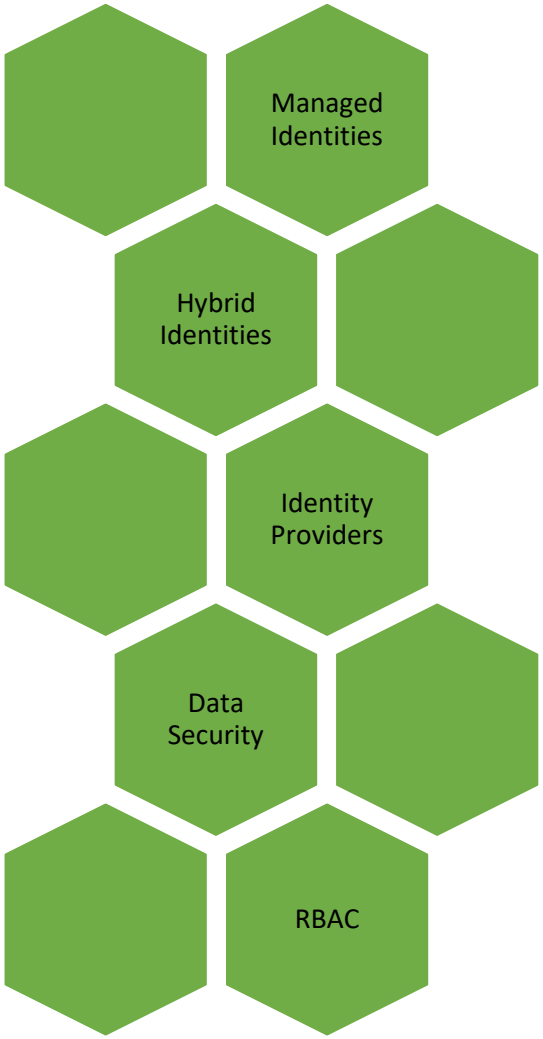
Securing Resources



Design Security and Identity Solutions (20%-25%)

- Design an identity solution
  - Design AD Connect synchronization; design federated identities using Active Directory Federation Services (AD FS); design solutions for Multi-Factor Authentication (MFA); design an architecture using Active Directory on-premises and Azure Active Directory (AAD); determine when to use Azure AD Domain Services; design security for Mobile Apps using AAD
- Secure resources by using identity providers
  - Design solutions that use external or consumer identity providers such as Microsoft account, Facebook, Google, and Yahoo; determine when to use Azure AD B2C and Azure AD B2B; design mobile apps using AAD B2C or AAD B2B
- Design a data security solution
  - Design data security solutions for Azure services; determine when to use Azure Storage encryption, Azure Disk Encryption, Azure SQL Database security capabilities, and Azure Key Vault; design for protecting secrets in ARM templates using Azure Key Vault; design for protecting application secrets using Azure Key Vault; design a solution for managing certificates using Azure Key Vault; design solutions that use Azure AD Managed Service Identity
- Design a mechanism of governance and policies for administering Azure resources
  - Determine when to use Azure RBAC standard roles and custom roles; define an Azure RBAC strategy; determine when to use Azure resource policies; determine when to use Azure AD Privileged Identity Management; design solutions that use Azure AD Managed Service Identity; determine when to use HSM-backed keys
- Manage security risks by using an appropriate security solution
  - Identify, assess, and mitigate security risks by using Azure Security Center, Operations Management Suite Security and Audit solutions, and other services; determine when to use Azure AD Identity Protection; determine when to use Advanced Threat Detection; determine an appropriate endpoint protection strategy

Secure resources by using managed identities

On-Premise Active Directory vs Azure AD

Active Directory On-Premise	Azure AD
Authentication Provider	Authentication Provider
Internal single customer directory service	Multi-customer public directory service
Hierarchical structure of: Users, Computers, Ous, Groups, Services	Flat structure of: Users and Groups
Group Policy and DNS data	NA
Can be accessed using LDAP	Can be accessed using Graph API
Primarily uses Kerberos for authentication	Authentication can use SAML, WS-Federation and Oauth
Can Join VM and computer to domain	Can’t join VMs and computer(Except Windows 10)
AD DS Forest, Trees, Domains e.g cloudapp.net	Azure AD Tenants eg. Contoso.onmicrosoft.com

Azure AD Edition Features

	FREE	BASIC	PREMIUM P1	PREMIUM P2
Common Features				
Directory Objects [1]	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
User/Group Management (add/update/delete)/ User-based provisioning, Device registration	✓	✓	✓	✓
Single Sign-On (SSO)	10 apps per user[2] (pre-integrated SaaS and developer-integrated apps)	10 apps per user[2] (free tier + Application proxy apps)	No Limit (free, Basic tiers +Self-Service App Integration templates[5])	No Limit (free, Basic tiers +Self-Service App Integration templates[5])
B2B Collaboration [7]	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓
Connect (Sync engine that extends on-premises directories to Azure Active Directory)	✓	✓	✓	✓
Security/Usage Reports	3 Basic Reports	3 Basic Reports	Advanced Reports	Advanced Reports
Premium + Basic Features				
Group-based access management/provisioning		✓	✓	✓
Self-Service Password Reset for cloud users		✓	✓	✓
Company Branding (Logon Pages/Access Panel customization)		✓	✓	✓
Application Proxy		✓	✓	✓
SLA		✓	✓	✓

https://azure.microsoft.com/en-us/pricing/details/active-directory/

Azure AD Premium Features

	FREE	BASIC	PREMIUM P1	PREMIUM P2
Premium Features				
Self-Service Group and app Management/Self-Service application additions/ Dynamic Groups			✓	✓
Self-Service Password Reset/Change/Unlock with on-premises writeback			✓	✓
Device objects two-way synchronization between on-premises directories and Azure AD (Device write-back)			✓	✓
Multi-Factor Authentication (Cloud and On-premises (MFA Server))	--[3]	--[3]	✓	✓
Microsoft Identity Manager user CAL[4]			✓	✓
Cloud App Discovery			✓	✓
Connect Health[6]			✓	✓
Automatic password rollover for group accounts			✓	✓
Conditional Access based on group and location			✓	✓
Conditional Access based on device state (Allow access from managed devices)			✓	✓
Identity Protection				✓
Privileged Identity Management				✓

https://azure.microsoft.com/en-us/pricing/details/active-directory/

Which Azure AD editions provide self service password reset?

1) Free
2) Basic
3) Premium

Which Azure AD editions provide self service password reset?

2) Basic
3) Premium

Access Azure AD using Graph API

REST API endpoints (OData 3.0 compliant)

Supports common CRUD operations:

- Create a new user in a directory
- Get a user's detailed properties
- Update a user's properties
- Check a user's group membership for role-based access
- Disable a user's account or delete it entirely

NOTE: **Microsoft Graph** is the next up and coming way to do this

Home - Microsoft Graph - Microsoft Developer

https://developer.microsoft.com/en-us/graph

Find out how you can use the **Microsoft Graph** API to connect to the data that drives productivity - mail, calendar, contacts, documents, directory, devices, and ...

Documentation

Users - Calendar - Mail - V1.0 reference - Groups - Quick starts

Quick Start

These quick starts use Microsoft Graph to access three services ...

Graph Explorer

The Microsoft Graph explorer is a tool that lets you make requests ...

Use the API

Microsoft Graph. Microsoft 365 · Azure · Office 365 · Dynamics ...

Examples

See examples of solutions that use Microsoft Graph.

User - Documentation

Represents an Azure AD user account. Inherits from ...

Graph Explorer

Authentication

You are currently using a sample account.
To access your own data:

Sign in with Microsoft

Sample Queries

Getting Started

- GET my profile
- GET my photo
- GET my mail
- GET all the items in my drive
- GET items trending around me
- GET my manager

show more samples

History

GET | v1.0 | https://graph.microsoft.com/v1.0/me/ | Run Query

Request Body | Request Headers

When you use the Microsoft Graph API, you agree to the Microsoft Graph Terms of Use and the Microsoft Privacy Statement.

Response Preview | Response Headers

Empower creativity and collaboration

Microsoft Graph is the API for Microsoft 365, securely connecting you to Office 365, Windows 10, and Enterprise Mobility + Security.

LEARN MORE >

Rich context

Get rich context for your applications, such as who someone's manager is, whether they are out of office, or what documents they've been working on.

Deep insights

Access deep insights generated from usage patterns, such as trending documents, best team meeting times, or who people typically work with.

Real-time updates

Respond to changes in Microsoft Graph data in real time. Reschedule a meeting based on responses, notify others when a file is modified, or continue a process after it's been approved.

Broad reach

Build solutions that target enterprise users in Azure and Office 365, consumers on Office Online (Outlook.com and OneDrive.com), or both.

90%

of all Fortune 500 companies have data in Microsoft Graph

135M

monthly active users on Office 365 commercial

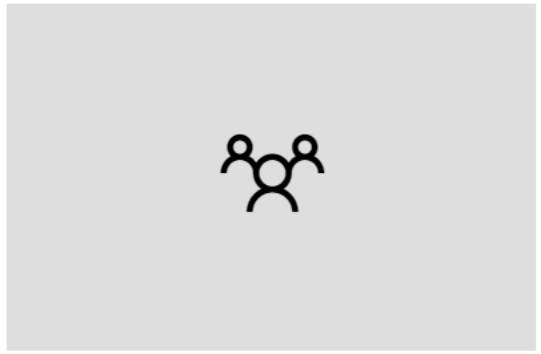
400M

Outlook.com active users

8T

resources (emails, events, users, files, groups, and more) in Microsoft Graph

See examples of what you can do with Microsoft Graph



Onboard users

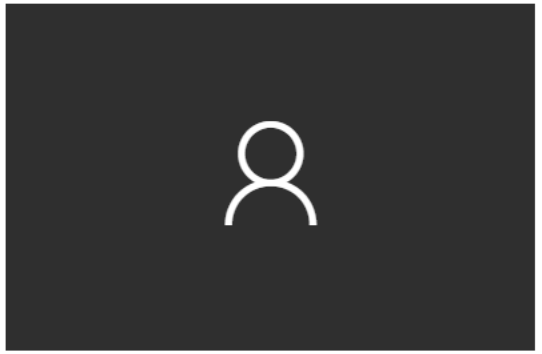
Automate user onboarding workflows and manage changes to user roles within an organization.

LEARN MORE >

Integrate with Excel

Tap into Excel data to build powerful workflows that automate data collection.

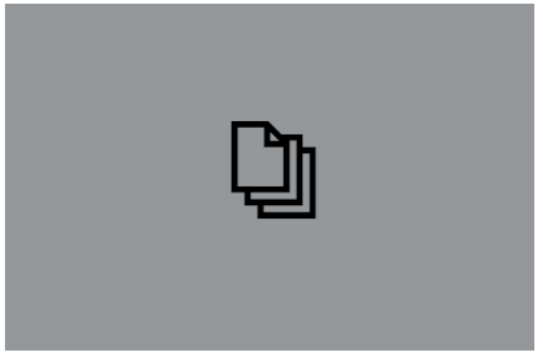
LEARN MORE >



Manage employee profiles

Manage employee information stored across various locations in the enterprise.

LEARN MORE >



Convert documents

Easily convert multiple file formats to PDFs for sharing and distribution.

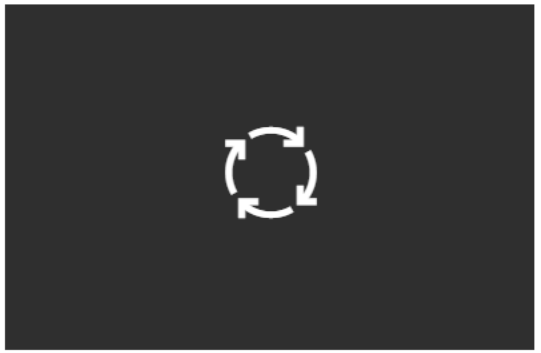
LEARN MORE >

SEE MORE >

Manage employee profiles

Manage employee information stored across various locations in the enterprise.

LEARN MORE >



Keep email data in sync

Subscribe to mailboxes for updates and sync data efficiently.

LEARN MORE >

How some of our partners are using Microsoft Graph

approved contact

zapier

smartsheet

hyperfish

harmon.ie

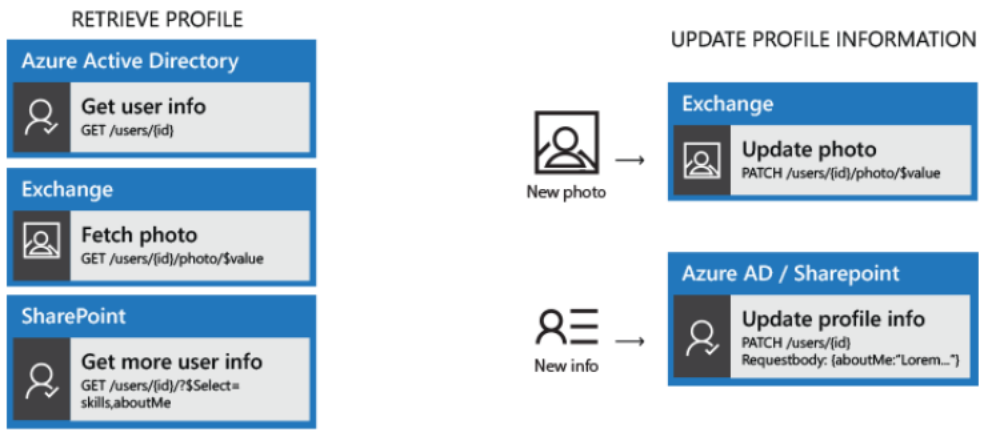
SEE MORE >

Use Microsoft Graph to manage employee profiles

hyperfish

With Microsoft Graph we are able to analyze and detect missing or incorrect profile information using a consistent, performant and secure API for organizations in the cloud.

Hyperfish



Keep your company directory up to date

Keeping company directory information up-to-date is a key concern for many organizations. You can use Microsoft Graph to update profile information stored in various locations via a single endpoint. Update profile photos stored in Exchange, directory information in Azure Active Directory, and profile information in SharePoint, all via Microsoft Graph APIs. You can use the same APIs to query for profile information, reducing issues around compliance and productivity loss caused by missing or out of date information.

Microsoft Graph API is the gateway for


Azure AD


Excel


Intune


Outlook


OneDrive


OneNote


SharePoint


Planner

Supported platforms


Android


Angular


ASP.NET MVC


iOS


JavaScript


PHP


Python


Ruby


UWP


Xamarin

TRY THE QUICK START >

** The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License.*

Microsoft Graph Quick Start

Build a simple app that connects to Office 365 and calls the Microsoft Graph API.

These quick starts use Microsoft Graph to access three services with one authentication: Microsoft account, OneDrive, and Outlook. The quick starts involve four steps:

1. Select your platform.
2. Get your app ID (client ID).
3. Build the sample.
4. Sign in, and send a profile photo via email.

To learn more about the quick starts, see the quick start FAQ.

1 Pick your platform

Android	Angular	ASP.NET MVC	iOS Swift	iOS Objective-C	Node.js
PHP	Python	Ruby	Universal Windows Platform (.NET)	Xamarin	

Which of the following are needed to interact with the Graph API?

1) Access Token
2) The Azure AD Application Key
3) The Azure AD Tenant ID
4) Refresh Token

Which of the following are needed to interact with the Graph API?

1) Access Token
2) The Azure AD Application Key
3) The Azure AD Tenant ID

OAuth 2.0 and OpenID Connect

- OAuth 2.0
  - Open standard for authorization
  - Implemented as an authorization protocol versus an authentication protocol
  - Focused on what resources you have access to
- OpenID Connect
  - Extends the OAuth 2.0 authorization protocol to use as an authentication protocol
  - Enables SSO with Oauth
  - Recommended for web applications hosted on a server and accessed via a browser

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols

Auth* Terms

client refers to the mobile app, web app, etc. that wants to access a resource

resource owner has control of resources that are being secured

security token is a collection of claims. It is often digitally signed, encrypted, and transferred through secured channels to ensure its confidentiality, integrity, and authenticity (aka **access token**)

service provider provides requested services (aka **relying party**)

identity provider authenticates entities and issues security tokens to relying parties (aka **security token service** STS or **authorization server** AS)

authentication is to verify if an entity is indeed what it claims to be

authorization is the process of determining whether an authenticated user has access to certain functionalities provided by the service provider

claim is an assertion made on an attribute of an entity (think property or descriptor or attribute)

refresh token is optionally issued with the access token and is a longer lasting credential (than the access token) solely used to request additional access tokens.

identity token or id token is OpenID's extension to OAuth 2. The structure is similar to the access token, but indicates user authentication -not authorization. (aka **authorization token**)

When using OAuth and OpenID Connect, which notification handler will you know the user is a valid logged in Azure AD user?

1) RedirectToIdentityProvider
2) MessageReceived
3) SecurityTokenReceived
4) SecurityTokenValidated
5) AuthorizationCodeReceived
6) AuthenticationFailed

When using OAuth and OpenID Connect, which notification handler will you know the user is a valid logged in Azure AD user?

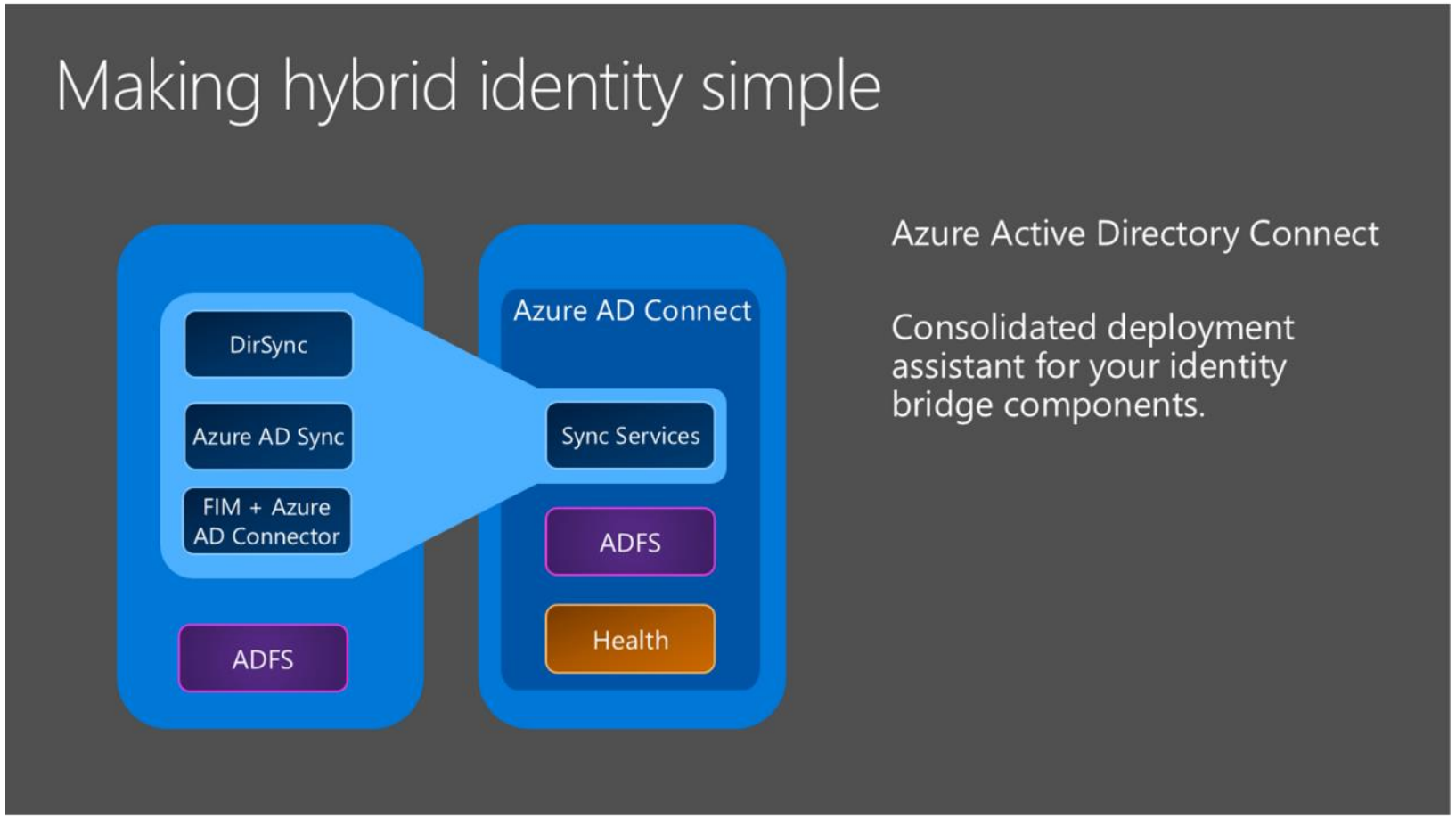
5) AuthorizationCodeReceived

Secure resources by using hybrid identities

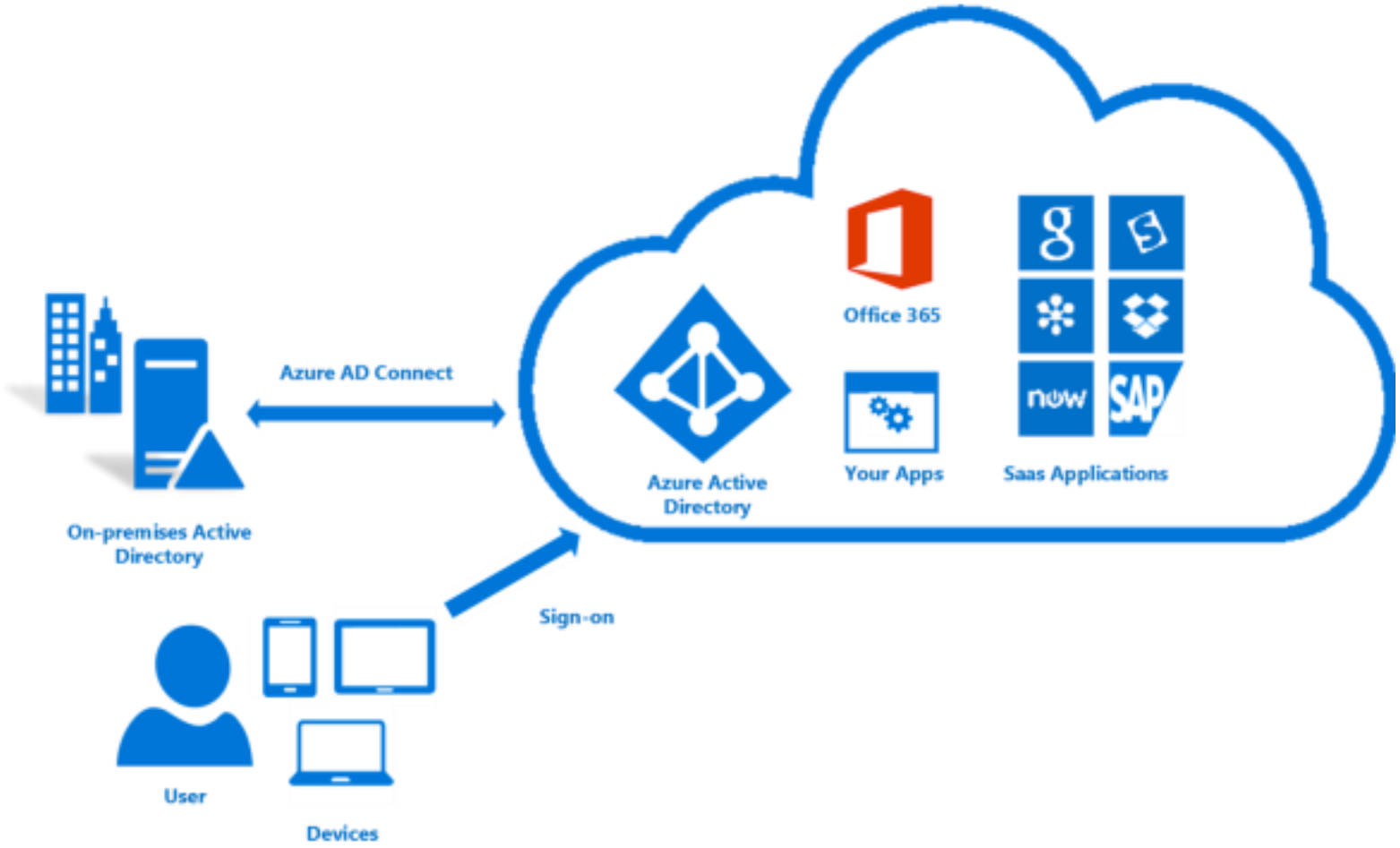
Azure AD Connect

- Connects your on-prem AD infrastructure to Azure
- Composed of 3 components
  - Sync Services
    - Replicates user/group information between On-Prem and Azure
  - ADFS (optional)
    - Addresses complex deployments, such as domain join SSO, enforcement of AD sign-in policy, and smart card or 3rd party MFA.
  - Health
    - Robust monitoring and provide a central location to view activity

Azure AD Connect



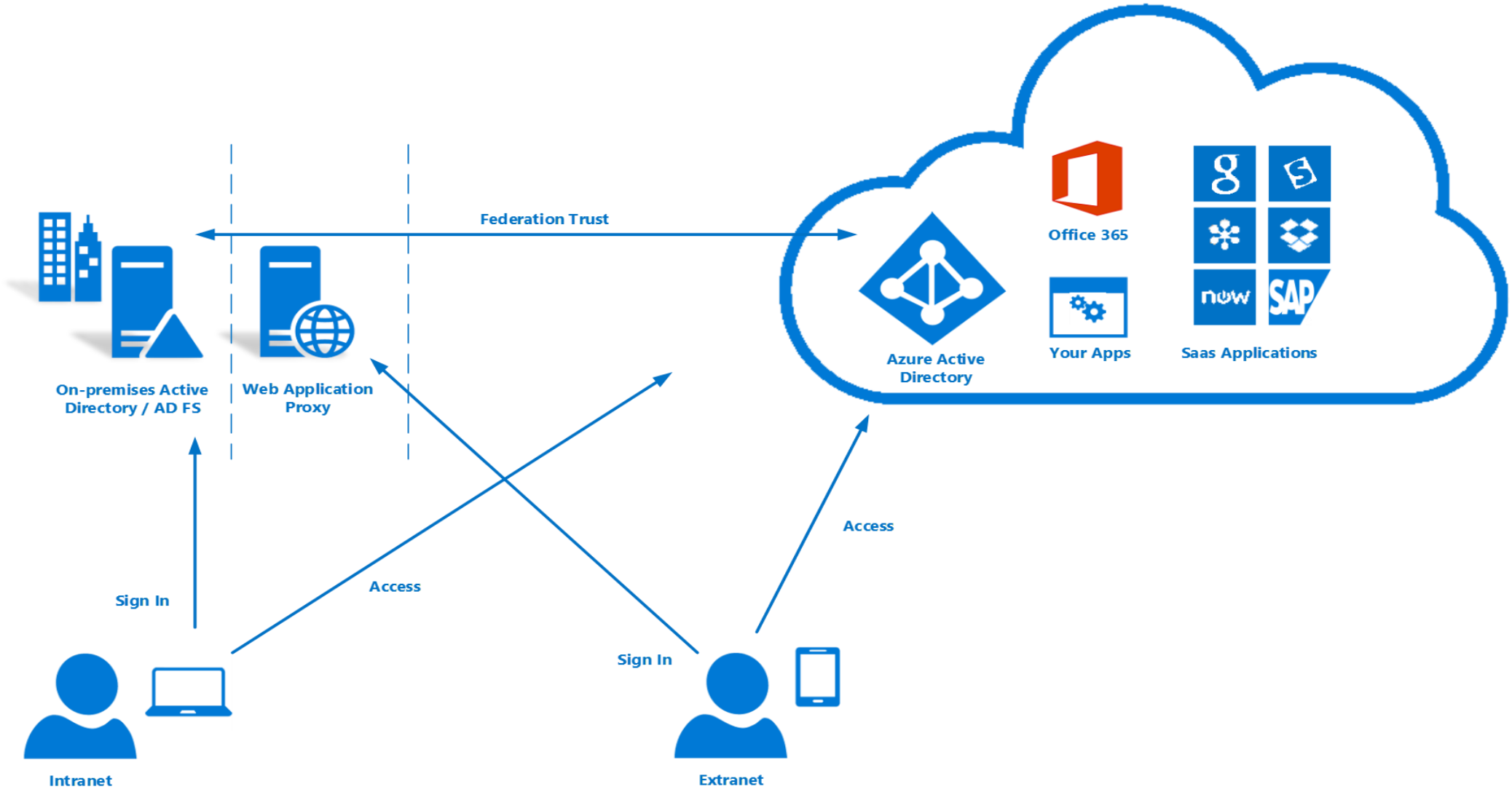
Azure AD Connect



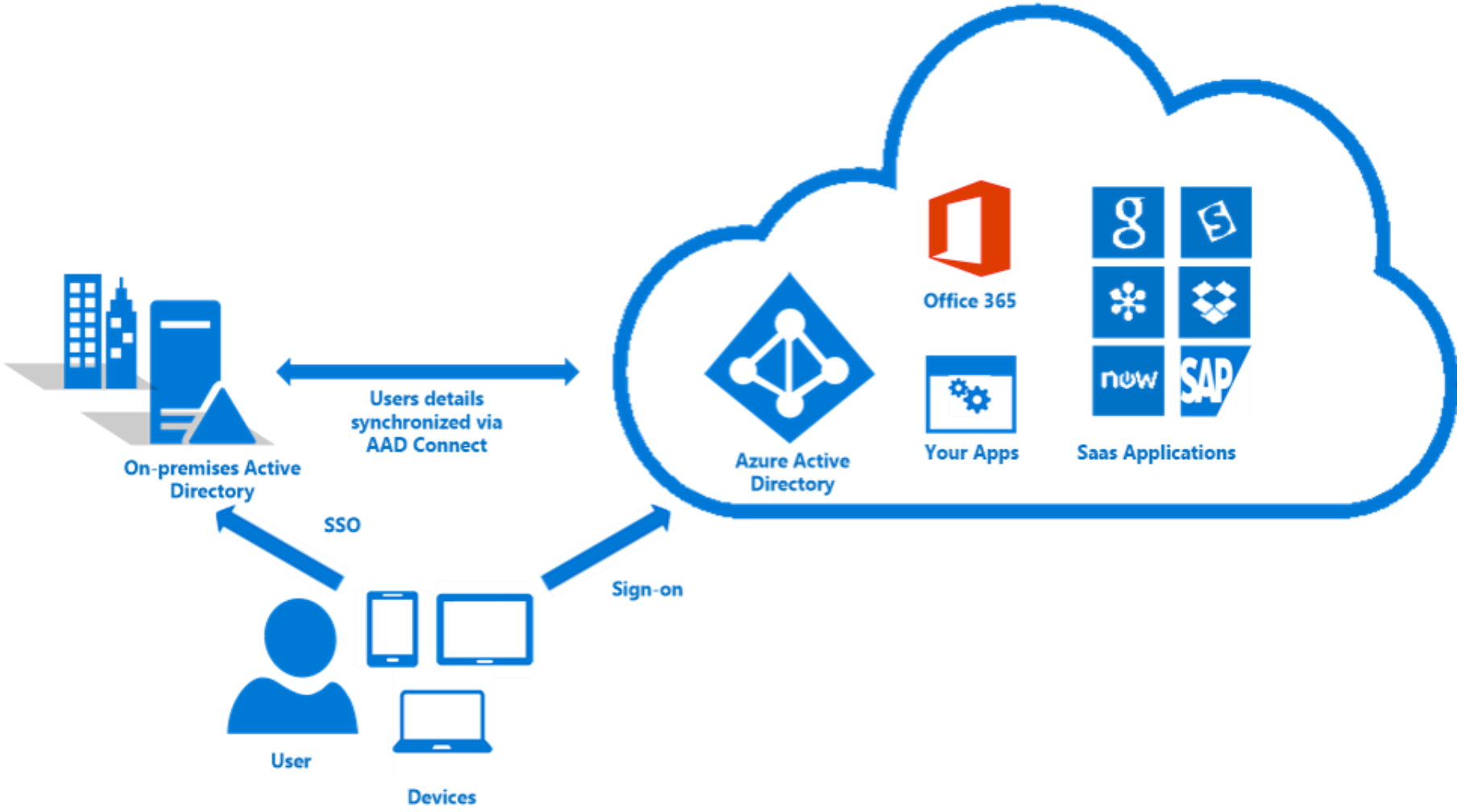
Azure AD Connect w/ADFS

- Simplicity and consistency
  - Use the same set of APIs and patterns to enable sign on
  - Use the same set of libraries you can already use to authenticate users against Azure AD
- Flexibility
  - In addition to standard user authorization, enable more complex scenarios
- Industry support
  - OAuth 2.0 and OpenID Connect enjoy wide utilization across the industry, so knowledge of these patterns will help you enable authentication and authorization outside of an Active Directory environment as well

Azure AD Connect w/ADFS



Azure AD Connect SSO



AD Connect SSO - Requirements

Your user is signing in on a corporate desktop.

The desktop has been previously joined to your Active Directory (AD) domain.

The desktop has a direct connection to your Domain Controller (DC), either on the corporate wired or wireless network or via a remote access connection, such as a VPN connection.

Our service endpoints have been included to the browser's Intranet zone.

Security token:

1) has control of resources that are being secured
2) is a collection of claims
3) aka **access token**
4) Is digitally signed, encrypted, and transferred through secured channels
5) is an assertion made on an attribute of an entity
6) provides requested services

Security token:

2) is a collection of claims
3) aka **access token**
4) Is digitally signed, encrypted, and transferred through secured channels

Secure resources by using identity providers

Azure AD B2B vs Azure AD B2C

B2B collaboration capabilities	Azure AD B2C stand-alone offering
Intended for: Organizations that want to be able to authenticate users from a partner organization, regardless of identity provider.	Intended for: Inviting customers of your mobile and web apps, whether individuals, institutional or organizational customers into your Azure AD.
Identities supported: Employees with work or school accounts, partners with work or school accounts, or any email address. Soon to support direct federation.	Identities supported: Consumer users with local application accounts (any email address or user name) or any supported social identity with direct federation.
Which directory the partner users are in: Partner users from the external organization are managed in the same directory as employees, but annotated specially. They can be managed the same way as employees, can be added to the same groups, and so on	Which directory the customer user entities are in: In the application directory. Managed separately from the organization's employee and partner directory (if any.
Single sign-on (SSO) to all Azure AD-connected apps is supported. For example, you can provide access to Office 365 or on-premises apps, and to other SaaS apps such as Salesforce or Workday.	SSO to customer owned apps within the Azure AD B2C tenants is supported. SSO to Office 365 or to other Microsoft and non-Microsoft SaaS apps is not supported.
Partner lifecycle: Managed by the host/inviting organization.	Customer lifecycle: Self-serve or managed by the application.
Security policy and compliance: Managed by the host/inviting organization.	Security policy and compliance: Managed by the application.
Branding: Host/inviting organization's brand is used.	Branding: Managed by application. Typically tends to be product branded, with the organization fading into the background.

Implement Azure AD B2B Collaboration

B2B collaboration allows you to invite users outside of your organization and manage access to applications and resources.

Can add invited users to:

- Enterprise applications
- Directory Users
- Groups

If the user doesn’t have a Microsoft account or an Azure AD account – one is created for them seamlessly at the time for offer redemption.

Can utilize API to build custom application using B2B

You have a web application using Azure AD for its users. You now need to add users that work for a partner company. What is the easiest way to give the new external users access to your web application?

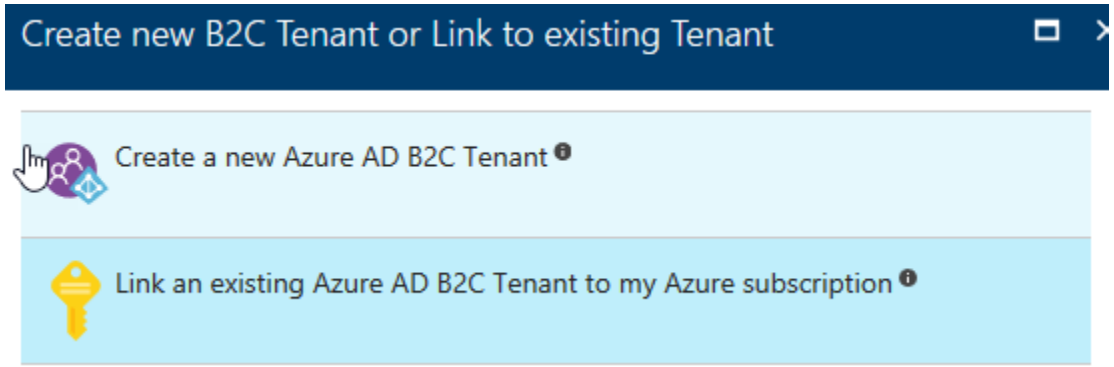
1) Change the web application to use a Azure B2C directory
2) Change your Azure AD to use the Premium edition
3) Invite the users from Azure AD (using Azure B2B)
4) Add the users to your internal Active Directory and sync

You have a web application using Azure AD for its users. You now need to add users that work for a partner company. What is the easiest way to give the new external users access to your web application?

3) Invite the users from Azure AD (using Azure B2B)

Manage Identity and access by using Azure AD B2C

Once you create Azure AD B2C, you need to link it

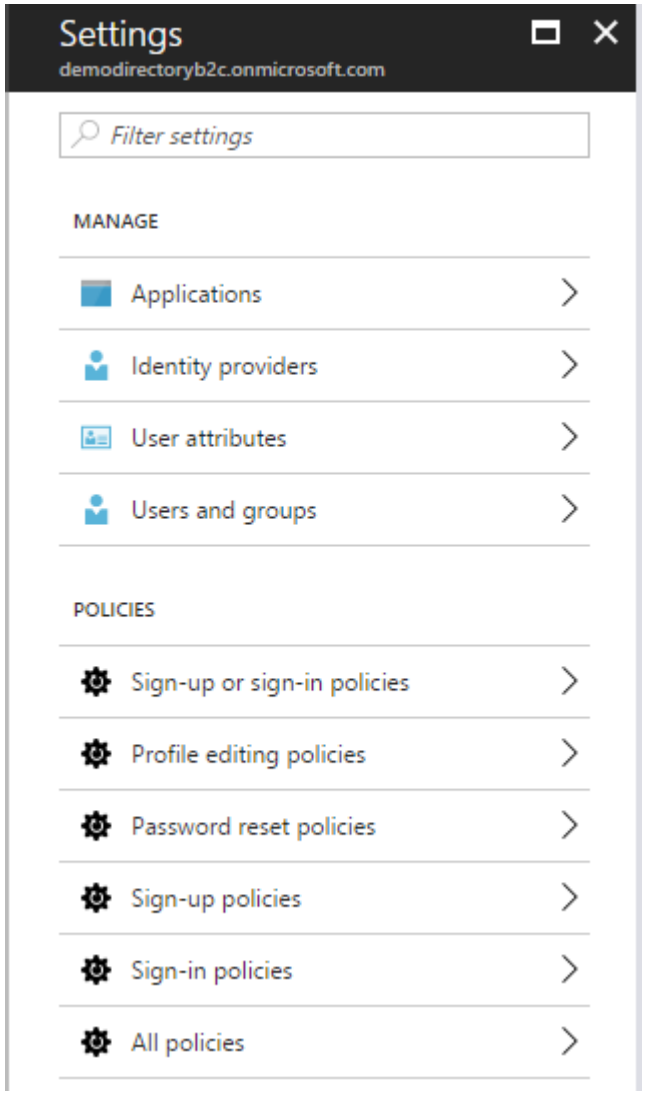


Allows you to add users from

- Social accounts
- Enterprise Accounts
- Local Accounts

Can set policies

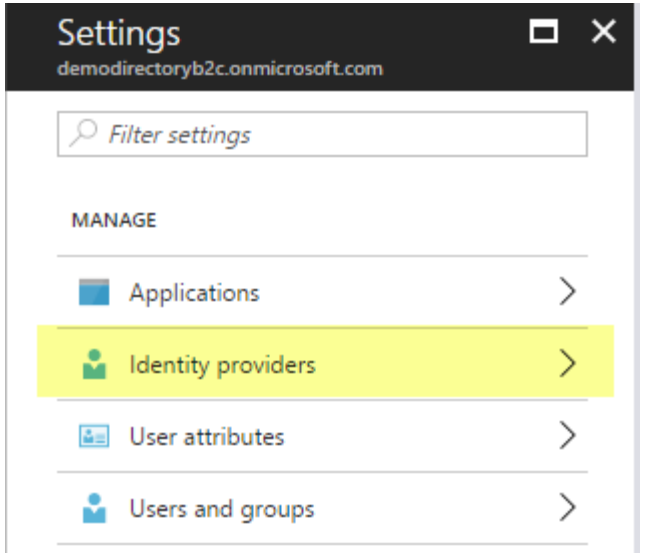
Can Brand login experience

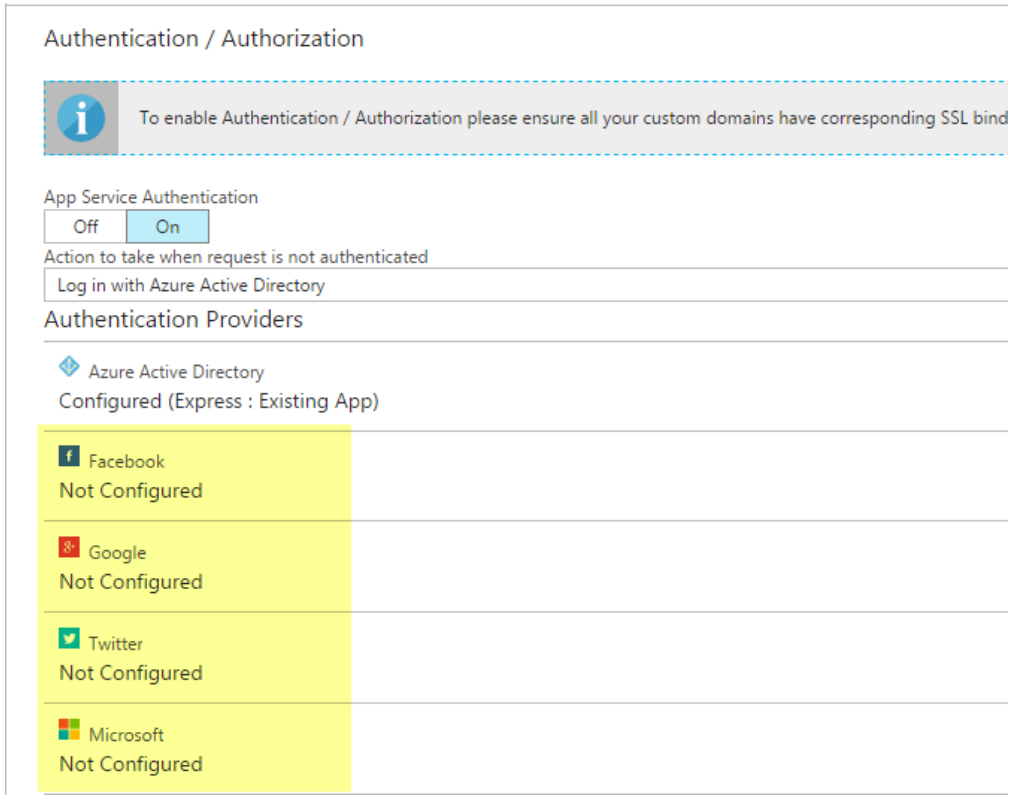


Provide access to resources using identity providers

Configure Identity Providers in Azure AD B2C

Configure in App Service Authentication blade





You have a web application that needs to support Single Sign On for your on-premise users and be able to add external users using their social logins. Which product will be the best to use?

1) Azure AD B2C
2) Key Vault
3) Security Center
4) Azure B2B Collaboration

You have a web application that needs to support Single Sign On for your on-premise users and be able to add external users using their social logins. Which product will be the best to use?

1) Azure AD B2C

EXAM TIP!

Azure B2C allows you to add social accounts, enterprise accounts and local accounts. It is very flexible and newer than Azure AD. The exam may not call out Azure B2C or Azure B2B Collaboration, but you will need to know how to provide the solutions they solve. In preparing for the exam, you should try to explore both types of Azure AD directories and learn the pros and cons.

Identify an appropriate data security solution

Data Security and Encryption

- Where is your data?
  - In Transit
  - At Rest
- Security Method
  - MFA
  - RBAC
  - Encryption
    - In transit (SSL)
    - At Rest (Disk, File, SQL Database)

Azure Storage

Storage

Durable, highly-available, and massively-scalable cloud storage

Blob storage

REST-based object storage for unstructured data

Queue Storage

Effectively scale apps according to traffic

File Storage

File shares that use the standard SMB 3.0 protocol

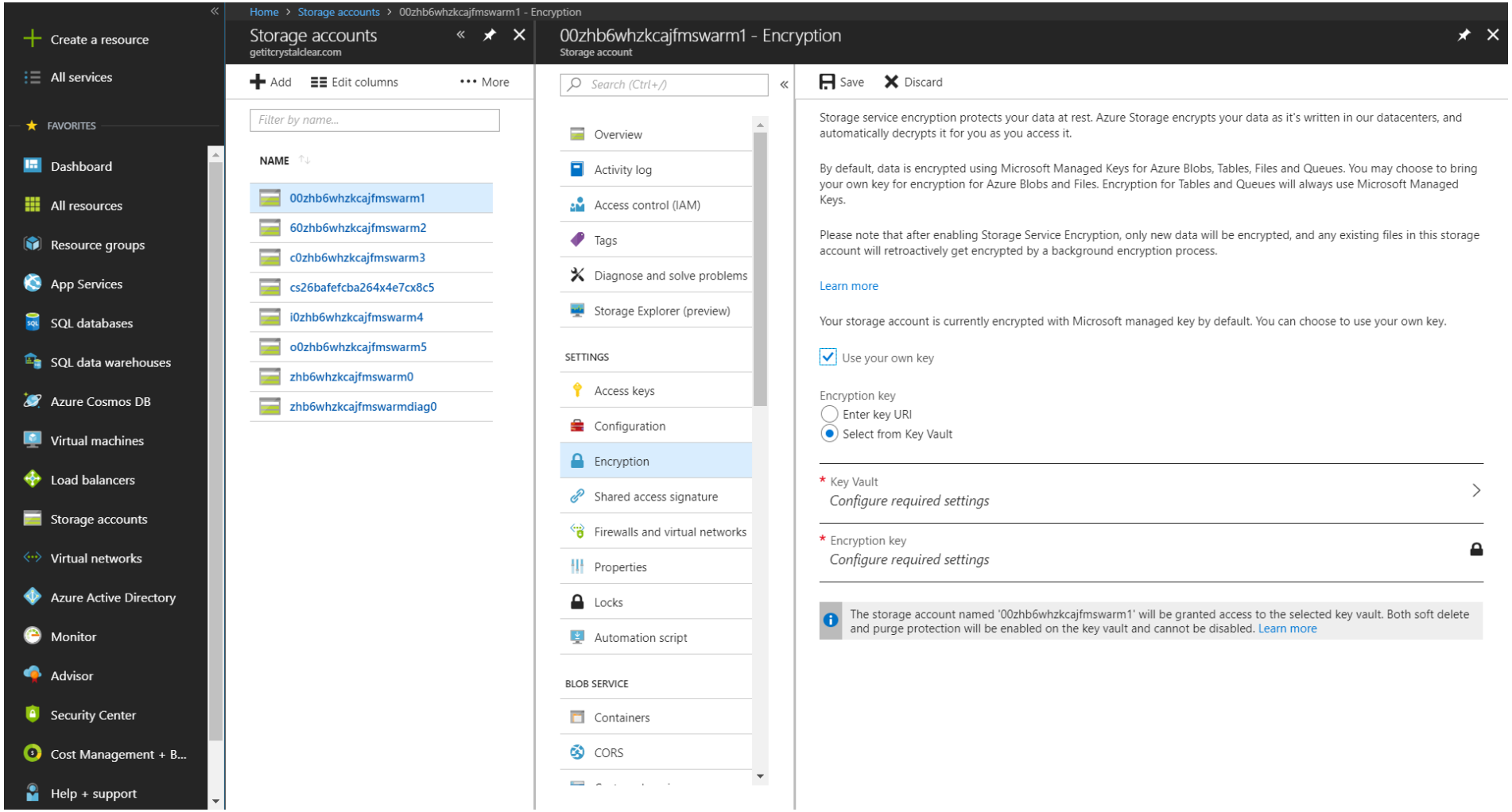
Disk Storage

Persistent, secured disk options supporting virtual machines

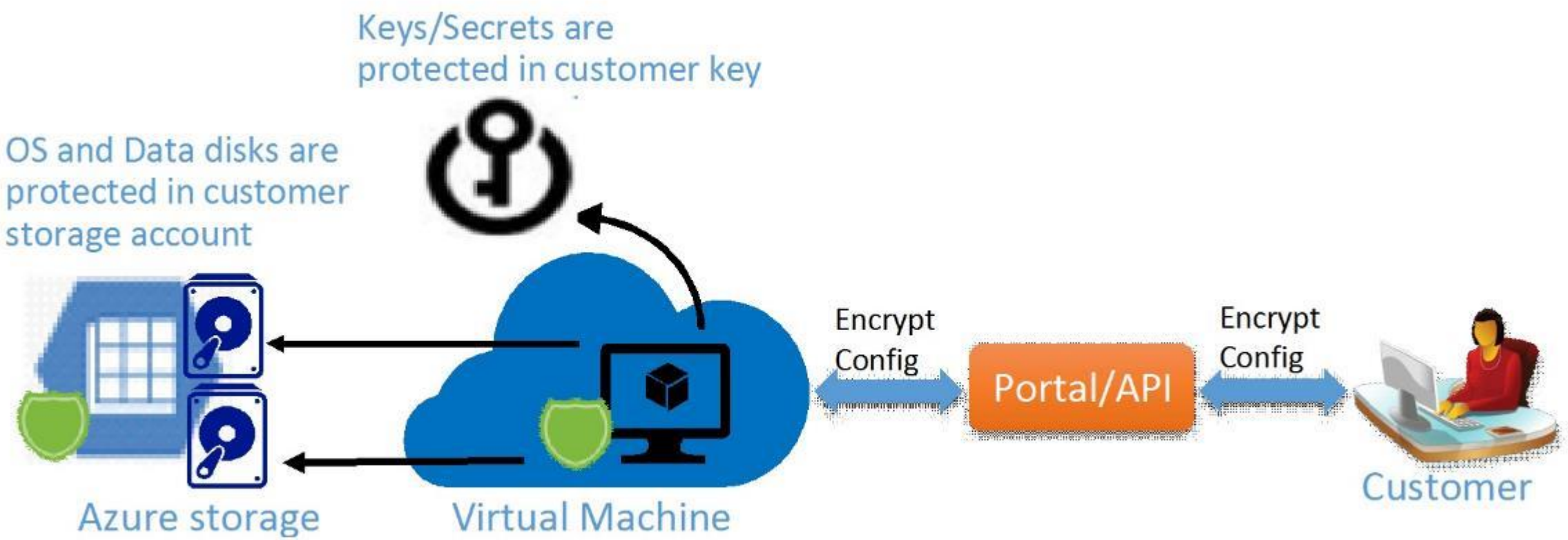
Data Lake Store

Hyperscale repository for big data analytics workloads

Storage Services Encryption



Azure Disk Encryption



Azure Disk Encryption Scenarios

- Enable encryption on new IaaS VMs created from pre-encrypted VHD and encryption keys
- Enable encryption on new IaaS VMs created from the Azure Gallery images
- Enable encryption on existing IaaS VMs running in Azure
- Disable encryption on Windows IaaS VMs
- Disable encryption on data drives for Linux IaaS VMs
- Enable encryption of managed disk VMs
- Update encryption settings of an existing encrypted non-premium storage VM
- Backup and restore of encrypted VMs, encrypted with key encryption key

Azure Databases

SQL Database

Managed relational SQL Database as a service

Azure Database for MySQL

Managed MySQL database service for app developers

Azure Database for PostgreSQL

Managed PostgreSQL database service for app developers

SQL Data Warehouse

Elastic data warehouse as a service with enterprise-class features

SQL Server Stretch Database

Dynamically stretch on-premises SQL Server databases to Azure

Azure Cosmos DB

Try Azure Cosmos DB for a globally distributed, multi-model database

Virtual Machines

Provision Windows and Linux virtual machines in seconds

SQL Server TDE

Transparent Data Encryption

Applies to both PAAS and IAAS offerings

Covers both “in transit” and “at rest” encryption requirements

Azure Storage Client Library

Encrypting data within client applications before uploading to Azure Storage

Decrypting data while downloading to the client

Integrates with Azure Key Vault for storage account key management

Azure Storage Client Library – Blob Example

```
// Create the IKey used for encryption.
 RsaKey key = new RsaKey("private:key1" /* key identifier */);

 // Create the encryption policy to be used for upload and download.
 BlobEncryptionPolicy policy = new BlobEncryptionPolicy(key, null);

 // Set the encryption policy on the request options.
 BlobRequestOptions options = new BlobRequestOptions() { EncryptionPolicy = policy };

 // Upload the encrypted contents to the blob.
 blob.UploadFromStream(stream, size, null, options, null);

 // Download and decrypt the encrypted contents from the blob.
 MemoryStream outputStream = new MemoryStream();
 blob.DownloadToStream(outputStream, null, options, null);
```

Azure Storage costs more if Storage Service Encryption SSE is enabled

1) True
2) False

Azure Storage costs more if Storage Service Encryption SSE is enabled

2) False

Azure Storage provides a comprehensive set of security capabilities which together enable developers to build secure applications. These options include:

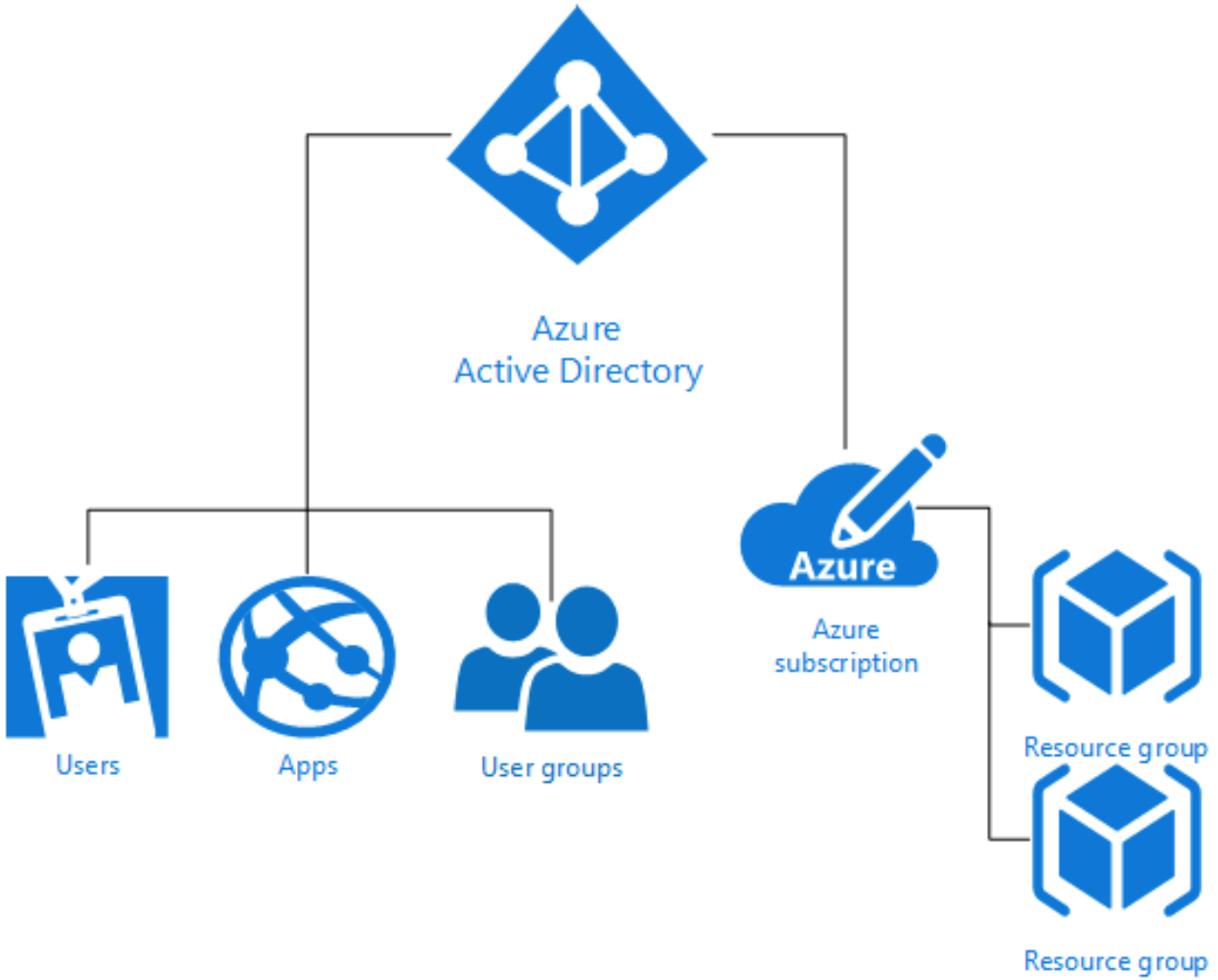
1) Securing your Storage Account
2) Securing Access to Your Data
3) Encryption in Transit
4) Encryption at Rest
5) Storage Analytics to audit access of Azure Storage

Azure Storage provides a comprehensive set of security capabilities which together enable developers to build secure applications. These options include:

1) Securing your Storage Account
2) Securing Access to Your Data
3) Encryption in Transit
4) Encryption at Rest
5) Storage Analytics to audit access of Azure Storage

Design a role-based access control (RBAC) strategy

RBAC Overview



Role Management

- Levels at which may be managed/assigned
  - Management Group Level
  - Subscription Level
  - Resource Group Level
  - Resource Level
- Built-In roles
- Custom Roles
- Access that you grant at parent scopes is inherited at child scopes

Custom Roles

Use when none of the built-in roles meet your needs

Each tenant can create up to 2000 custom roles.

Shared across all subscriptions that use a tenant

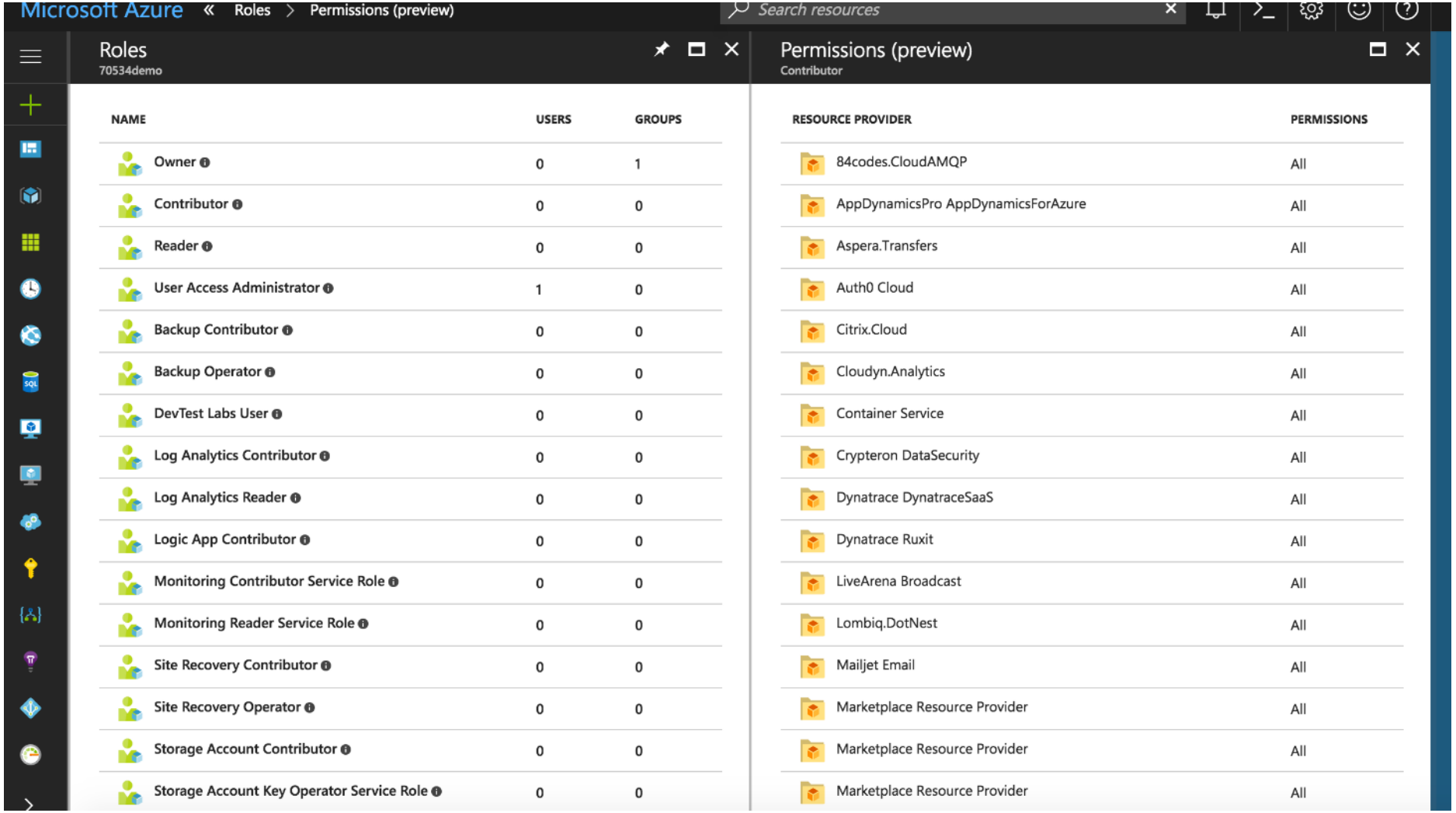
Comprised of Actions, NotActions, and AvailableScopes

Managed via Portal, PowerShell, Azure CLI, or the REST API

Custom Role Example

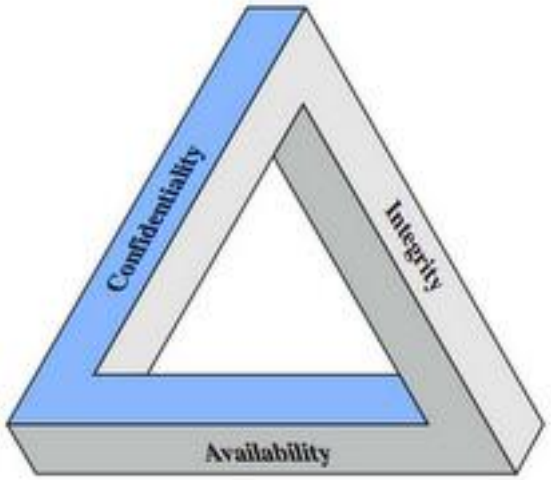
```
{
  "Name": "Virtual Machine Operator",
  "Id": "cadb4a5a-4e7a-47be-84db-05cad13b6769",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [

  ],
  "AssignableScopes": [
    "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e",
    "/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624",
    "/subscriptions/34370e90-ac4a-4bf9-821f-85eeedeae1a2"
  ]
}
```

RBAC in the Azure Portal



Manage security risks by using an appropriate security solution

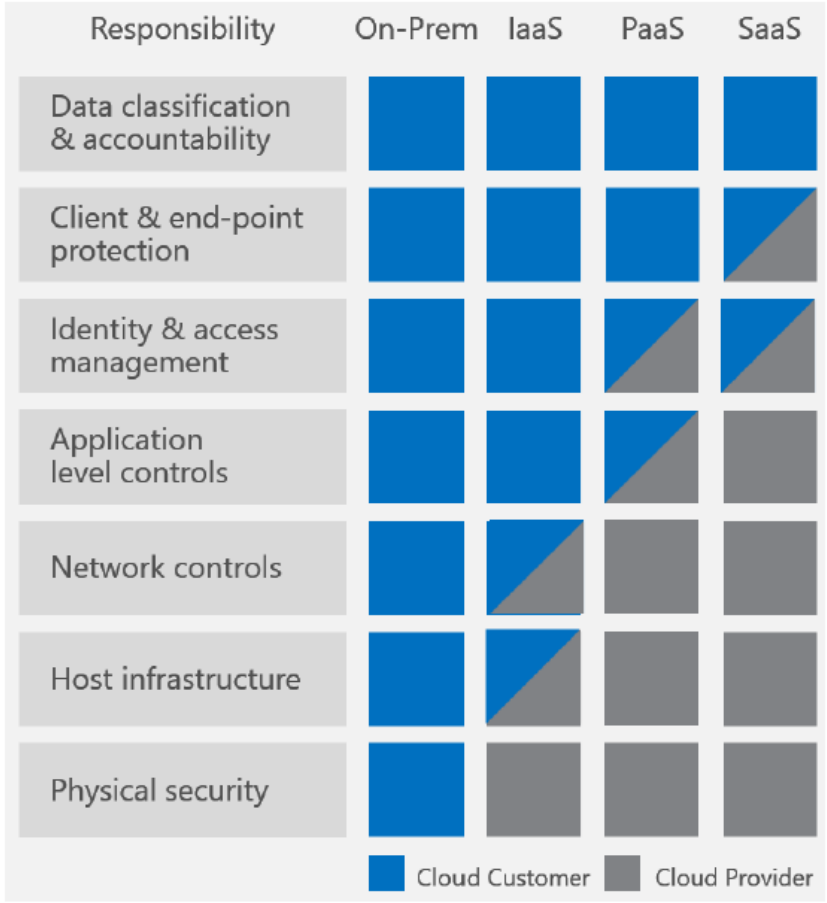
CIA-Triad Security Model



- Confidentiality: Prevention of unauthorized access to system
- Integrity: Prevention of unauthorized modification of system
- Availability: Prevention of disruption of service/availability of system

Shared Security Responsibility Model

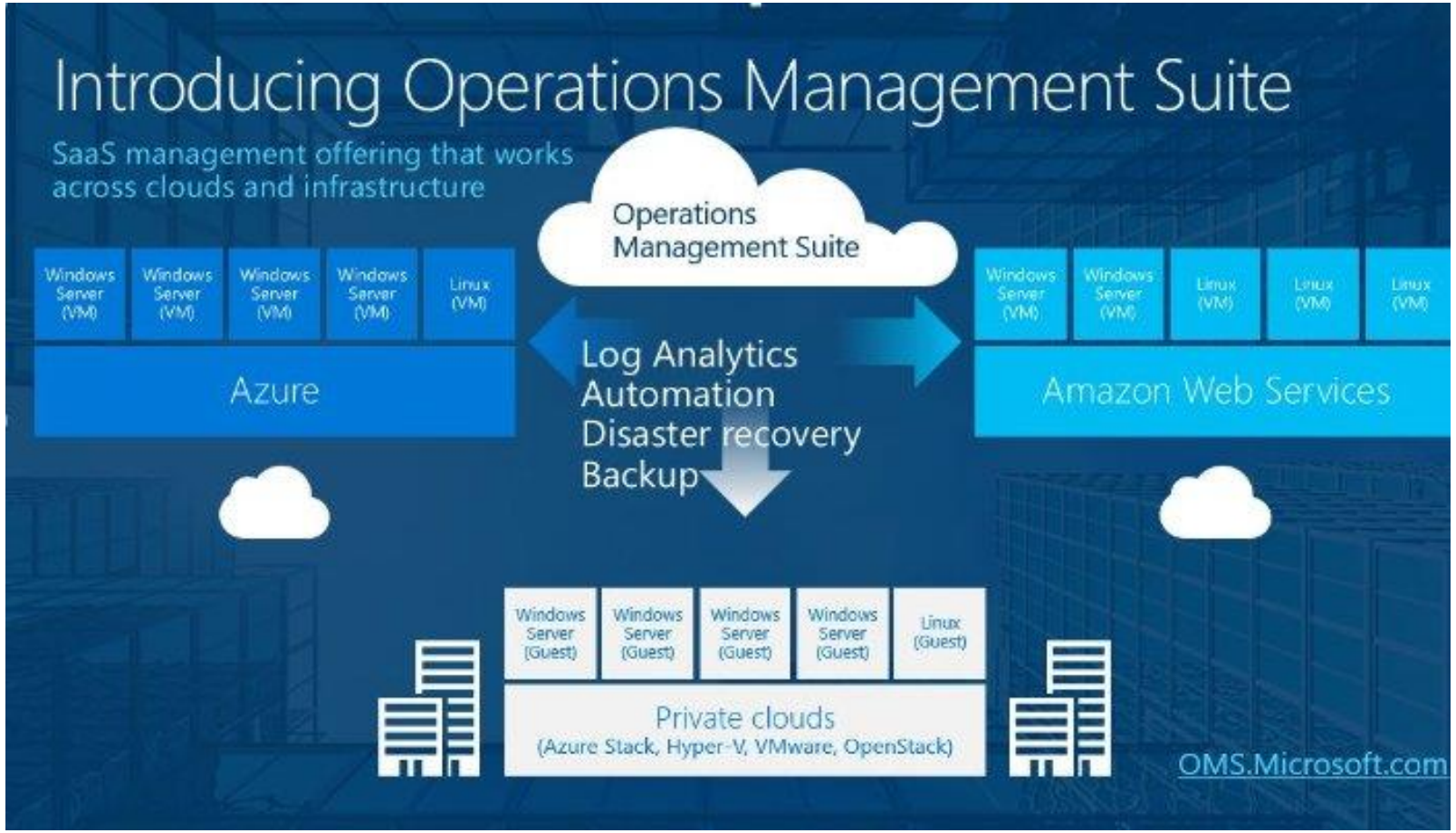
- Microsoft Azure is your security partner
- Security responsibilities depend on delivery model
  - Vulnerabilities are portable!
- Azure “security toolbox”
  - Operations Management Suite (OMS)
  - Activity Log
  - Azure Security Center (ASC)



Operations Management Suite

- Single integration/control point for Azure Services
  - Integrates with 3rd party services from marketplace
  - Anything with an agent
- Provides operational intelligence across hybrid environments
- Process automation and monitoring of resources
- Cloud-based SaaS (thus highly available)
- Protects privacy and security of data, while delivering software and services to manage the IT infrastructure.

Operations Management Suite



Operations Management Suite

- Log Analytics
  - Central monitoring and analysis of logs from multiple sources
- Automation
  - Process automation
  - Configuration enforcement
- Backup
  - Backup and restore critical data
- Site Recovery
  - High availability for critical applications

Operations Management Suite

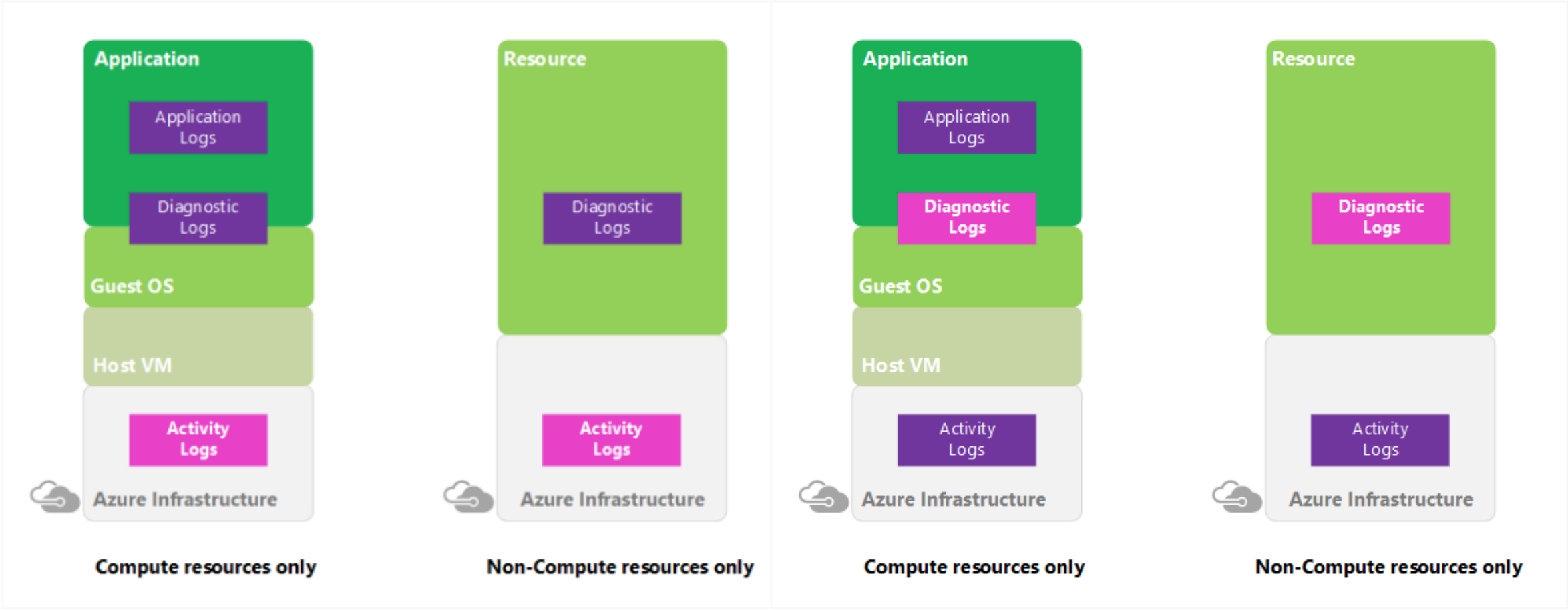
Integrating OMS

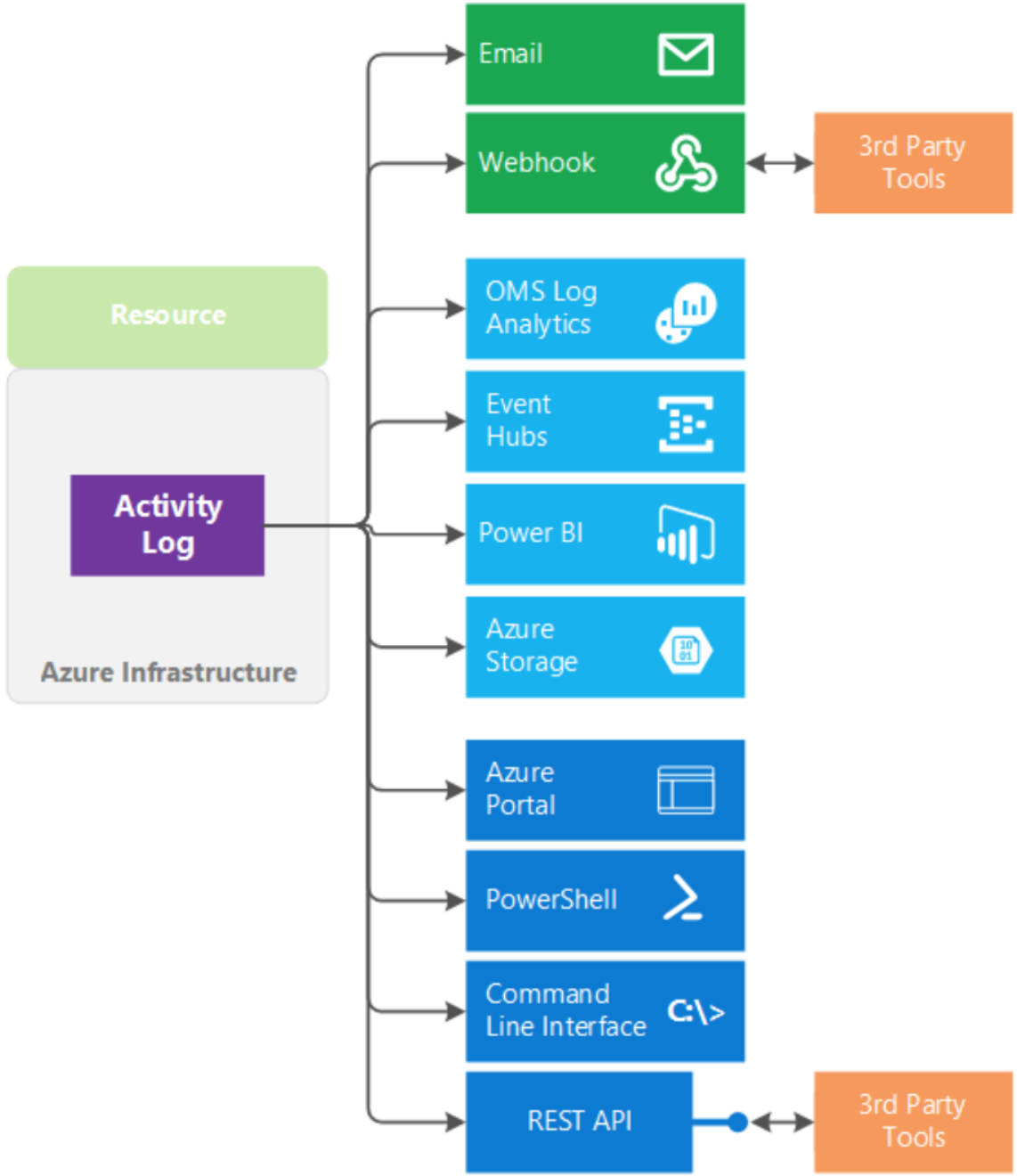
- Workspace in Azure
- Multiple Connection Methods
  - OMS agent installed directly on Windows/Linux host
  - SCOM
  - Azure diagnostic VM extension storage account

Activity Log

- Provides visibility into subscription-level activity (control-plane)
  - Information about operations performed ON resources not WITHIN
  - Answers the question: “What, Who, and When?”
    - Azure Resource Manager operational data
    - Service Health events/updates
- Limited to Azure Infrastructure and Services
    - Cannot provide information about OS or custom application events
- Differ from resource-level diagnostic logs

Activity vs. Diagnostic Logs

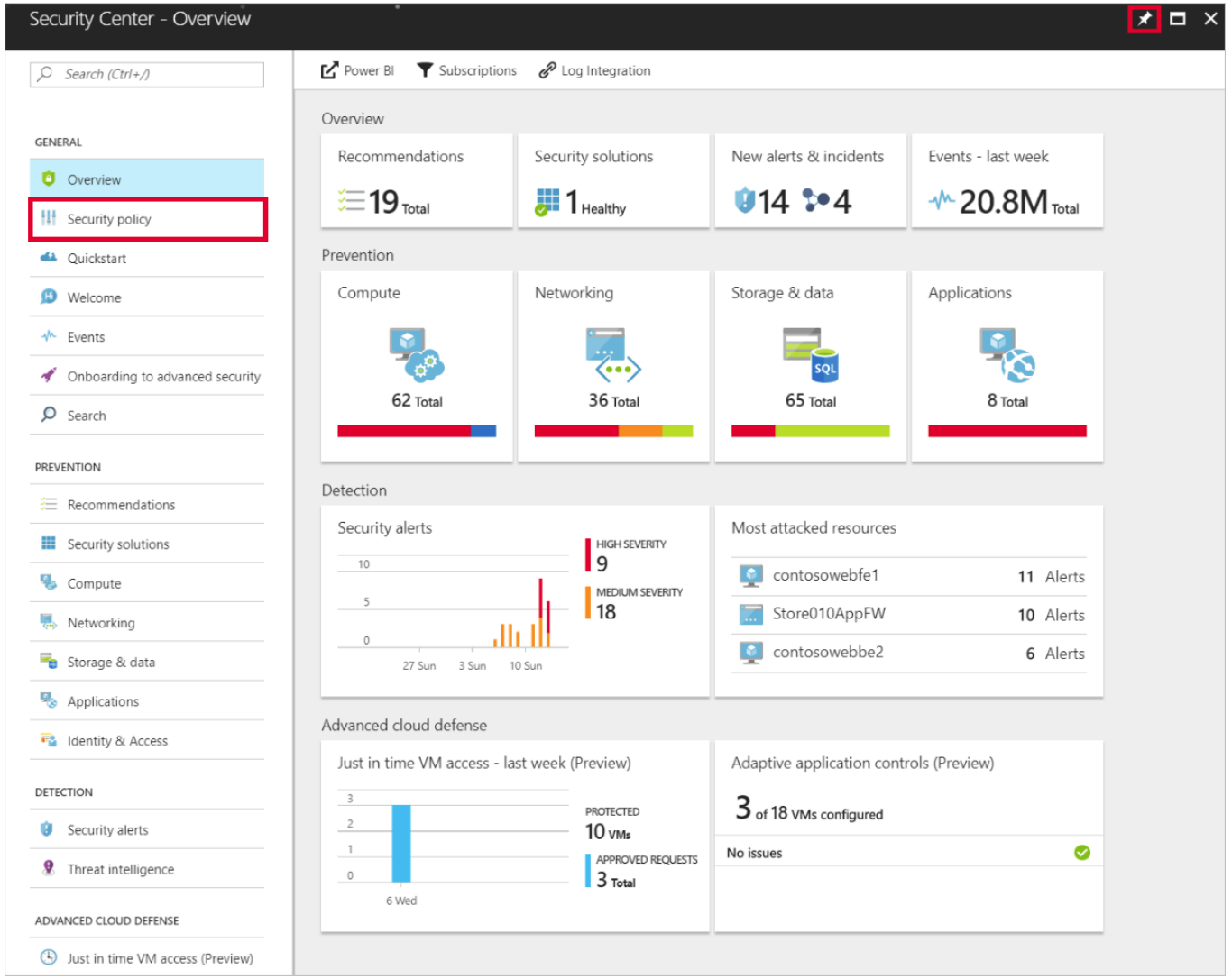



Email
Webhook
3rd Party Tools
Resource
OMS Log Analytics
Event Hubs
Activity Log
Power BI
Azure Storage
Azure Infrastructure
Azure Portal
PowerShell
Command Line Interface
C:\>
REST API
3rd Party Tools

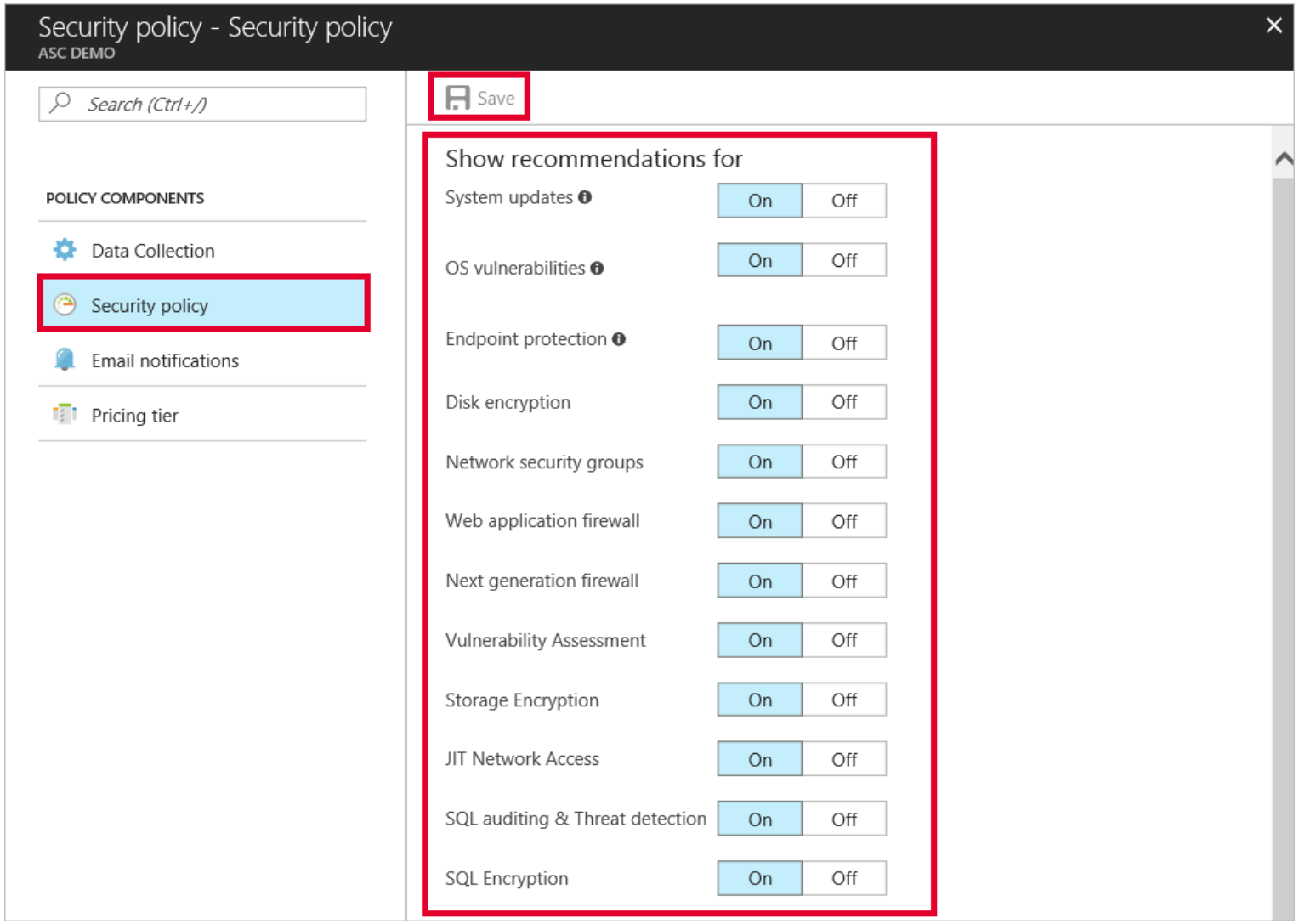
Azure Security Center

- Provides a central view of security state
  - Azure resources
  - On-Premises
  - Other clouds
- Unified Visibility and Control
  - Define security configuration policies
  - Monitor policy adherance
- Adaptive Threat Prevention
  - Continuous security assessment
- Threat detection

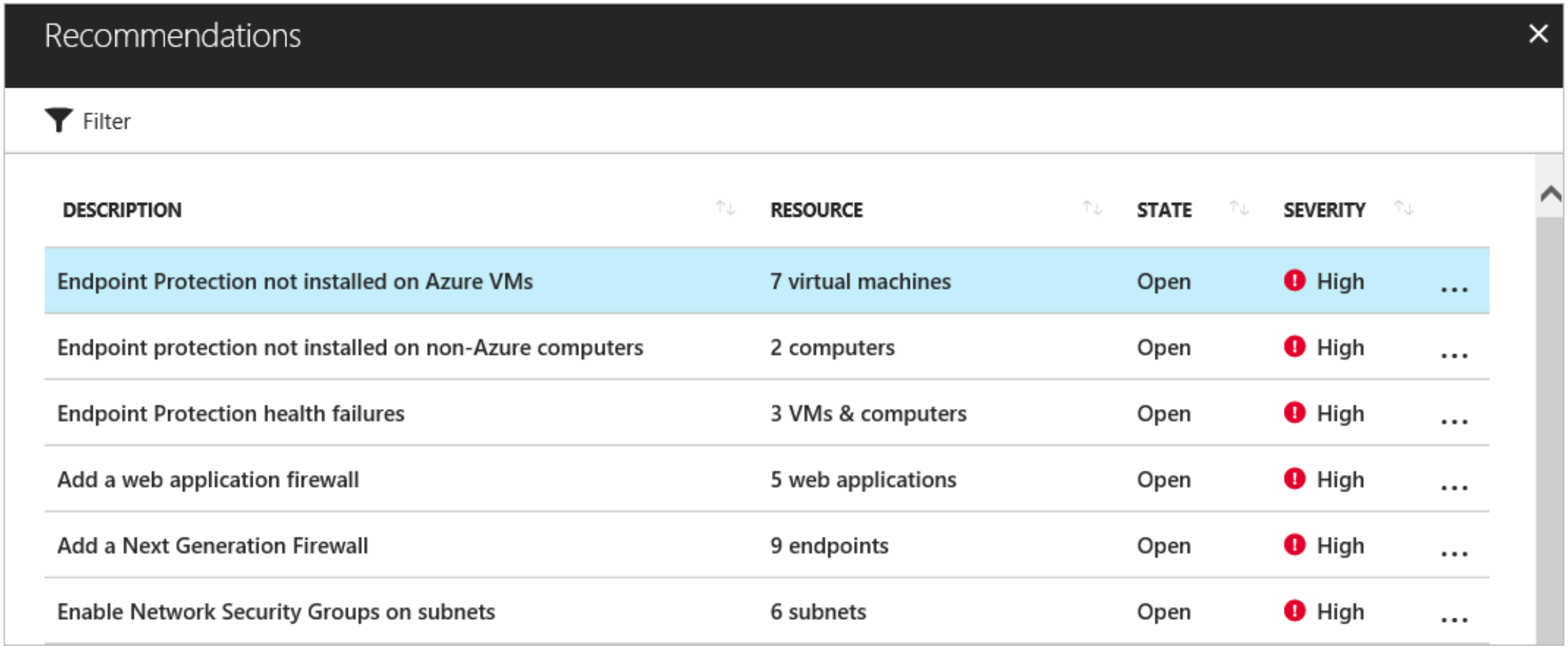
Azure Security Center

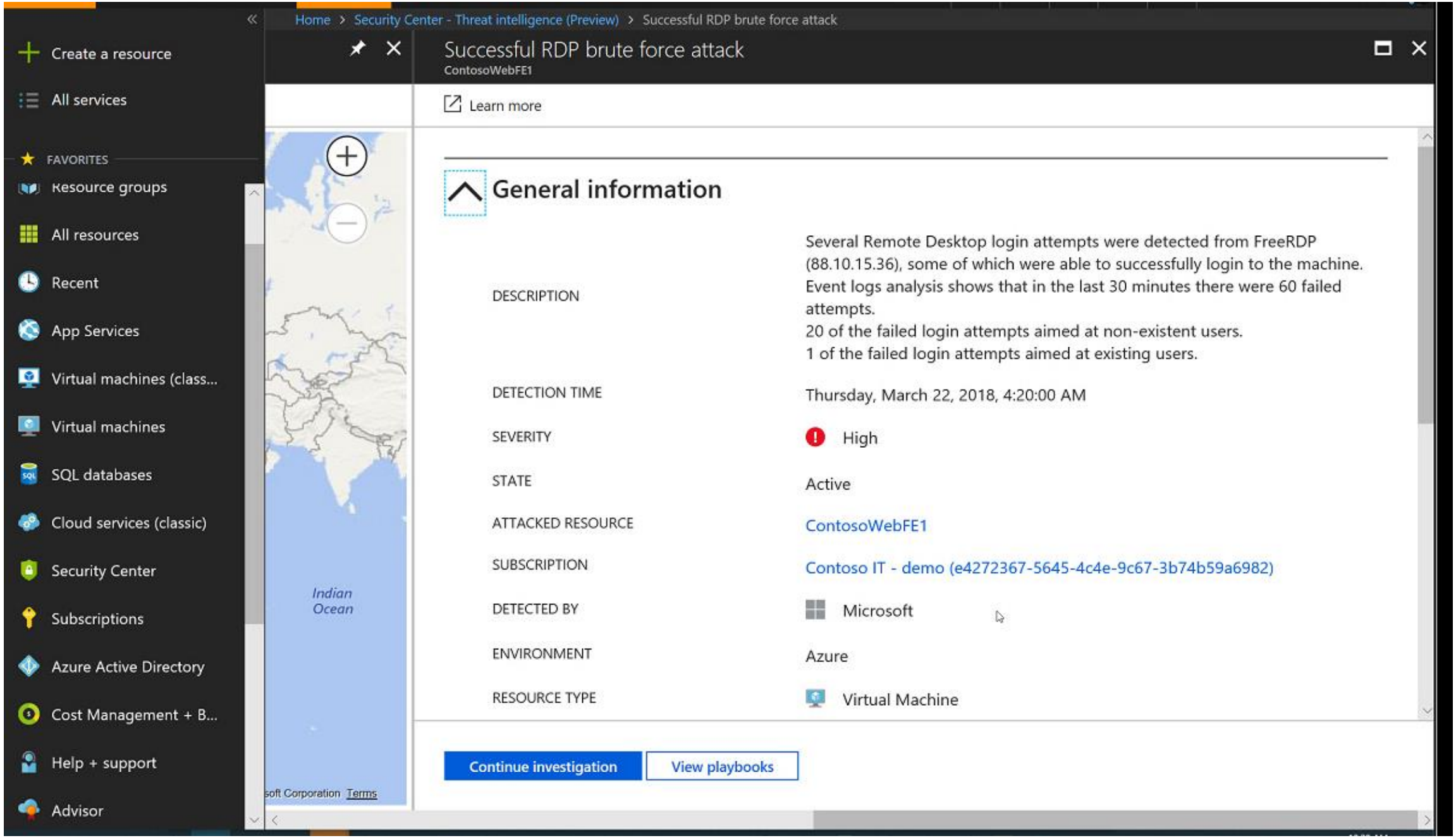


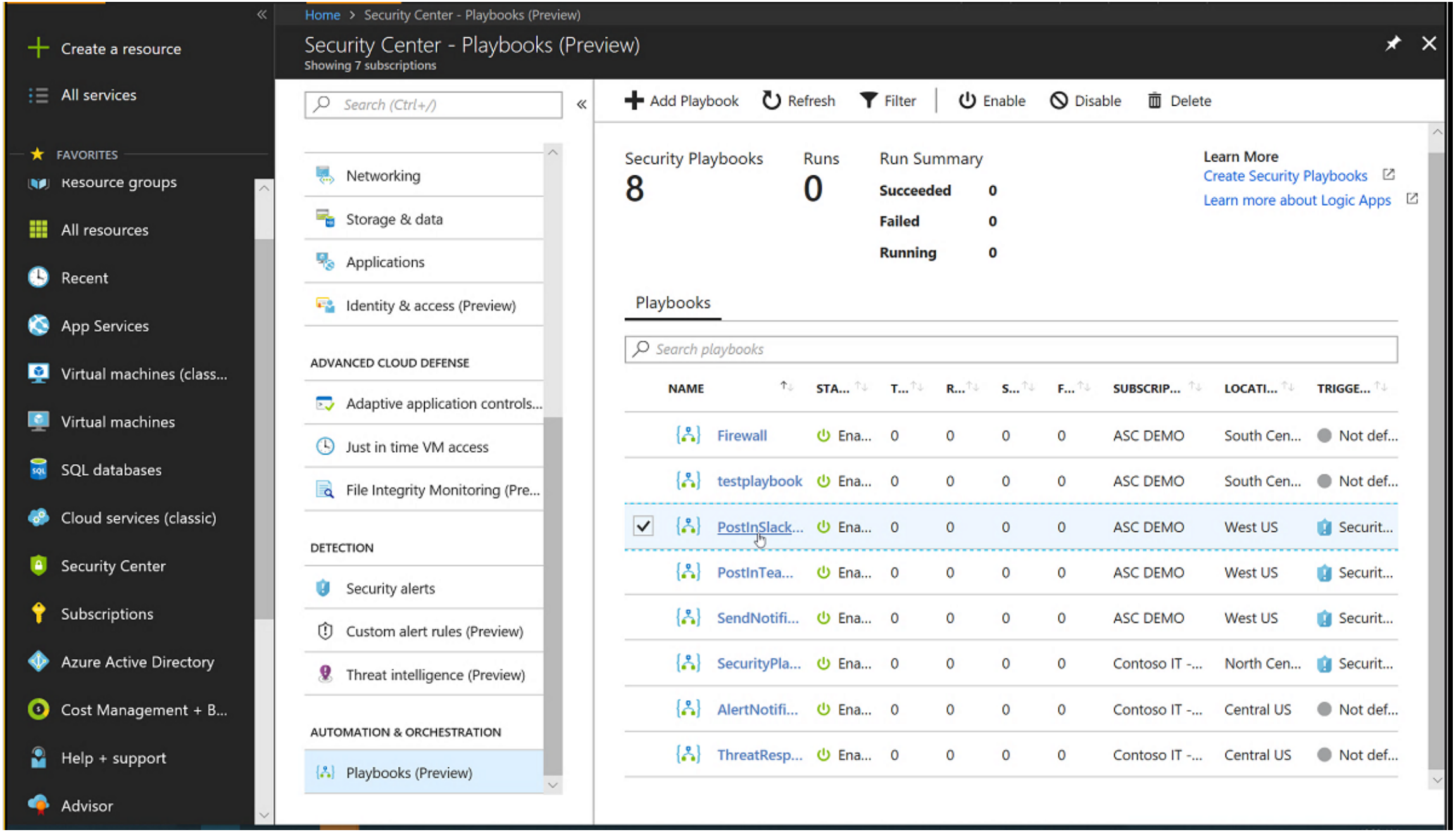
Azure Security Center



Azure Security Center




Create a resource
All services
FAVORITES
Resource groups
All resources
Recent
App Services
Virtual machines (class...
Virtual machines
SQL databases
Cloud services (classic)
Security Center
Subscriptions
Azure Active Directory
Cost Management + B...
Help + support
Advisor
Home > Security Center - Threat intelligence (Preview) > Successful RDP brute force attack
Successful RDP brute force attack
ContosoWebFE1
Learn more
Indian Ocean
soft Corporation Terms
General information
DESCRIPTION
Several Remote Desktop login attempts were detected from FreeRDP (88.10.15.36), some of which were able to successfully login to the machine.
Event logs analysis shows that in the last 30 minutes there were 60 failed attempts.
20 of the failed login attempts aimed at non-existent users.
1 of the failed login attempts aimed at existing users.
DETECTION TIME
Thursday, March 22, 2018, 4:20:00 AM
SEVERITY
High
STATE
Active
ATTACKED RESOURCE
ContosoWebFE1
SUBSCRIPTION
Contoso IT - demo (e4272367-5645-4c4e-9c67-3b74b59a6982)
DETECTED BY
Microsoft
ENVIRONMENT
Azure
RESOURCE TYPE
Virtual Machine
Continue investigation
View playbooks


Create a resource
All services
FAVORITES
Resource groups
All resources
Recent
App Services
Virtual machines (class...
Virtual machines
SQL databases
Cloud services (classic)
Security Center
Subscriptions
Azure Active Directory
Cost Management + B...
Help + support
Advisor
Home > Security Center - Playbooks (Preview)
Security Center - Playbooks (Preview)
Showing 7 subscriptions
Search (Ctrl+/)
Networking
Storage & data
Applications
Identity & access (Preview)
ADVANCED CLOUD DEFENSE
Adaptive application controls...
Just in time VM access
File Integrity Monitoring (Pre...
DETECTION
Security alerts
Custom alert rules (Preview)
Threat intelligence (Preview)
AUTOMATION & ORCHESTRATION
Playbooks (Preview)
Add Playbook
Refresh
Filter
Enable
Disable
Delete
Security Playbooks
8
Runs
0
Run Summary
Succeeded 0
Failed 0
Running 0
Learn More
Create Security Playbooks
Learn more about Logic Apps
Playbooks
Search playbooks
NAME STA... T... R... S... F... SUBSCRIP... LOCATI... TRIGGE...
Firewall Ena... 0 0 0 0 ASC DEMO South Cen... Not def...
testplaybook Ena... 0 0 0 0 ASC DEMO South Cen... Not def...
PostInSlack... Ena... 0 0 0 0 ASC DEMO West US Securit...
PostInTea... Ena... 0 0 0 0 ASC DEMO West US Securit...
SendNotifi... Ena... 0 0 0 0 ASC DEMO West US Securit...
SecurityPla... Ena... 0 0 0 0 Contoso IT -... North Cen... Securit...
AlertNotifi... Ena... 0 0 0 0 Contoso IT -... Central US Not def...
ThreatResp... Ena... 0 0 0 0 Contoso IT -... Central US Not def...

Audience

Job Roles

Topic

Level

Product

security

security clear all

9 Self-paced Labs

Sort by: Most Popular

Configure your network for security

★★★½☆ (858)

Duration 1h 0m

Scenario: In this lab you will configure your network to maximize security, create a new Virtual Network with subnets, and create NSG's and subnets to mimic configuration for a standard three-layer security zone model.

View details >

Secure your Environment with Azure Security Center - Getting Started

★★★½☆ (1270)

Duration 1h 0m

Scenario: In this lab, you will investigate the built-in security reporting and analysis tools in Azure. You will enable Azure Security Center and open the console to see what the analysis is reporting for the Azure environment.

View details >

Deploy Network Security Groups and Load Balancers

★★★☆☆ (271)

Duration 0h 25m

This lab provides an overview of advanced Azure networking concepts using network security groups (NSGs) and Azure load balancers.

View details >

Secure Your Cloud Resources with Azure Security Center

★★★☆☆ (340)

Duration 0h 40m

In this lab, you will explore how to protect your resources with Azure Security Center. This will include reviewing security policies, security recommendations, just-in-time access configuration, and security alerts.

View details >

Which Azure component allows you to monitor security across on-premises and cloud workloads

1) Advanced analytics
2) Azure Security Center
3) RBAC Monitor
4) SCOM

Which Azure component allows you to monitor security across on-premises and cloud workloads

2) Azure Security Center

Securing Resources