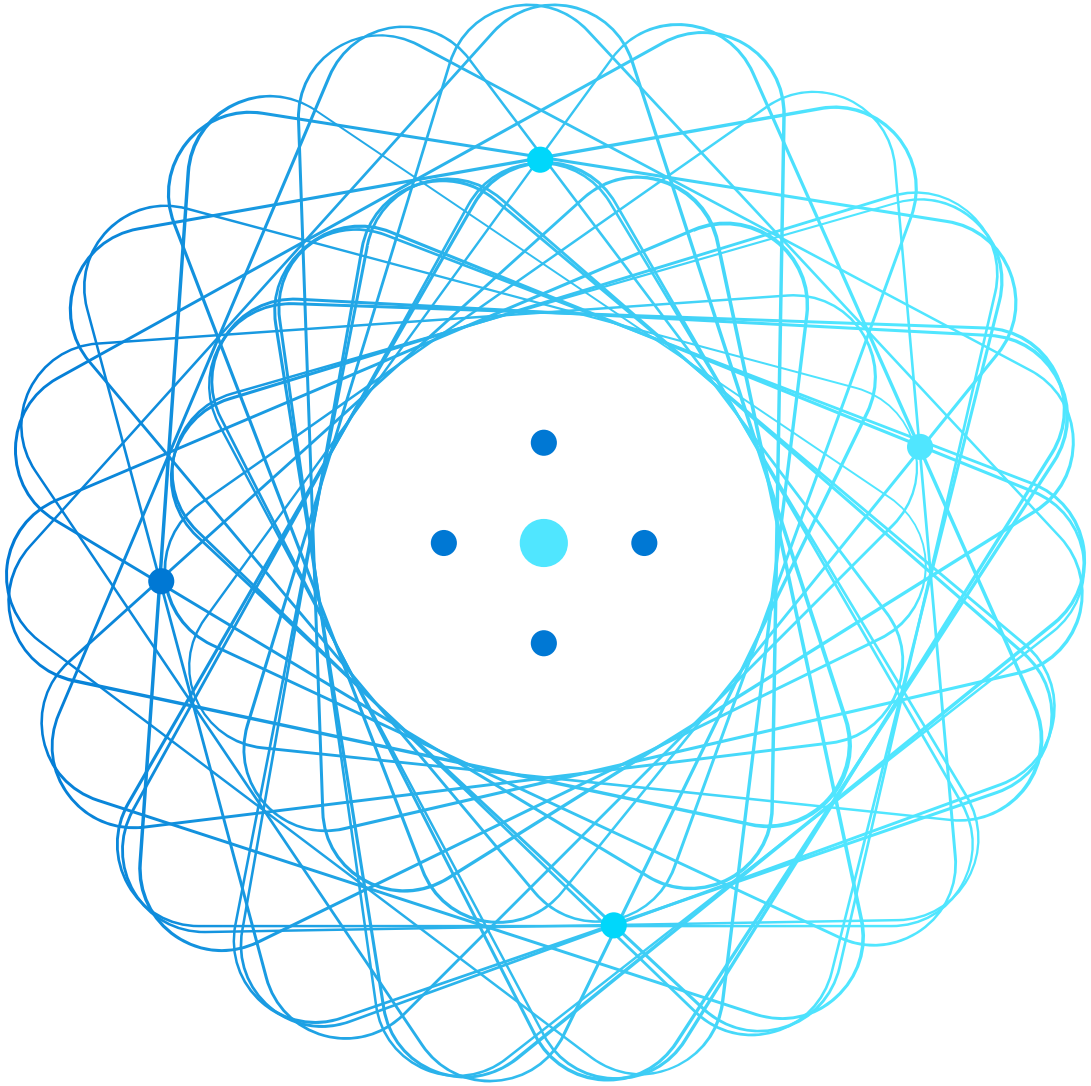
Microsoft Azure

Identity, Access, and Security



Identity, Access, and Security - Objective Domain

Describe the benefits and usage of:

- Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services.
- Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication (MFA), and password-less.
- Describe external identities and guest access in Azure.
- Describe Microsoft Entra Conditional Access.
- Describe Azure Role Based Access Control (RBAC).
- Describe the concept of Zero Trust.
- Describe the purpose of the defense in depth model.
- Describe the purpose of Microsoft Defender for Cloud.

Active Directory Domain Services (AD DS)

- AD DS and its related services form the foundation for enterprise networks that run Windows operating systems.
- The AD DS database is the central store of all the domain objects, such as **user accounts**, **computer accounts**, and **groups**.
- AD DS provides a searchable, hierarchical directory and a method for applying configuration and security settings for objects in an enterprise.
- In addition, you can use AD DS options to perform actions such as:
  - Installing, configuring, and updating apps.
  - Managing the security infrastructure.
  - Enabling Remote Access Service and DirectAccess.
  - Issuing and managing digital certificates.

What is an AD DS forest?

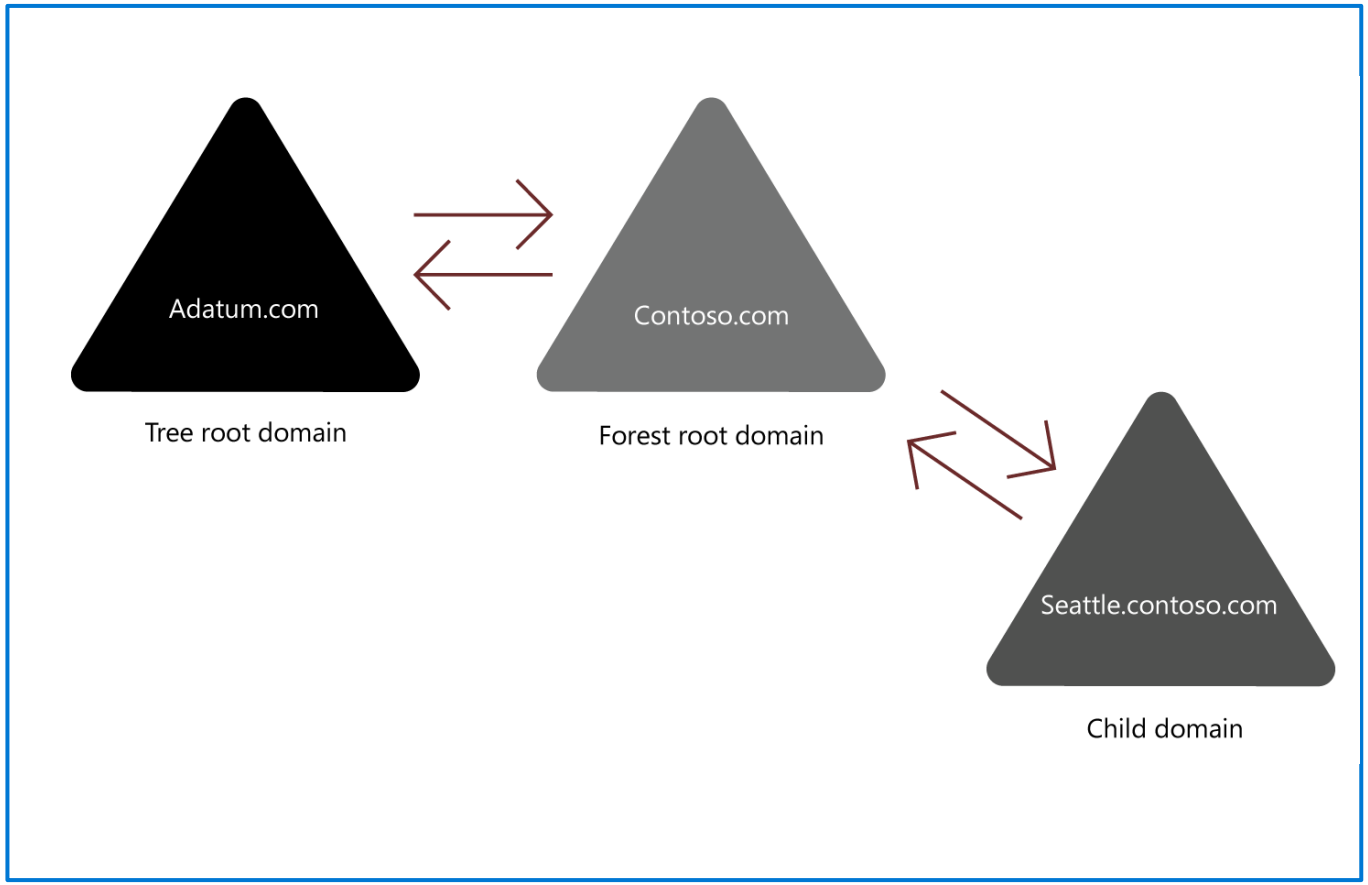
A Forest is a top-level container in AD DS

AD DS forest often described as:

- Security boundary
- A replication boundary

Trust relationships

- Provide access to resources in a complex AD DS environment



What is an AD DS domain?

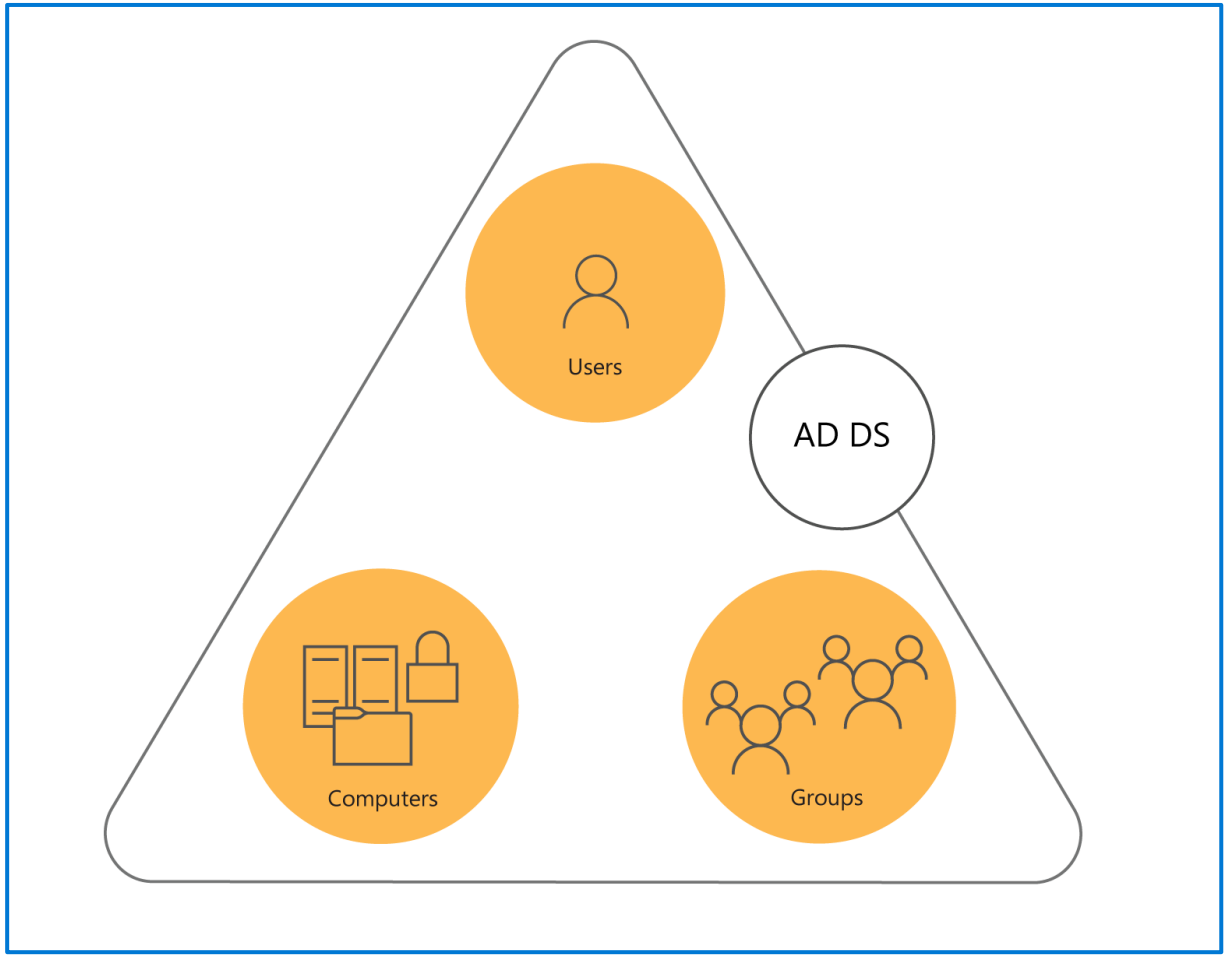
AD DS domain is logical container for managing user, computer, group, and other objects

AD DS domain is often described as:

- A replication boundary
- An administrative unit

An AD DS domain provides:

- Authentication
- Authorization

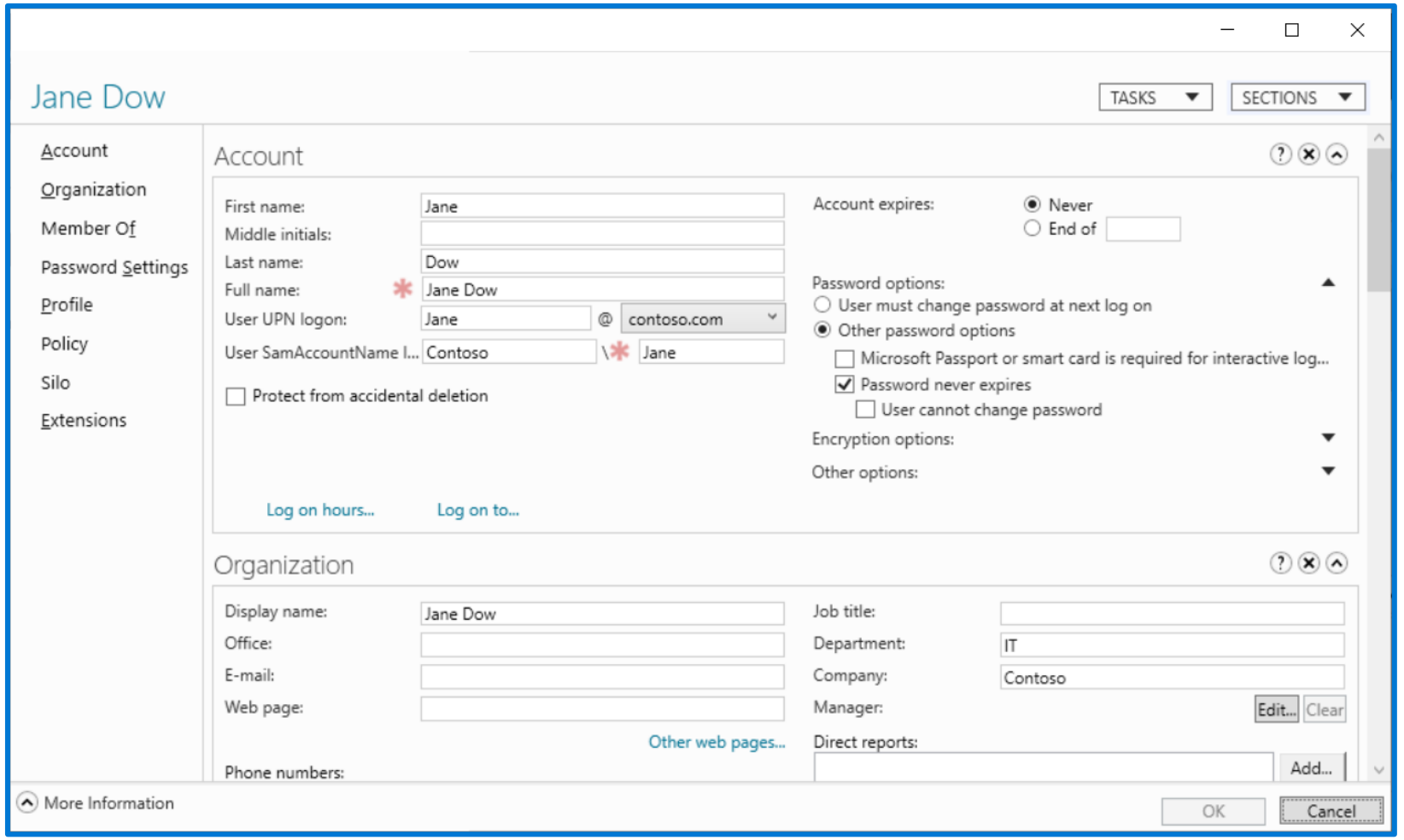


Define user objects

Create user objects

A user account includes:

- The username
- A user password
- Group memberships



Define group objects

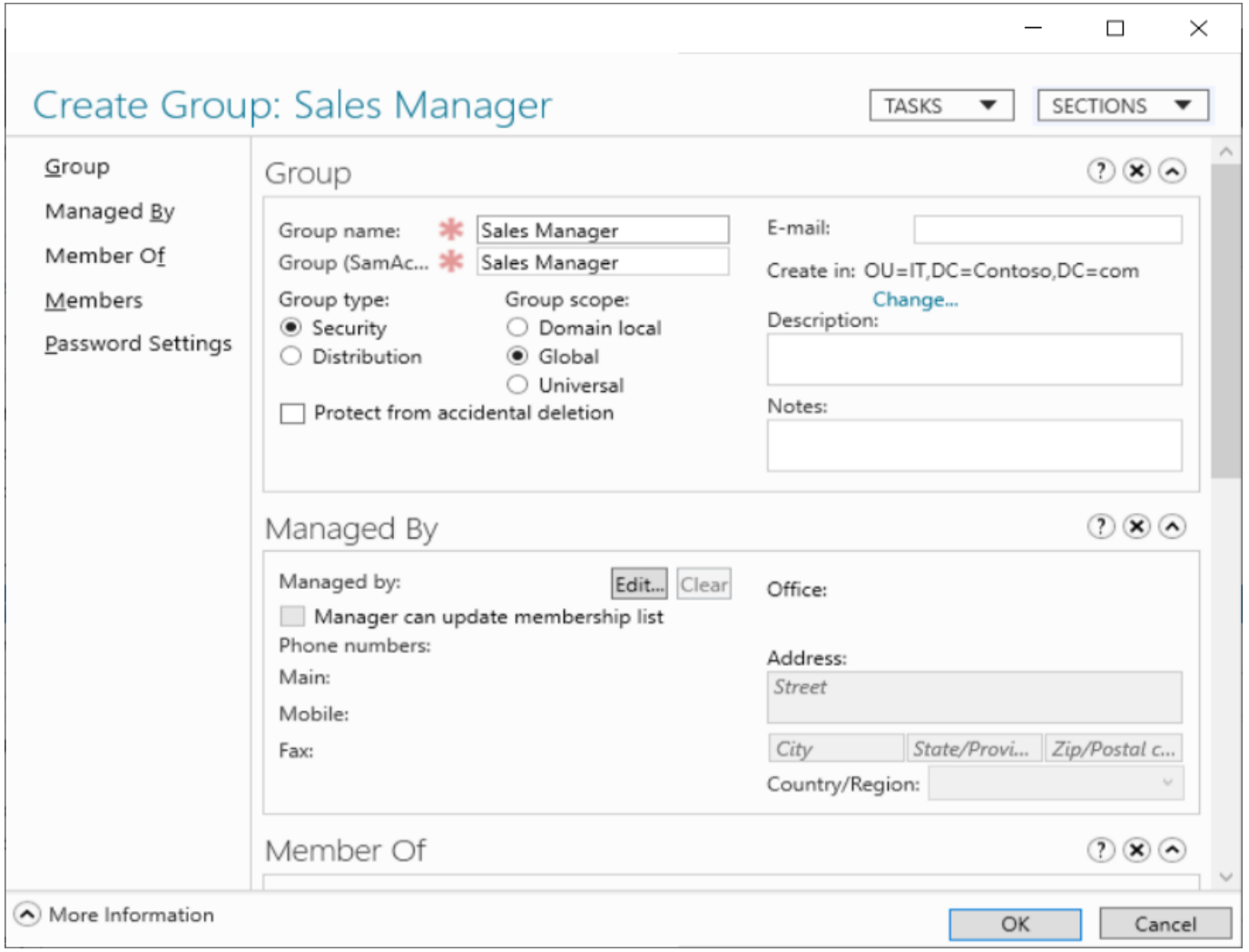
What are group objects?

Group types

- Security
- Distribution

Group scopes

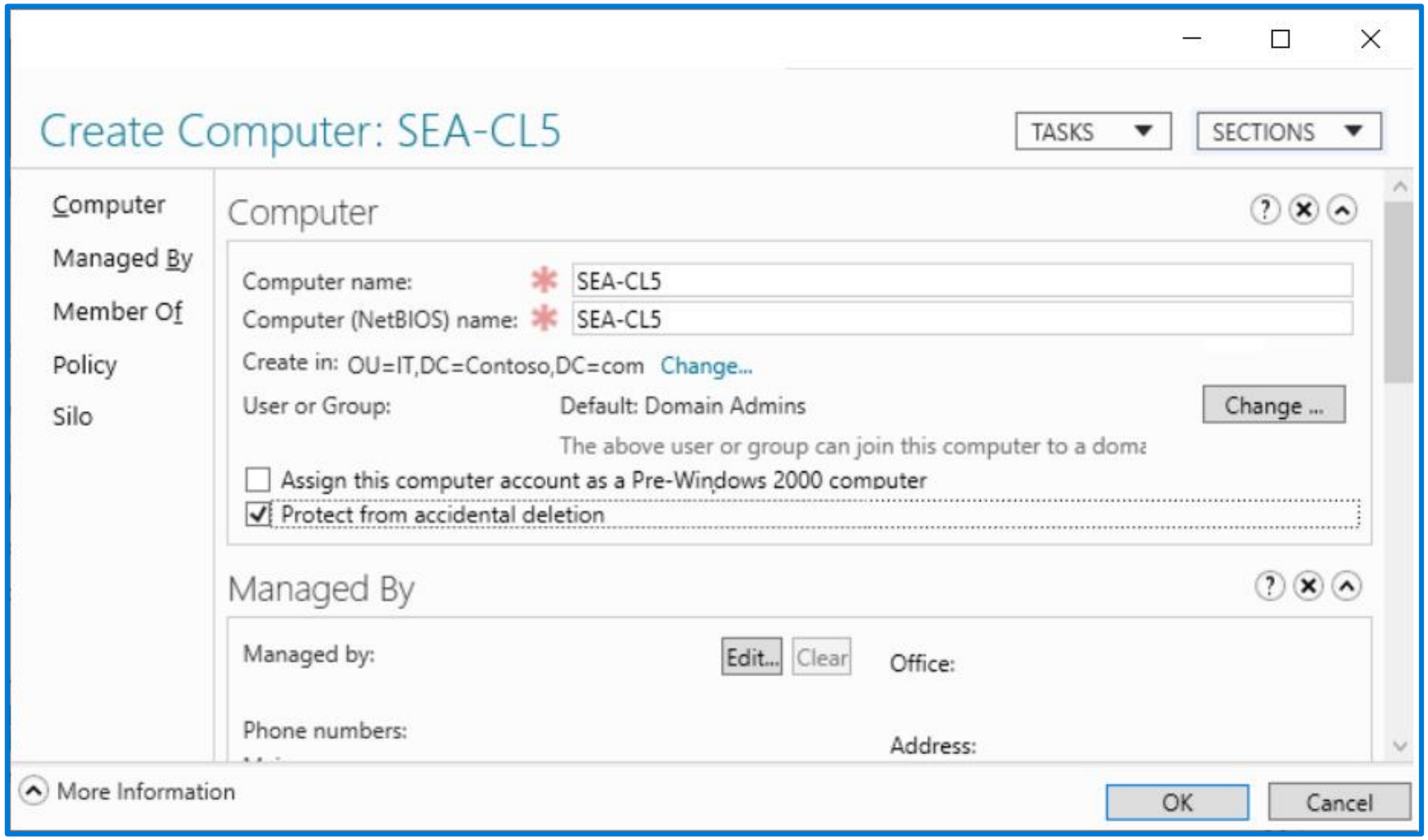
- Local
- Domain-local
- Global
- Universal



Define computer objects

Computers are security principals:

- They have an account with a sign-in name and password.
- They authenticate with the domain.
- They can belong to groups and have access to resources



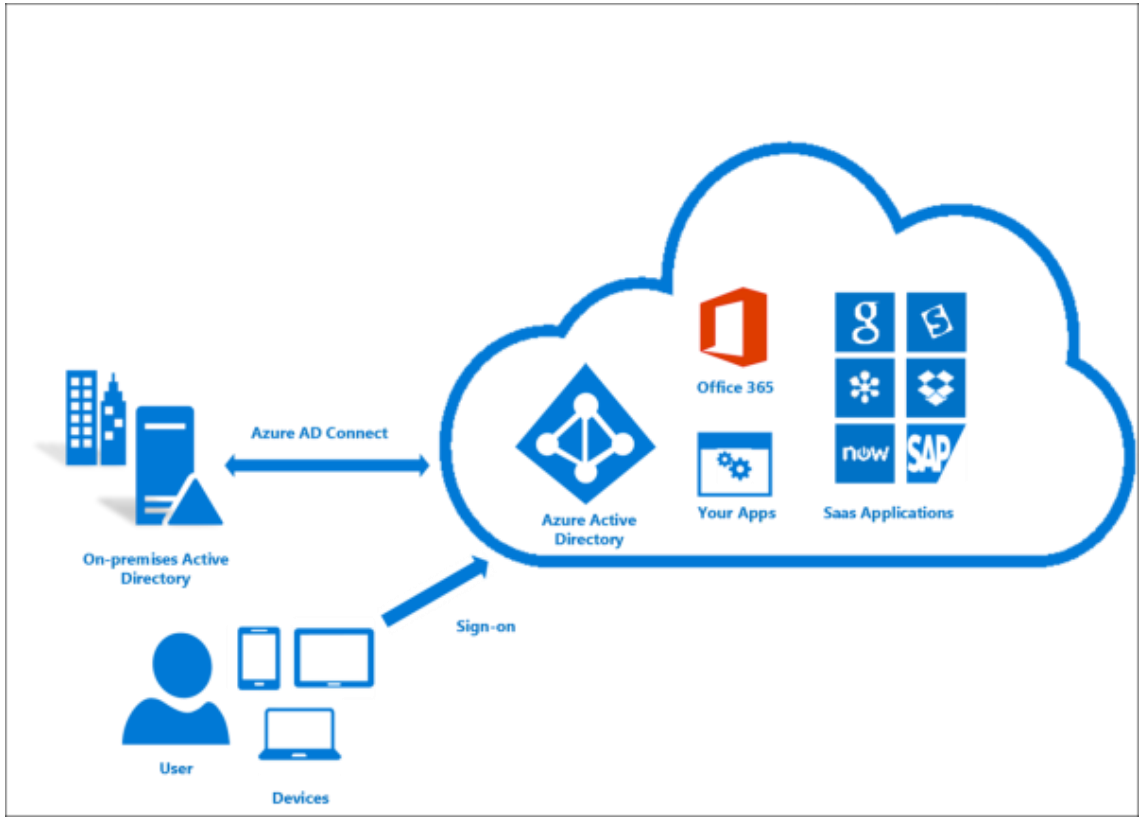
Azure Entra ID

Azure Entra ID

- Microsoft Entra ID is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop.
- For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization.
- Microsoft Entra ID is Microsoft's cloud-based identity and access management service. With Microsoft Entra ID, you control the identity accounts, but Microsoft ensures that the service is available globally.

Entra ID Connect

- Azure AD Connect provides the following features:
  - Password Hash Sync
  - Users & Groups Synch
- Users can use a single identity to access on-premises applications and cloud services such as Microsoft 365.



Entra ID Usage

Microsoft Entra ID is for:

•**IT administrators**. Administrators can use Microsoft Entra ID to control access to applications and resources based on their business requirements.

•**App developers**. Developers can use Microsoft Entra ID to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.

•**Users**. Users can manage their identities and take maintenance actions like self-service password reset.

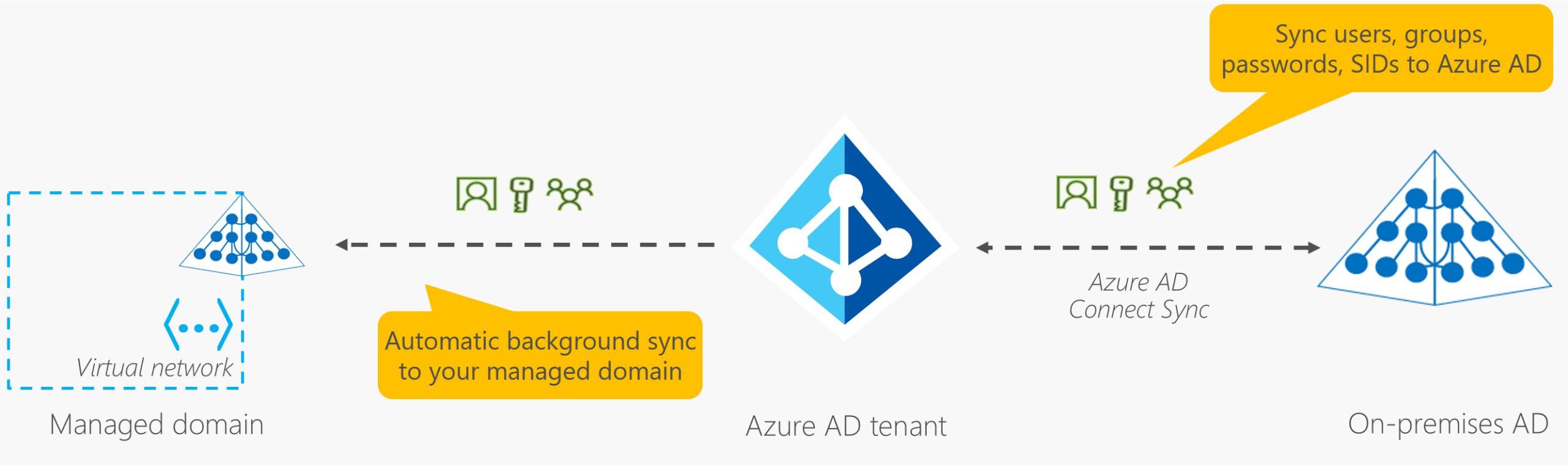
•**Online service subscribers**. Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Microsoft Entra ID to authenticate into their account.

Azure Entra ID

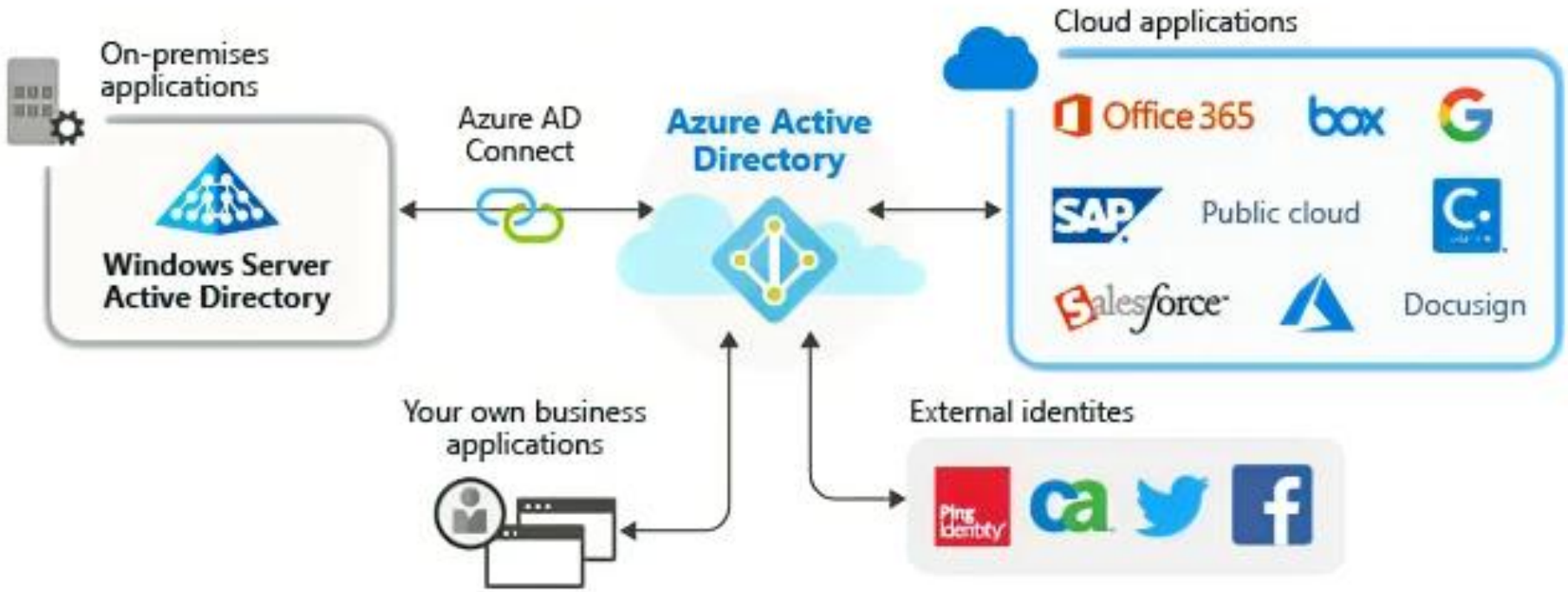
Microsoft Entra ID is a cloud-based identity and access management service that an organization's employees can use to access internal and external resources. It provides services such as:

- **Authentication**: Verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on (SSO)**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications.
- **Application management**: You can manage your cloud and on-premises apps by using Microsoft Entra ID. Features like Application Proxy, SaaS apps, the My Apps portal, and single sign-on provide a better user experience.
- **Device management**: Microsoft Entra ID supports the registration of devices, which enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Entra Domain Services



- Gain the benefit of cloud-based domain services without managing domain controllers
- Run legacy applications (that can't use modern auth standards) in the cloud
- Automatically sync from Azure AD



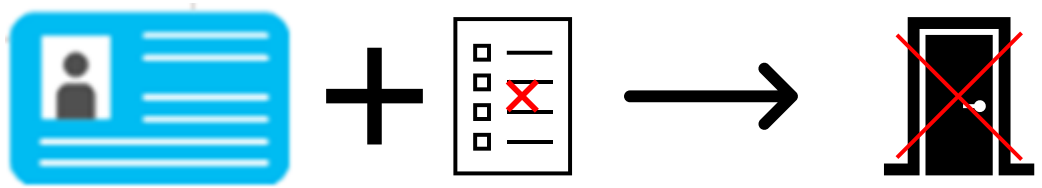
Compare Authentication and Authorization

Authentication

- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.

Authorization

- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.

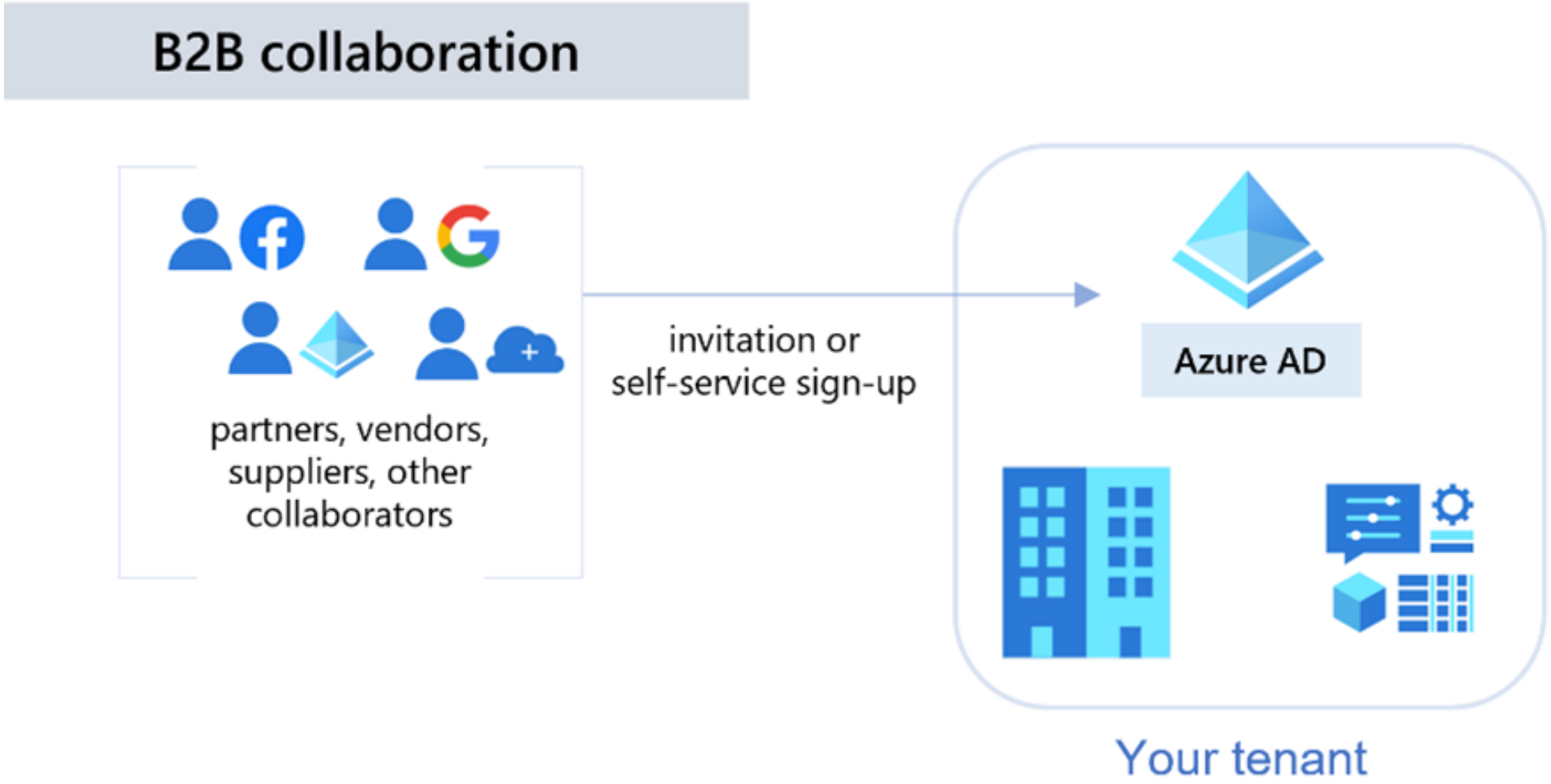


Azure Multi-Factor Authentication

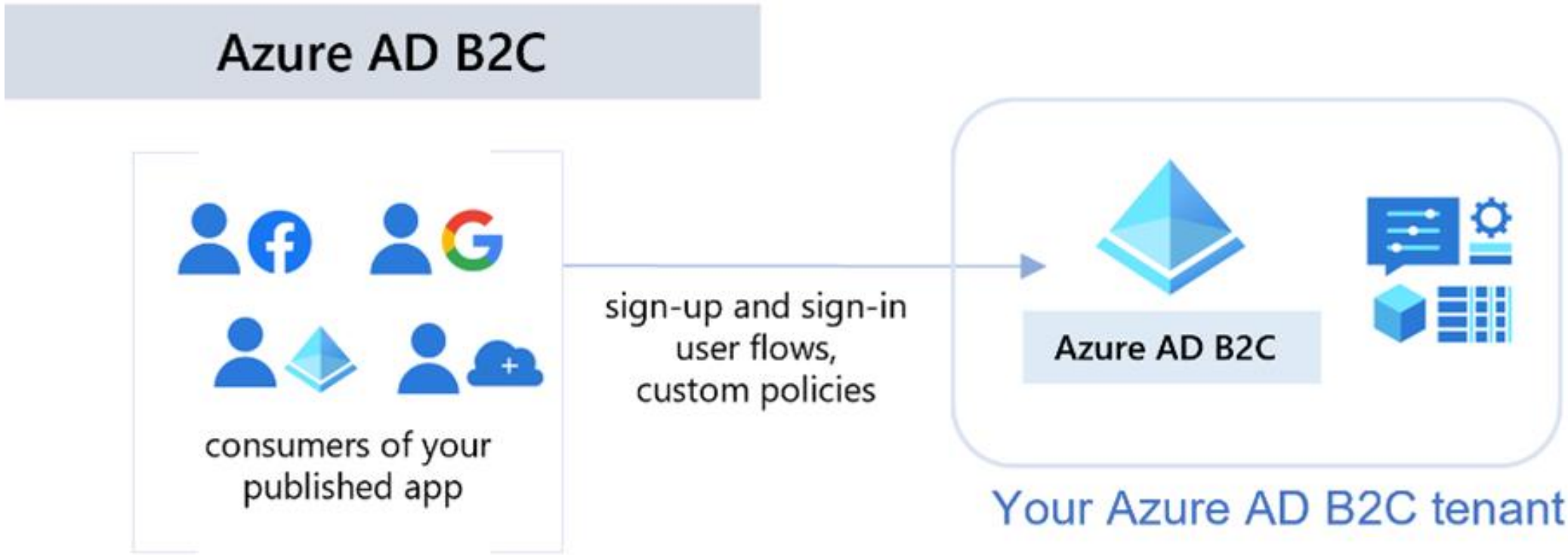
Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know ←→ Something you possess ←→ Something you are

External Identities B2B

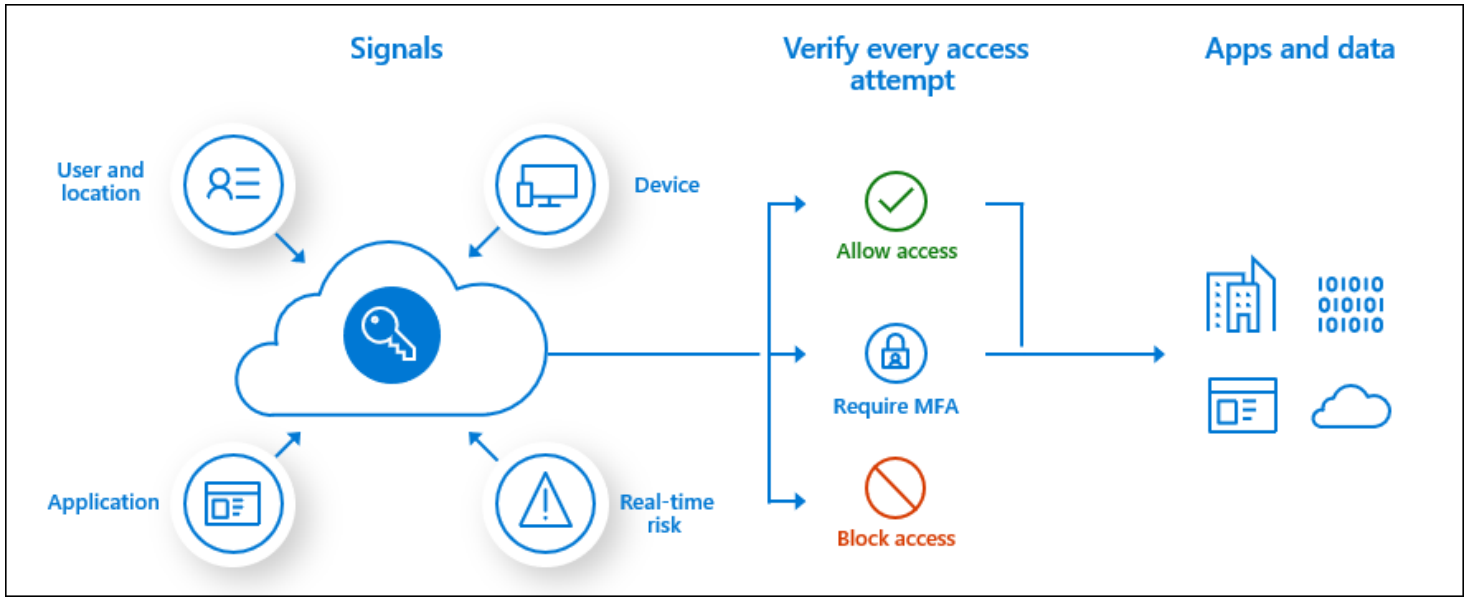


External Identities B2C



Conditional Access

- **Conditional Access is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals.**
- **These signals include who the user is, where the user is, and what device the user is requesting access from.**
  - User or Group Membership
  - IP Location
  - Device
  - Application
  - Risk Detection



Conditional Access

- Here, the signal might be the user's location, the user's device, or the application that the user is trying to access.
- Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.
- Enforcement is the action that carries out the decision. For example, the action is to allow access or require the user to provide a second form of authentication.

When can I use Conditional Access?

Conditional Access is useful when you need to:

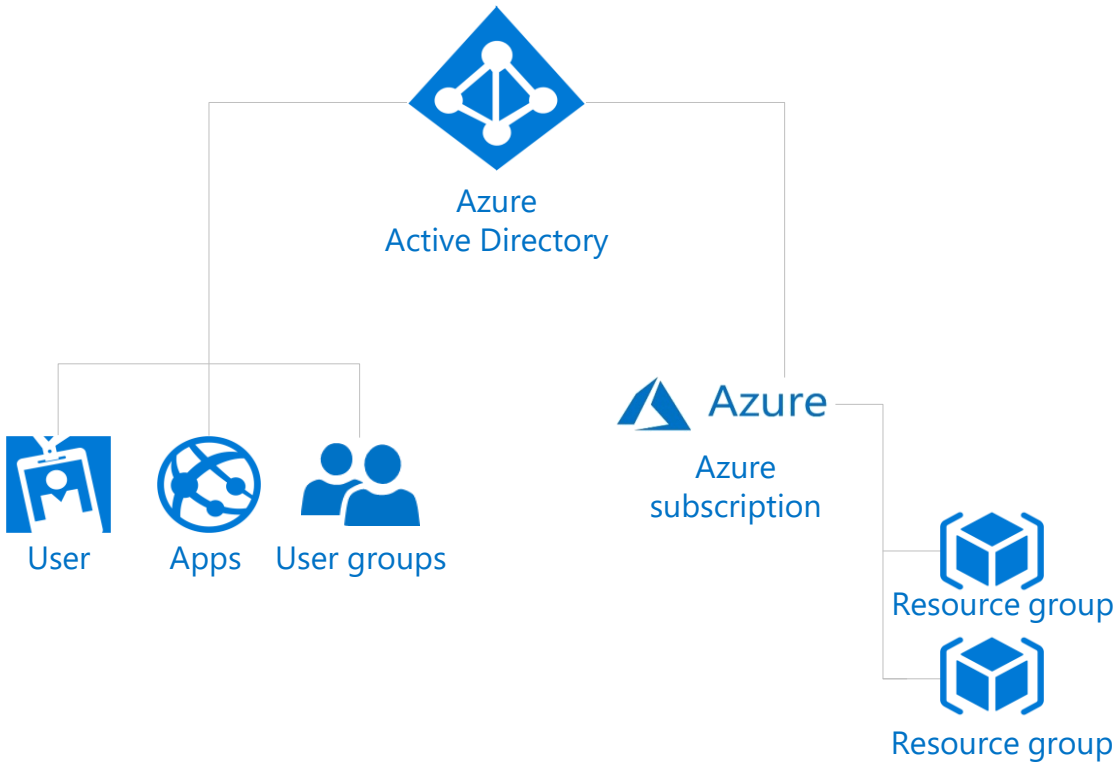
•Require multifactor authentication (MFA) to access an application depending on the requester's role, location, or network. For example, you could require MFA for administrators but not regular users or for people connecting from outside your corporate network.

•Require access to services only through approved client applications. For example, you could limit which email applications are able to connect to your email service.

•Require users to access your application only from managed devices. A managed device is a device that meets your standards for security and compliance.

•Block access from untrusted sources, such as access from unknown or unexpected locations.

Azure role-based access control (Azure RBAC)

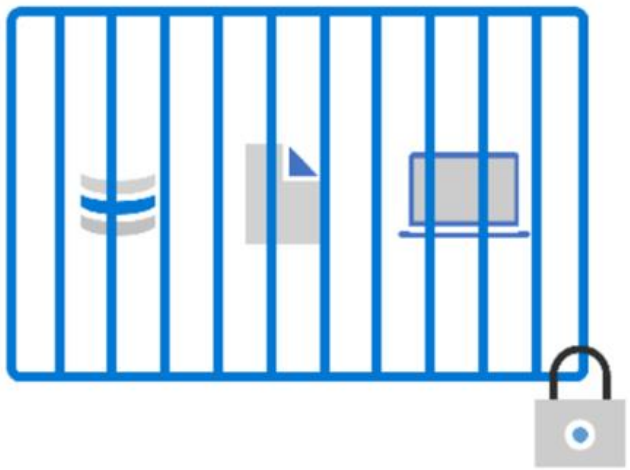


- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.

Zero Trust

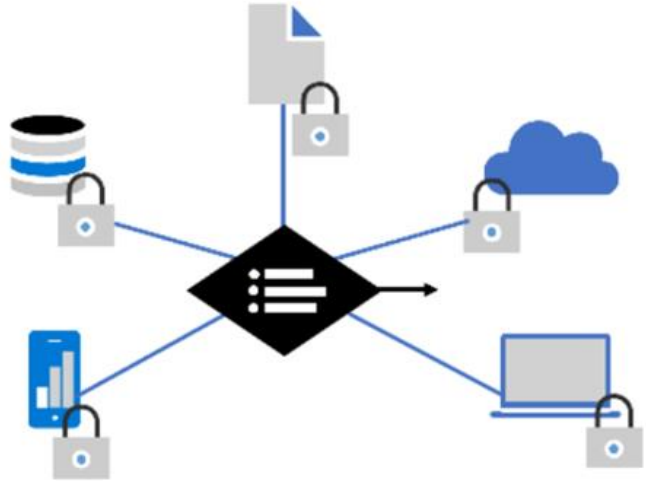
Secure assets where they are with Zero Trust

Simplify security and make it more effective



Classic Approach

Restrict everything to a 'secure' network

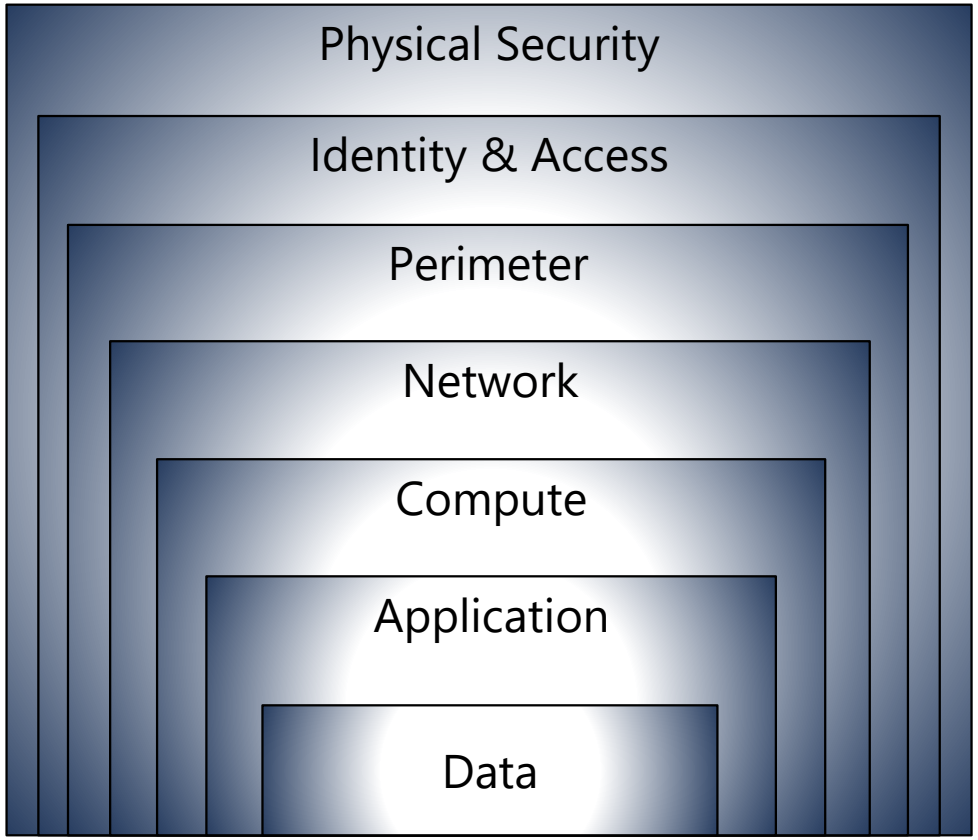


Zero Trust

Protect assets anywhere with central policy

Defense in depth

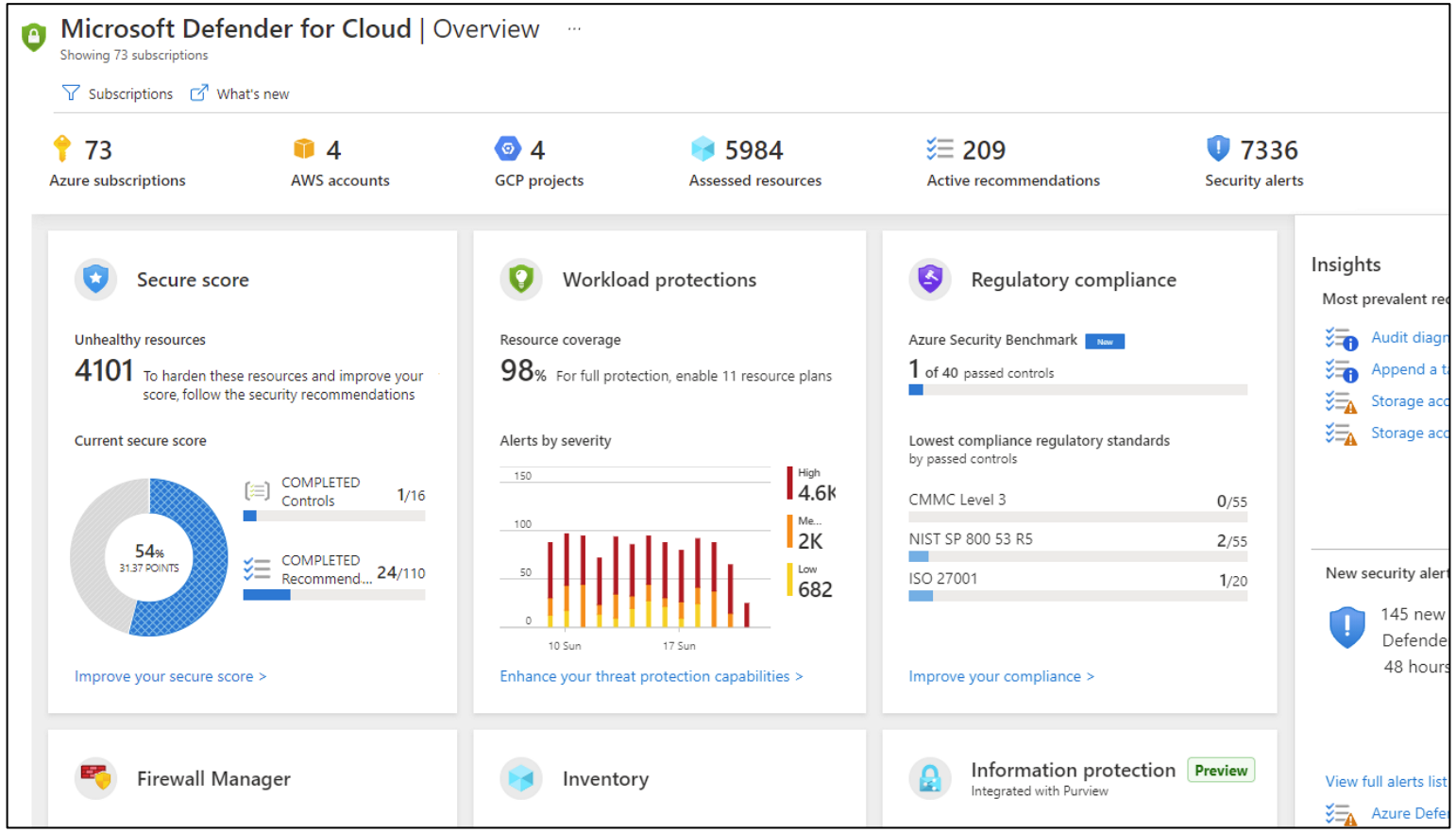
- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Microsoft Defender for Cloud

Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multicloud environments to provide guidance and notifications aimed at strengthening your security posture.

- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports



Defender for Cloud

Defender for Cloud helps you detect threats across:

•Azure PaaS services – Detect threats targeting Azure services including Azure App Service, Azure SQL, Azure Storage Account, and more data services. You can also perform anomaly detection on your Azure activity logs using the native integration with Microsoft Defender for Cloud Apps (formerly known as Microsoft Cloud App Security).

•Azure data services – Defender for Cloud includes capabilities that help you automatically classify your data in Azure SQL. You can also get assessments for potential vulnerabilities across Azure SQL and Storage services, and recommendations for how to mitigate them.

•Networks – Defender for Cloud helps you limit exposure to brute force attacks. By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access. You can set secure access policies on selected ports, for only authorized users, allowed source IP address ranges or IP addresses, and for a limited amount of time.