Microsoft

Empower your workforce and reduce IT friction with Azure Active Directory

In the current landscape, it is more important than ever for IT to meet user needs for seamless remote access while maintaining the security the business requires. A recent study by Microsoft revealed that through 2021, the single most important focus for identity decision makers is enabling highly productive end-user experiences.

Even before the recent shift to remote work, organizations were managing 180 unique applications on average while dealing with the push and pull of driving modernization and reducing friction versus establishing security policies robust enough to deal with advanced threats. But how do you accomplish those sometimes-competing goals of seamless access versus robust security, all while IT teams are trying to accomplish more with less? Although it may sound like increased security and great end user experiences are conflicting priorities, they don't have to be.

Azure Active Directory (Azure AD), Microsoft's cloud identity and access management solution, can not only meet your end-user needs to get work done and gain access to various apps and data, but it can also provide end-user self-service, thereby lightening the workload of your IT department. The efficiency and scalability of a universal control plane for unified access management means your IT department can focus on other business critical tasks instead of frustrated users and costly password reset calls.

Productivity

Grant one-click access to apps and data and help employees discover all the apps they need via app launching experiences and single sign-on (SSO)

Security

Reduce user access friction with intelligent policies that trigger strong authentication upon risky access situations and conveniently verify identity

Self-Service

Delegate identity management, password resets, security monitoring, and access requets to your workforce with robust self-service tools and save IT time and budget

Onboarding

Rapidly on-board users by integrating your identity tools with HR systems and automatically update access upon role changes

Seamless Access

Free your users of your greatest security risk by enabling passwordless sign-in to devices and services

Productivity

Azure AD allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources, allowing you to mitigate access risk by protecting, monitoring, and auditing access to critical assets -while ensuring employee and business partner productivity.

SSO – With single sign-on (SSO), users sign in once with only one account to access domain-joined devices, company resources, software as a service (SaaS) applications, and web applications. Azure AD ensures IT administrators can centralize user account management, and automatically add or remove user access to applications based on group membership.

Application access – To simplify application discovery and launch, Microsoft provides three unique application portal experiences that meet your users needs. The My Apps portal surfaces all apps connected to Azure AD and where access permissions exist, and users can organize their apps into intuitive and customized collections. These app collections extend to the Office portal, where app launching is integrated with seamless collaboration tools. Finally, Company Portal delivers app experiences to a mobile setting so users can discover and download permitted apps on domain-joined devices.

Access requests – Some users may not be auto-enrolled in groups based on organizational policies, but IT can still drive user empowerment through access requests on the My Apps portal. This allows IT to define a safe set of apps that users can self-enroll and add to their app launching and SSO experience.

Guest user collaboration – Many modern organizations need to enable secure collaboration with guest contacts and vendors. Azure AD allows guest users to collaborate using their primary identity provider, so IT doesn't have to create secondary accounts for guests in their own domain and the guest experiences is as familiar as working in their usual work access experience.

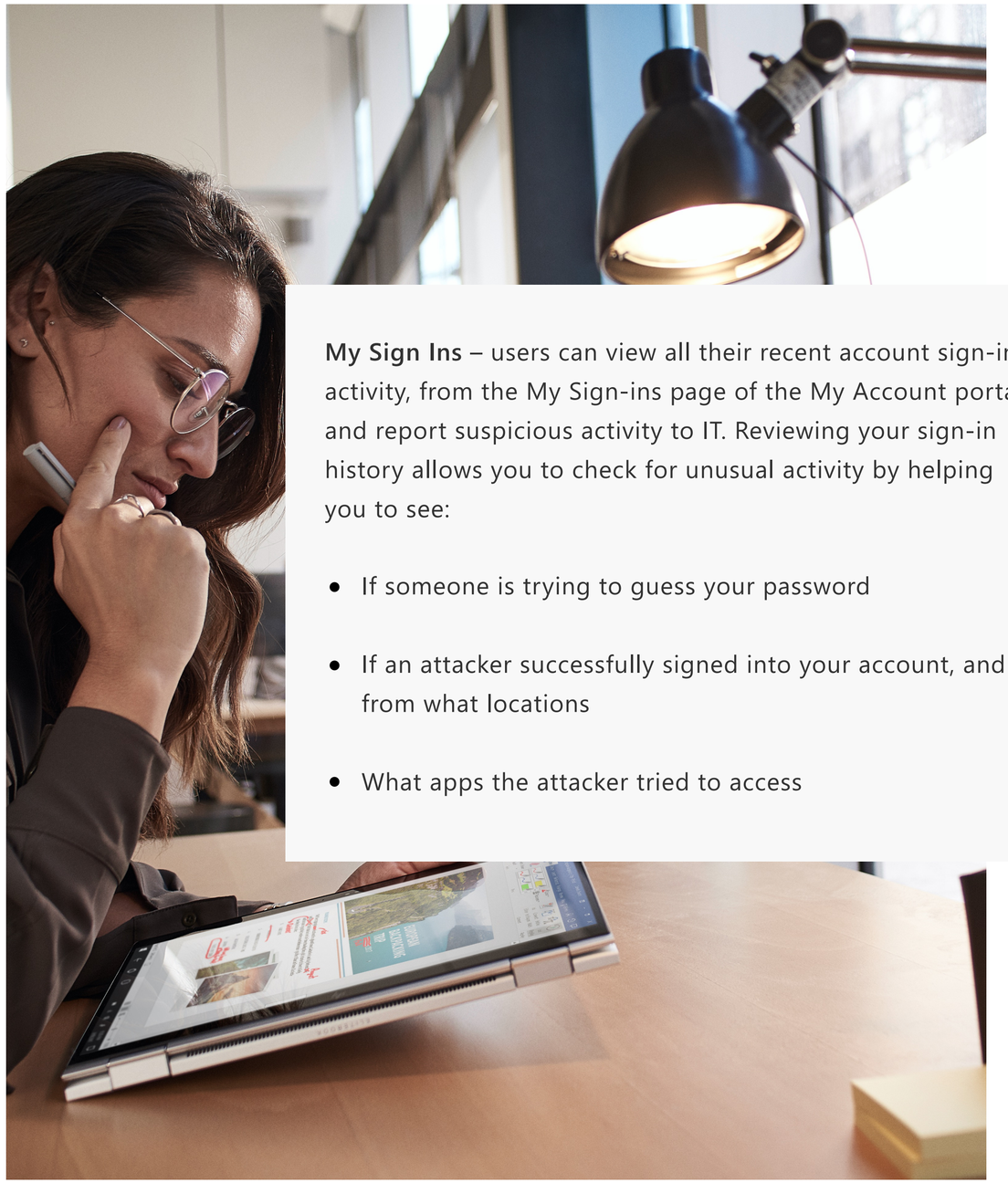
Security

Thinking about security means giving careful consideration to identity management procedures and processes, and Azure AD has the tools to help manage that progression.

Microsoft identity and access management solutions help IT protect access to applications and resources across the corporate datacenter and into the cloud. Such protection enables additional levels of validation. Monitoring suspicious activity through advanced security reporting, auditing, and alerting helps mitigate potential security issues, and allows users to be part of your security solution by helping spot and report potential breaches to IT.

MFA – Multi-factor authentication is when a user is prompted during the sign-in process for an additional form of identification, such as entering a code on their cellphone or to provide a fingerprint scan. Azure AD allows IT admins to select either Microsoft MFA experiences or other vendor services and define which forms of secondary authentication can be used to meet their organization's security needs. Also, to aid with adoption and enrollment, users can register themselves for both self-service password reset and Azure Multi-Factor Authentication in one step with the same security contact information.

Microsoft Authenticator App – Azure App Service provides built-in authentication and authorization support, so you can sign in users and access data by writing minimal or no code in your web app, RESTful API, and mobile back end, or Azure Functions.



My Sign Ins – users can view all their recent account sign-in activity, from the My Sign-ins page of the My Account portal and report suspicious activity to IT. Reviewing your sign-in history allows you to check for unusual activity by helping you to see:

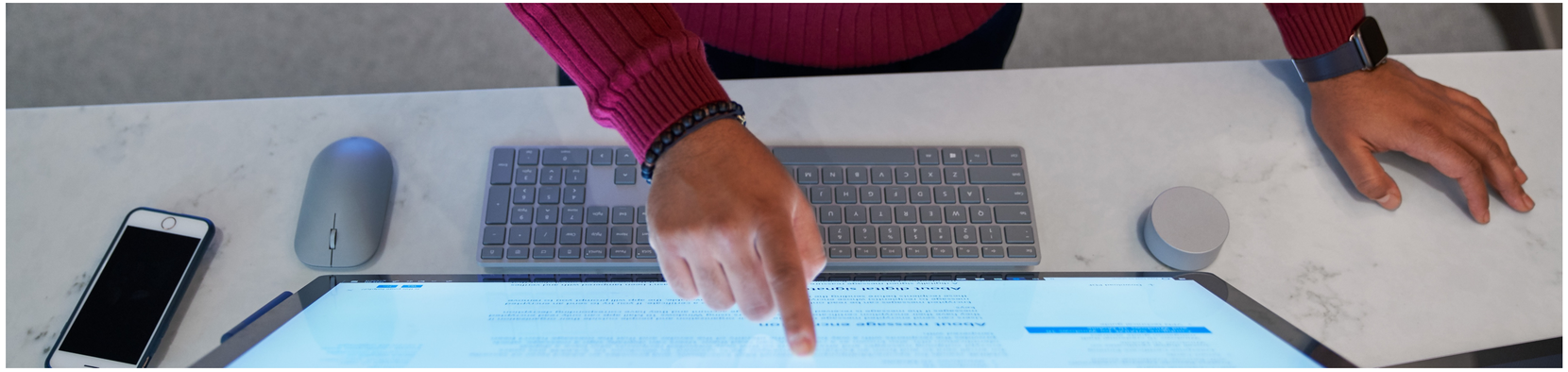
- If someone is trying to guess your password
- If an attacker successfully signed into your account, and from what locations
- What apps the attacker tried to access

Self-Service

Giving users the ability to reset their own passwords and manage their own profiles and apps is an important step towards alleviating the IT burden of constant password resets and dealing with users justified frustrations with blocked access. It allows IT to provide the guardrails for access but puts the day to day management and security of identity into the user's hands.

Self-service password reset – Password reset requests tend to be the largest percentage of IT help desk workload – sometimes upwards of 20%. With self-service password reset (SSPR), users are empowered to reset their own passwords from a web interface that can be accessed remotely. IT can also set the right level of security for their organization by dictating which forms of second factor confirmation will be allowed to authorize the reset.

Profile management – To further empower users self-sufficiency and save IT time and budget, the My Account profile manager is a one-stop-shop for users to manage their own identity. From here, they can reset their security contact info, update their authorized work devices, review Sign-in information, register second factor form-factors, and more.



Onboarding

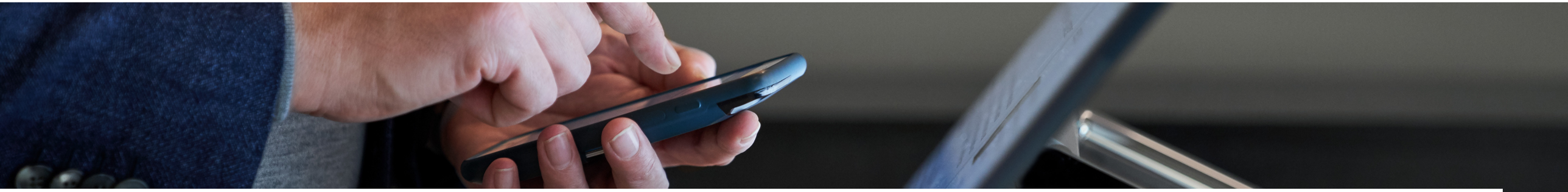
Azure AD can continue to help you meet your IT needs as the world settles in to our new normal of remote productivity and access-including your HR processes.

Azure AD's is designed to scale to your workforce. As an employee moves through their journey in your organization, you can rest assured Azure AD will make seamless access updates to increase their productivity and help you maintain access compliance.

Seamless Access

The idea of going passwordless may seem daunting at first, but if you're already taking steps to embrace a seamless IT and user experience, you're already halfway there.

Passwordless authentication is a form of multi-factor authentication (MFA) that replaces passwords with two or more verification factors secured and encrypted on a user's device, such as a fingerprint, facial recognition, a device pin, or a cryptographic key. The credentials never leave the device, eliminating the risk of phishing. These alternatives are based on new technology agnostic industry standards No passwords are stored in the cloud, and your system is 99.9% less likely to be compromised when you enable MFA.



81% of hacking-related breaches use stolen or weak passwords.

Moving to passwordless authentication offers improved security and a better user experience but requires you and your users to adopt a new way of thinking about security. We suggest starting with a low risk group, explaining the benefits of eliminating passwords. Deploy MFA with a passwordless authentication option until people are comfortable with it and then start replacing passwords and dependencies on passwords in the background, continuing to educate your users as you roll out the new identity solution.

For more information on going passwordless, visit **microsoft.com/identity**

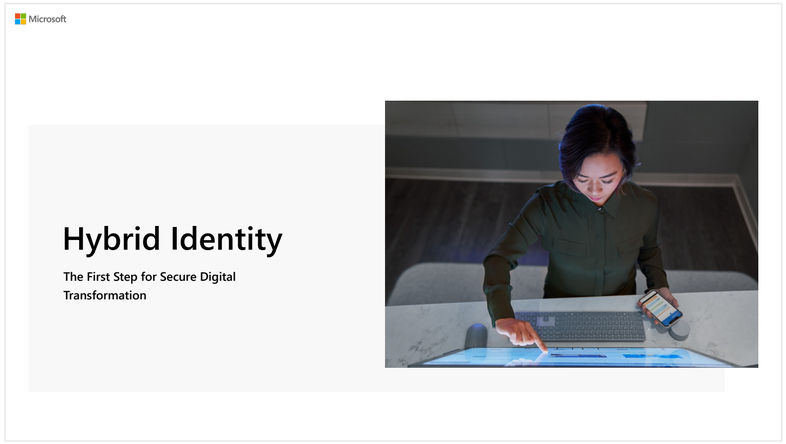
Next Steps

With Azure AD, you can have the best for your users and for your IT department - seamless remote access for increased productivity and collaboration while maintaining the security the business requires that scales and includes app experiences.

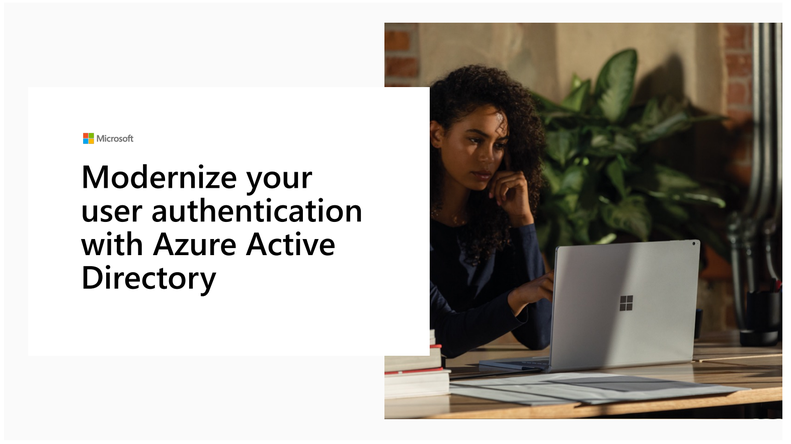
To learn more about the end-user capabilities discussed here and get started on empowering users and freeing your IT department, visit aka.ms/identityexperiences

Microsoft

If you’re ready to modernize your productivity and security by moving to the cloud, check out our two e-books dedicated to getting you into there.



Step 1 is to modernize your identity and move to the cloud by stepping through the process outlined in Hybrid Identity: The first step for Secure Digital Transformation



Step 2 is embracing the end user experience as outlined in Modernize your user authentication with Azure AD.

Already in the cloud and ready to focus on your end user experiences? Join us at aka.ms/identityexperiences