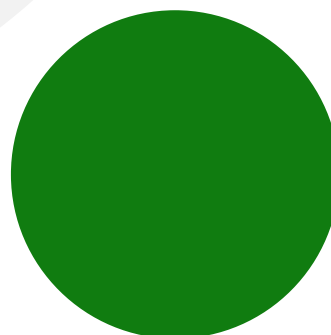


# Azure Active Directory

Transform Your Identity Solution with  
a Hybrid Approach



# Contents

<b>Introduction</b>	3
Why hybrid identity?	4
<b>Azure AD hybrid outcomes</b>	5
Secure authentication	7
Optimized end user experience	9
Robust access management	11
Identities managed at scale	13
Identity protection	15
Business continuity	16
Optimized monitoring and reporting	17
<b>Conclusion</b>	19

# Introduction

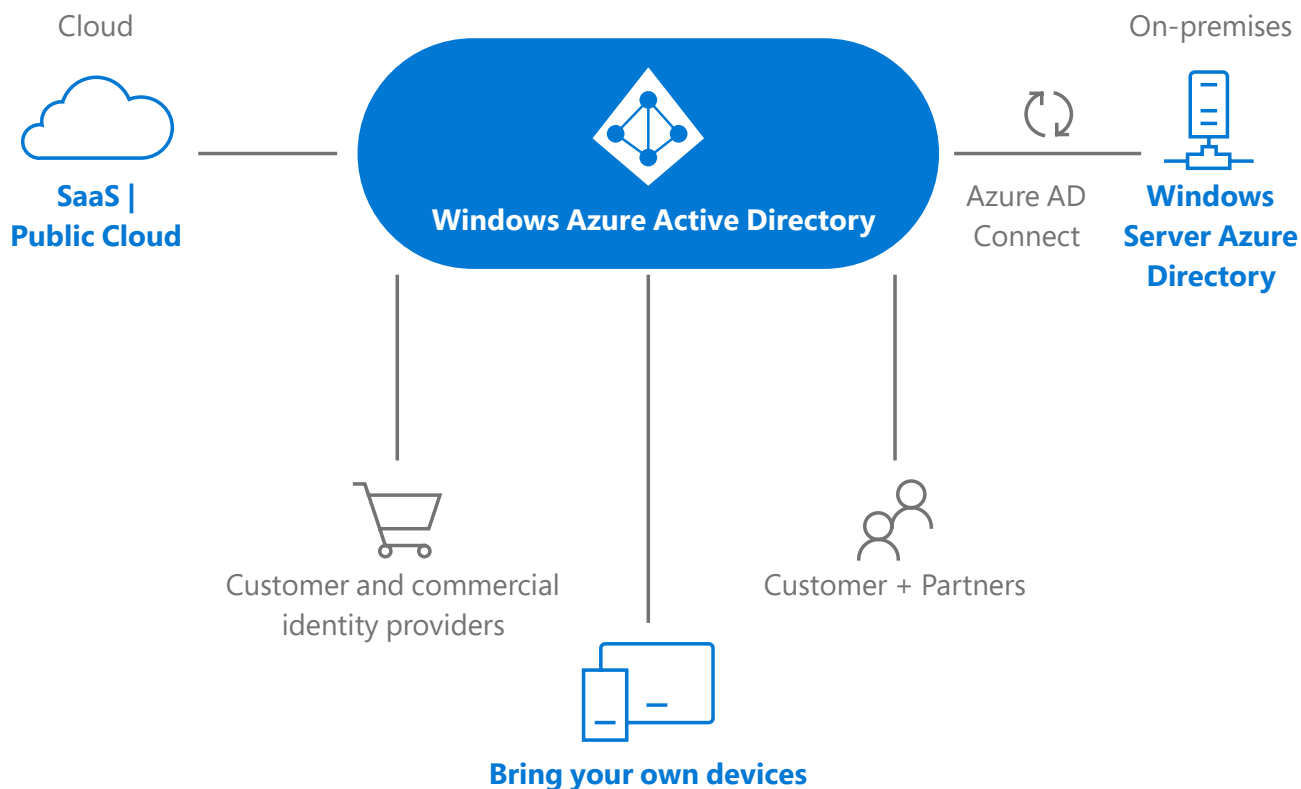
Digital transformation has spurred tremendous growth in the movement of digital resources outside of corporate network boundaries. More and more apps and data are now in the cloud and a dispersed workforce needs to access to them from anywhere on multiple devices. Meanwhile, bad actors have grown more sophisticated and cyberattacks more advanced, so classic network security strategies are no longer sufficient for managing access to digital resources.

A new way to defend against this is a Zero Trust security strategy. In this approach, organizations should explicitly verify identity before approving access, give the least amount of privilege necessary, and take an assume-breach security posture. A cloud-based identity and access management solution is the lynchpin of a Zero Trust strategy. This approach has emerged as the best way to maintain control over and visibility into how and when users and devices access corporate apps and data, while meeting today's security and compliance requirements.

Microsoft Azure Active Directory (Azure AD) enables hybrid management with existing on-premises directories to provide secure authentication for access to on-premises and cloud apps. It's a comprehensive identity and access management solution that gives you a robust set of capabilities to manage users and groups both inside and outside your organization.

## Why hybrid identity?

One of the most significant challenges for organizations today is keeping pace with the changing IT environment. For most businesses, keeping pace means a journey of migration, from connecting solely via their on-premises networks and onboarding to a hybrid approach with the cloud.



A hybrid approach allows for accelerated transition to a more agile and efficient organization, enabling you to expand your on-premises IT systems to use more scalable, and highly available, services in the cloud while keeping risks and costs down. When your organization moves to the cloud using a hybrid approach, you don't have to give up your existing on-premises IT architecture, allowing you to gradually expand into the cloud without compromising security.

A fully implemented Azure AD hybrid identity solution will help future-proof your organization as technology and security continue to evolve.

# Azure AD hybrid outcomes

**Your organization may have to clean up its existing on-premises identity solution before you can establish an Azure AD hybrid identity solution. This includes establishing a consistent identity governance architecture if multiple identities exist across many systems that will form part of the Azure AD hybrid identity solution.**

Next, you should verify the internal integrity of the on-premises directory to ensure only clean and up-to-date identities are provisioned with Azure AD Connect.

In order to implement a complete Azure AD hybrid identity solution, we have identified seven business outcomes that organizations should focus on.

**A fully realized Azure AD hybrid identity solution that balances security with productivity and maximizes the benefits of the cloud will have achieved all of the following:**



### **Secure authentication**

When a cloud app or on-premises app published to the cloud authenticates a user and device, the process is trusted, secured, and optimal.



### **Optimized end user experience**

Besides improving authentication security, implementing a complete Azure AD hybrid identity solution can significantly improve users' sign-in experience when many apps use the same authentication platform.



### **Robust access management**

To manage access to apps, organizations must control which users and their devices have access over an app's lifetime.



### **Identities managed at scale**

To maintain strong control of identities, it is critical for organizations to have clear insights of groups and privileged roles in apps.



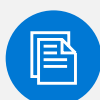
### **Identity protection**

Moving to the cloud helps organizations defend against malicious attacks.



### **Business continuity**

Organizations should not leave themselves vulnerable to failures of hardware systems or components susceptible of going down and preventing the authentication process.



### **Optimized monitoring and reporting**

The Azure AD hybrid identity solution provides useful insights, reporting, and actions for events happening in Azure AD.



# Secure authentication

---

Authentication is the critical path for user access to resources. Not only should authentication methods be secure, but also the process should be intelligently aware of a user's state when they access apps. For example, when a user accesses an app from one location and a few seconds later tries to access the same app from across the world, the second access attempt should be denied or extra verification requirements should be requested before access is granted.

**To achieve secure authentication, we recommend the following:**



**Common identity between cloud and on-premises:** Organizations with an existing on-premises Active Directory solution should extend their directory to Azure AD using Azure AD Connect. This will ensure that users can use the same identity to access resources in the cloud.



**Privileged users use stronger authentication:** Accounts such as global admins can do a lot of harm in the wrong hands. To ensure that your global admins are who they say they are and not a victim of password theft or sharing, always use multifactor authentication for privileged accounts.



**Cloud apps use risk-appropriate sign-in:**

Cloud apps are more secure when they can detect risks associated with the sign-in process to ensure the user is appropriately validated. Azure AD can evaluate factors such as location and user risk level to decide if any extra security measures should be triggered, such as a multifactor authentication challenge if necessary.

**Users self-manage credentials:**

With Azure AD self-service password reset, users can reset their passwords on their own when and where they need to. At the same time, admins can control how a user's password is reset. By eliminating help desk interventions for password management, users can be more productive and secure when accessing the cloud.

**User devices managed in the cloud:**

User devices should be known to the identity solution. This enables you to apply security policies and uses the device state to evaluate if access to a cloud app should be granted. Microsoft provides comprehensive device management via Microsoft Endpoint Manager.

**All cloud apps require modern**

**authentication:** Many older apps do not support modern authentication methods. These apps can pose a security risk for accessing resources and data via legacy authentication methods that can leave organizations vulnerable. We recommend that legacy authentication methods in apps be blocked from accessing cloud resources.

**Restricted access to sensitive apps:**

Some apps should be restricted to a limited duration. These sensitive apps may provide users with valuable data, and the access can be limited using specifically defined refresh tokens for authentication.

**Selected cloud apps are restricted to managed devices:**

As part of registering devices in the cloud, an organization can evaluate the device state (e.g., is the device registered?) to allow access to the cloud app. This ensures greater security for the cloud app and information the app can provide on a specific device. With this type of management, organizations can prevent rogue devices from accessing sensitive apps and data.





# Optimized end user experience

---

Security can be a hassle for users, and they will sometimes push back on security measures that slow their productivity and access to cloud apps. Organizations should make the process easier or more intuitive without compromising valuable security measures.

**To achieve an optimized user experience, we recommend the following:**



**Users get single sign-on across all of their apps:** Azure AD can allow a user to access Microsoft services, cloud (SaaS) apps, and on-premises apps with their corporate credentials. Users don't need to remember individual app credentials and admins gain the control they need to allow appropriate user access.



**Users get a familiar sign-in experience:** The logo and company name can be configured for Azure AD sign-in pages in cloud apps. This gives users confidence that they are using the correct sign-in process with which they are familiar.



**Users have one-click app launching:**

When users have access to many apps, they need to know which apps are enabled to do their jobs. Azure AD provides a central app discovery and portal called My Apps. Users can also organization their apps into intuitive collections for a personalized experience.



**Users need managed devices to access cloud apps:**

Users accessing apps from managed devices can gain access automatically without the need for extra verification steps. Requiring managed devices that are registered in the cloud can significantly enhance an organization's security.

**Users have passwordless authentication:**

Multifactor authentication (MFA) is a great way to enforce stronger authentication when apps require extra levels of security. By embracing passwordless authentication, a form of MFA, users can use strong factors

like a PIN or biometrics to access resources and never need to know or use their password. Microsoft allows for a variety of passwordless options like Windows Hello for Business, the Microsoft Authenticator app, or FIDO2 security keys.





# Robust access management

---

Organizations should clearly and thoroughly define the policies and methods that allow them to manage access to apps.

**To achieve robust access management, we recommend the following:**



**Admins use groups to manage access:**

Azure AD groups can manage access to many features in Azure AD and Azure without requiring admins to directly assign access at an individual user level. Self-service group management alleviates admins from group management operations by delegating the responsibilities to the users directly for groups that the admins have chosen.



**Users get single sign-on across all their on-premises apps:** Azure AD Application Proxy provides a way for organizations to effortlessly publish on-premises apps to the cloud. Those apps become part of the My Apps page available to users, which they can easily access from anywhere.



**Secure users' devices:** Organizations should make sure devices have the latest updates installed and are up-to-date with anti-malware detection capabilities. Devices can be secured by applying policies to meet the organization's security requirements.



**Access to cloud apps determined by multiple factors:** Consider the location and device state of the user with Conditional Access (CA) policies and leverage Azure AD Identity Protection to more dynamically determine risk-based access to cloud apps. When Azure AD determines a higher risk from a specific user, location, or device, the users can be challenged for more verification methods or blocked if the risk is too high.



**Admins have an automated way to manage users' devices:** Organizations can prevent access by unknown devices or devices running older operating systems that may have vulnerabilities. They should

have an automated way to register devices in the cloud as part of their device provisioning process to support restrictive access conditions.





# Identities managed at scale

---

Scalable identity management helps organizations manage the identity lifecycle as well as the integration of Azure AD with other business apps, such as HR systems. This ensures that users' roles and access stay aligned.

**To achieve identity management at scale, we recommend the following:**



**Admins manage users more efficiently:**

With Azure AD dynamic groups, membership can be determined and adjusted automatically based on rules that consider identity attributes like location or job role, and update as the user's responsibilities change. Group expiry can delete a group automatically unless the group's existence is renewed.



**Admins manage users using automated workflows:**

Organizations should have the necessary security tools, integrations, and capabilities defined to do governance workflows for their Azure AD hybrid identity solution. This could include integration with HR systems to provision and manage user identities.



**Admins use break-glass accounts for incident response:**

Users can lose access to apps when organizations are reliant on strong policies. We recommend that you create special cloud-only admin accounts, called break-glass accounts, to access the Azure AD portal when you are in an emergency, like a cyberattack, which may prevent normal access to Azure AD. These break-glass accounts should be physically secured and only available in emergencies.



**Admins operate with least privileged**

**access:** Azure AD can prevent privileged user accounts, such as global admins, from doing harm by only providing the necessary access to the admin process for a limited time with a feature called Privileged Identity Management (PIM). With this feature,

privileged admin accounts must first request access to perform sensitive operations from another admin. The other admin can then grant the access to the admin account for a limited time to complete the operation. When the time expires, the admin will fall back to restricted account privileges.





# Identity protection

---

Identity protection helps organizations moving to the cloud defend against risks, such as users with weak or reused credentials.

**To achieve identity protection, we recommend the following:**



**Admins actively triage security incidents:**

The reporting capabilities in Azure AD show admins any suspicious incidents happening during the user sign-in process. It is critical that the incidents are investigated and quickly resolved.



**Security monitoring to detect anomalous activity:**

On top of reactively scanning reports, admins should have the necessary monitoring in place to detect and alert for unusual user activity.



**Anomalous activity automatically detected and remediated:**

Azure AD's Identity Protection can identify vulnerabilities affecting your organization's identities and automatically remediate them, including forcing users to change their password or blocking a user from accessing a cloud app.







# Business continuity

---

Organizations must consider the necessary tools and processes needed to survive outages when on-premises infrastructure or other dependencies fail.

**To achieve business continuity, we recommend the following:**



**Identity infrastructure resilient to on-premises failures:** Authentication that is dependent on on-premises infrastructures, like a federation farm or pass-through authentication agents, can prevent their users from accessing cloud apps when those components fail. We recommend that organizations deploy multiple agents in the case of pass-through authentication and password hash sync as a failback option.



**Identity infrastructure designed to handle cyberattacks:** Organizations should develop a detailed response and recovery plan to mitigate the risks of a cyberattack, including steps for what to do to ensure users remain productive and how to get back to normal business operations.







# Optimized monitoring and reporting

---

It is important that organizations manage their identity infrastructure proactively to stay ahead of any incidents that may occur.

**To achieve optimized monitoring and reporting, we recommend the following:**



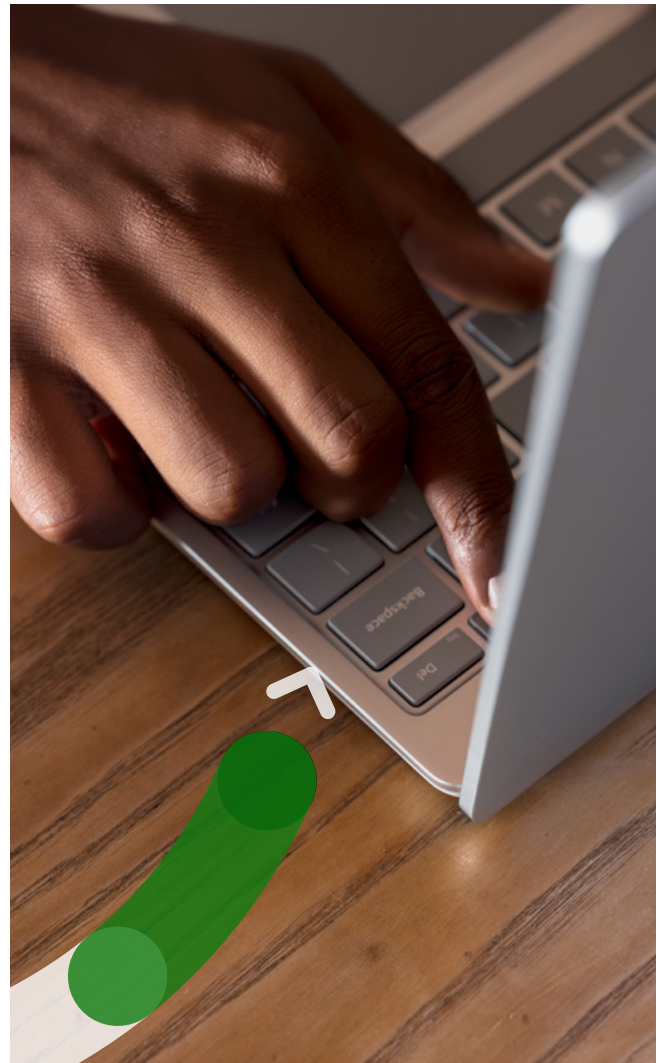
**Admins actively monitor sign-in patterns:**

Azure AD reporting provides insight into user activity via sign-in reports. These reports should be reviewed on a regular basis to ensure all activity is normal and users were not hacked in the cloud. Organizations using a security information and event management (SIEM) system, like Azure Sentinel, should set up their system to automatically import events and logs to perform analysis of sign-in activity.



**Admins have robust change management processes:**

Organizations should have a proper change management process in place to approve changes before they are implemented in Azure AD. Changes admins make in Azure AD can be captured in audit activity logs to verify the changes were made correctly according to the change request.





**Admins have operational insights into their identity infrastructure:** Azure AD Connect Health agents can augment the health status of identity infrastructure for administrators to have better insight into their identity solution.



**Admins have holistic security monitoring setup:** Organizations should have a complete integrated security monitoring and policy management solution in place across all on-premises and cloud workloads. Apply policies to ensure compliance with security standards and find and fix vulnerabilities before they can be exploited.



# Conclusion

By transforming your identity solution with a hybrid approach and taking advantage of the tools in Azure AD, you will be able to:

- ✓ **Securely handle authentication for apps.**
- ✓ **Optimize your users' experiences and empower them to be more productive with self-help features.**
- ✓ **Efficiently manage access to cloud apps.**
- ✓ **Govern identities to ensure compliance with your business practices.**
- ✓ **Protect your identities from new risk vectors in the cloud.**
- ✓ **Implement business continuity to survive cyberattacks.**
- ✓ **Operationalize monitoring and reporting to gain insights into your identity infrastructure.**

Azure AD can ensure your organization is future-proof while your organization evolves to support a secure connected world.



©2021 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.