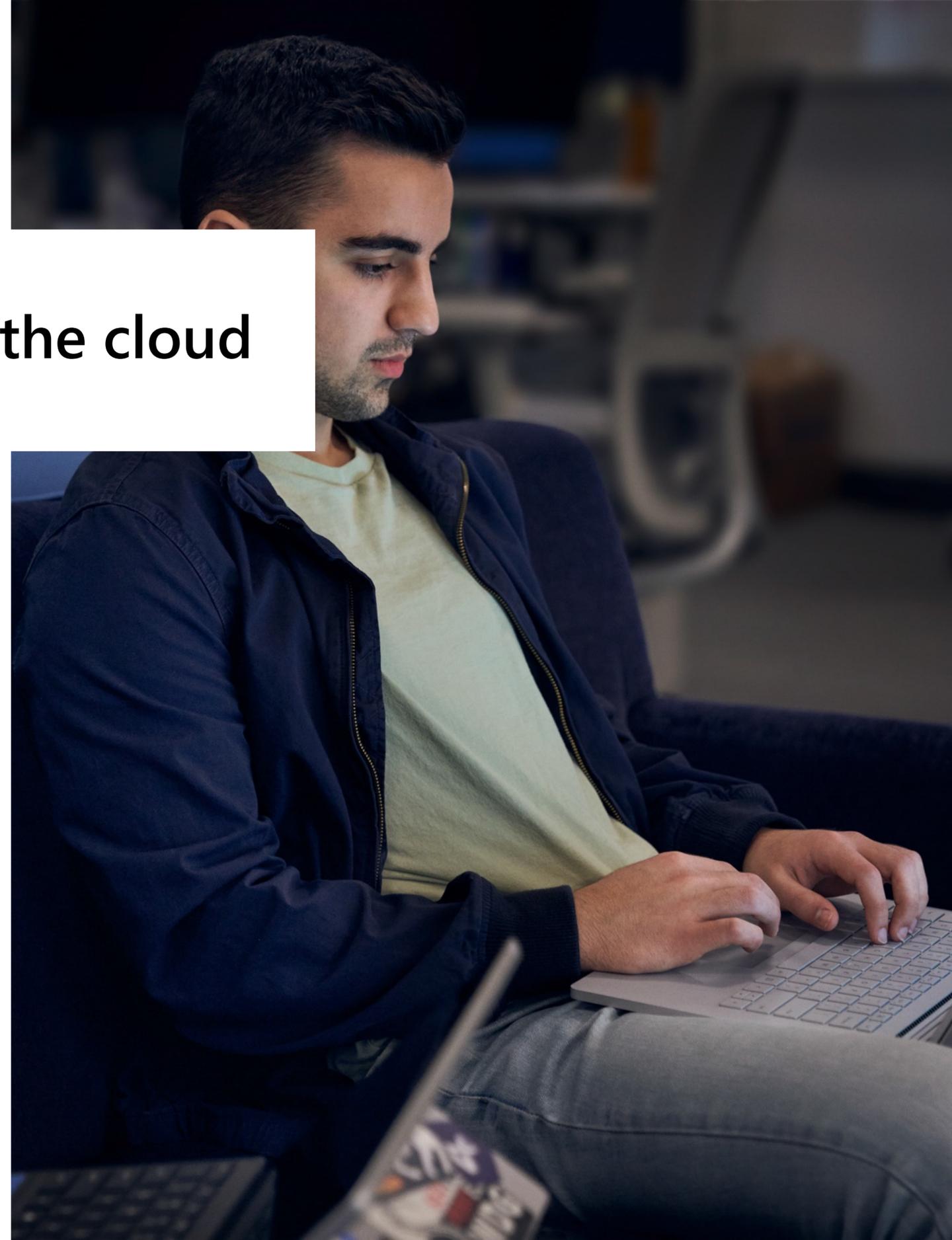
Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources with Azure AD Connect sync. Users and organizations can take advantage of:

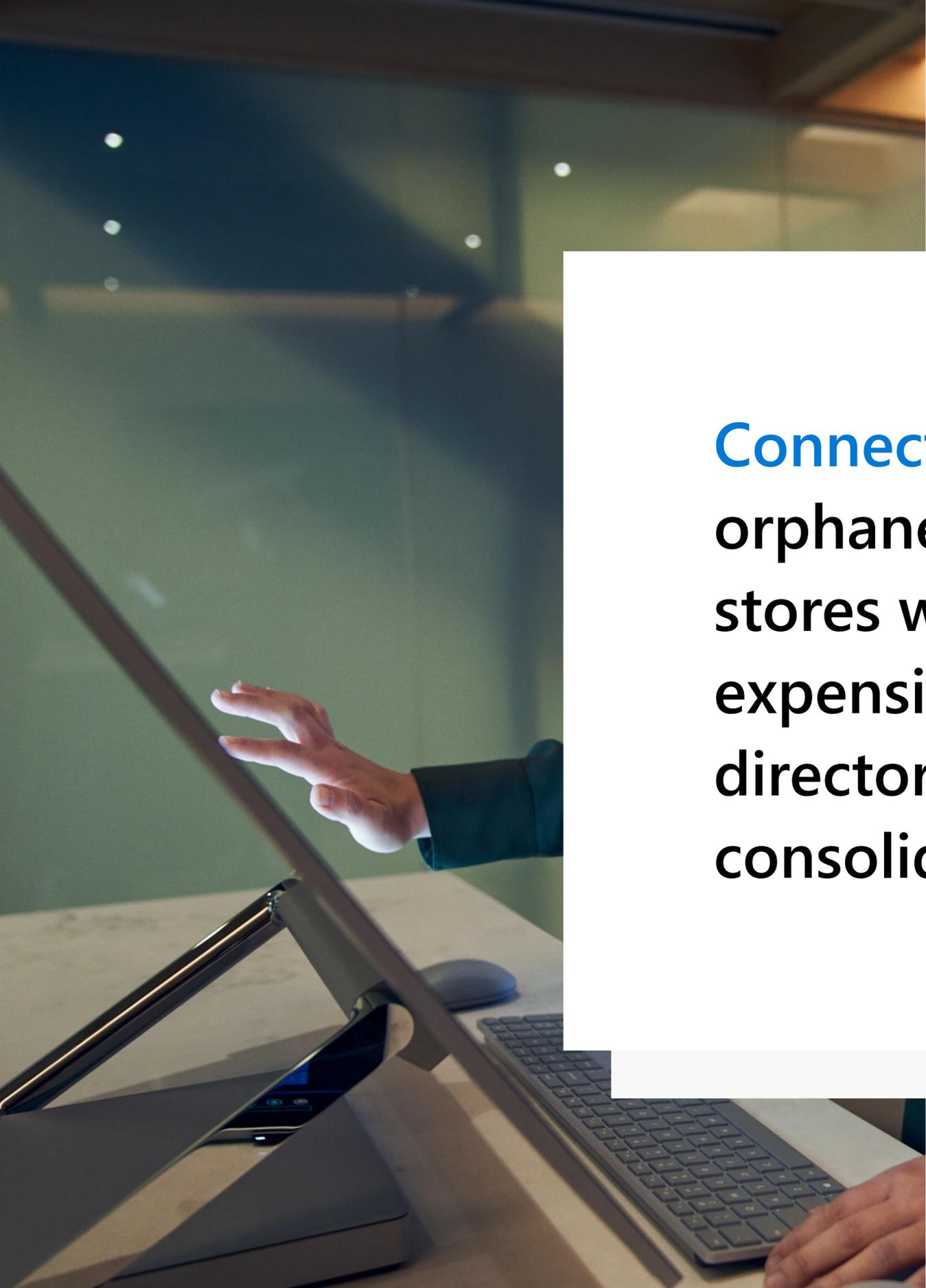


A single identity to access cloud applications like Concur, Salesforce, Box, or Office 365, on-premises applications hosted on your network, and cloud infrastructure such as AWS, Google Cloud, or Azure.



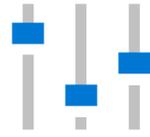
A single tool provides a smooth deployment experience for synchronization and sign-in for users in your primary AD forest.





Connect orphaned user stores without expensive directory consolidation

An orphaned directory store is a domain controller that has a server object in the configuration container but does not have a corresponding computer account in the domain controller organizational unit. Azure AD can help connect those orphaned directory stores by connecting lightweight connectors driven by the cloud with Azure AD Connect cloud provisioning, so users across directory boundaries can still collaborate and be productive.



Centralized hybrid infrastructure health monitoring

Azure AD Connect Health provides robust monitoring of your on-premises identity infrastructure. It enables you to maintain a reliable connection to Office 365 and Microsoft Online Services. This reliability is achieved by providing monitoring capabilities for your key identity components. Also, it makes the key data points about these components easily accessible.

Use the Azure AD Connect Health portal to view alerts, performance monitoring, usage analytics, and other information. Azure AD Connect Health enables the single lens of health for your key identity components in one place.

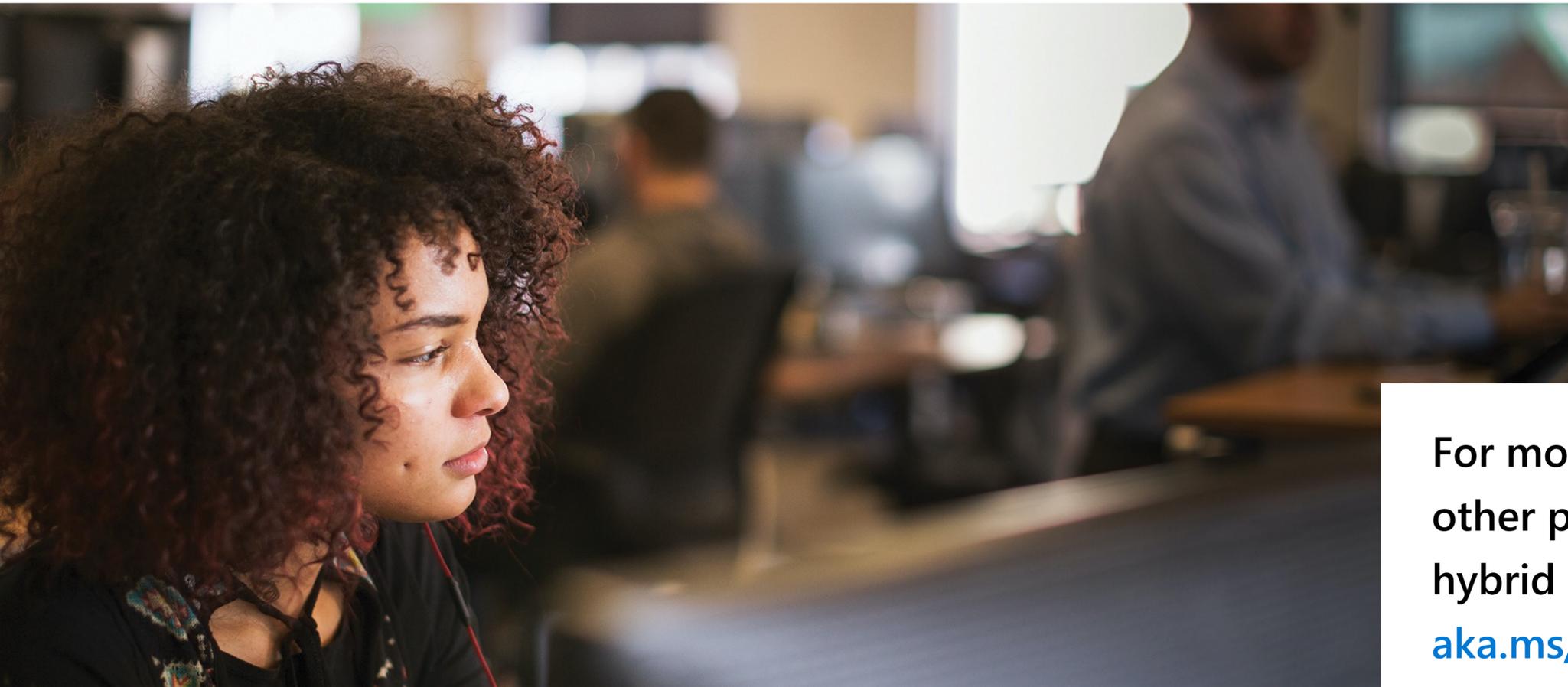


Inbound HR and user data from external data stores

Information used to support business intelligence and contribute to strategic planning can be derived from data both generated and held within organizations and from data generated and hosted by external data collectors and organizations. With a hybrid identity solution, you can ensure that inbound data is cleared through inbound provisioning, maintaining the high degree of security your business needs.



Next Steps



Now more than ever, moving to the cloud to manage your user identity is the path forward for any business that is seeking to modernize their digital transformation. The first step to the cloud is getting a hybrid solution in place. Once you have adopted a hybrid identity infrastructure, you are ready to embrace modern authentication to provide seamless, secure access to all of your resources.

For more information on **Azure AD Connect** and other products designed to make your move to hybrid identity smoothly, visit aka.ms/hybrididentity

