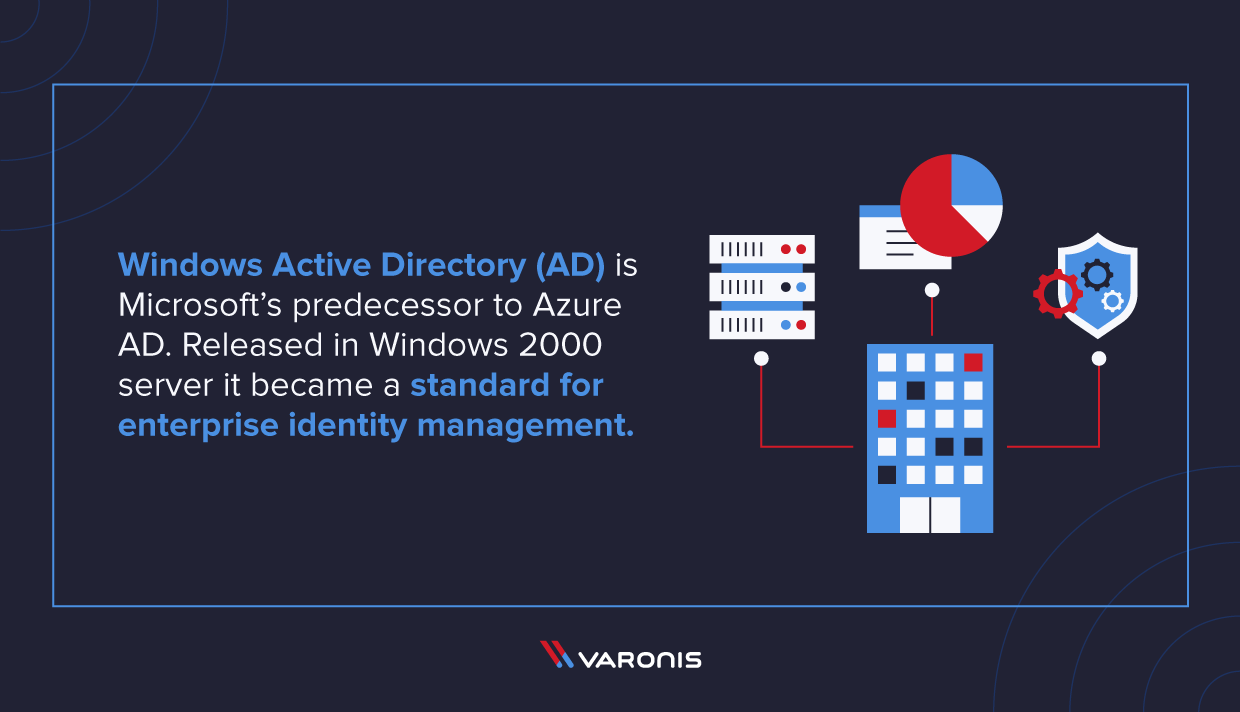
Azure Active Directory

## What is Windows Active Directory?

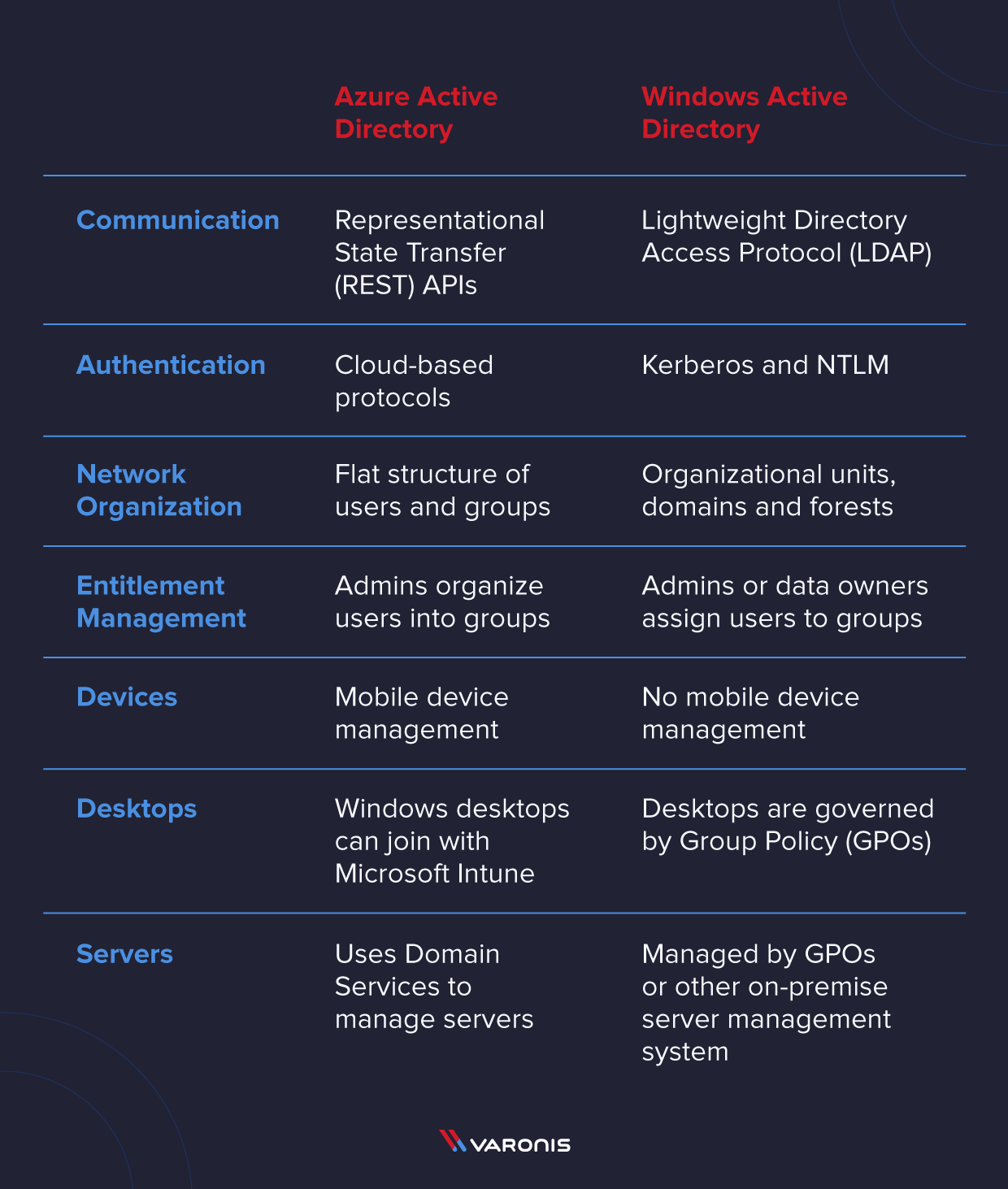


[**Windows Active Directory**](https://www.varonis.com/blog/what-is-active-directory/?hsLang=en)**(AD) is Microsoft’s predecessor to Azure AD. Microsoft released Active Directory in Windows 2000 server, and it became a standard for enterprise identity management.**

**Active Directory lives on-premise in servers called Domain Controllers (DC). Each DC contains a catalog of users and computers that are authorized to access resources on the network. Users authenticate to DCs via**[**Kerberos**](https://www.varonis.com/blog/kerberos-authentication-explained/?hsLang=en)**or NTLM authentication.**

**AD security is one of our favorite topics because many attacks the Varonis Incident Response team researches involve AD at some point in the**[**cyber kill chain**](https://www.varonis.com/blog/cyber-kill-chain/?hsLang=en)**. It could be a simple brute force attack to crack an old**[**NTLM**](https://www.varonis.com/blog/investigate-ntlm-brute-force/?hsLang=en)**password or a privilege escalation attempt to take over an administrator account. AD security has been the topic of many conference talks and we even wrote a comprehensive**[**guide to pen testing your AD environment**](https://www.varonis.com/blog/binge-read-pen-testing-active-directory-series/?hsLang=en)**to ensure its resilience to common off-the-shelf attacks.**

## Difference Between Windows and Azure AD



zure AD and Windows AD are both created by Microsoft, and they are both IAM systems, but that’s pretty much where the comparisons stop. They are fundamentally different systems that exist in an interconnected enterprise environment.

**Azure Active Directory**

* **REST APIs:** Azure AD uses Representational State Transfer (REST) APIs to support communication to other web-based services
* **Authentication:** Azure AD uses cloud-based authentication protocols like OAuth2, SAML, and WS-Security for user authentication
* **Network Organization:** Each Azure AD instance is called a “tenant” which is a flat structure of users and groups
* **Entitlement Management:** Admins organize users into groups, and then give groups access to apps and resources
* **Devices:** Azure AD provides mobile device management with Microsoft Intune
* **Desktops:** Windows desktops can join Azure AD with Microsoft Intune
* **Servers:** Azure AD uses [Azure AD Domain Services](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/) to manage servers that live in the Azure cloud virtual machine environment

**Windows Active Directory**

* **LDAP:** Windows AD uses [Lightweight Directory Access Protocol](https://www.varonis.com/blog/the-difference-between-active-directory-and-ldap/?hsLang=en) (LDAP) to pass data between clients and servers and DCs.
* **Authentication:** Windows AD uses Kerberos and NTLM to validate user credentials
* **Network Organization:** Windows AD is organized into Organizational Units, Domains, and [Forests](https://www.varonis.com/blog/active-directory-forest/?hsLang=en)
* **Entitlement Management:** Admins or data owners assign users to groups, and those groups have access to resources on the network
* **Devices:** Windows AD does not manage mobile devices
* **Desktops:** Desktops joined to Windows AD are governed by [Group Policy](https://www.varonis.com/blog/azure-active-directory) (GPOs)
* **Servers:** Servers in Windows AD are managed and governed by GPOs or other on-premise server management system

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. It provides authentication and authorization services for users and applications, allowing organizations to manage user identities and control access to resources in the cloud. Azure AD integrates with various Microsoft and third-party services and applications, enabling single sign-on (SSO), multi-factor authentication (MFA), device management, and more.

**Key features of Azure AD include:**

1. **Single Sign-On (SSO)**: Users can access multiple applications with a single set of credentials, enhancing user experience and productivity.
2. **Identity and Access Management**: Azure AD enables organizations to centrally manage user identities, groups, and access policies across cloud and on-premises environments.
3. **Multi-Factor Authentication (MFA)**: Adds an extra layer of security by requiring users to provide additional verification (such as a phone call, text message, or app notification) when signing in.
4. **Application Integration**: Azure AD supports integration with thousands of cloud-based and on-premises applications, allowing organizations to secure access to these applications and enforce policies.
5. **Device Management**: Provides tools for managing and securing devices, including Windows, macOS, iOS, and Android devices, accessing organizational resources.
6. **Conditional Access**: Allows organizations to enforce access controls based on various conditions, such as user location, device health, or the sensitivity of the resource being accessed.
7. **Identity Protection**: Helps detect and respond to identity-based threats by analyzing user sign-in behavior and applying risk-based conditional access policies.
8. **Self-Service Password Reset**: Enables users to reset their passwords without IT intervention, reducing help desk calls and improving efficiency.

Azure AD is widely used by organizations of all sizes to securely manage user identities and access to resources, both in the cloud and on-premises. It plays a critical role in modern identity and access management strategies, particularly in hybrid and cloud-only environments.

**Identity and authentication in the public cloud**

Identity and authentication in the public cloud are critical components of ensuring security, compliance, and efficient access management for organizations leveraging cloud services. Let's delve into these concepts in detail:

**Identity Management:**

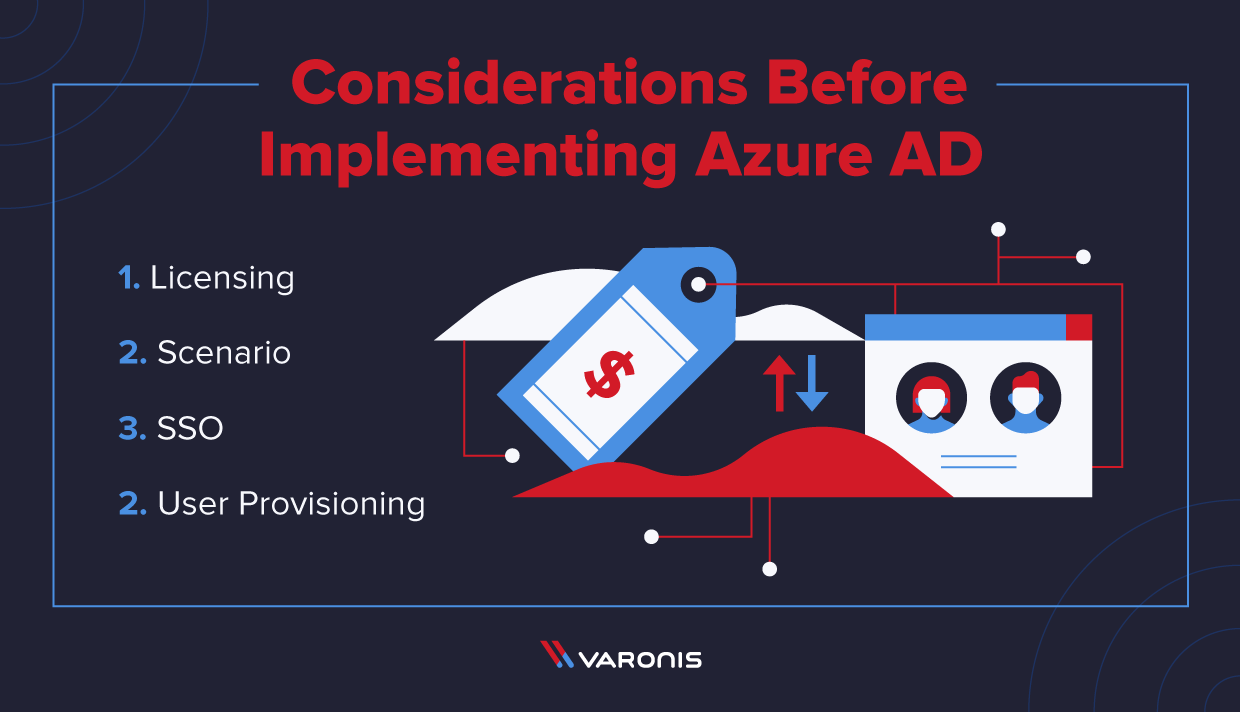
1. **User Identity**: Public cloud platforms like Azure, AWS, and Google Cloud Platform (GCP) provide identity management services to manage user identities accessing cloud resources. These identities are typically associated with user accounts created within the cloud platform or synced from an on-premises directory service like Active Directory.
2. **Service Identity**: Apart from user identities, cloud services often require their own identities for accessing other services or resources within the cloud environment. These service identities are used for automated processes, APIs, and inter-service communication.
3. **Directory Services Integration**: Public cloud platforms offer integration with existing directory services like Active Directory or LDAP. This integration enables organizations to leverage their existing identity infrastructure for managing cloud identities, ensuring consistency and ease of management.
4. **Role-Based Access Control (RBAC)**: RBAC is a fundamental concept in cloud identity management, allowing organizations to assign permissions to users and services based on their roles and responsibilities. RBAC helps enforce the principle of least privilege, ensuring that users and services have access only to the resources they need to perform their tasks.
5. **Group Management**: Cloud identity services support the creation and management of groups, allowing organizations to assign permissions to multiple users or services simultaneously. Group membership can be dynamically managed based on attributes such as job role or department.

**Authentication:**

1. **Single Sign-On (SSO)**: SSO enables users to authenticate once and access multiple cloud services without having to re-enter their credentials. Public cloud platforms support various SSO protocols such as SAML, OAuth, and OpenID Connect, allowing organizations to integrate with identity providers (IdPs) like Azure AD, Okta, or Google Workspace.
2. **Multi-Factor Authentication (MFA)**: MFA adds an extra layer of security by requiring users to provide additional verification beyond their passwords during the authentication process. Cloud platforms offer built-in MFA capabilities or integrate with third-party MFA providers to enhance authentication security.
3. **Identity Federation**: Identity federation allows organizations to establish trust relationships between their on-premises identity providers and cloud identity services. This enables seamless authentication and access to cloud resources using existing corporate credentials, enhancing user experience and simplifying identity management.
4. **Token-Based Authentication**: Cloud services typically use token-based authentication mechanisms to grant access to resources after successful authentication. Tokens are issued to authenticated users and contain information about their identity and permissions. These tokens are validated by cloud services to authorize access to resources.
5. **Identity and Access Management (IAM) Policies**: IAM policies allow organizations to define fine-grained access controls for cloud resources based on user identities, roles, and conditions. These policies specify what actions users and services are allowed or denied to perform on specific resources, helping enforce security and compliance requirements.

In summary, identity and authentication in the public cloud are foundational aspects of cloud security and access management. By effectively managing user and service identities and implementing robust authentication mechanisms, organizations can ensure secure and efficient access to cloud resources while maintaining compliance with regulatory requirements.

## Azure Active Directory Considerations



OK, so if you have made it this far, you might be considering implementing Azure AD for your organization. Now you have real decisions to make.

**1. Licensing:** Azure AD [licensing](https://azure.microsoft.com/en-us/pricing/details/active-directory/) follows the same monthly subscription licensing as the Office 365 licenses. There are four license levels – Free, Office 365 Apps, Premium P1, and Premium P2.

Office 365 Apps comes as part of your Office 365 subscription, and the Premium packages are a separate item. You get the Free license as part of a subscription to Azure, Dynamics 365, Intune, and Power Platform.

The Premium tier adds features like advanced password protection, self-service password management for your users,  advanced group access management, and conditional access.

The features lists for Azure AD and [Microsoft 365](https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products-b?=&ef_id=Cj0KCQjwpNr4BRDYARIsAADIx9y1hTBeXy__YfVD9i6zcQbOvJnTx8N_duUoMOIoVtFPwer5wcYa4JAaAsaFEALw_wcB:G:s&OCID=AID2100139_SEM_teun3PRg&MarinID=steun3PRg%7C430908156619%7C%2boffice%7Cb%7Cc%7C%7C57207468844%7Caud-312771920589:kwd-597936864&lnkd=Google_O365SMB_Brand&gclid=Cj0KCQjwpNr4BRDYARIsAADIx9y1hTBeXy__YfVD9i6zcQbOvJnTx8N_duUoMOIoVtFPwer5wcYa4JAaAsaFEALw_wcB&SilentAuth=1) are separate, and you need to look at both of them to understand everything available to you so you can build your implementation strategy.

Ed. Note: Office 365 recently got renamed to Microsoft 365. At the time of this writing, Microsoft’s documentation contains both names, but they are the same thing.

**2. Choose your scenario:** Hybrid Azure AD or Azure AD? If you already have Windows AD, Hybrid might be your best option. If you are trying to build a cloud-only infrastructure, Azure AD is the better choice.

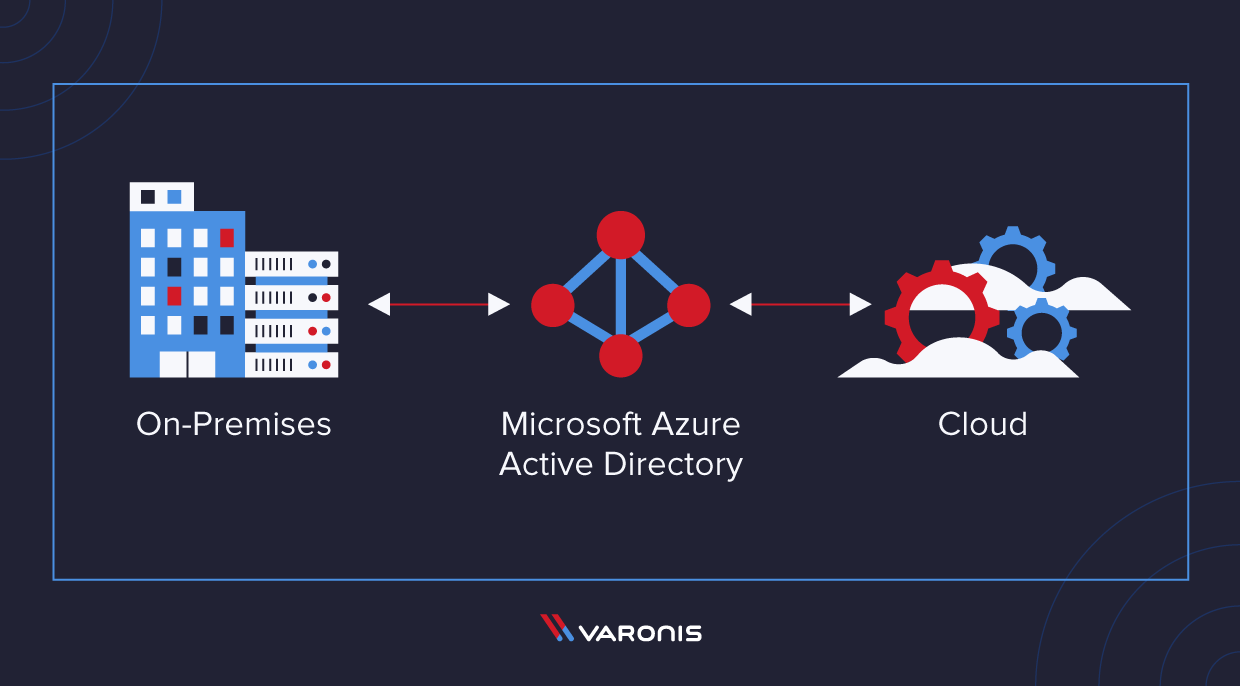
For your Hybrid environment, you can go with Managed or Federated configurations. If you are going to create users in Windows AD, you need to have Azure AD Connect to sync with Azure AD.

Are you going to use the device management in Azure AD? If so, you need Windows 10 on all those devices.

**3. SSO:** Are you going to enable Single Sign-on(SSO) with Azure AD? You will need to configure your cloud apps and services to use the Azure SSO, and set up a hybrid cloud for printing.

**4. User Provisioning:** How are you going to add your existing users to Azure? You can set up self-enrollment where users run the process themselves, [Windows Autopilot](https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot), or have an admin enroll your users.

## How Does Azure Active Directory Work?



Azure AD is a new system that Microsoft designed from the ground up to support cloud infrastructure. Azure AD uses REST APIs to pass data from one system to other cloud applications and systems that support REST (which is most cloud applications).

Unlike Windows AD, Azure AD is a flat structure in a single tenant. Think of the tenant as a circle that surrounds all your stuff. You can control the stuff inside the tenant, but once it leaves that circle you lose some agency over what happens to your stuff.

At Varonis, our approach to data security aligns with [zero-trust principles](https://www.microsoft.com/security/blog/2020/04/30/zero-trust-deployment-guide-azure-active-directory/), so as we continue we will weave in zero-trust when appropriate.

### Users and Groups

Users and groups are the basic building blocks for Azure AD. You can further organize users into groups that will all behave similarly. For example, you may put your Product Management team in one Azure AD group and grant permissions at the group level, so when users leave the organization, you only need to deactivate one account, and the rest of the group stays the same.

Users in Azure AD can come from both inside and outside of Azure AD. Let me restate that. Your Azure AD can contain identities for users inside of your organization and users from outside your organization that have a Microsoft account. See below:

[](https://info.varonis.com/hubfs/Imported_Blog_Media/image1-2.png?hsLang=en)

What this means is that you can bring people outside of your organization inside your tenant and grant them specific permissions just like they are part of your organization. When done correctly, this provides an additional level of security to the organization’s data.

### Adding User and Groups to Azure AD

There are several methods to populate your users and groups in Azure AD.

* Use Azure AD Connect to sync users from Windows AD to Azure AD. Most enterprises that already have Windows AD use this method.
* You can create users manually in the Azure AD Management Portal.
* You can script the process to add new users with [PowerShell](https://info.varonis.com/course/powershell?hsLang=en).
* Or you could program the process with the Azure AD Graph API.

**No matter which option you start with or use, later on, there are a few key points to make about adding users in Azure AD.**

1. Establish your authentication method and password policies, and enforce multi-factor authentication.
2. Only add users that you need to Azure AD. Leave service accounts or stale accounts in Windows AD, or delete them.
3. Keep privileged access in Azure AD to a minimum and follow [Microsoft’s guidance](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure) to keep privileged access secure.
4. Organize users into groups, and only give groups access to the applications and resources they need to do their job.
5. Connect users to their devices (mobile phones, laptops, etc.), so you can establish limits on how confidential data is downloaded or saved from approved and monitored devices.

### Custom Domains

Adding a custom domain to Azure AD will reduce the frustration that your users’ experience as they migrate to the new system. The default Azure AD domain looks like this:

* @notarealdomain.onmicrosoft.com

That’s a lot to type. If you configured Azure AD to use a domain that you own, your users would thank you. It would look something like @notarealdomain.com instead. That’s much easier to deal with.