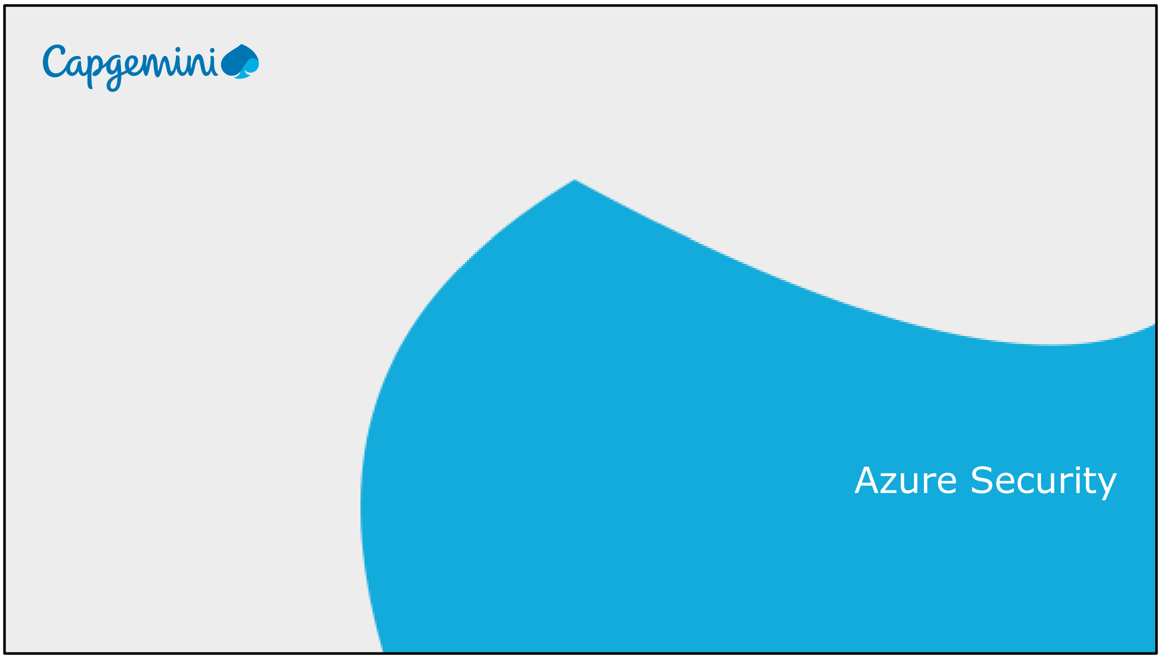
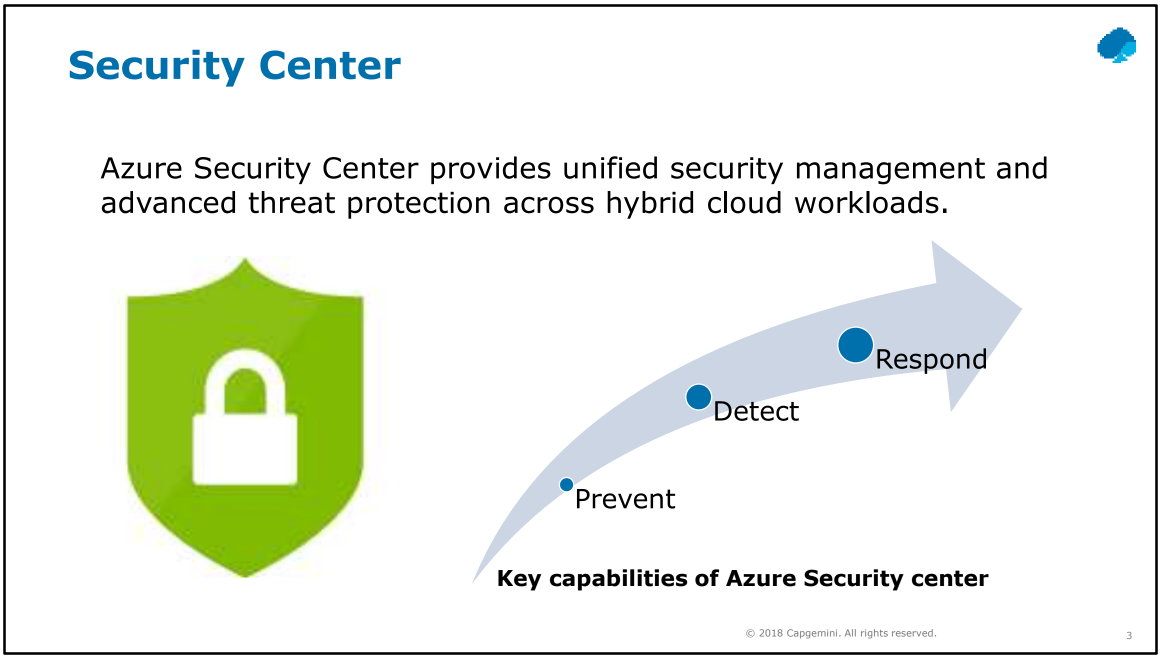


Azure Security

Lesson Objectives

At the end of this module you will be able to:

- ✓ Understand Azure Security
- ✓ Understand the usage of Azure Key Vault
- ✓ Explain the key principles of Azure Active Directory
- ✓ Demonstrate Role Based Access Control
- ✓ Enable multi factor authentication for Azure account



Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

Key capabilities of Azure Security center

Security Center helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions.

Below are the key capabilities of Azure Security center.

Prevent

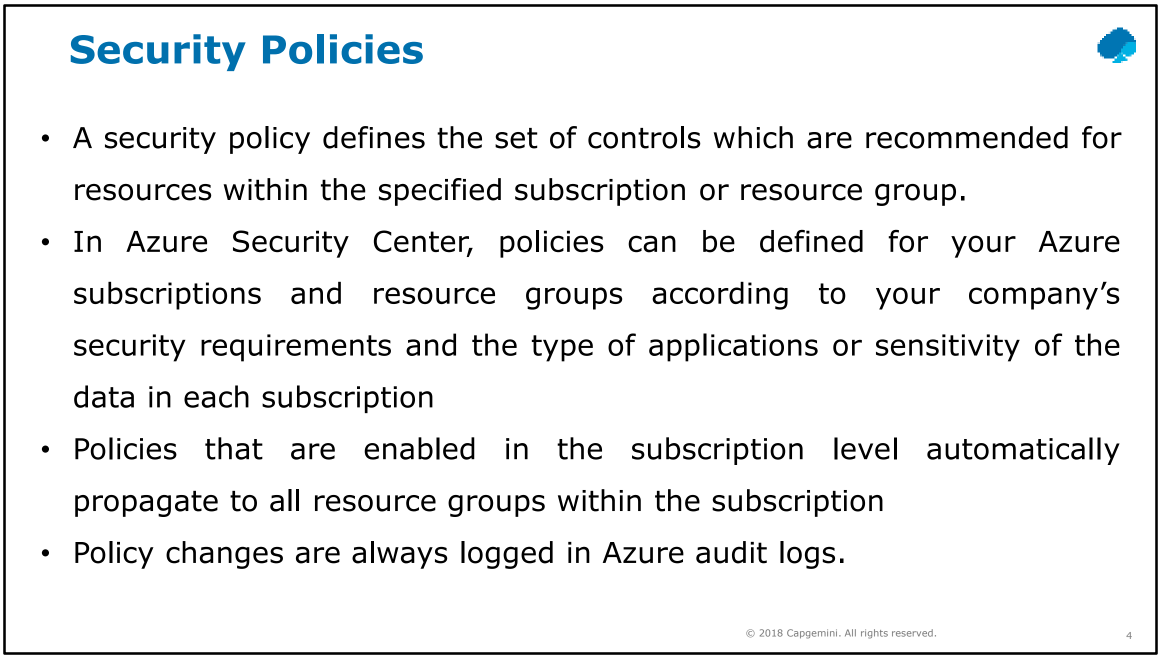
- Policy definition for Azure subscriptions and resource groups
- Azure resources security state monitoring

Detect

- Automatically collects and analyzes security data from Azure resources
- Leverages global threat intelligence from Microsoft products and services
- Applies advanced analytics

Respond

- Provides prioritized security incidents/alerts
- Offer insight into source of the attack
- Suggest way to stop the attack and prevent future attacks



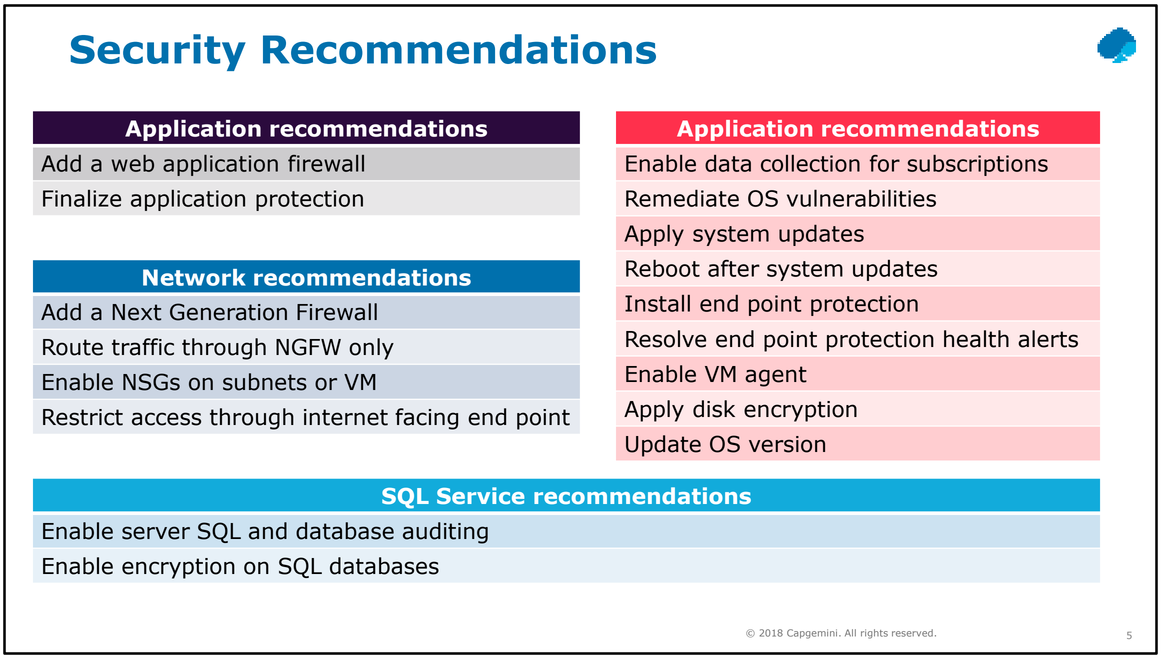
Security Policies

- A security policy defines the set of controls which are recommended for resources within the specified subscription or resource group.
- In Azure Security Center, policies can be defined for your Azure subscriptions and resource groups according to your company’s security requirements and the type of applications or sensitivity of the data in each subscription
- Policies that are enabled in the subscription level automatically propagate to all resource groups within the subscription
- Policy changes are always logged in Azure audit logs.

In case of a conflict between subscription level policy and resource group level policy, the resource group level policy takes precedence.

Security Center threat detection works by automatically collecting security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.

Security alerts are prioritized in Security Center along with recommendations on how to remediate the threat.



Security Recommendations

Application recommendations
Add a web application firewall
Finalize application protection

Network recommendations
Add a Next Generation Firewall
Route traffic through NGFW only
Enable NSGs on subnets or VM
Restrict access through internet facing end point

Application recommendations
Enable data collection for subscriptions
Remediate OS vulnerabilities
Apply system updates
Reboot after system updates
Install end point protection
Resolve end point protection health alerts
Enable VM agent
Apply disk encryption
Update OS version

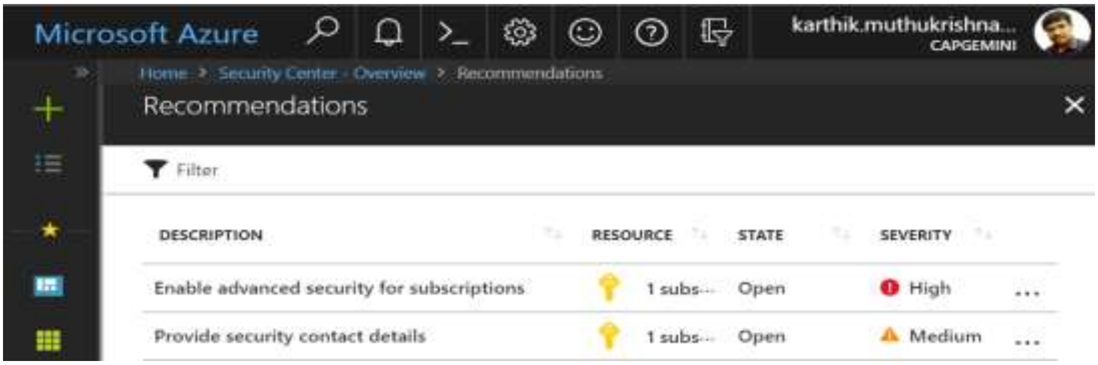
SQL Service recommendations
Enable server SQL and database auditing
Enable encryption on SQL databases

Security Center collects data from virtual machines in order to assess their security state, provide security recommendations and alert you to threats. Data that is collected will be stored in a storage account for further analysis.

Security Center periodically analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates recommendations

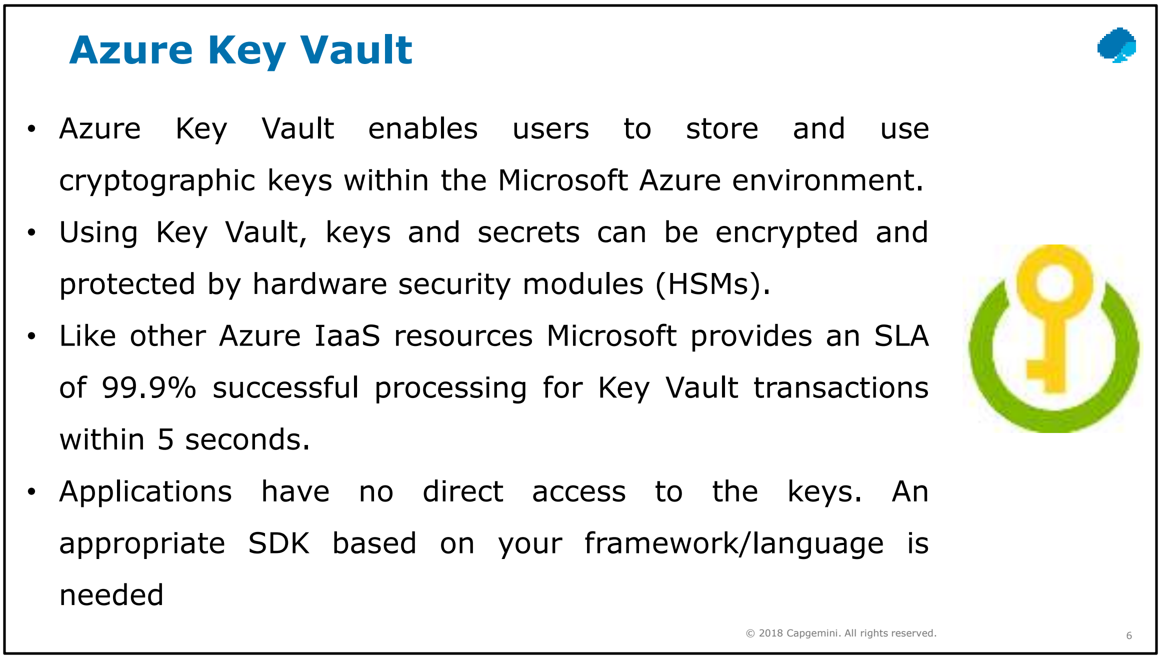
In order for security center to create recommendation, you have to
1. Configure security policies 2. Turn on data collection 3. Choose which recommendations to see as part of your security policy

The recommendations are shown in a table format where each line represents one particular recommendation.



Recommendations

DESCRIPTION	RESOURCE	STATE	SEVERITY
Enable advanced security for subscriptions	1 subs...	Open	High
Provide security contact details	1 subs...	Open	Medium



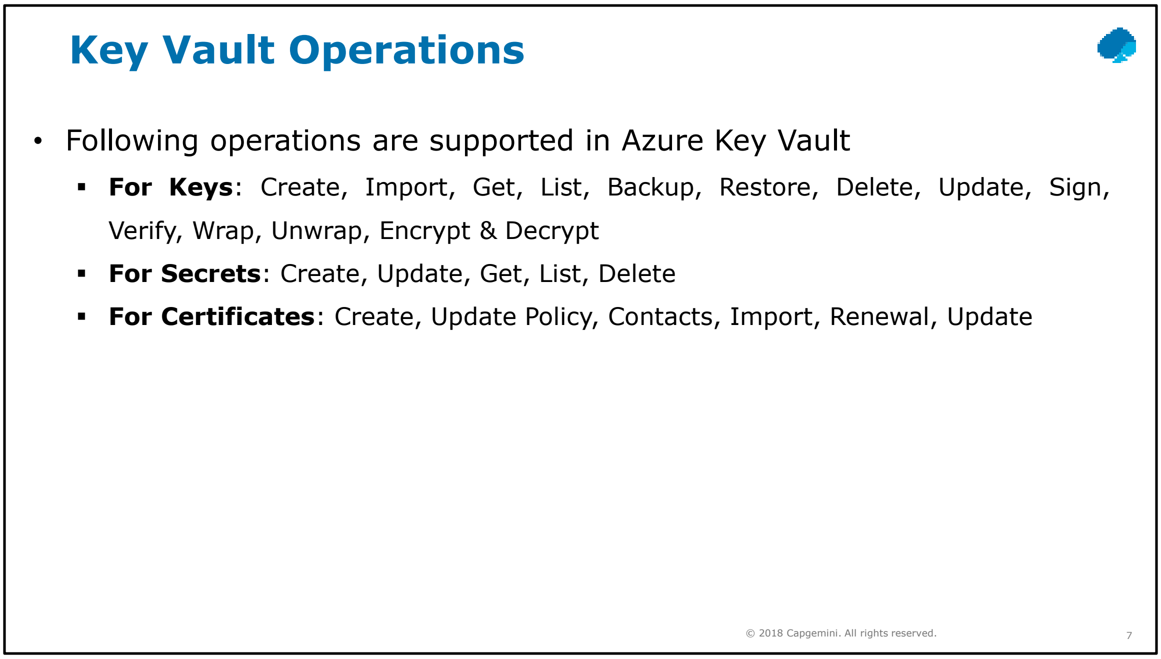
Azure Key Vault

- Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment.
- Using Key Vault, keys and secrets can be encrypted and protected by hardware security modules (HSMs).
- Like other Azure IaaS resources Microsoft provides an SLA of 99.9% successful processing for Key Vault transactions within 5 seconds.
- Applications have no direct access to the keys. An appropriate SDK based on your framework/language is needed

Azure Key Vault helps safeguard cryptographic keys and secrets used by Azure applications and services. You could store your storage account keys in an Azure Key Vault.

When you can’t control access to the data objects directly using Active Directory, you can control access to an Azure Key Vault using Active Directory. This means you can put your storage account keys in Azure Key Vault and then grant access to them for a specific user, group, or application.

Let’s say you have an application running as a Web App that uploads files to a storage account. You want to be really sure nobody else can access those files. You add the application to Azure Active Directory and grant it access to the Azure Key Vault with that storage account’s keys in it. After that, only that application can access those keys. This is much more secure than putting the keys in the web.config file where a hacker could get to them.



Key Vault Operations

- Following operations are supported in Azure Key Vault
  - **For Keys**: Create, Import, Get, List, Backup, Restore, Delete, Update, Sign, Verify, Wrap, Unwrap, Encrypt & Decrypt
  - **For Secrets**: Create, Update, Get, List, Delete
  - **For Certificates**: Create, Update Policy, Contacts, Import, Renewal, Update

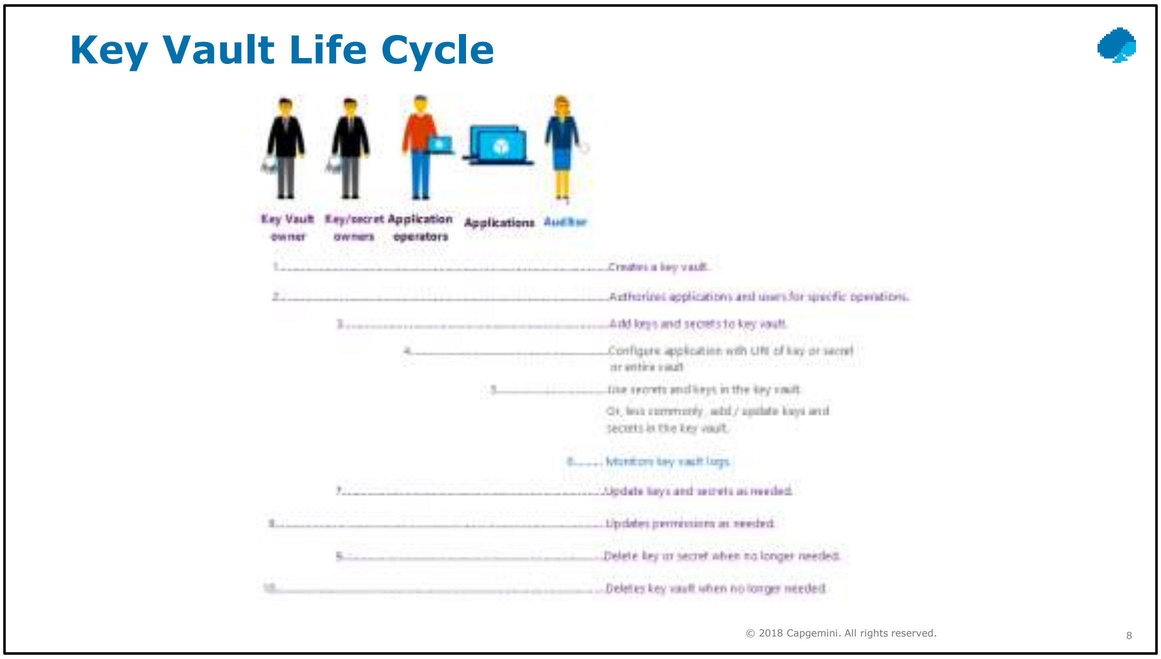
A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.

The HSM is used when security is paramount. As with other hardware devices, there is a fair bit of technicality involved in procuring, cost, installation, upgrade and maintenance (to name a few)... and that's before you can use it for all the benefit it provides!

To help you out of this hardware misery, Microsoft offers you Azure Key Vault (AKV) in the cloud. It offers the benefits of HSM, minus the headache in managing it.

Storing information in a database and an HSM is very different. The data doesn't simply stay in a file on your server. This information is stored in hardware device and the device offers you many features like auditing, tamper-proofing, encryption, etc. What Microsoft provides in the form of AKV is an interface using which you can access the HSM device in a secure way.

Secrets which are less than 10KB should be stored in the AKV. You can also store PFX files and manage SSL certificates using AKV. Database Connection strings, Social Network client keys, Subscription Keys, License Keys, and many other keys could be stored and managed easily using AKV

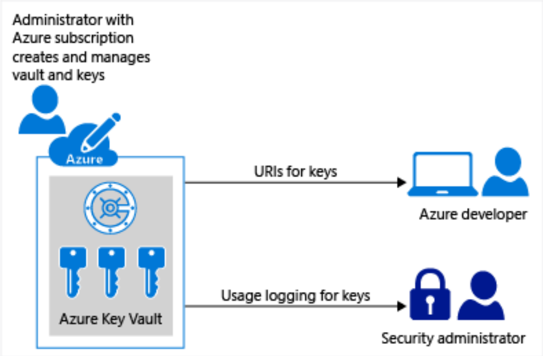


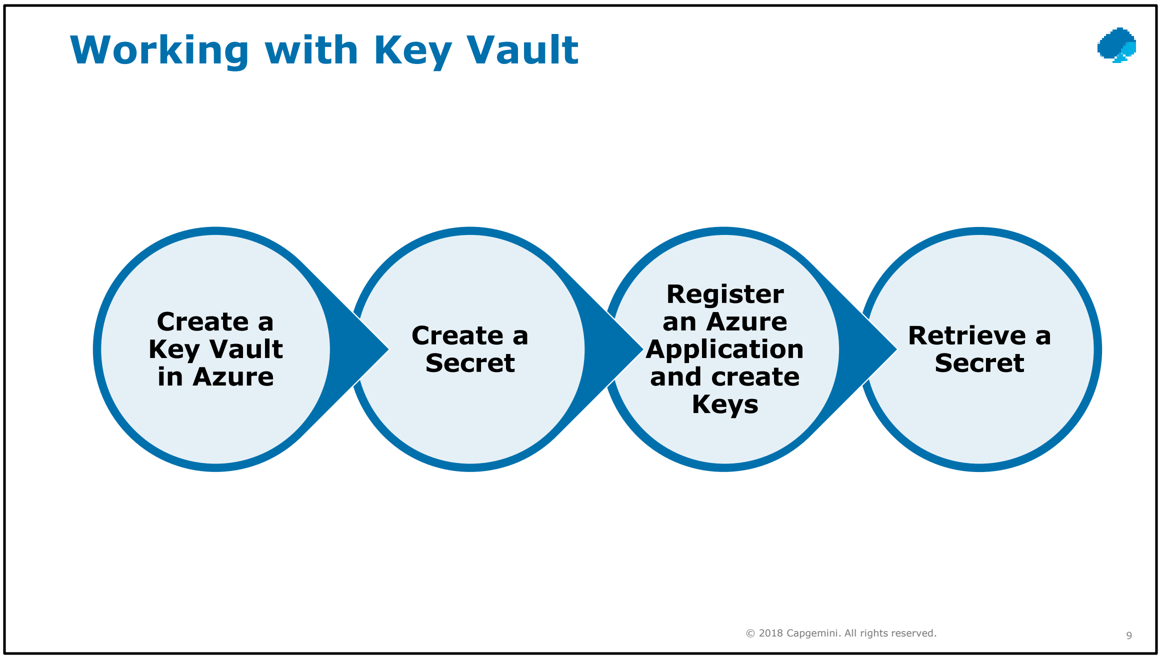
Key Vault Life Cycle

1. Creates a key vault.
2. Authorizes applications and users for specific operations.
3. Add keys and secrets to key vault.
4. Configure application with URI of key or secret or entire vault
5. Use secrets and keys in the key vault.
Or, less commonly, add / update keys and secrets in the key vault.
6. Monitors key vault logs.
7. Update keys and secrets as needed.
8. Updates permissions as needed.
9. Delete key or secret when no longer needed.
10. Deletes key vault when no longer needed.

Anybody with an Azure subscription can create and use key vaults. Although Key Vault benefits developers and security administrators, it could be implemented and managed by an organization’s administrator who manages other Azure services for an organization.
For example, this administrator would sign in with an Azure subscription, create a vault for the organization in which to store keys, and then be responsible for operational tasks, such as:

- Create or import a key or secret
- Revoke or delete a key or secret
- Authorize users or applications to access the key vault, so they can then manage or use its keys and secrets
- Configure key usage (for example, sign or encrypt)
- Monitor key usage





Working with Key Vault

Create a Key Vault in Azure

Create a Secret

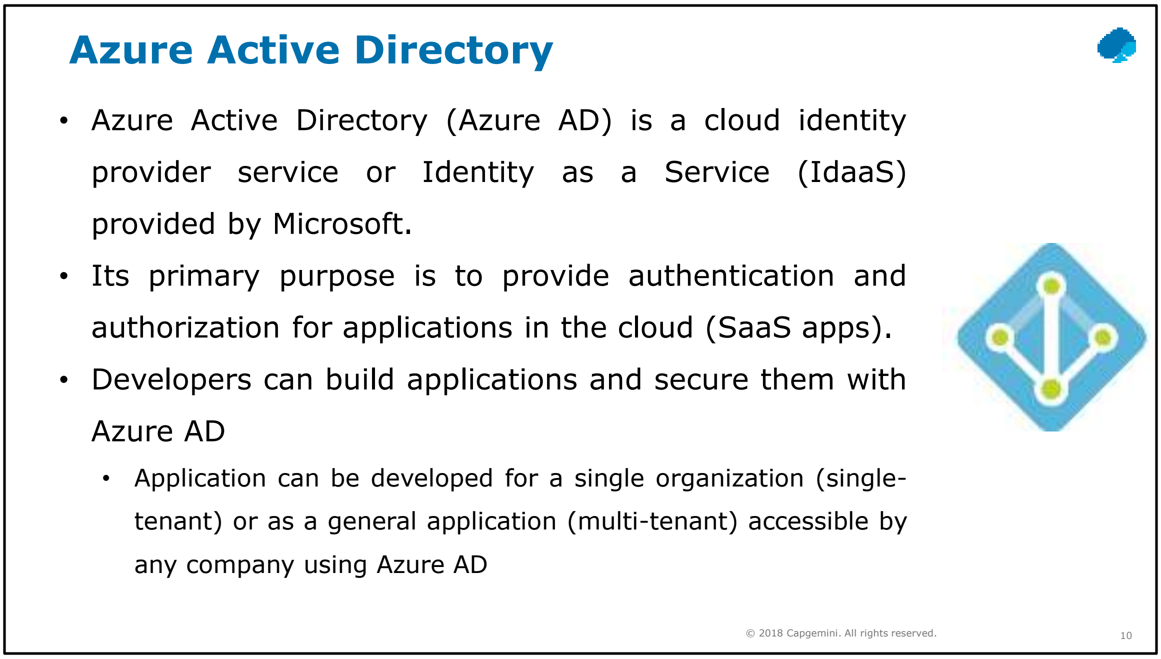
Register an Azure Application and create Keys

Retrieve a Secret

Keys are stored in a vault and invoked by URI when needed.

Keys are safeguarded by Azure, using industry-standard algorithms, key lengths, and hardware security modules (HSMs).

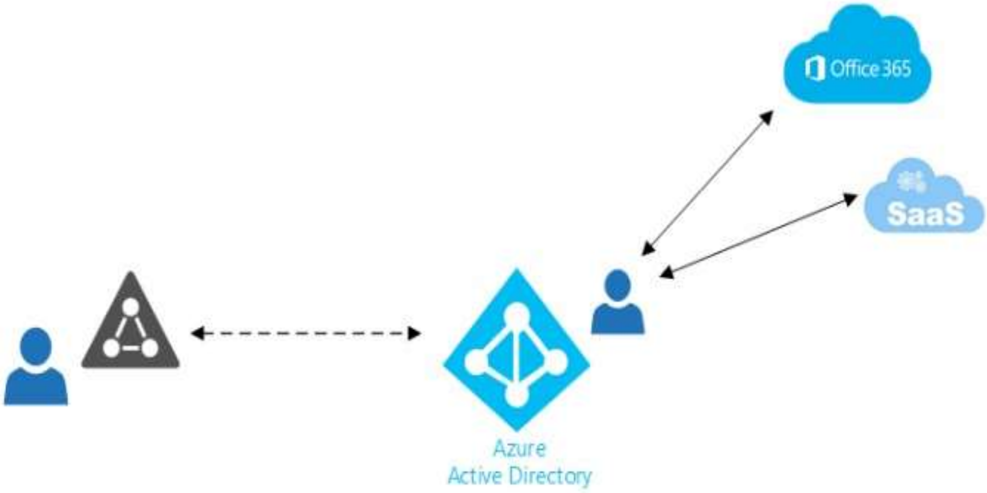
Keys are processed in HSMs that reside in the same Azure datacenters as the applications. This provides better reliability and reduced latency than if the keys reside in a separate location, such as on-premises.

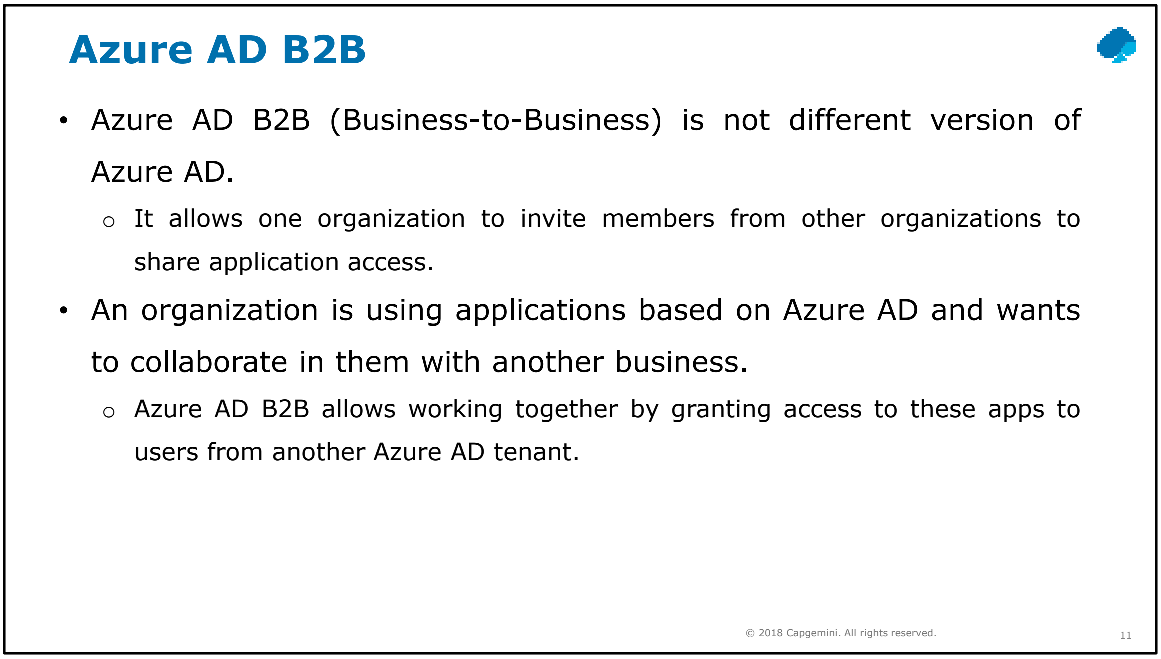


Azure Active Directory

- Azure Active Directory (Azure AD) is a cloud identity provider service or Identity as a Service (IdaaS) provided by Microsoft.
- Its primary purpose is to provide authentication and authorization for applications in the cloud (SaaS apps).
- Developers can build applications and secure them with Azure AD
  - Application can be developed for a single organization (single-tenant) or as a general application (multi-tenant) accessible by any company using Azure AD

Azure AD is meant for businesses to allow their users to work with cloud applications. Corporate users can be logged with your domain name. We can also create users on-premises and synchronize them with Azure AD or create them in the cloud directly



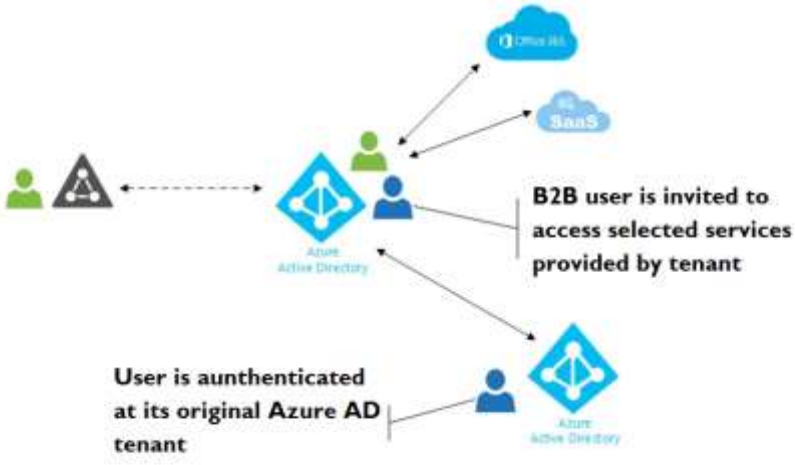


Azure AD B2B

- Azure AD B2B (Business-to-Business) is not different version of Azure AD.
  - It allows one organization to invite members from other organizations to share application access.
- An organization is using applications based on Azure AD and wants to collaborate in them with another business.
  - Azure AD B2B allows working together by granting access to these apps to users from another Azure AD tenant.

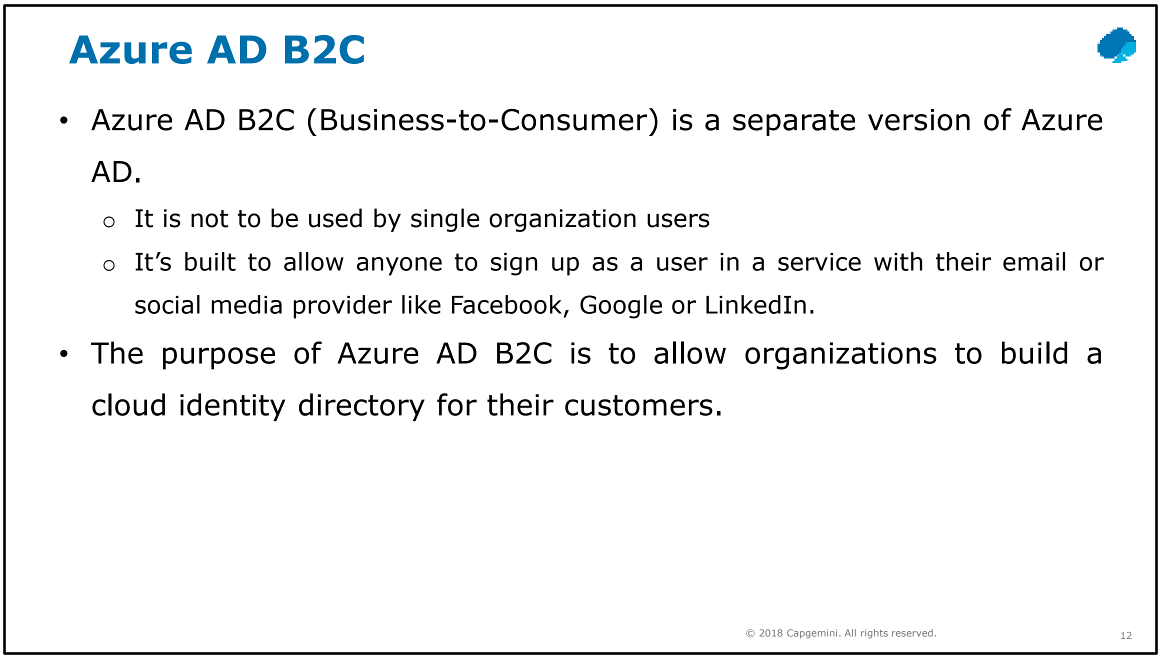
Azure AD B2B aims to address cross-organization problem. When you invite a user to your application, they will get access using their Azure AD account. No need to create an account for them. No need for a new password. They sign on to your app with their credentials.

Note: Azure is controlled by Azure AD. If you want to grant access to your Azure instance for an external consultant, don't use a Microsoft Account for that. Invite them with Azure B2B if they have an account in this service



B2B user is invited to access selected services provided by tenant

User is aunthenticated at its original Azure AD tenant

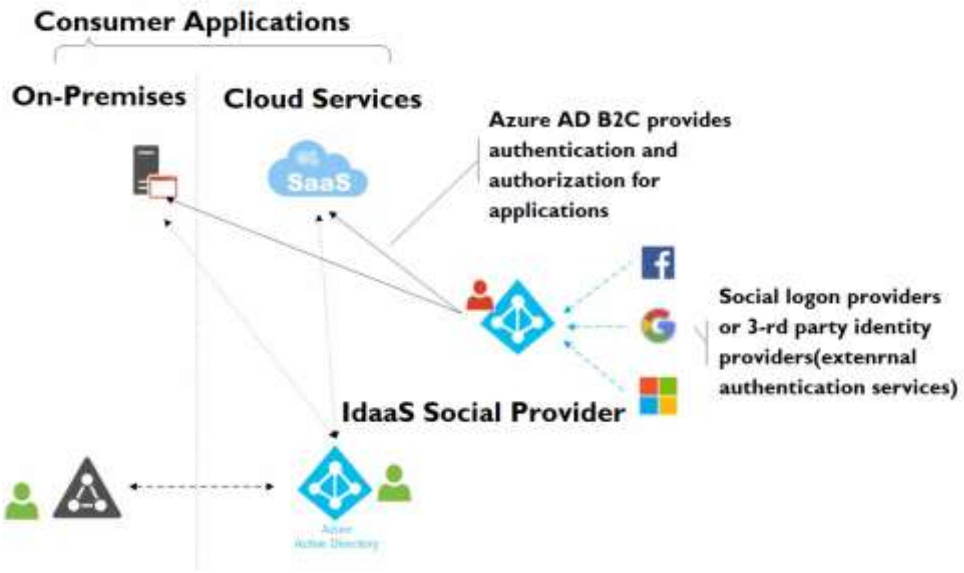


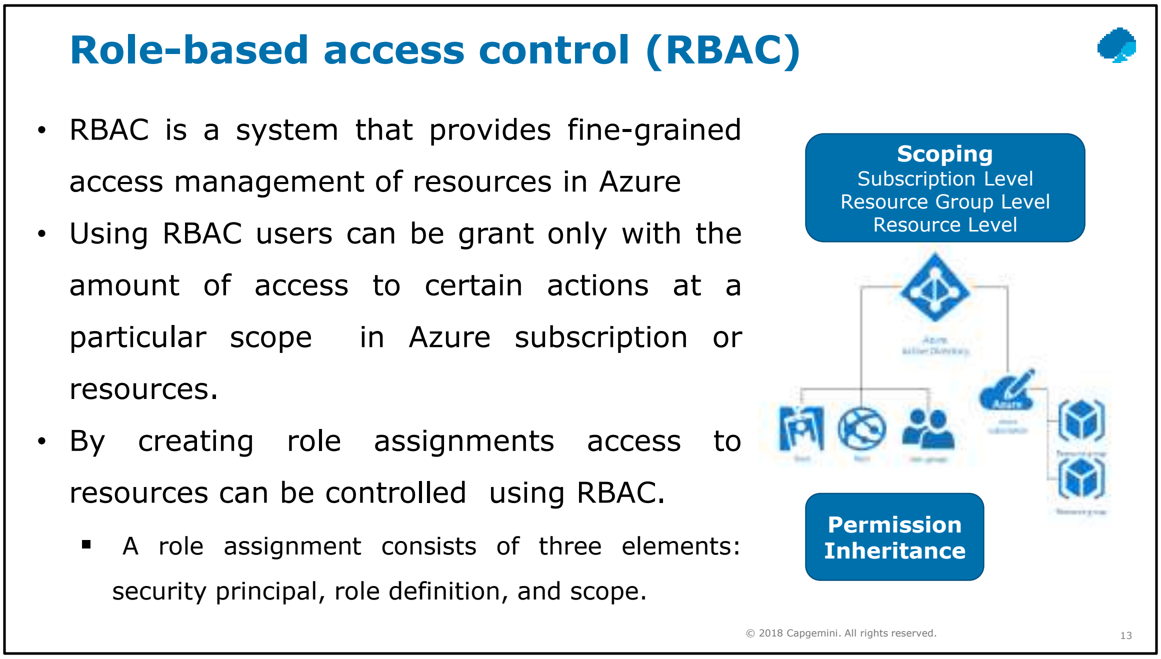
Azure AD B2C

- Azure AD B2C (Business-to-Consumer) is a separate version of Azure AD.
  - It is not to be used by single organization users
  - It’s built to allow anyone to sign up as a user in a service with their email or social media provider like Facebook, Google or LinkedIn.
- The purpose of Azure AD B2C is to allow organizations to build a cloud identity directory for their customers.

Azure AD B2C is an identity repository in the cloud that allows your users to sign up for your applications with an email address and password (no restrictions on the email domain) or social media logins. The service itself handles all the processes like sign-up, sign-in, password reset and so on. You don’t have to worry about it.

If you establish it once and your customer is signed up, and later you spin off a new application – it is all there. They don’t have to sign up again. They can use their existing account for your applications. Multiple applications can use the same directory to provide the client with SSO experience in your applications.


Consumer Applications
On-Premises
Cloud Services
SaaS
Azure AD B2C provides authentication and authorization for applications
Social logon providers or 3-rd party identity providers(extenrnal authentication services)
IdaaS Social Provider
Azure Active Directory



Role-based access control (RBAC)

- RBAC is a system that provides fine-grained access management of resources in Azure
- Using RBAC users can be grant only with the amount of access to certain actions at a particular scope in Azure subscription or resources.
- By creating role assignments access to resources can be controlled using RBAC.
  - A role assignment consists of three elements: security principal, role definition, and scope.

Scoping
Subscription Level
Resource Group Level
Resource Level

Permission Inheritance

Here are some examples of what you can do with RBAC:

- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- Allow an application to access all resources in a resource group

Security principal

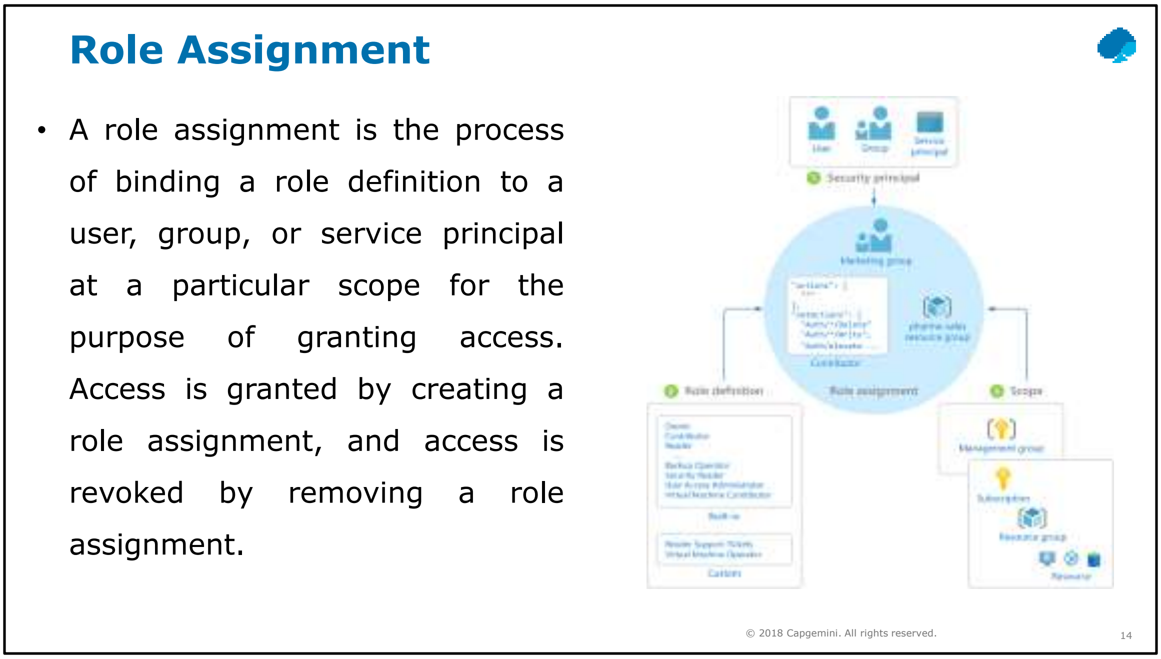
A *security principal* is an object that represents a user, group, or service principal that is requesting access to Azure resources.

Role definition

A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the operations that can be performed, such as read, write, and delete.

Scope

Scope is the boundary that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope. This is helpful if you want to make someone a Website Contributor, but only for one resource group.



Role Assignment

- A role assignment is the process of binding a role definition to a user, group, or service principal at a particular scope for the purpose of granting access. Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

User
Group
Service principal
Security principal
Marketing group
"actions": [
"*"
],
"notActions": [
"Authorization/*/Delete",
"Authorization/*/Write",
"Authorization/elevateAccess/Action"
Contributor
pharma-sales resource group
Role definition
Role assignment
Scope
Owner
Contributor
Reader
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor
Built-in
Reader Support Tickets
Virtual Machine Operator
Custom
Management group
Subscription
Resource group
Resource

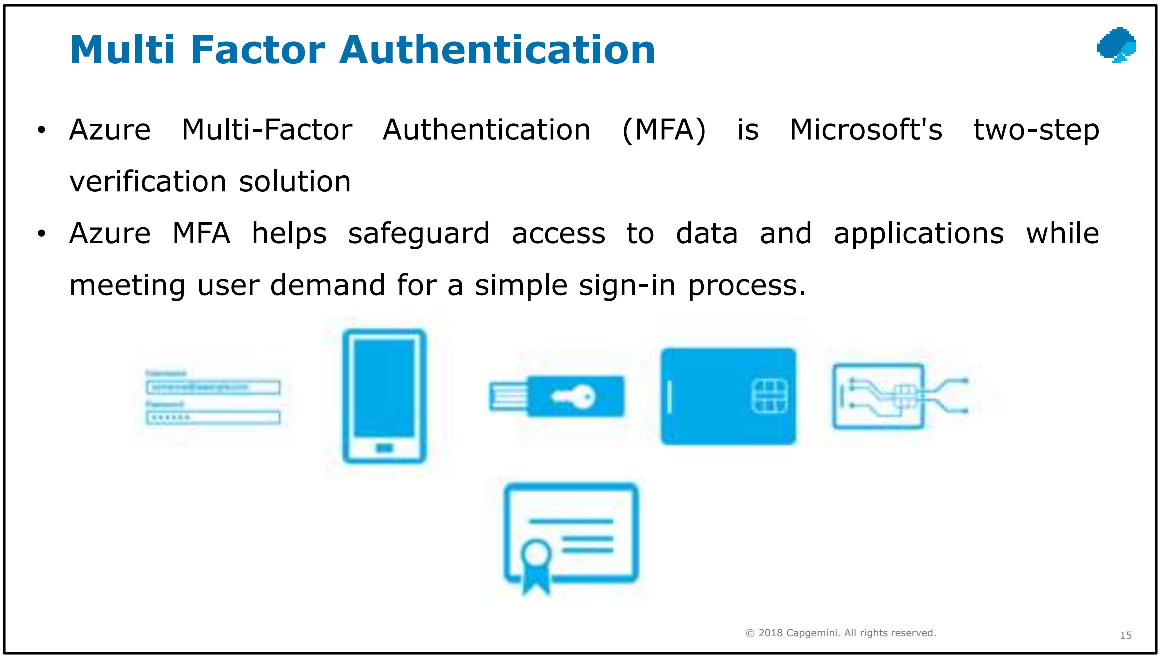
Roles

Owner:
Full access

Contributor:
Full resource access but no grant/revoke privileges

Reader:
Read-only resource access

Custom:
Defined programmatically with PowerShell, CLI, or REST API



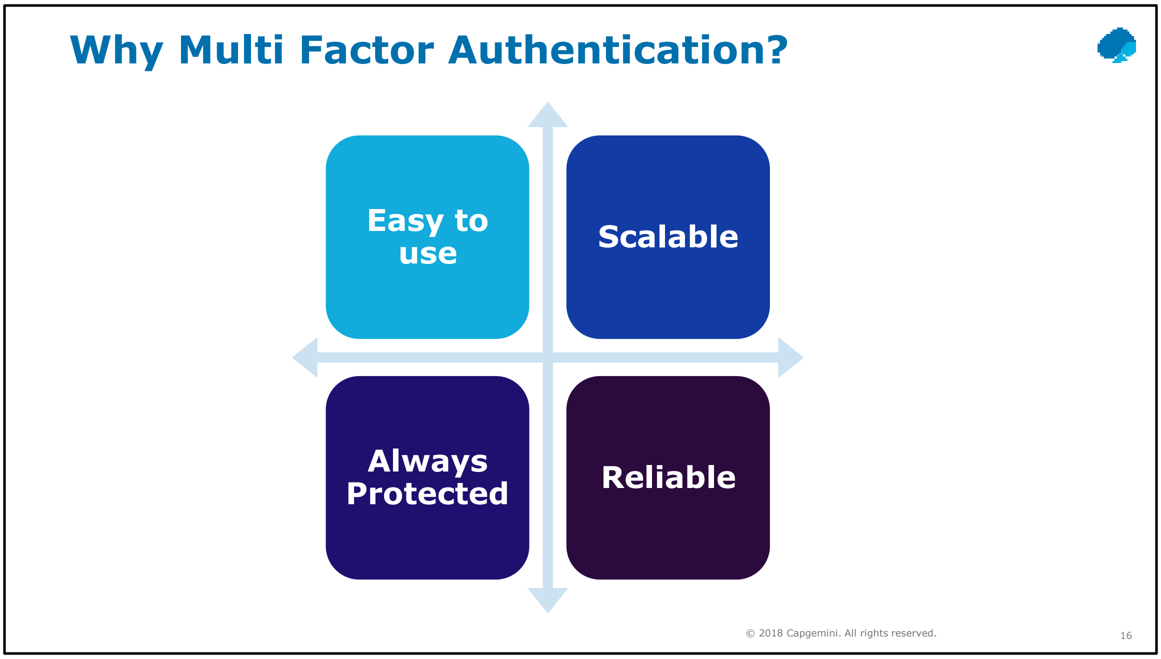
Multi Factor Authentication

- Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution
- Azure MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process.

Two-step verification is a method of authentication that requires more than one verification method and adds a critical second layer of security to user sign-ins and transactions.

It works by requiring any two or more of the following verification methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)



Why Multi Factor Authentication?

Easy to use

Scalable

Always Protected

Reliable

Today, more than ever, people are increasingly connected. With smart phones, tablets, laptops, and PCs, people have multiple options to access their accounts and applications from anywhere and stay connected at any time.

Azure Multi-Factor Authentication is an easy to use, scalable, and reliable solution that provides a second method of authentication to protect your users.

Easy to Use

Azure Multi-Factor Authentication is simple to set up and use. The extra protection that comes with Azure Multi-Factor Authentication allows users to manage their own devices. Best of all, in many instances it can be set up with just a few simple clicks.

Scalable

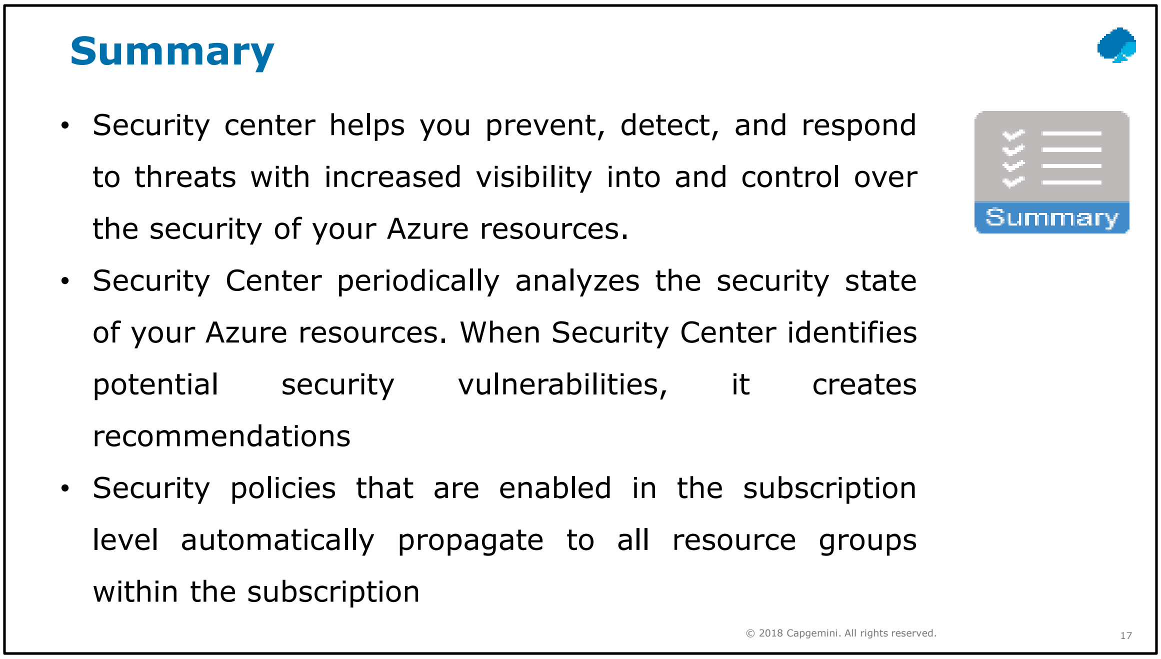
Azure Multi-Factor Authentication uses the power of the cloud and integrates with your on-premises AD and custom apps. This protection is even extended to your high-volume, mission-critical scenarios.

Always Protected

Azure Multi-Factor Authentication provides strong authentication using the highest industry standards.

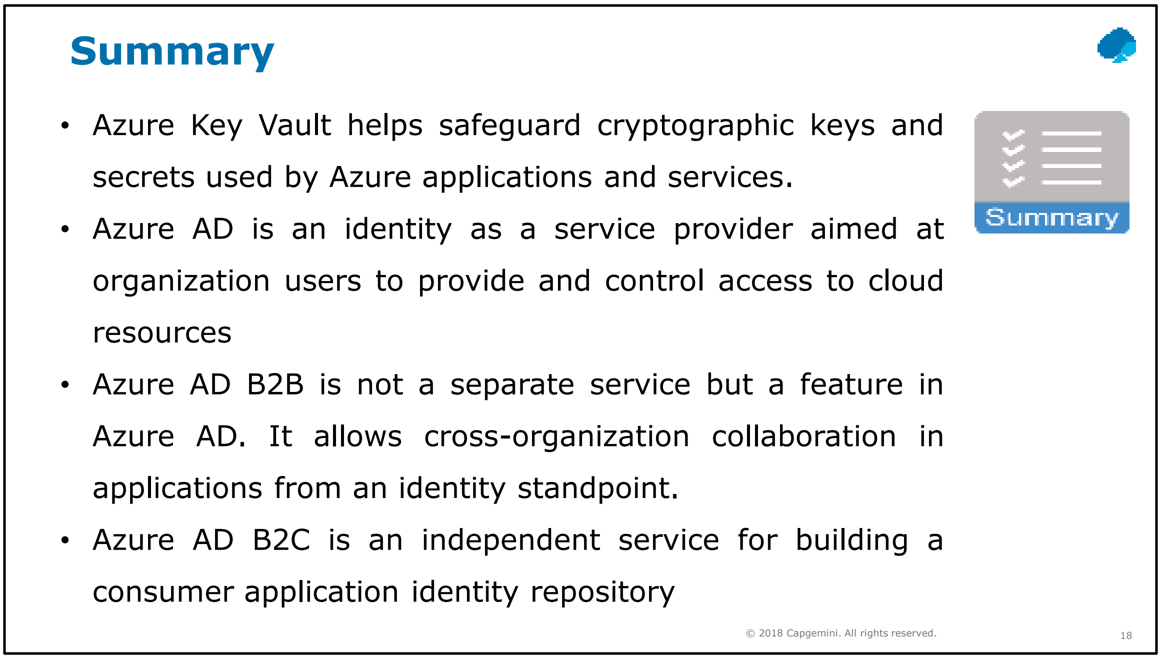
Reliable

Microsoft guarantees 99.9% availability of Azure Multi-Factor Authentication. The service is considered unavailable when it is unable to receive or process verification requests for the two-step verification.



Summary

- Security center helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources.
- Security Center periodically analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates recommendations
- Security policies that are enabled in the subscription level automatically propagate to all resource groups within the subscription



Summary

- Azure Key Vault helps safeguard cryptographic keys and secrets used by Azure applications and services.
- Azure AD is an identity as a service provider aimed at organization users to provide and control access to cloud resources
- Azure AD B2B is not a separate service but a feature in Azure AD. It allows cross-organization collaboration in applications from an identity standpoint.
- Azure AD B2C is an independent service for building a consumer application identity repository

People matter, results count.

This message contains information that may be privileged or confidential and is the property of the Capgemini Group.

About Capgemini

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR 12.5 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at

www.capgemini.com

This message is intended only for the person to whom it is addressed. If you are not the intended recipient, you are not authorized to read, print, retain, copy, disseminate, distribute, or use this message or any part thereof. If you receive this message in error, please notify the sender immediately and delete all copies of this message.