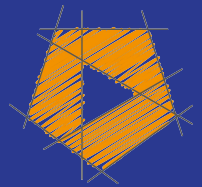
SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Exam Released May 2021

Latest Update July 2024

SCI - Security, Compliance, Identity

Microsoft Azure SCI Fundamentals

“familiar with Microsoft Azure and Microsoft 365 and want to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution”

Microsoft Azure SCI Fundamentals

- Business stakeholders
- New or existing IT professionals
- Students who have an interest in security, compliance and identity solutions

Microsoft Azure SCI Fundamentals

- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft Entra
- Describe the capabilities of Microsoft security solutions
- Describe the capabilities of Microsoft compliance solutions

You'll be prepared to take and pass the SC-900 exam

Created by Adrien Coquet
from Noun Project

But you don’t have to, if you just want to learn security, compliance, and identity concepts

Created by Adrien Coquet
from Noun Project

Security is a fundamental design requirement

Created by Alvida Biersack
from Noun Project

Exam covers both Azure and Microsoft 365

What Basic Azure Security Capabilities Exist?

Network Security Group

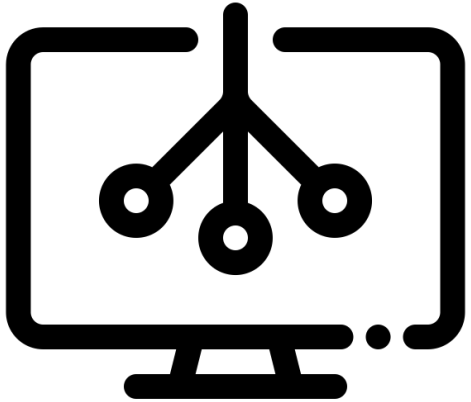
Azure DDoS Protection

Azure Firewall

Azure Bastion

Web Application Firewall (WAF)

Key Vault



Created by Timofei Rostilov
from Noun Project

What Azure Security Management Services Exist?

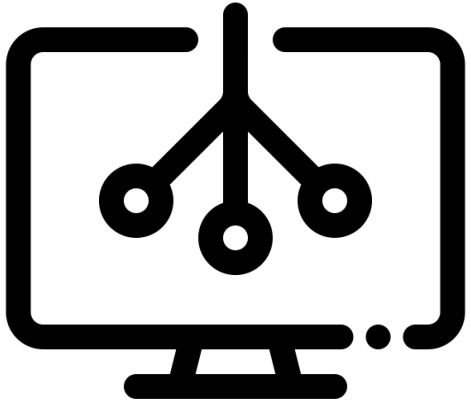
Microsoft Defender for Cloud
(was Azure Defender & Azure Security Center)

Cloud Security Posture Management (CSPM)

Secure score in Microsoft Defender for Cloud

Enhanced security in Microsoft Defender for Cloud

Microsoft Sentinel (was Azure Sentinel)



Created by Timofei Rostilov
from Noun Project

What Microsoft Defender XDR Capabilities Exist?

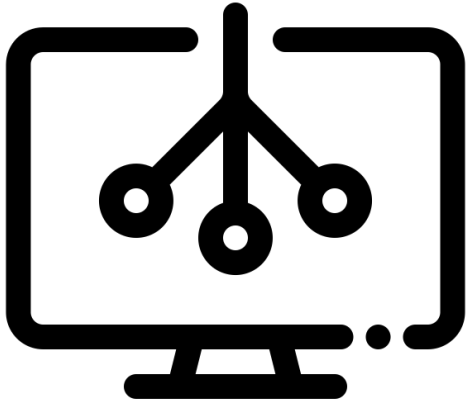
Microsoft 365 Defender XDR

Microsoft Defender for Identity
(formerly Azure ATP)

Microsoft Defender for Office 365
(formerly Office 365 ATP)

Microsoft Defender for Endpoint
(formerly Microsoft Defender ATP)

Microsoft Defender for Cloud Apps
(formerly Cloud App Security)



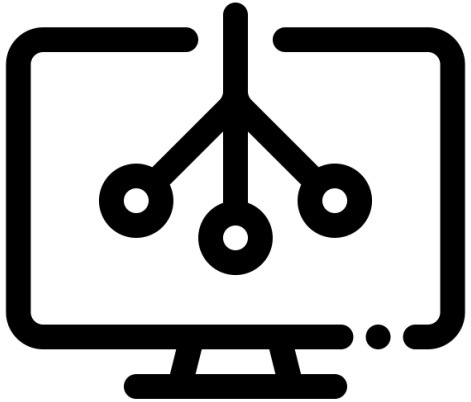
Created by Timofei Rostilov
from Noun Project

What Microsoft Defender XDR Capabilities Exist?

Microsoft Defender Vulnerability Management

Microsoft Defender Threat Intelligence (Defender TI)

Microsoft Defender portal



Created by Timofei Rostilov
from Noun Project

What M365 Compliance Capabilities Exist?

Microsoft Purview

Microsoft Priva

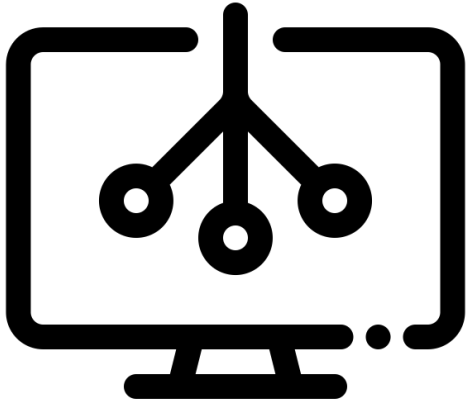
Retention Policies and Retention Labels

Records Management

Data Loss Prevention

eDiscovery

Advanced Auditing



Created by Timofei Rostilov
from Noun Project

What Basic Azure Identity Capabilities Exist?

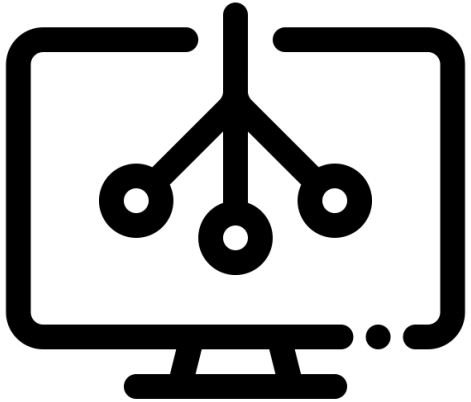
Active Directory

Entra ID (formerly Azure Active Directory)

Windows Hello for Business

Microsoft Entra ID Protection

Privileged Identity Management (PIM)



Created by Timofei Rostilov
from Noun Project

CERTIFICATION

Microsoft Certified: Security, Compliance, and Identity Fundamentals

Demonstrate foundational knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions.

At a glance

Level
Beginner

Product
Azure

Role
Security Engineer

Subject
Security

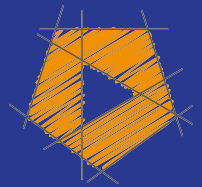
Last Updated
07/26/2024

Jump to

Prepare for the exam
Practice for the exam
Take the exam

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the Concepts of Security, Compliance, and Identity (10-15%)

Describe the concepts of security, compliance, and identity (10–15%)

Describe security and compliance concepts

- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Zero-Trust Model

Don’t assume everything behind the firewall is safe

Zero Trust Principles

- Verify explicitly
- Use least privileged access
- Assume breach

Real-World Examples of Zero Trust:

Verify explicitly - my bank requires my secret code any time I try to transfer money, even after I have logged into the app

Real-World Examples of Zero Trust:

Least privileged access - every August, the boss (Sally) goes on vacation for the whole month, and Bob covers her role. Every time Bob needs to perform an administrative task, he needs to request permission from the system which only grants him short-term access. This is called “just in time (JIT) access”.

Real-World Examples of Zero Trust:

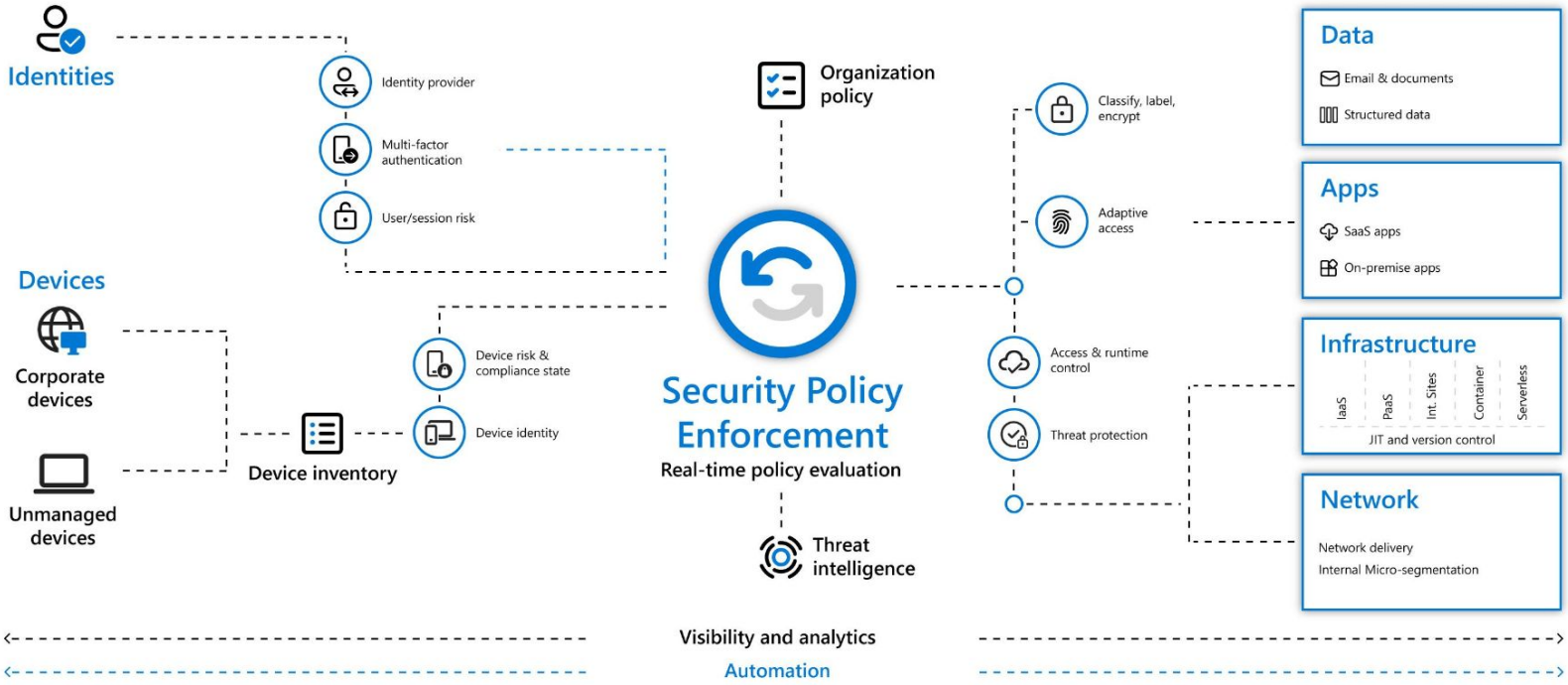
Assume breach - All sensitive data is encrypted at rest and in transit even between servers in the same data center. Even if a hacker was to find the data files, or could listen over the transmission wires inside your data center, they'd need the decryption keys to get the data.

Use every available method to validate identity and authorization

Just-in-time (JIT)

Just-enough-access (JEA)

Security even inside the network; encryption, segmentation, threat detection



Identity: Verify and secure each identity

Devices: ensure compliance and health status

Applications: appropriate in-app permissions, monitor user actions

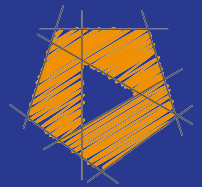
Data: data-driven protection, encrypt and restrict access

Infrastructure: robust monitoring to detect attacks, block and flag risky behavior

Network: encrypt all communications

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the concepts of security, compliance, and identity (10–15%)

Describe security and compliance concepts

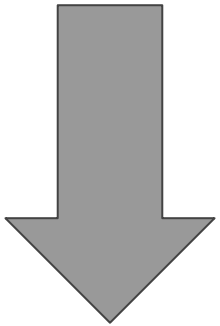
- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Encryption and hashing

Encryption (n):

the process of converting information or data into a code, especially to prevent unauthorized access.

“Hello.”



f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

Symmetric Encryption

There is ONE KEY

Same key locks the message (encrypt) and unlocks the message (decrypts)

Example: **WhatsApp** uses symmetric encryption

There is a shared secret between two people - “master secret key”

And nobody in the middle (including Meta) can decrypt the message

Asymmetric Encryption

There are two keys - PUBLIC and PRIVATE

You can use either key to encrypt the message, and the other one decrypts

Public can be published to anyone, and private must stay private

Example: **HTTPS** is asymmetric encryption

Hashing (Preventing Forgery)

Hashing uses cryptography but is not encryption

It is a way to turn plain text into a short unique code

The unique code cannot be turned back into plain text (one-way function)

But hashes can be used to ensure the data received has not been altered

Dear Student,

This is a message from the instructor, Scott Duffy.

This message is not encrypted, in that anyone can read it. But you can be 100% sure that it's from me because it's signed. I have used my private key to encrypt the hash, and you can use my public key to decrypt it. You can then check the SHA-1 signature attached to this message against an SHA-1 generator and verify that the contents have not been altered.

Generate | Clear All | MD5 | SHA256 | SHA512 | Password Generator

☐ Treat each line as a separate string ☐ Lowercase hash(es)

SHA1 Hash of your string: [Copy to clipboard]

63904A42D4114E0ED28F03FBA5767A0803017914

Enter your text below:

Dear Student,

This is a message from the instructo John Doe.

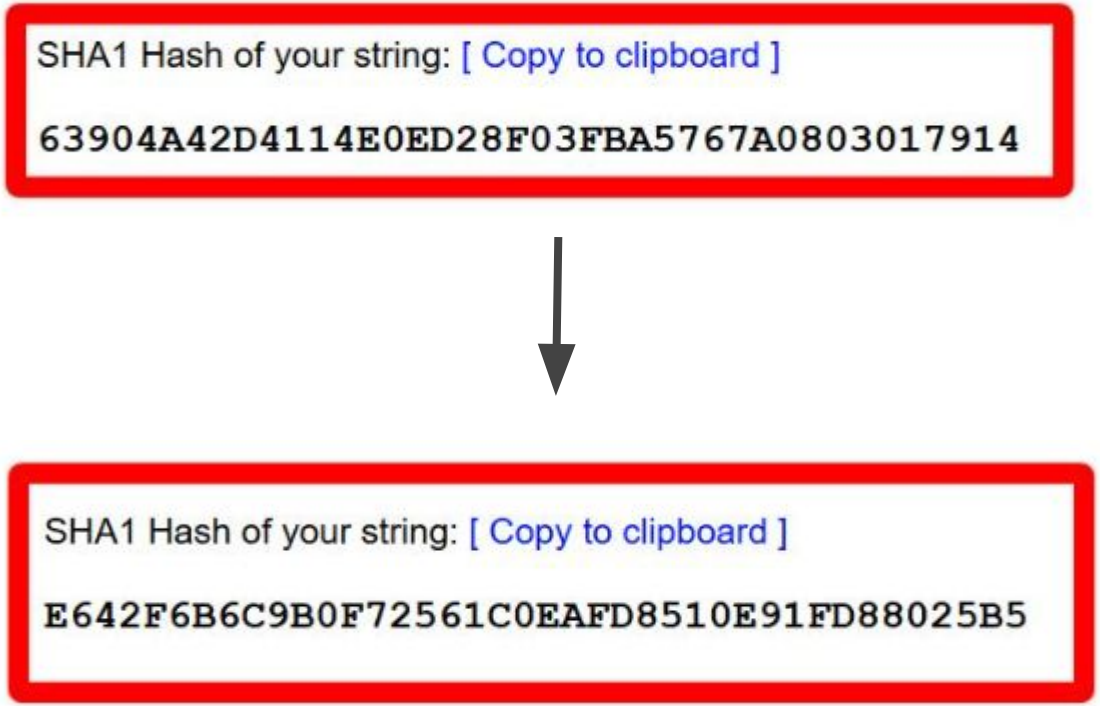
This message is not encrypted, in that anyone can read it. But you can be 100% sure that it's from me because it's signed. I have used my private key to encrypt the hash, and you can use my public key to decrypt it. You can then check the SHA-1 signature attached to this message against an SHA-1 generator and verify that the contents have not been altered.

Generate | Clear All | MD5 | SHA256 | SHA512 | Password Generator

☐ Treat each line as a separate string ☐ Lowercase hash(es)

SHA1 Hash of your string: [Copy to clipboard]

E642F6B6C9B0F72561C0EAFD8510E91FD88025B5



Scott Duffy.

John Doe.

Hashing (Storing Passwords)

A lot of companies use “hashes” to store passwords in a database

So you’ll see, when a company gets hacked, the hackers don’t get passwords, they get hashes

Dropbox Sign hack: how it happened and what data was stolen

Unidentified attackers have managed to compromise the Dropbox Sign service account, and thus gain access to the platform's internal automatic configuration mechanism. Using this access, hackers were able to lay their hands on a database that contains information about Dropbox Sign users.

As a result, the following data of registered users of the Sign service was stolen:

- usernames;
- email addresses;
- phone numbers;
- passwords (hashed);
- authentication keys for the DropBox Sign API;
- OAuth authentication tokens;
- SMS and application two-factor authentication tokens.

How Passwords are Hashed

When you create a new account at a website

You enter your desired password (**not** “password123!”)

The company **should not** store your password as **plain-text** in their database!

They will hash the password (in some secure fashion) and store the hash

When you log into the website, they take the password you enter to log in and hash it, and compare that hash with what is stored

Salting involves adding a random, unique value to each password before hashing

Peppering involves using a secret value to hash the password again before storing

Work factors is a way of making the hash function more expensive in computing power

Examples of Symmetric Encryption Algorithms

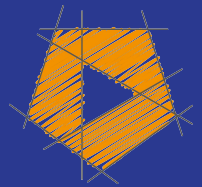
- AES (Advanced Encryption Standard)
  - The most commonly used symmetric encryption algo
- DES (Data Encryption Standard)
  - Considered too weak for modern powerful computers
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

Examples of Asymmetric Encryption Algorithms

- RSA
  - Encryption used by HTTPS/SSL (asymmetric in the most common usage)
- Diffie-Hellman
- ECC
  - Encryption used by Bitcoin
- ElGamal
  - Used in recent versions of PGP
- DSA
  - US Government FIPS standard for signing messages

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the concepts of security, compliance, and identity (10–15%)

Describe security and compliance concepts

- Describe the shared responsibility model
- Describe defense-in-depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe Governance, Risk, and Compliance (GRC) concepts

Governance, Risk, and Compliance (GRC)

Governance - a set of policies, rules or frameworks designed to achieve business goals

Risk management - identify the different risks that a business faces and mitigate them

Compliance - following rules, laws and regulations

Examples of compliance regulations:

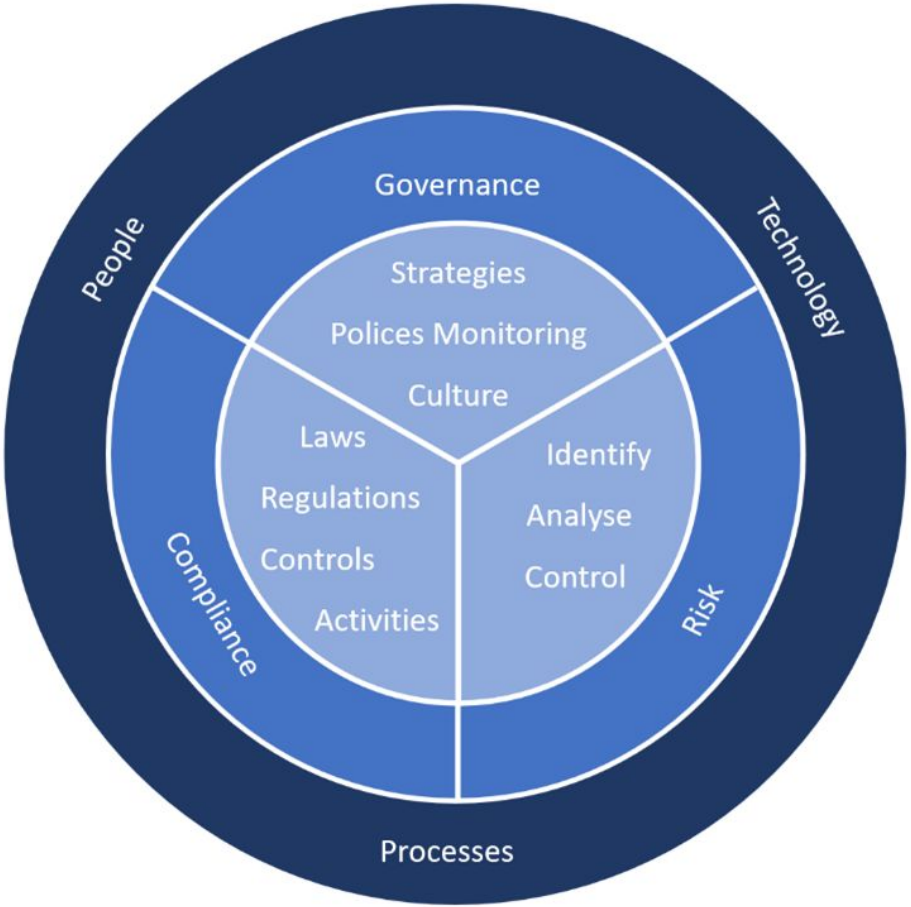
- CCPA (California Consumer Privacy Act; USA)
- GDPR (General Data Protection Regulation; Europe)
- HIPAA (Health Insurance Portability and Accountability Act; USA)
- PCI DSS (Payment Card Industry Data Security Standard; international)
- SOX (Sarbanes–Oxley Act; US)

GRC is about making better decisions while being aware of all of the risks

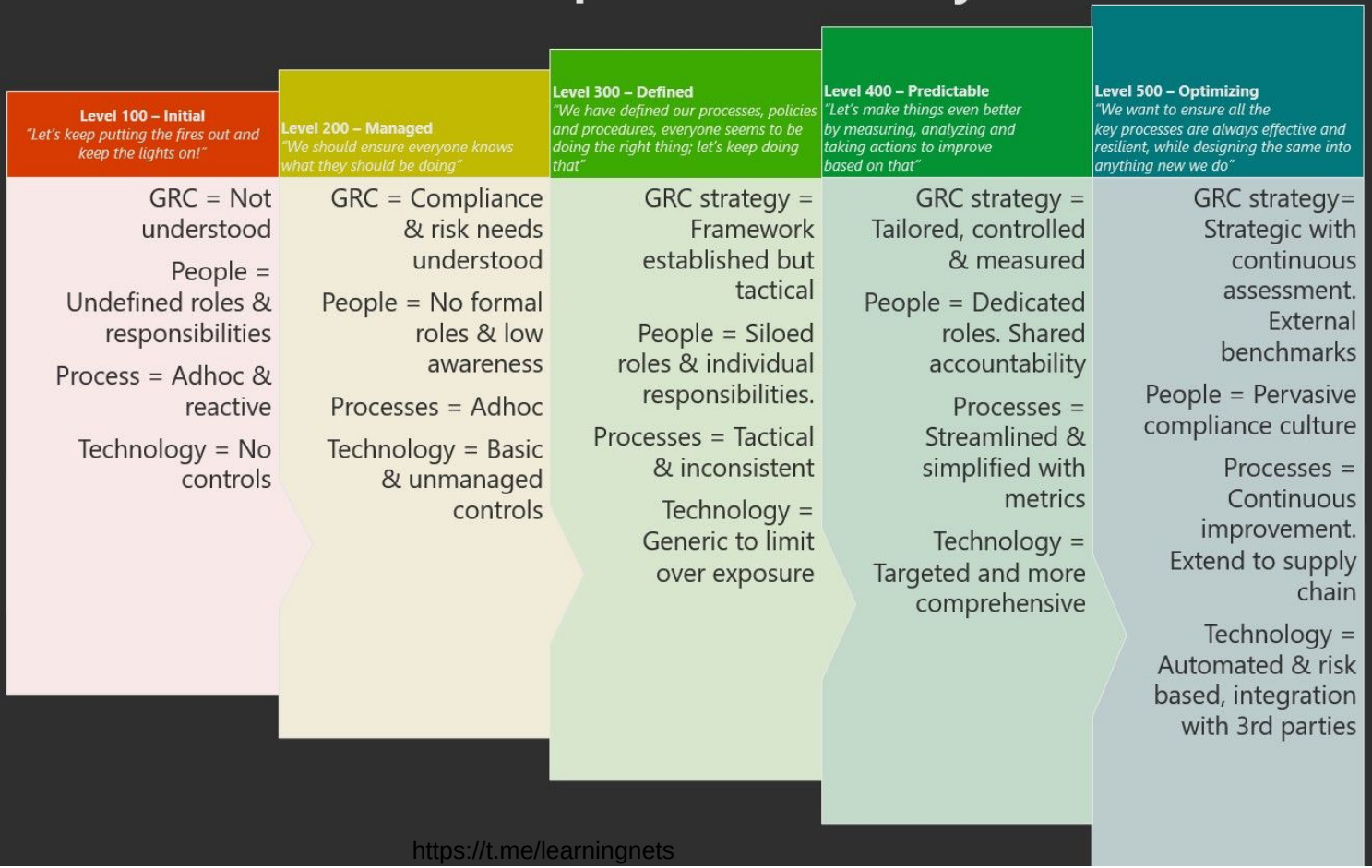
GRC programs

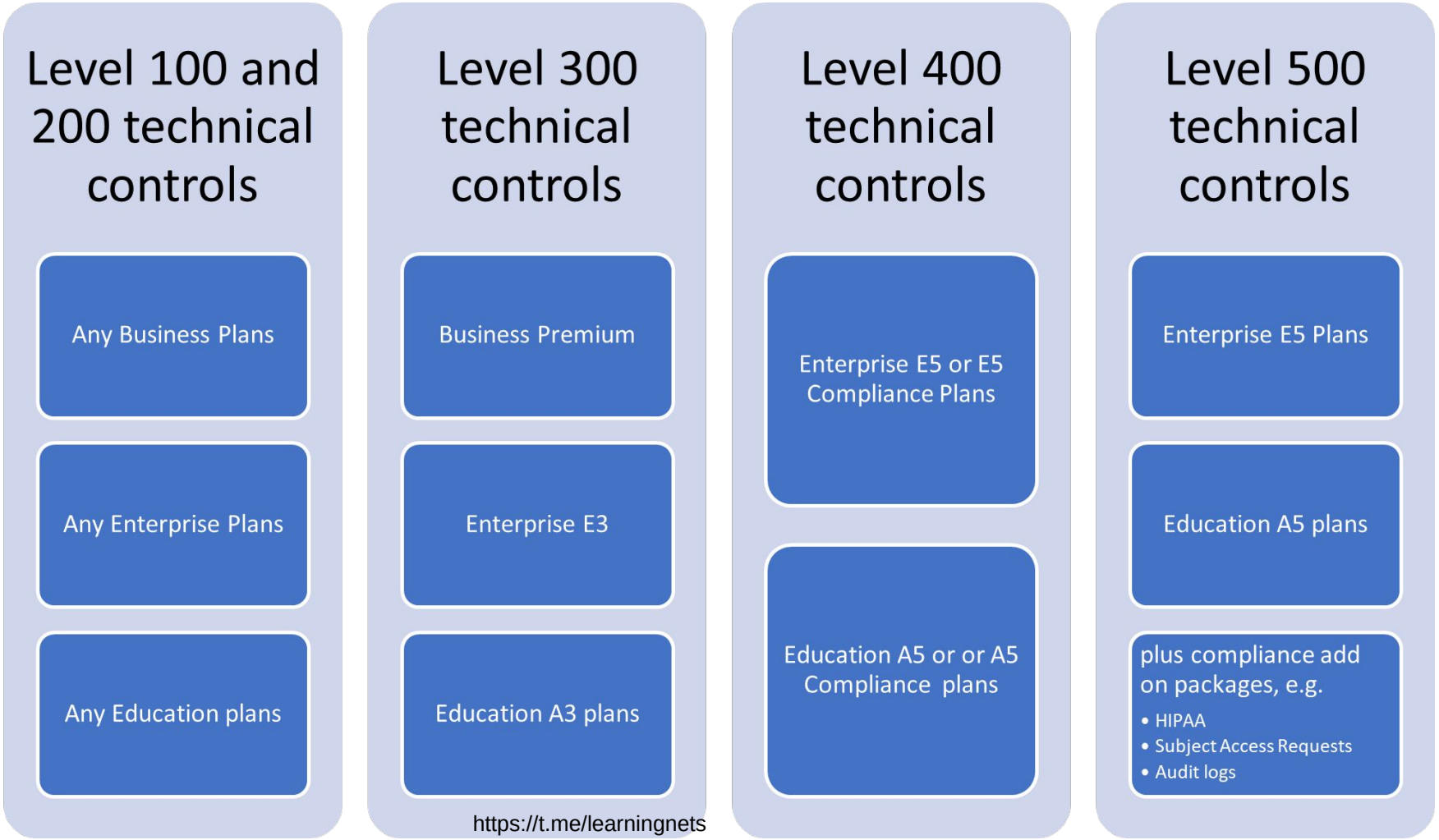
- Data-driven decision making
- Responsible operations
- Improved cybersecurity

Microsoft 365 Maturity Model



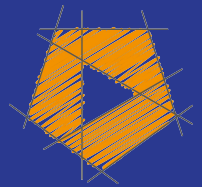
Governance Risk and Compliance maturity levels





SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Identity as the Primary Security Perimeter

Security Perimeters

The person is who they say they are

Company owned network

Company owned device

Services are provided only inside company data center

Security Perimeters

The person is who they say they are - Verified identity

~~Company owned network~~ - Work from home

~~Company owned device~~ - Using your own computers/mobile

~~Services are provided only inside company data center~~ - Cloud computing

Identity is now the primary security perimeter

Identity is not just a “person”

Employees

Partners and customers

Cloud apps

On-prem apps

Devices

Zero trust model

Advances in security focus on ensuring identity is trustable

Ways to verify identity

Beyond the simple user id/password

Single sign-on (using AD everywhere)

Multi-factor authentication

Just-in-time access requests

More granular security + logging

Intelligent monitoring that detects strange behavior

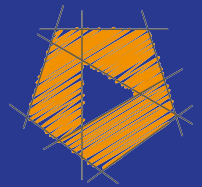
More granular security on data and documents

Restrict unrequired and unwanted lateral movement of traffic

Least privilege / default deny

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

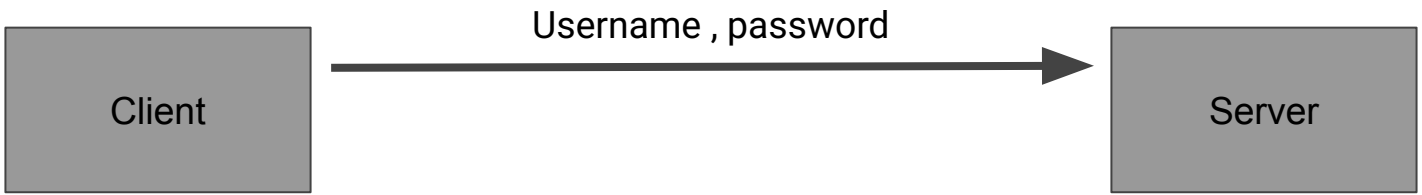
Define Authentication (AuthN)

How much proof do you need for me to prove my identity to you?

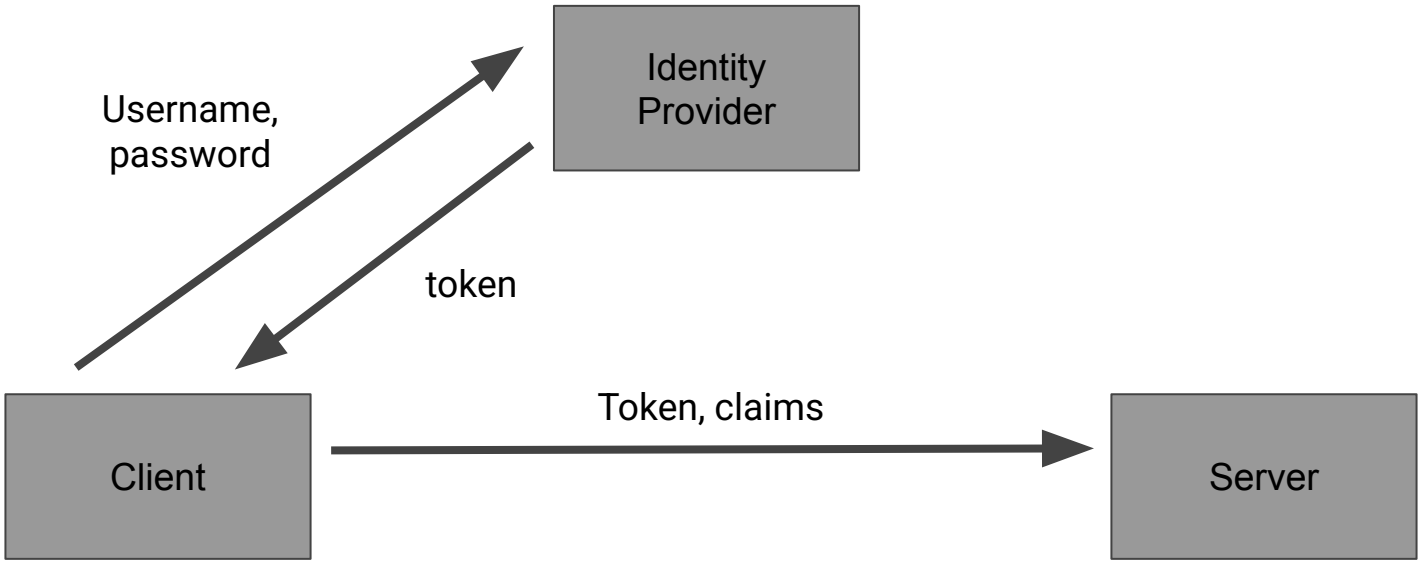
“Modern Authentication”

Server should use an identity provider to validate identity

The Old Way



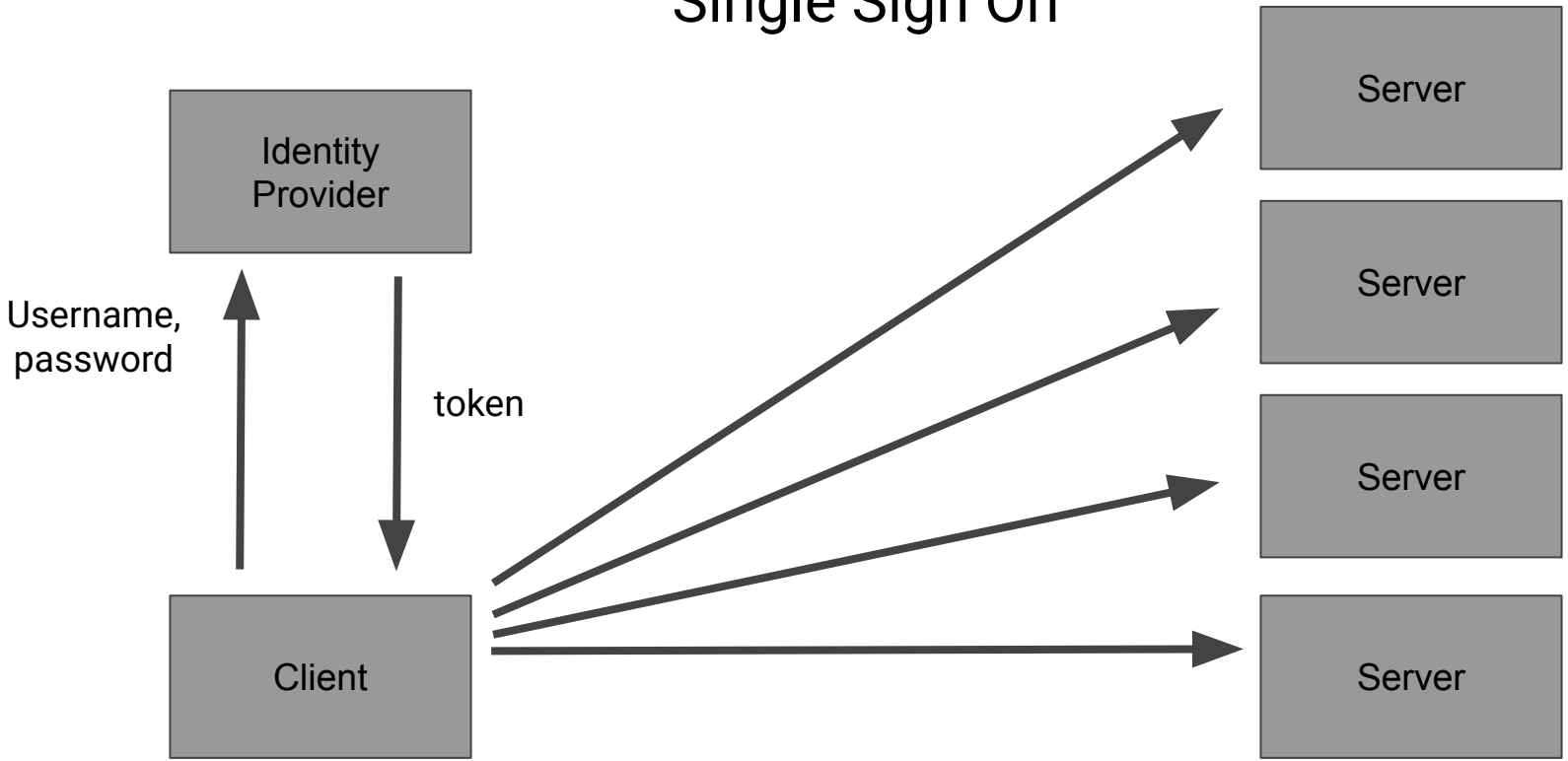
The New Way



A ***token*** is a digital credential, signed by the server, that verifies your identity

Claims are details about the authenticated user such as username or roles

Single Sign On



Define Authorization (AuthZ)

The level of access an authenticated person has

“Permissions”

Principle of least privilege

A user
is granted a set of permissions to perform some tasks

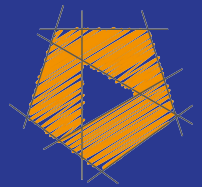
A ~~user~~ role
is granted a set of permissions to perform some tasks

What role do you have?

Users can have multiple roles

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

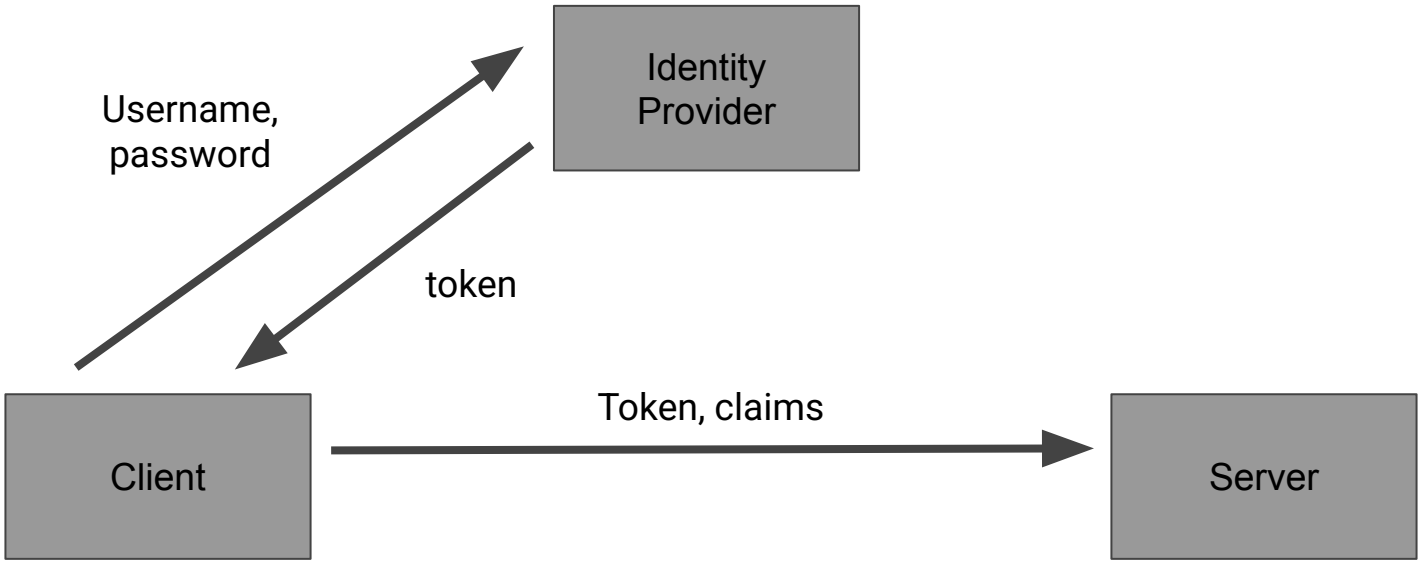


Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Identity Providers

The New Way



Creates, maintains and manages identity information...

Plus offers authentication, authorization and auditing services

Microsoft Entra ID

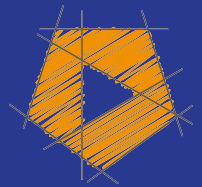
Formerly
Azure Active Directory (Azure AD)

Active Directory

Google
Facebook
Twitter
LinkedIn
GitHub

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Active Directory

What is a “directory”?

“A **directory** is a **hierarchical structure**
that stores information about
users, groups, devices, applications,
and other resources within an organization”

What is a “directory service”?

“A **directory service** stores **directory data**
and makes this information accessible to
network users, administrators, services, and applications”

What is “Active Directory”?

“**Active Directory (AD)** is a set of directory services developed by Microsoft, initially released as part of Windows 2000.
It's primarily used for managing identities within **on-premises domain-based networks**”

What is “Active Directory Domain Services”?

“**Active Directory Domain Services (AD DS)** is the most well-known service within Active Directory. It acts as a **central repository** of information about domain members, including users and devices”

Key Functions of AD DS

Storing information: users, devices, groups, and other objects within the domain

Credential verification: verifies user credentials during login attempts

Access control: AD DS defines and enforces access rights, determining what resources users are permitted to access based on their roles and permissions

What is a “Domain Controller”?

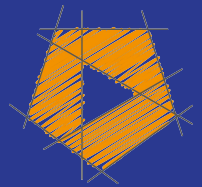
This is a server running “Active Directory Domain Services”.

Limitations of AD DS

- Limited Support of Modern Authentication Methods
  - Old methods: Kerberos, NTLM, LDAP
  - New methods: OAuth 2.0, OpenID Connect, MFA, SSO across Federation
- On-Premises Focus

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Federation

The use of multiple identity providers

The identity providers have a trust relationship between each other

Company A AD trusts Company B AD

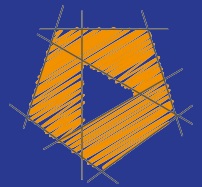
User from Company B can log in to Company A app

Trust isn’t always bi-directional

Azure AD B2C can be configured to use social media sites for identity

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft Entra (25–30%)

Describe function and identity types of Microsoft Entra ID

- Describe Microsoft Entra ID
- Describe types of identities
- Describe hybrid identity

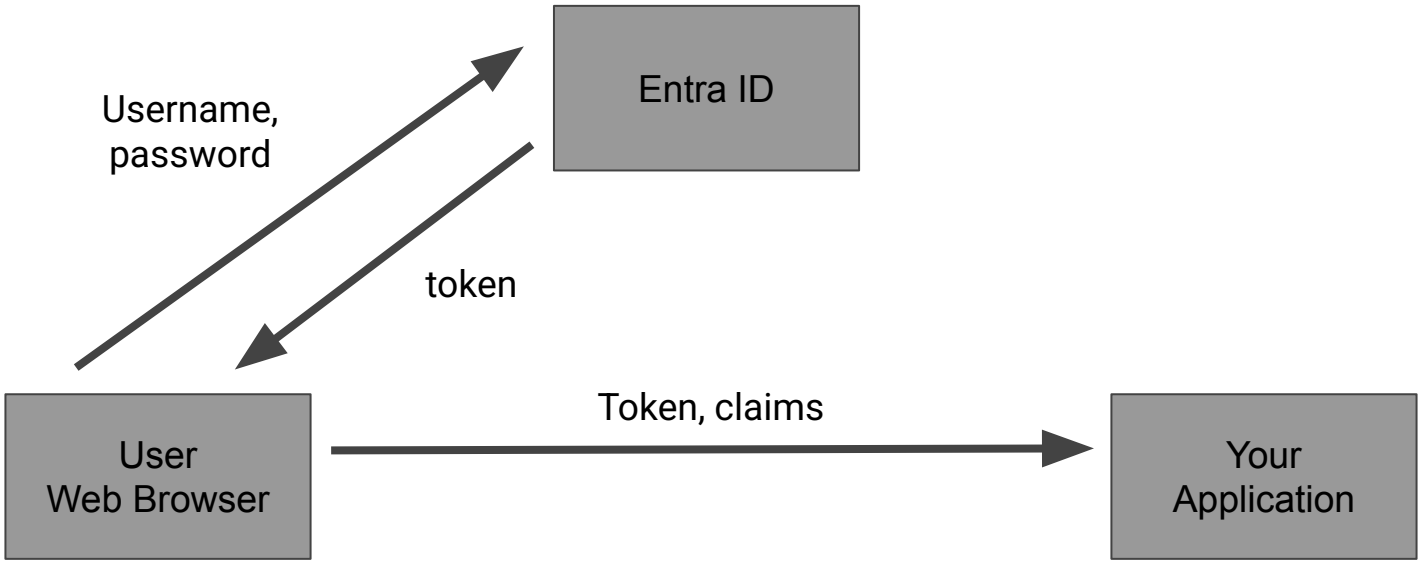
Microsoft Entra ID

Identity as a Service in Azure

What is a “directory”?

“A **directory** is a **hierarchical structure**
that stores information about
users, groups, devices, applications,
and other resources within an organization”

Entra ID



A Tenant =
An Organization

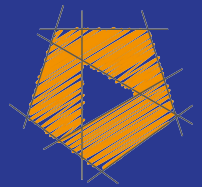
A tenant can have a subscription to enable compute resources to be created

Applications can register with Entra ID

Demo of Entra ID

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Types of Identities

Man or Machine?

When it comes to the user…

They can be a **human** (employee, customer, partner, contractor…)

Or **computer program** (virtual machine, application, device, service…)

Inside or Outside?

They can be…

Managed by Entra ID (internal users)

Managed outside (external users / Federation)

Cloud Identities (Internal Users)

Identities that exist solely in the cloud

Typically only used for cloud-based resources and applications

Managed entirely in Entra ID

Users who access cloud-based application like Microsoft 365, Azure services, and other SaaS offerings

Suitable for cloud-native organizations

Cloud Identities (Internal System/Apps)

Sometimes called “**service principals**” or “**managed identities**”

Applications or services that need access to resources

Not associated with human users

Managed entirely in Entra ID

Assigned permissions based on their intended functions

On-Premises Identities

Identity originates from an on-premises directory such as Active Directory

For users who access the company internal network

Managed in AD

May be synchronized with Entra ID for hybrid scenarios

Suitable for organizations with significant on-prem infrastructure

External Identities (Internal Guest Users)

Users are from outside the company’s primary directory

Granted access as partners, customers, contractors or guests

Suitable for collaboration scenarios

Managed entirely in Entra ID

Could be temporary access, or access to shared resources

External Identities (B2B)

Users are from outside the company’s primary directory

Granted access as partners, customers, contractors or guests

Suitable for collaboration scenarios

Uses Federation - identity managed by an outside directory

Could be temporary access, or access to shared resources

Hybrid Identities

A bridge between on-premises and cloud identities

Users can access resources on-premises and in the cloud with a single set of credentials

Suitable for organizations transitions between two environments

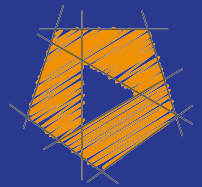
Cloud Synchronized

Single Sign-on

Centralized identity management

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft Entra (25–30%)

Describe function and identity types of Microsoft Entra ID

- Describe Microsoft Entra ID
- Describe types of identities
- Describe hybrid identity

Function of Entra ID

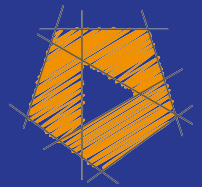
Entra ID can work with the on-premises Active Directory

To provide Single Sign On experience using:

- Your work computer
- Any custom apps your company creates that need authentication
- Third-party apps like Dropbox and Adobe (Enterprise Apps)

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe authentication capabilities of Microsoft Entra ID

- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities

Azure AD Password Protection

Global Banned Password List

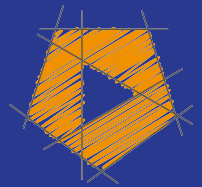
Custom Banned Password List

Bad password attempts and lockout duration

Can also protect Windows Server Active Directory

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe authentication capabilities of Microsoft Entra ID

- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities

Something you are
Something you have
Something you know

Authenticator app
OATH Hardware token
SMS
Voice call

MFA: Enabled by administrators

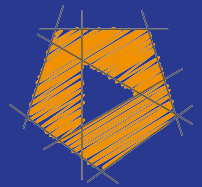
MFA: Signed up by users

Conditional access

Session lifetime

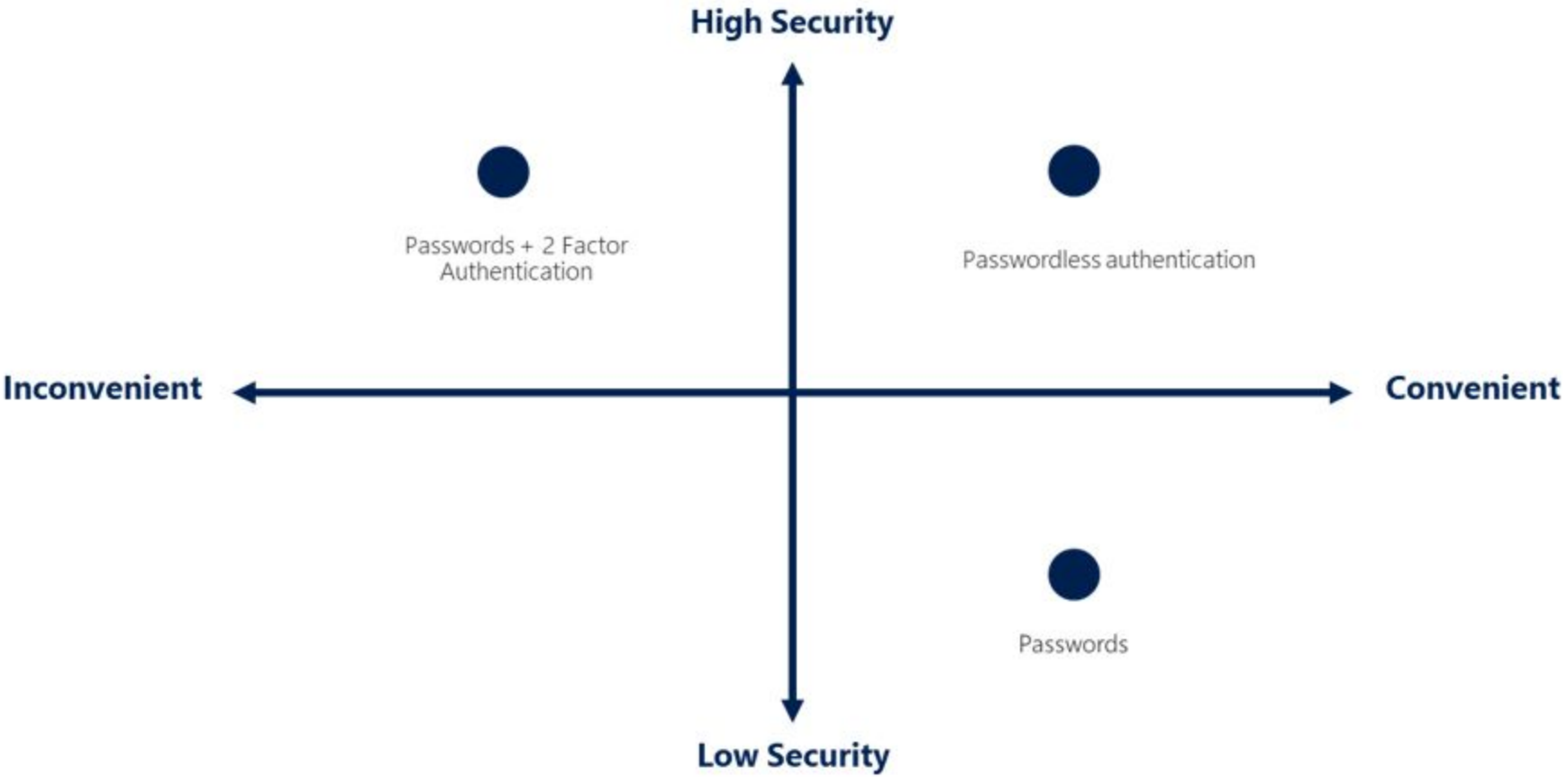
SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe authentication capabilities of Microsoft Entra ID

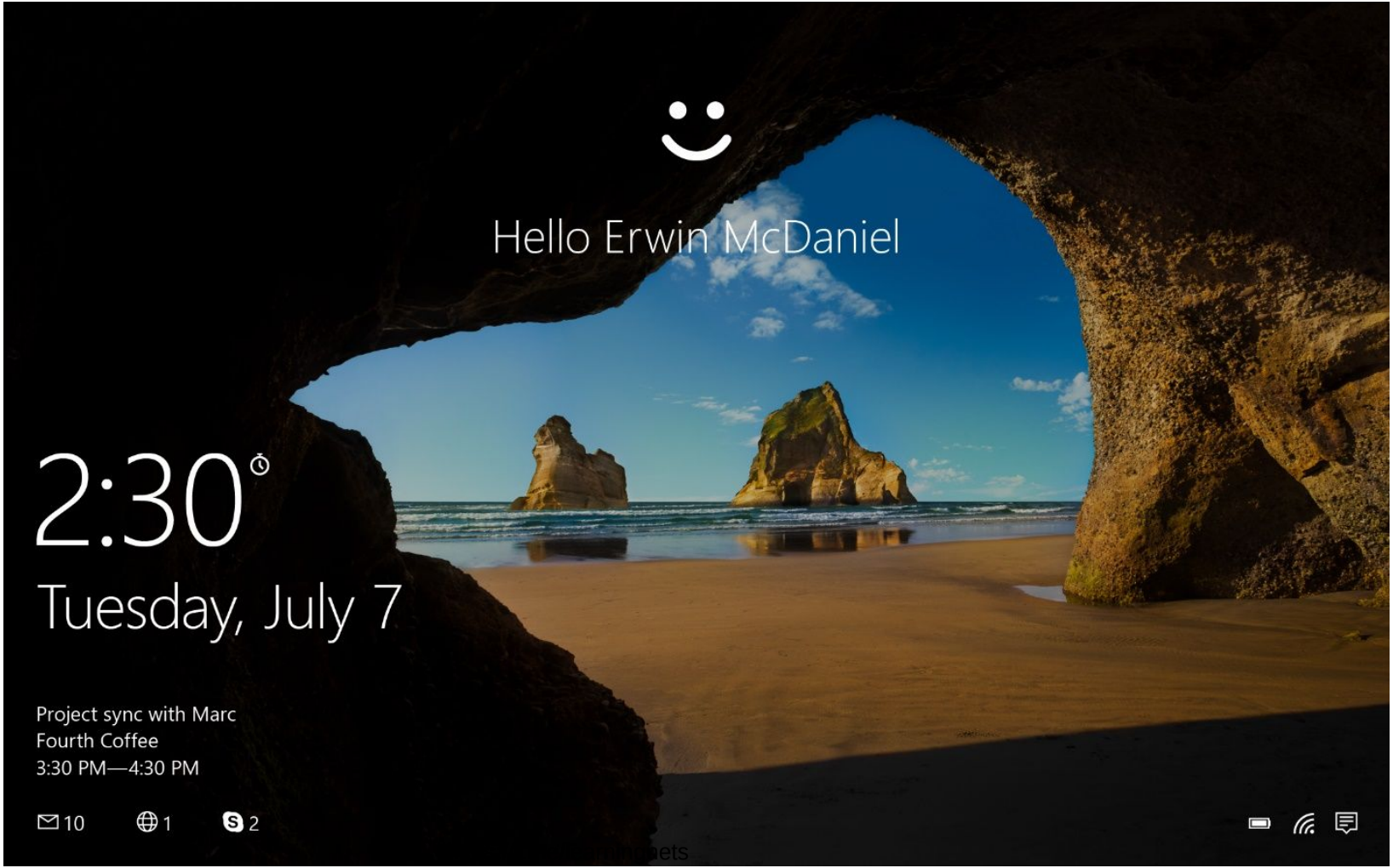
- Describe the authentication methods
- Describe multi-factor authentication (MFA)
- Describe password protection and management capabilities



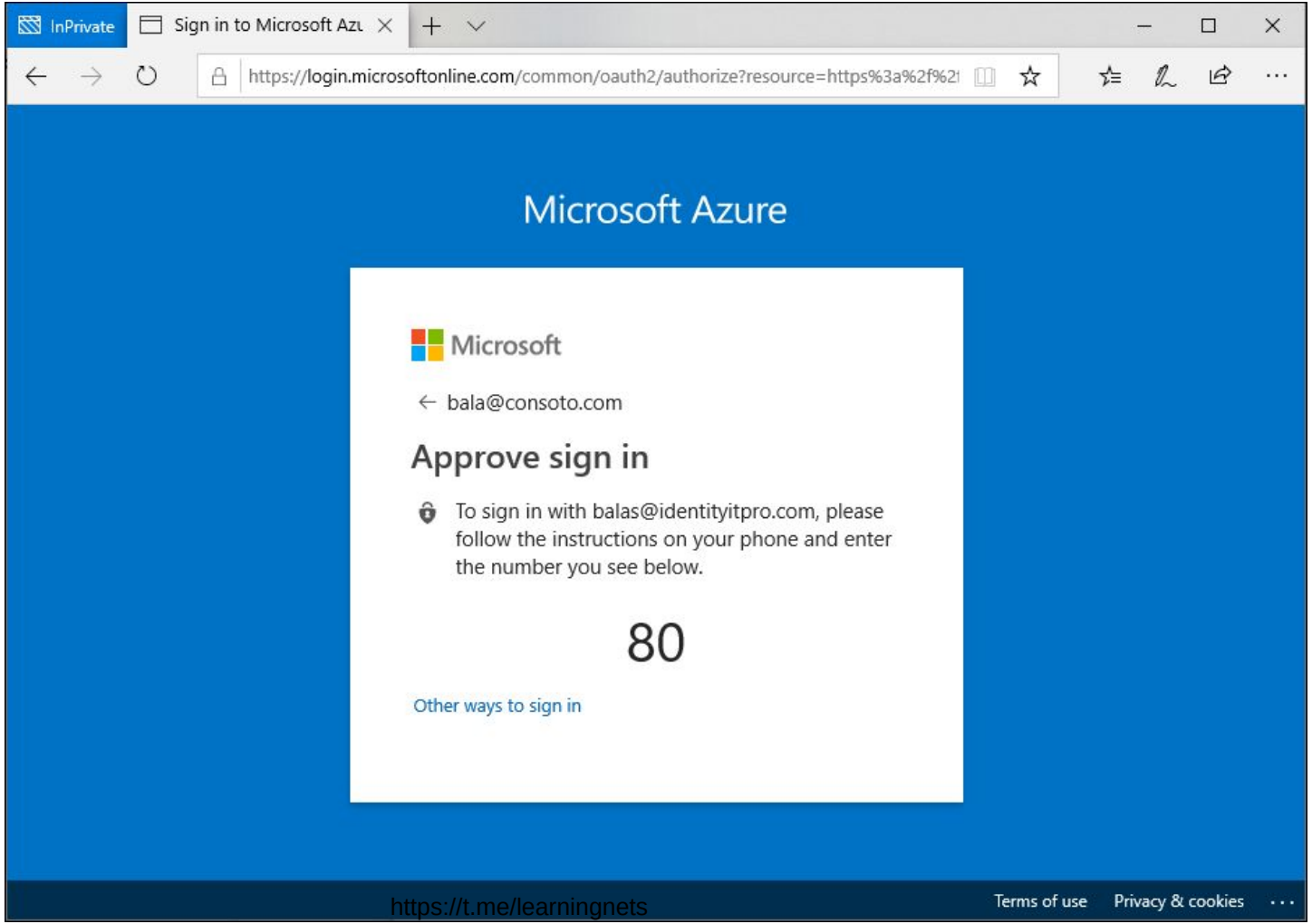
Passwordless

Gestures to sign in

Sign in using a PIN or biometric recognition (facial, iris, or fingerprint) with Windows devices.

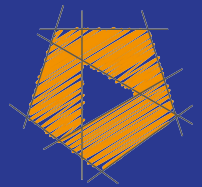

Hello Erwin McDaniel
2:30
Tuesday, July 7
Project sync with Marc
Fourth Coffee
3:30 PM—4:30 PM
10
1
2

Your phone:
“Are you attempting to sign in to this app?”



SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe access management capabilities of Microsoft Entra ID

- Describe Conditional Access
- Describe Microsoft Entra roles and role-based access control (RBAC)

Conditional Access

Using signals to make decisions and enforce policies

User and location
Device
Application
Risk

Allow access
Require MFA
Deny access

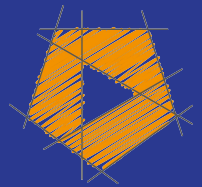
Require MFA for all Admin users

Require MFA signup from trusted locations

Some minimum standard for device, location, or risk

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe identity protection and governance capabilities of Microsoft Entra

- Describe Microsoft Entra ID Governance
- Describe access reviews
- Describe the capabilities of Microsoft Entra Privileged Identity Management
- Describe Microsoft Entra ID Protection
- Describe Microsoft Entra Permissions Management

Identity Governance

Balance the need for security...

… and employee productivity

Identity Lifecycle

From the time you start your first day with the company, to the time you retire

Integration with the HR system

Your role is managed by HR

And access is granted or revoked based on that HR system

Access Lifecycle

How to request access to things you need to get access to?

Understanding the data handling policies for different regions of the world

Dynamic groups

Azure AD Access Reviews

Azure AD Entitlement Management

Conditional Access can enforce terms of use acceptance

Privileged Access Lifecycle

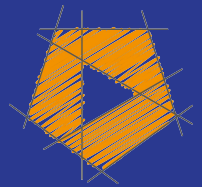
Azure AD Privileged Identity Management (PIM)

Just-in-time access

Access reviews

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

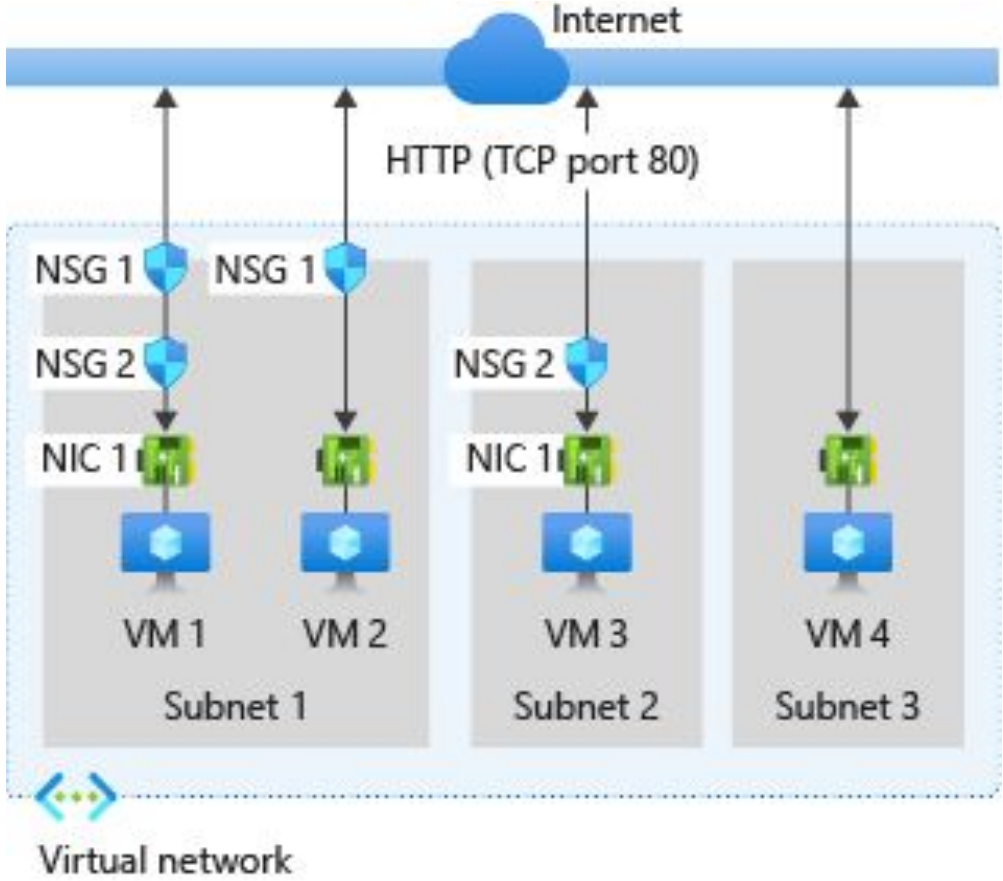
Network Security Group

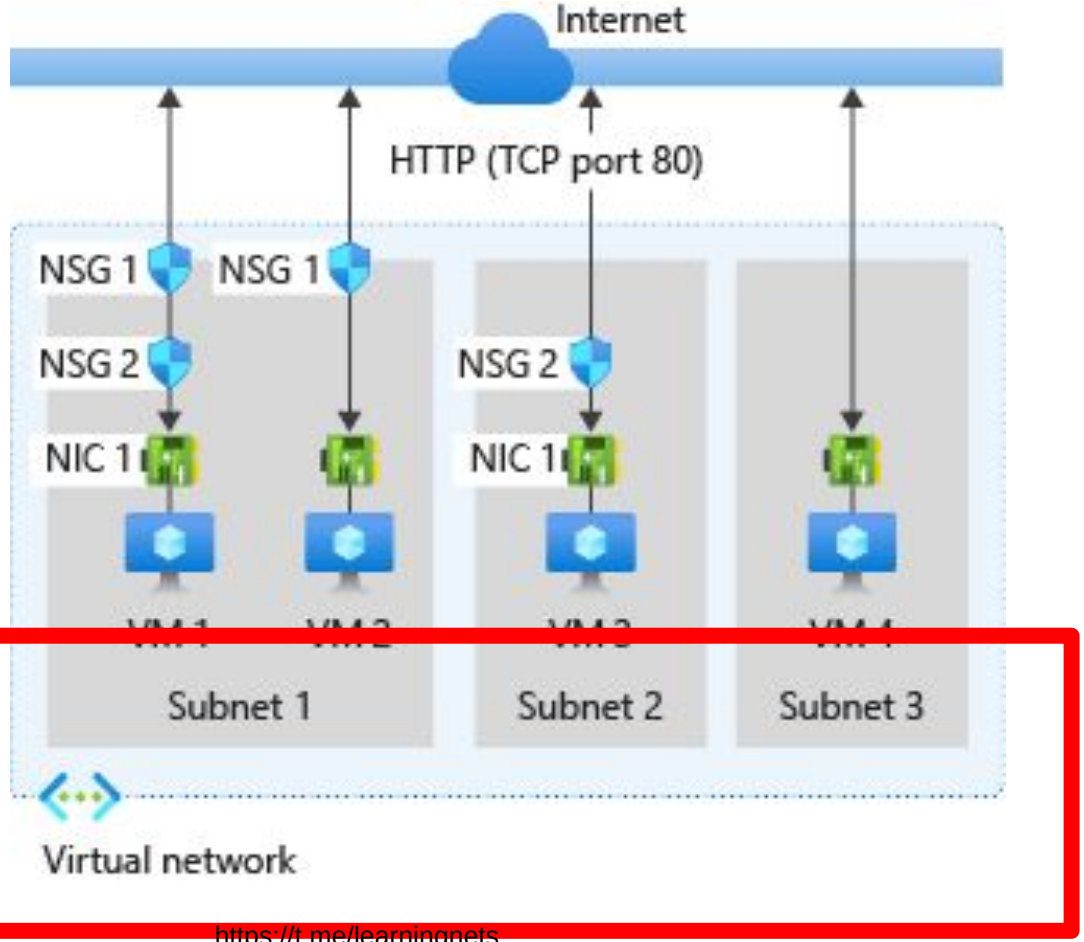
Simple, rules-based control that allows or denies traffic travelling over a network boundary

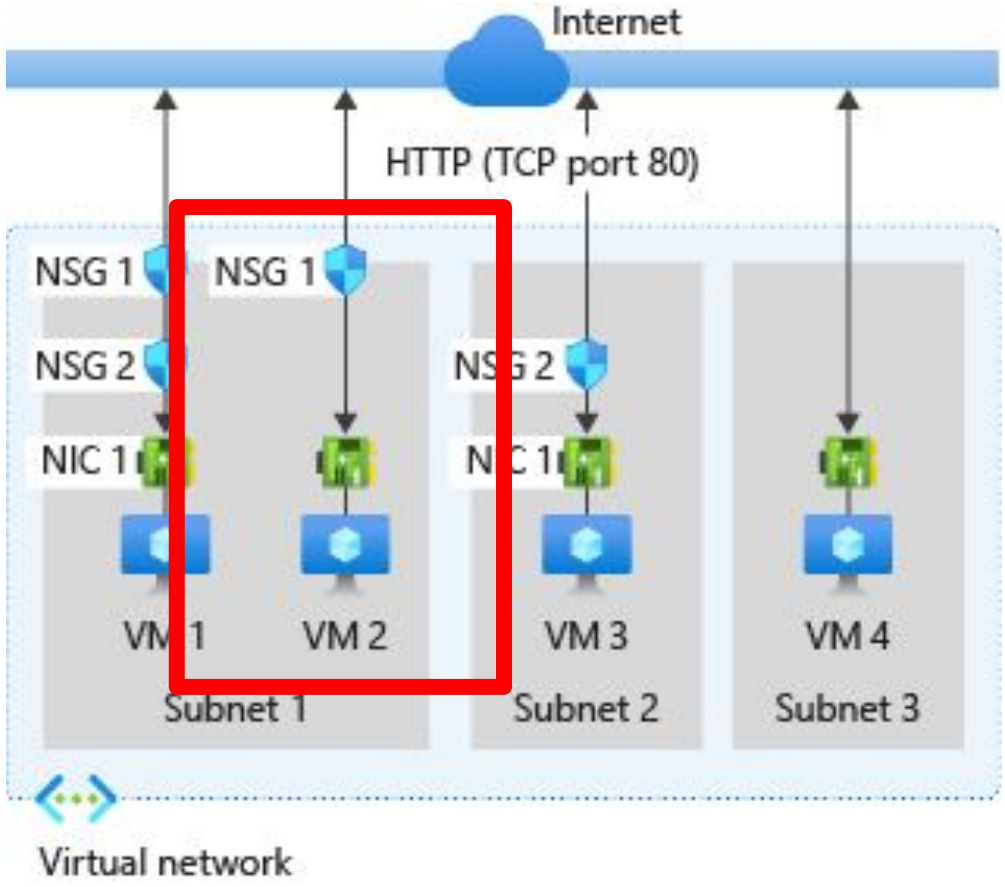
Inbound and outbound can have separate rules

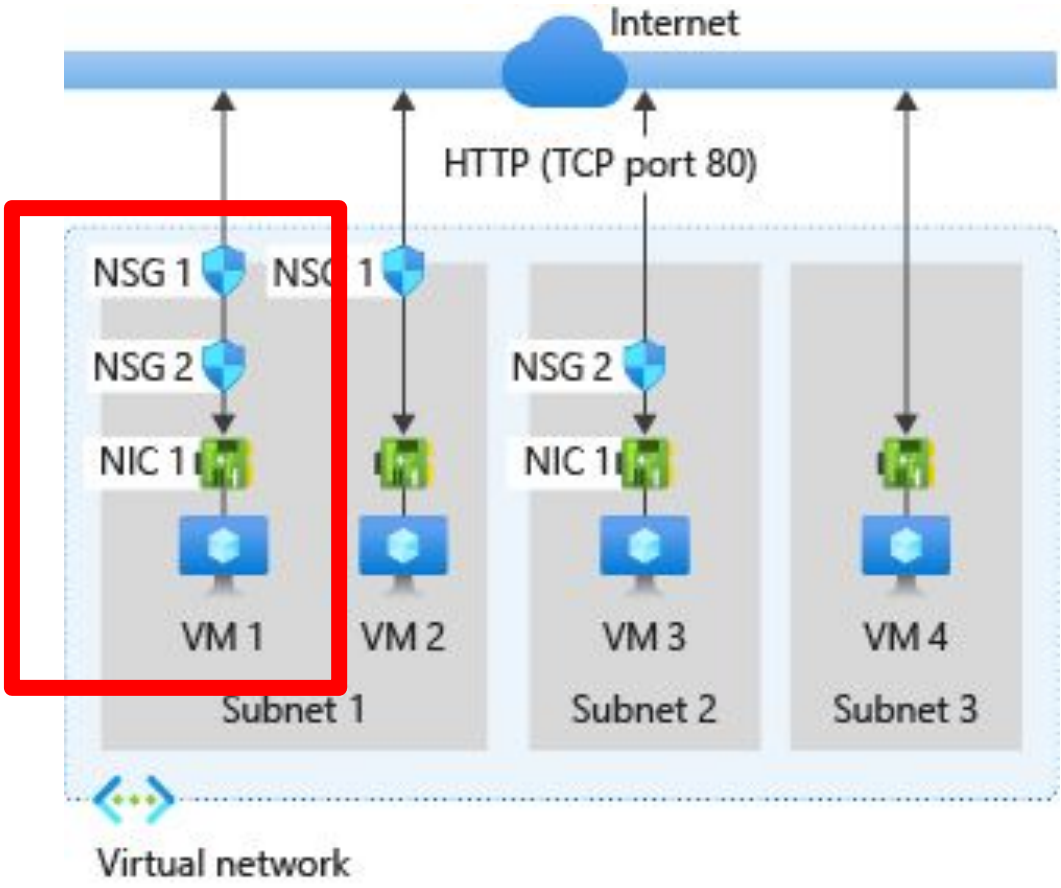
Two network boundaries - the subnet and a network interface card (NIC)

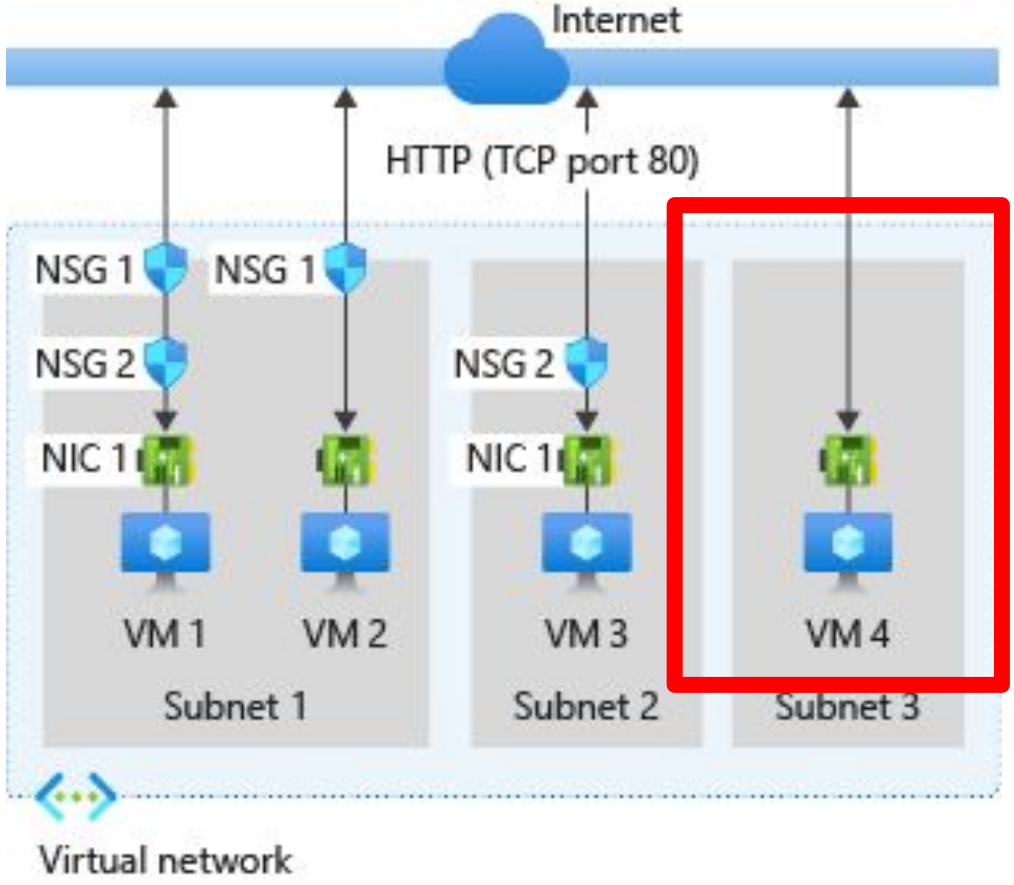
Deny by default





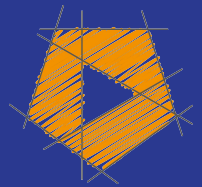






SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

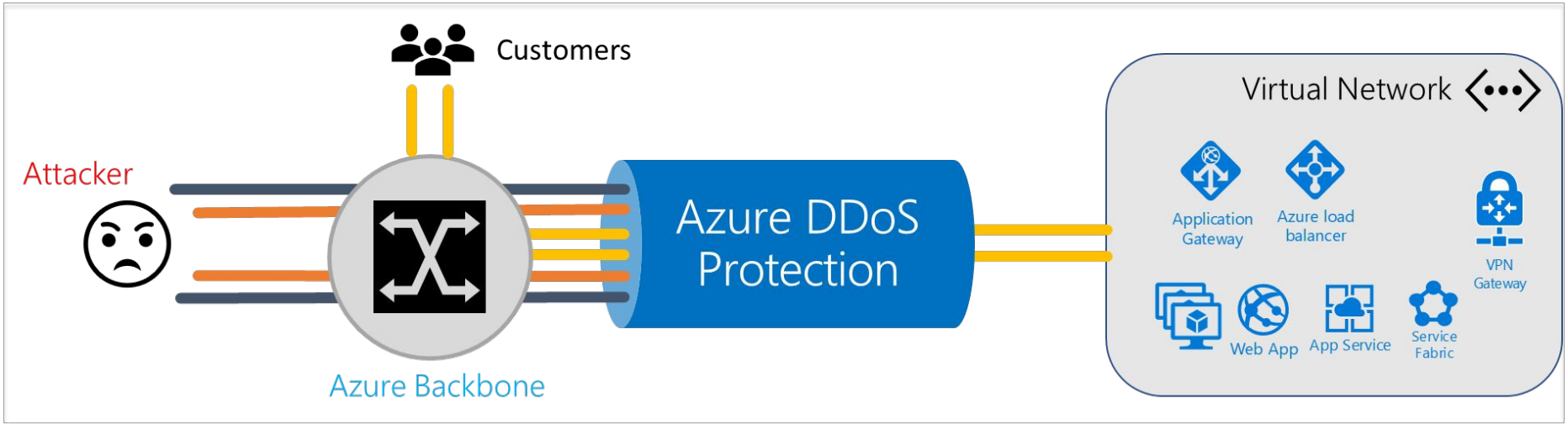


Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

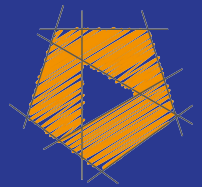
Azure DDoS Protection



Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee		●
Cost Protection		●
Mitigation policies tuned to customers application		●
Metrics & alerts		●
Mitigation reports		●
Mitigation flow logs		●
DDoS rapid response support		●

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

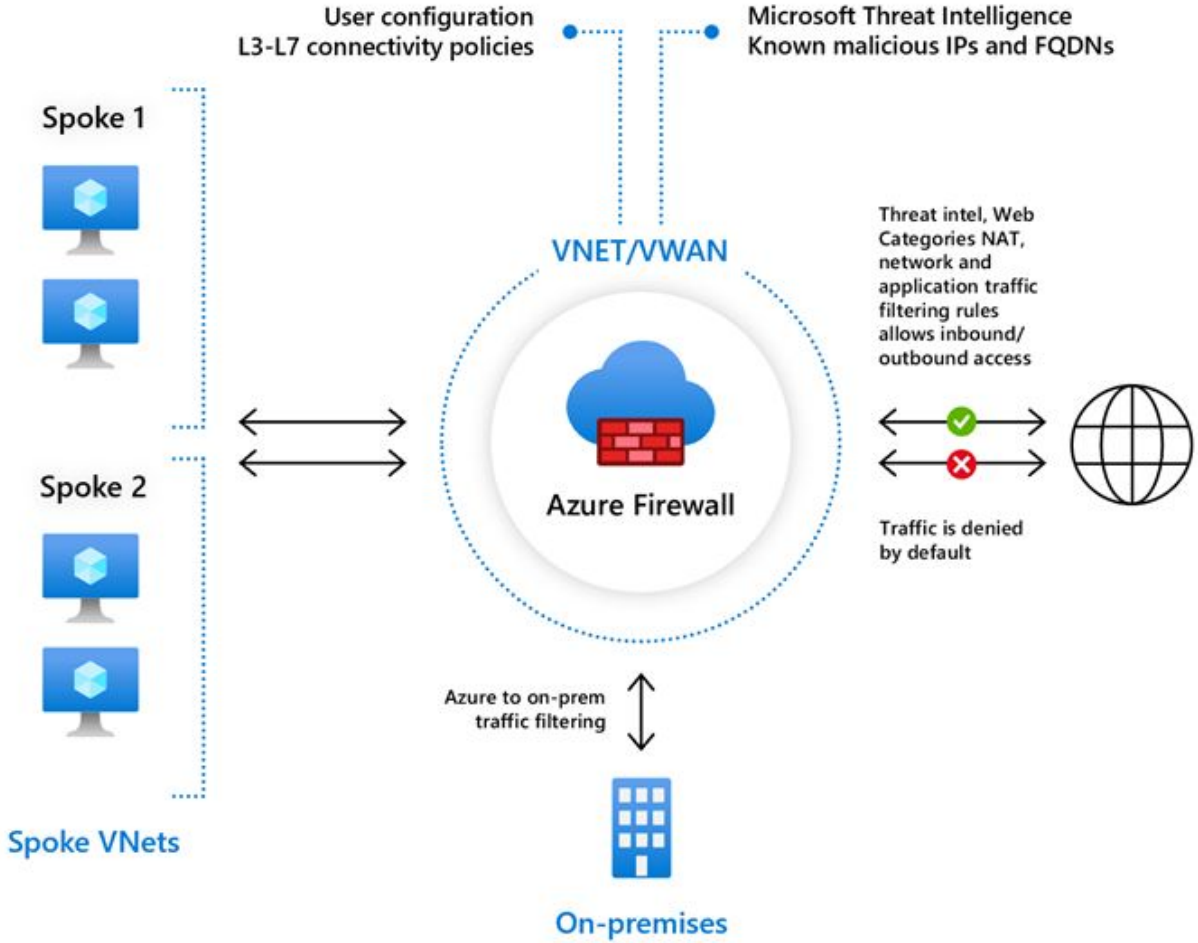
Scott Duffy, Instructor

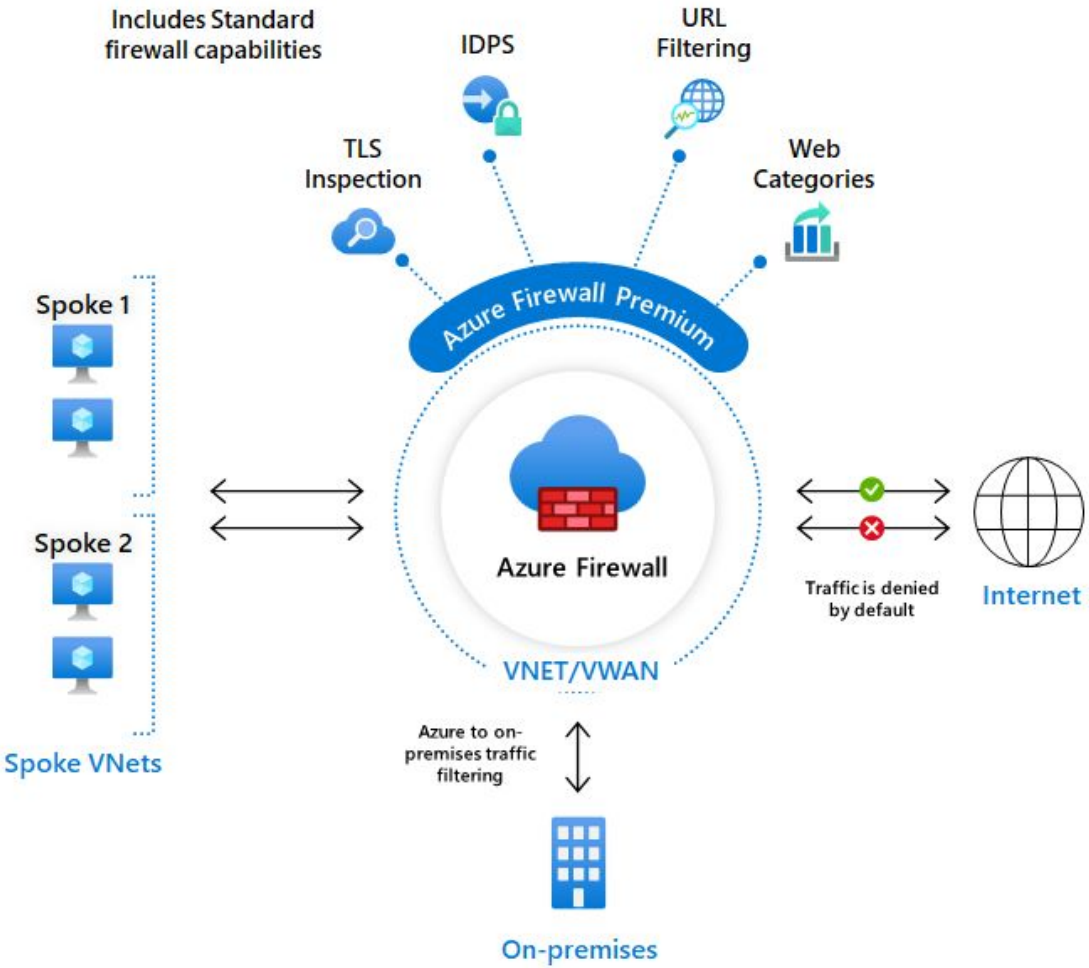


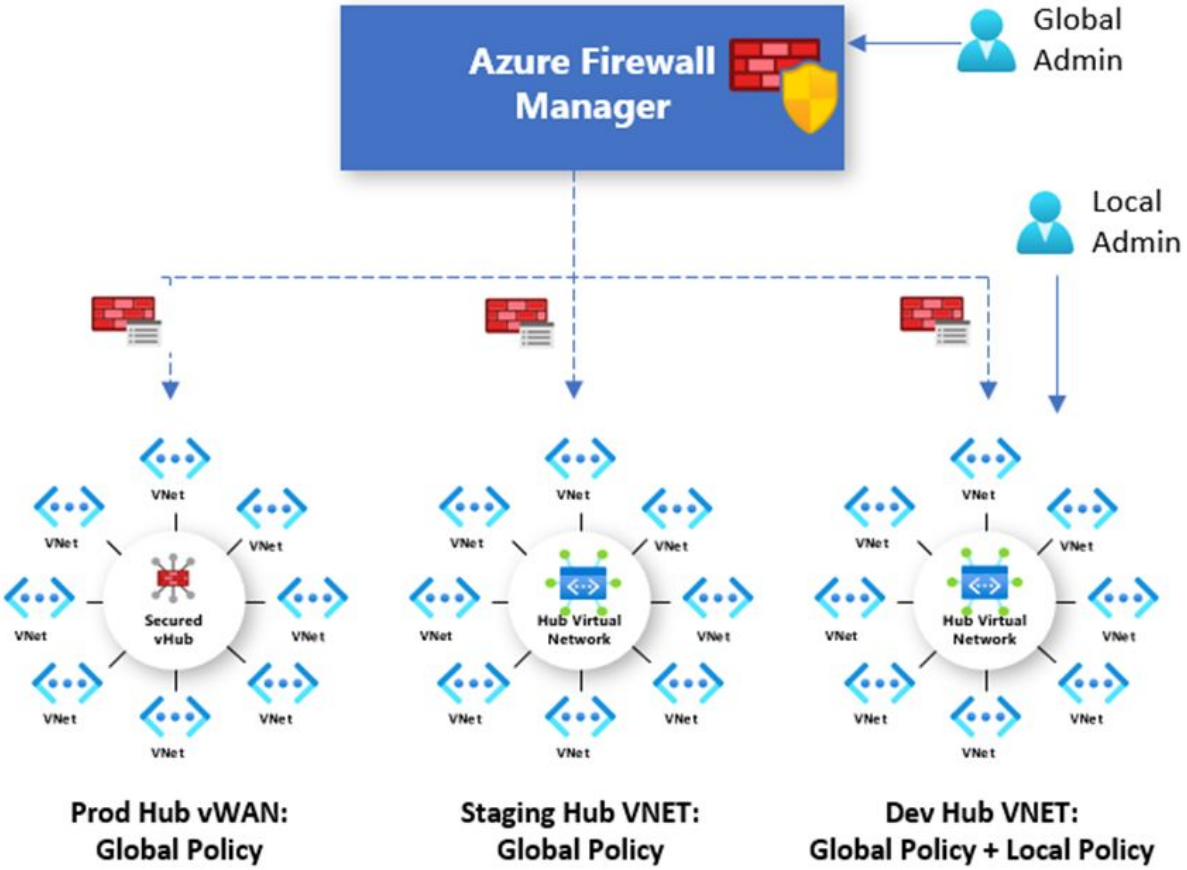
Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

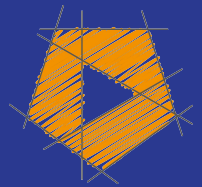






SC-900 Microsoft Security, Compliance, and Identity Fundamentals

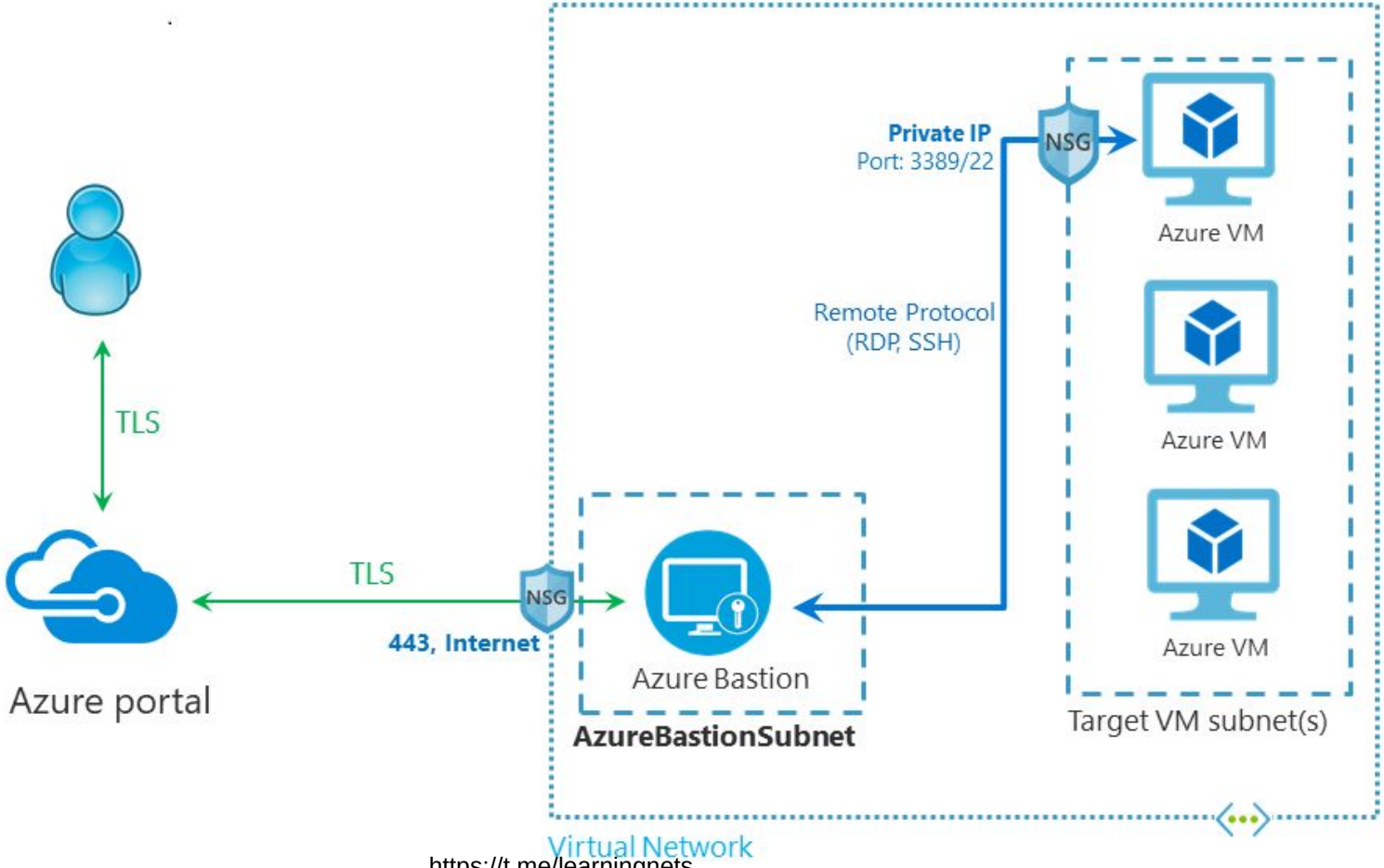
Scott Duffy, Instructor

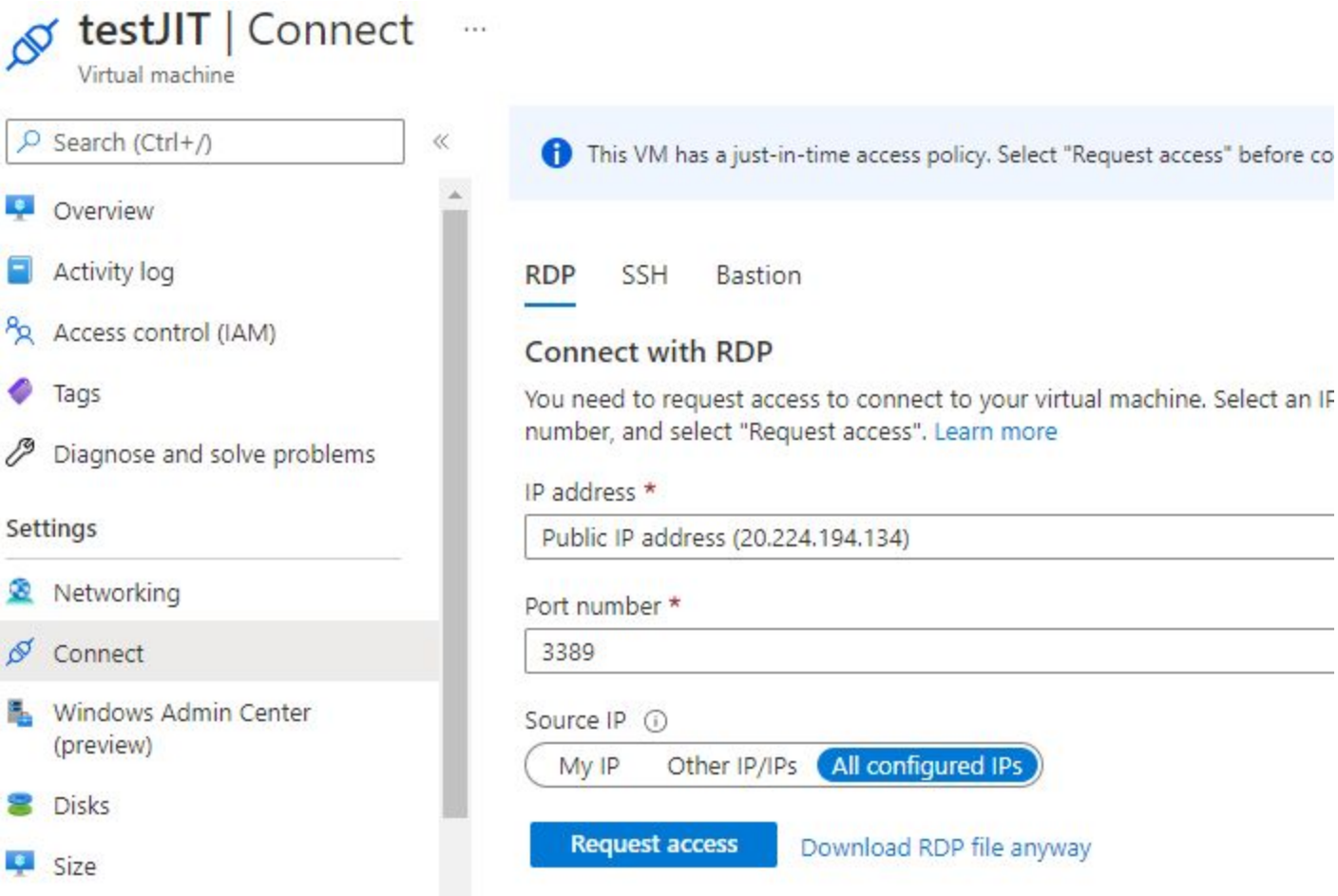


Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

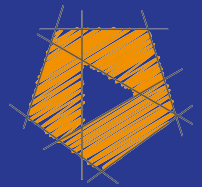
- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data





SC-900 Microsoft Security, Compliance, and Identity Fundamentals

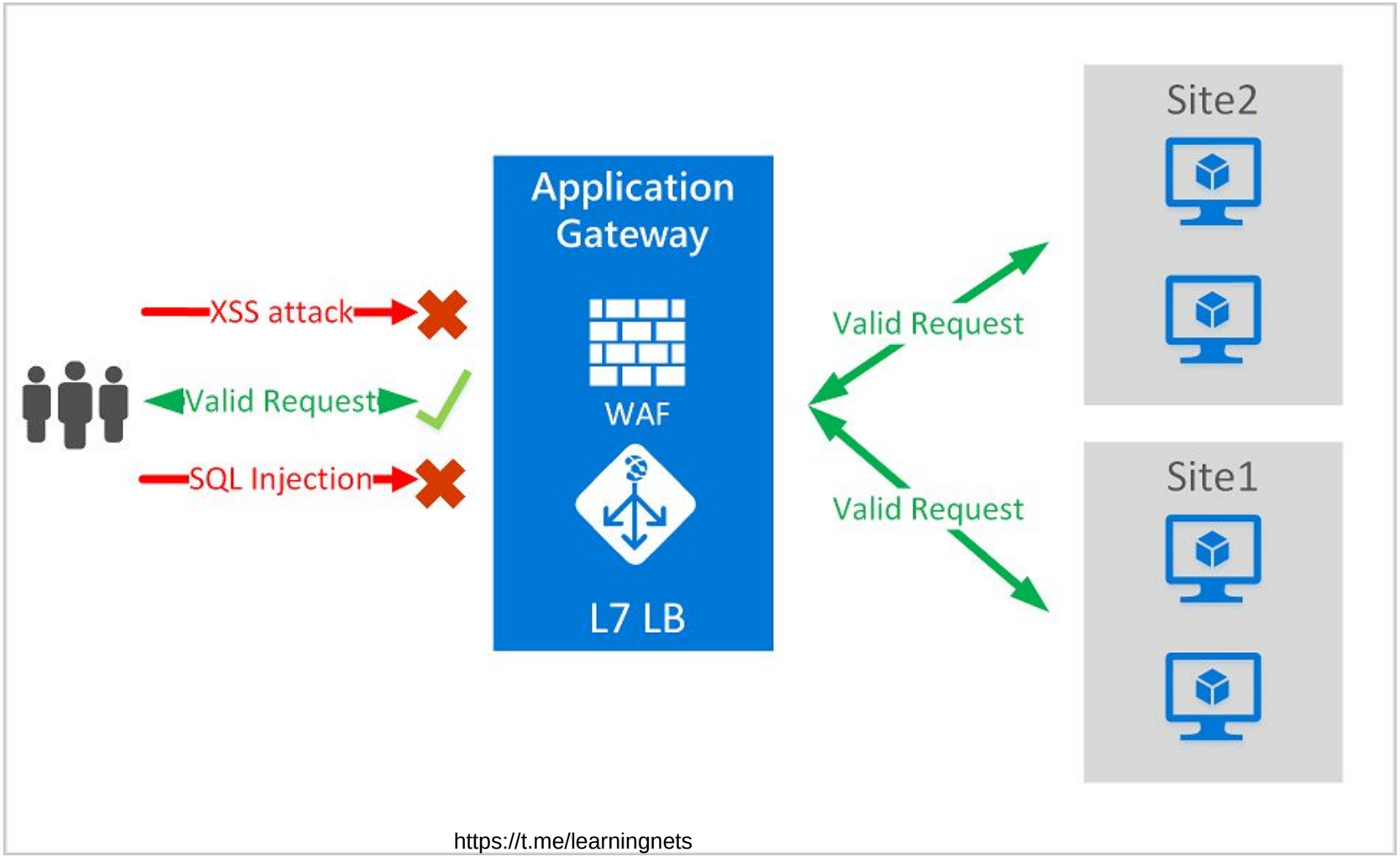
Scott Duffy, Instructor



Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data



WAF Features

- SQL-injection attacks
- Cross-site scripting attacks
- Other common attacks, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion
- HTTP protocol violations
- HTTP protocol anomalies, such as missing host user-agent and accept headers
- Bots, crawlers, and scanners
- Common application misconfigurations (for example, Apache and IIS)

OWASP Rule Sets

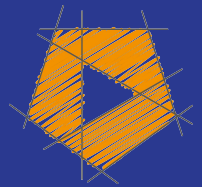
Core Rule Sets 3.1, 3.0, and 2.2.9

Custom Rules

Geomatch Rules

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft Security solutions (25—30%)

Describe basic security capabilities in Azure

- Describe Azure DDoS protection
- Describe Azure Firewall
- Describe Web Application Firewall
- Describe Network Segmentation with VNet
- Describe Azure Network Security groups
- Describe Azure Bastion and JIT Access
- Describe ways Azure encrypts data

Data Encryption

Data at rest

Data in transit

Key management

Data At Rest

Server-Side Service-Managed Key - All Azure Database, Storage, AI, etc encrypted

Server-Side Customer-Managed Key - Using Azure Key Vault

Client-Side Client-Managed Key - SQL Server, SQL Database

Double Encrypted Option - VM managed disks

Data In Transit

SSL / HTTPS / TLS

Data encrypted internally between Azure datacenters (MACsec)

Option to enable for all data leaving Azure going to customers

You can force “HTTPS only” when accessing storage accounts

Can force “HTTPS only” for shared access signatures (SAS)

Azure Key Vault

Designed to securely store secrets, certifications and keys

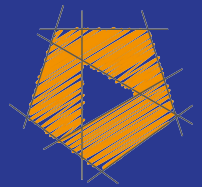
Requires authenticated and authorized access to get key

Removes keys from common storage, code, source control

Can expire keys, generate new keys, etc.

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe security management capabilities of Azure

- Describe Microsoft Defender for Cloud
- Describe Cloud Security Posture Management (CSPM)
- Describe how security policies and initiatives improve the cloud security posture
- Describe enhanced security features provided by cloud workload protection

Microsoft Defender for Cloud

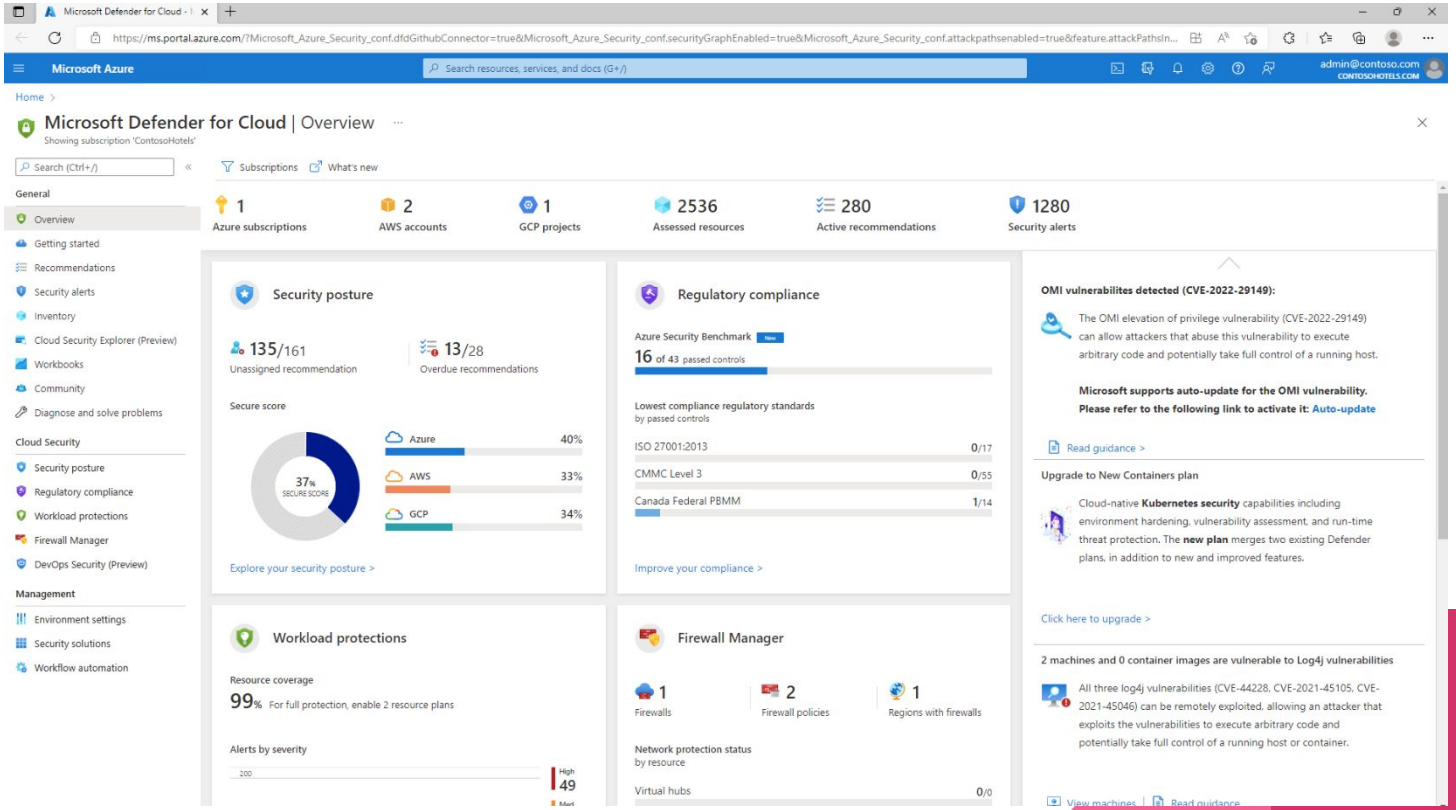
Defender for Cloud

1. Manage your cloud security posture
2. Prevent, detect, and respond quickly to modern threats
3. Unify DevOps security management

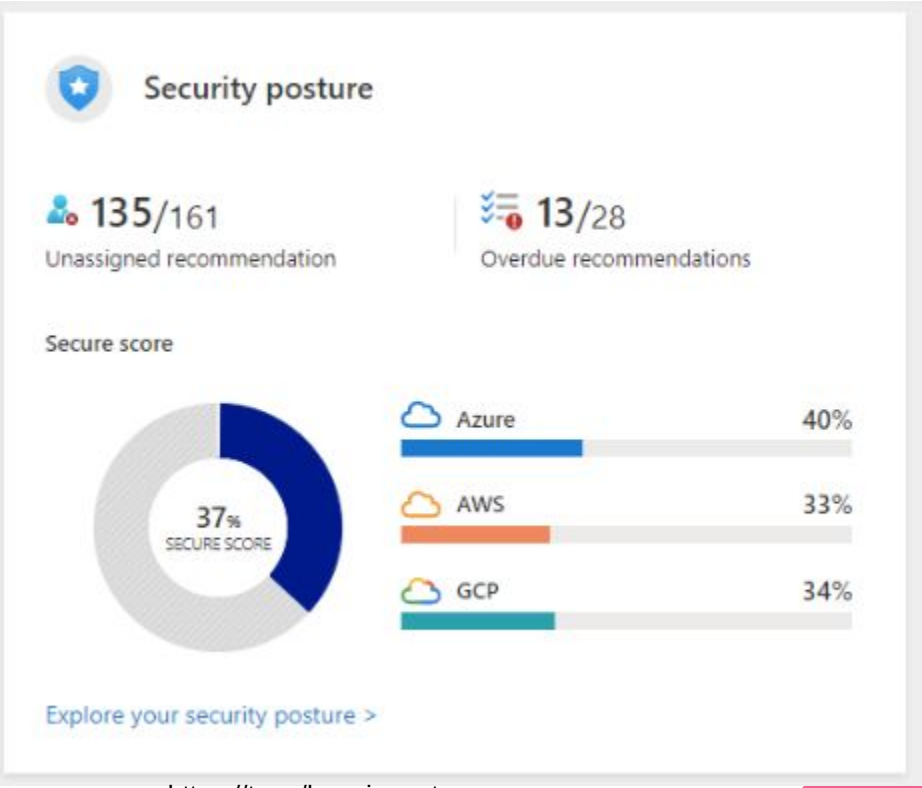
Manage Your Cloud Security Posture

- Identify the riskiest security issues
- Meet regulatory compliance requirements
- Assign recommendations

Security Dashboard

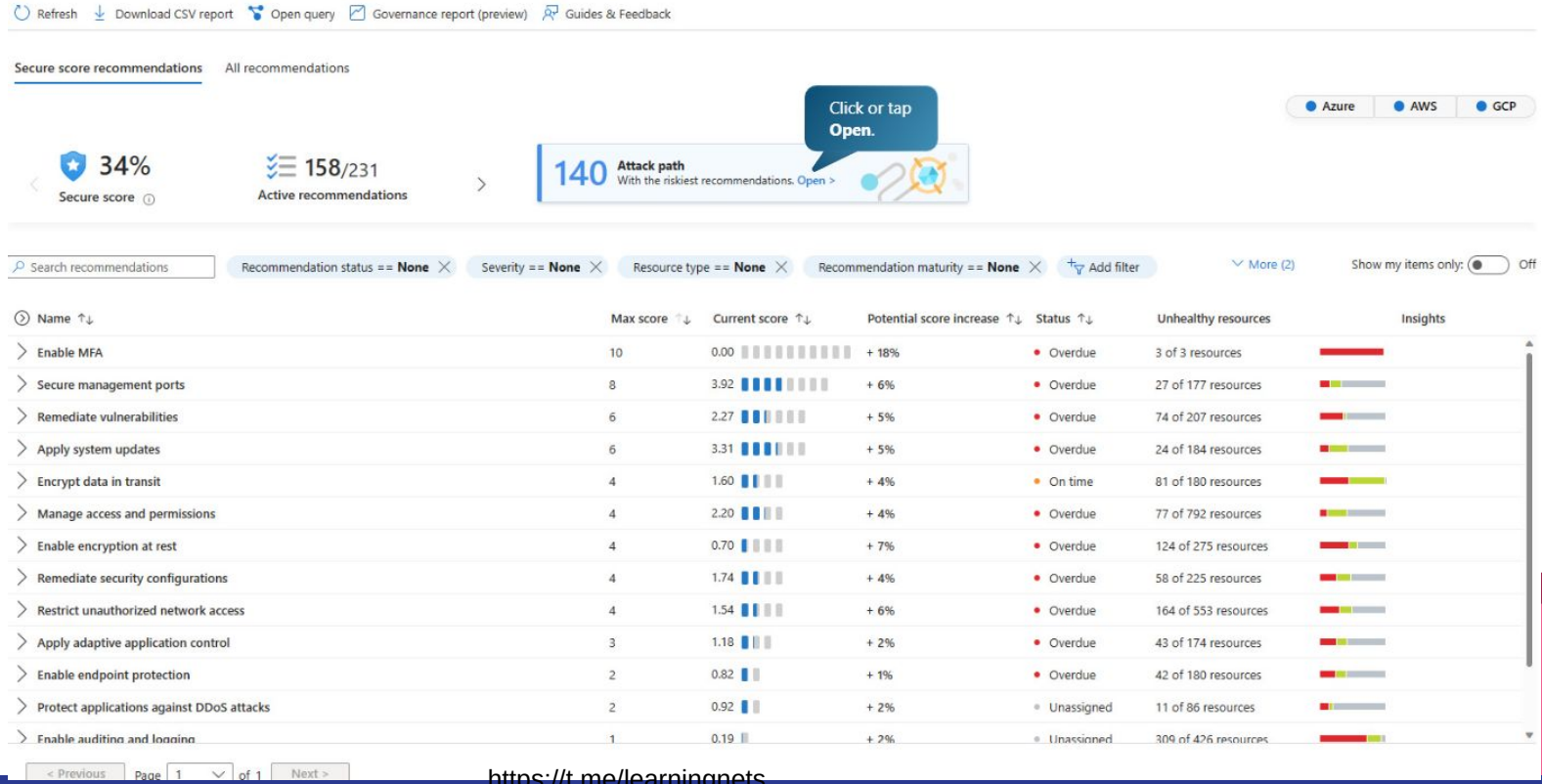


Security Posture

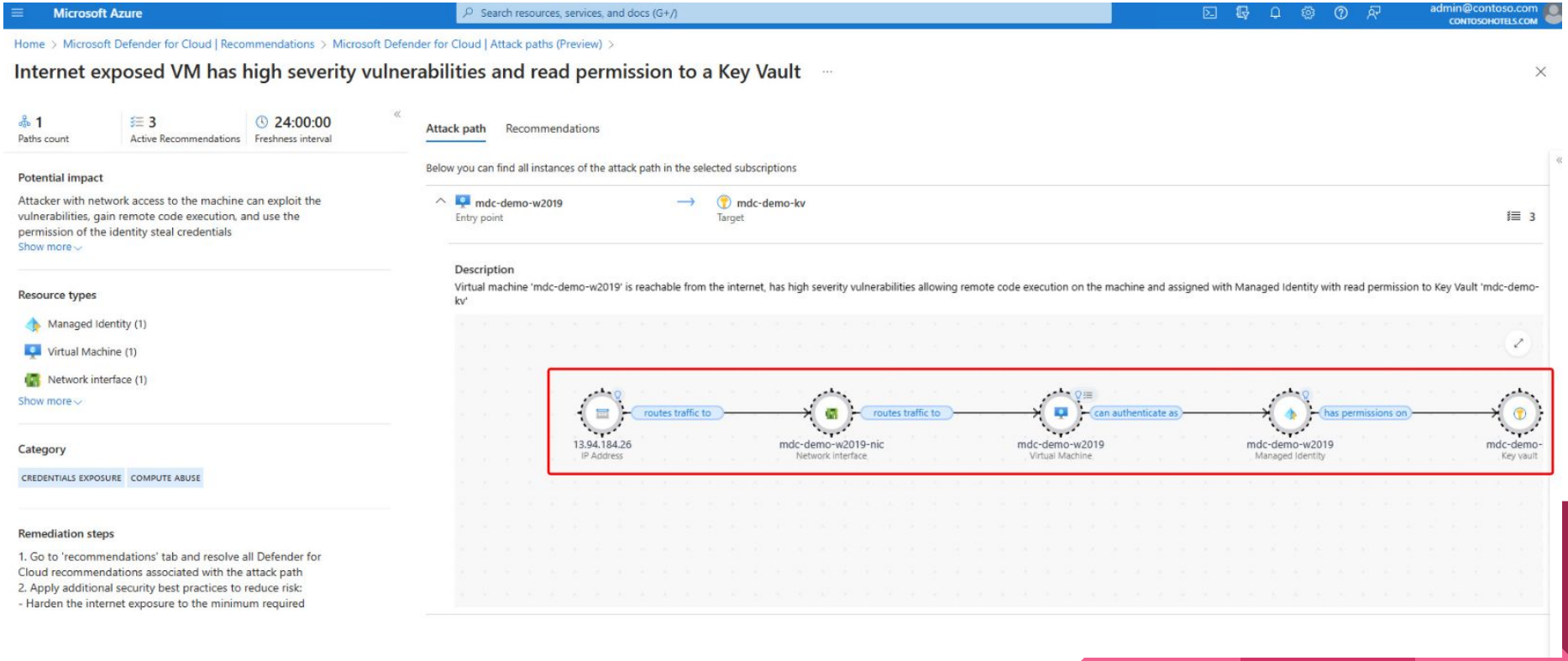


Recommendations

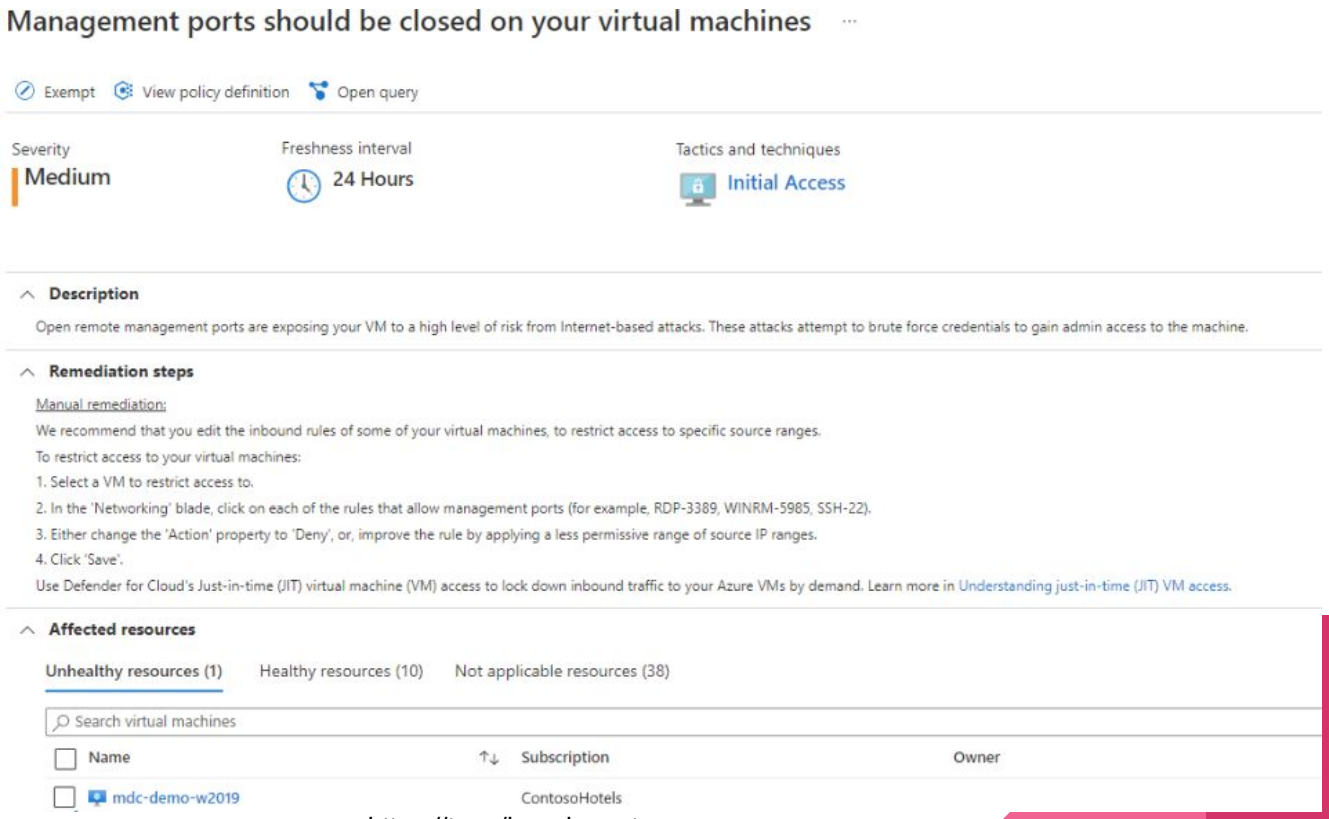
Recommendations



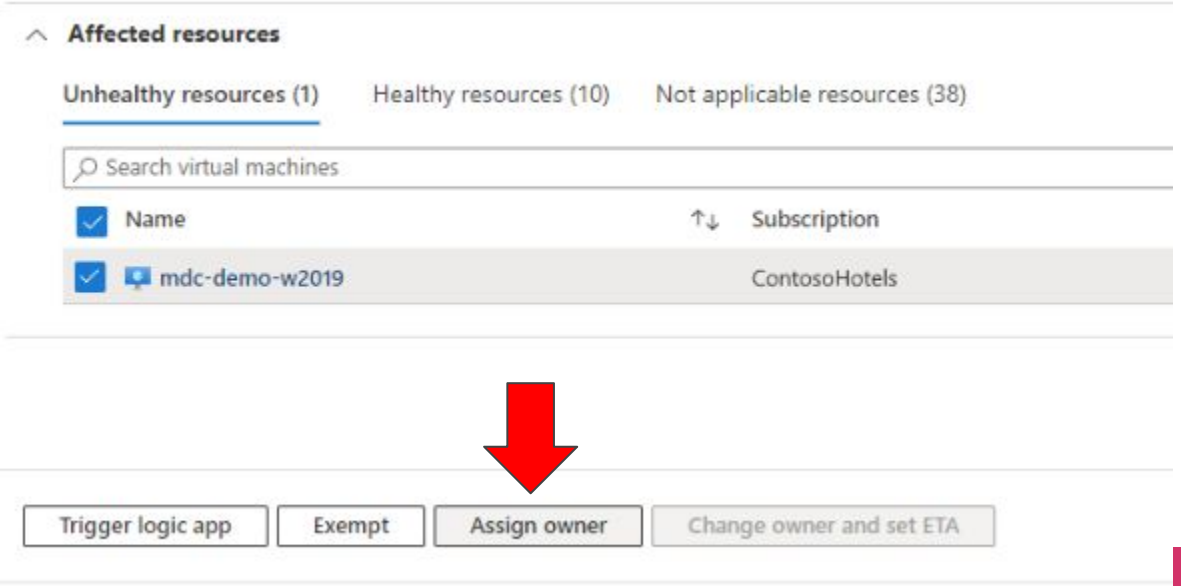
Complex Scenarios



Steps to Fix

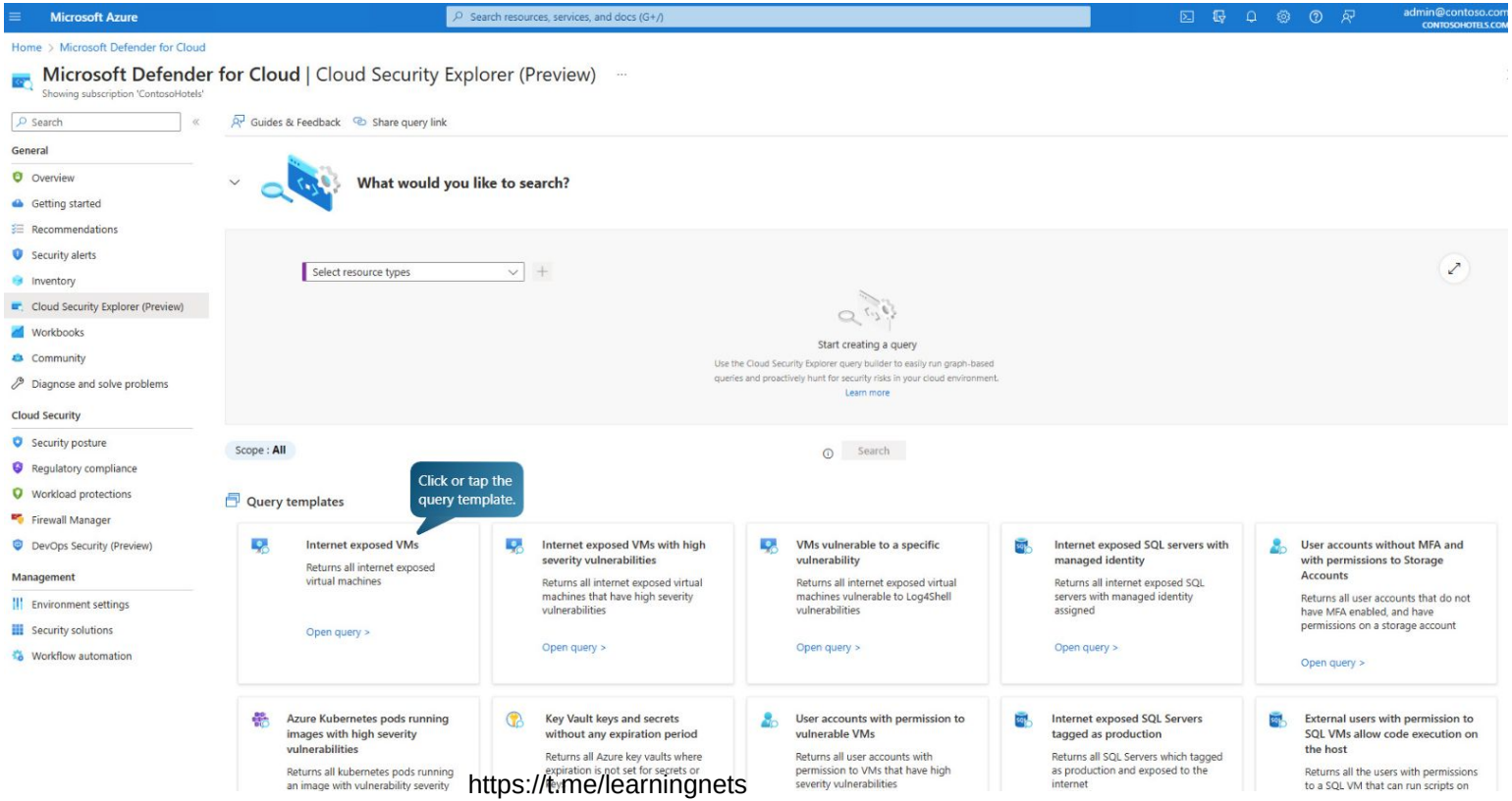


Assign an Owner

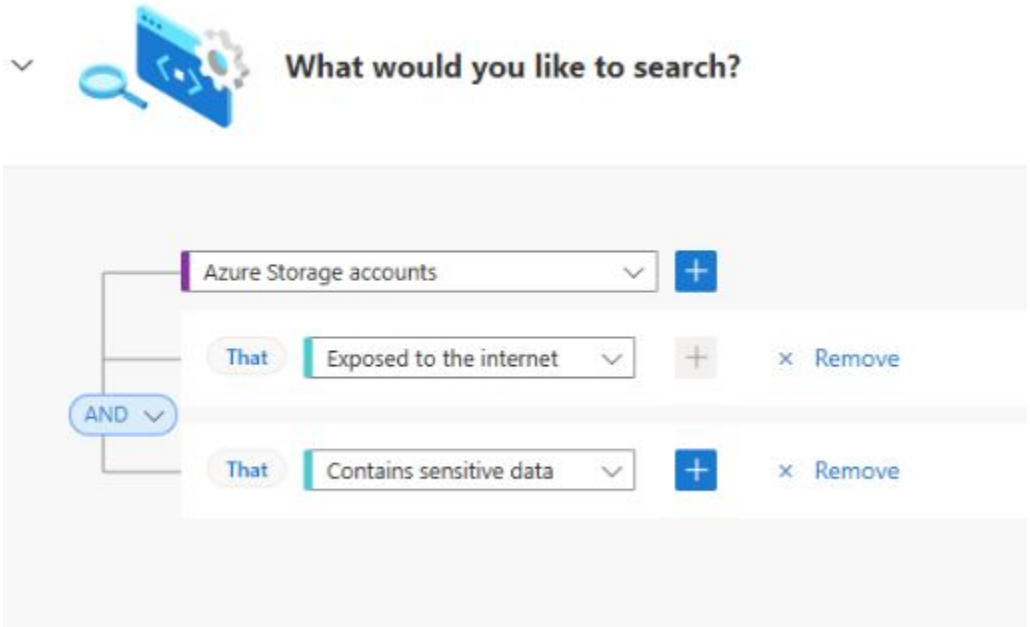


Risk Hunting

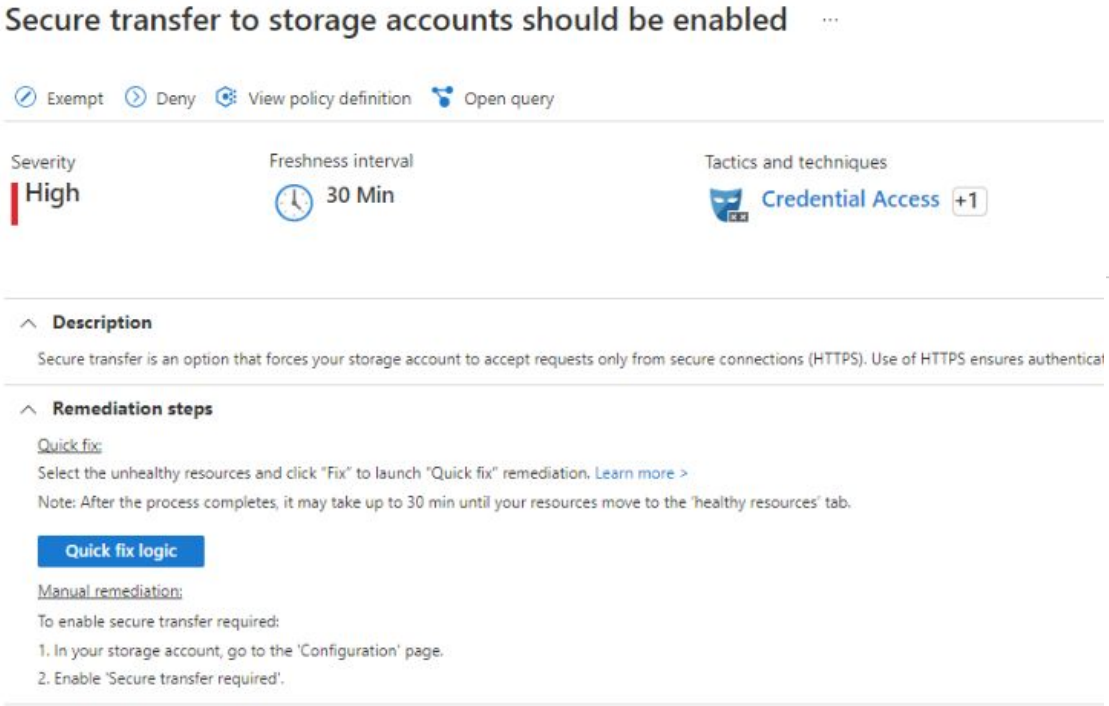
Cloud Security Explorer

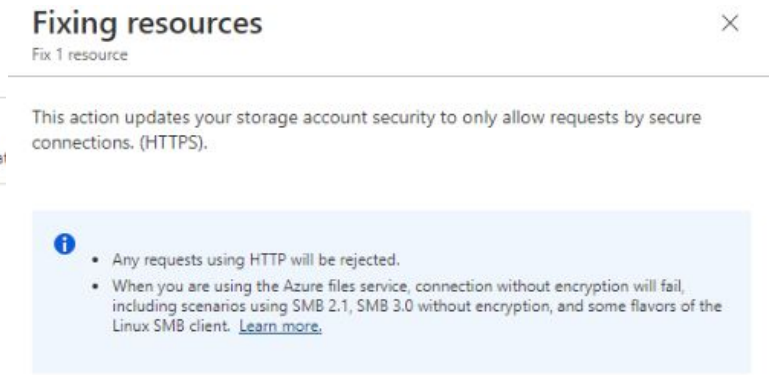


Query for Conditions



Fix Recommendations





See Hacking Attempts

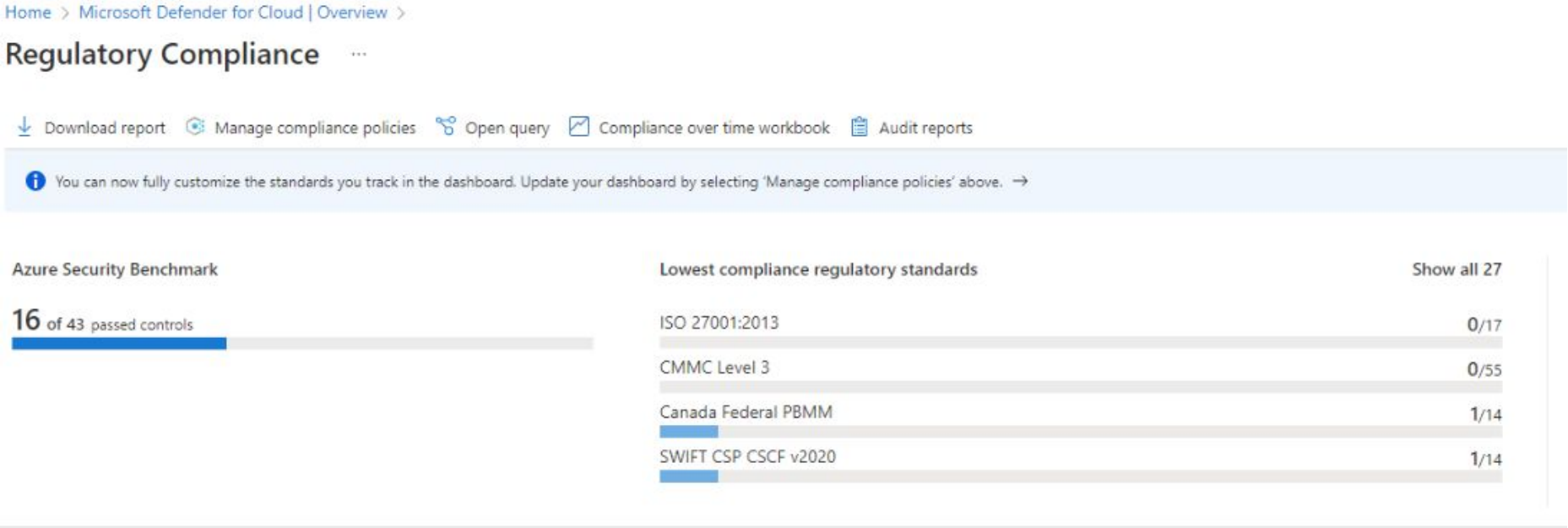
Recommendations Alerts

Search by ID, title, or affected resource | Subscription == **All** | Status == **Active** | Severity == **Low, Medium, High** | Add filter

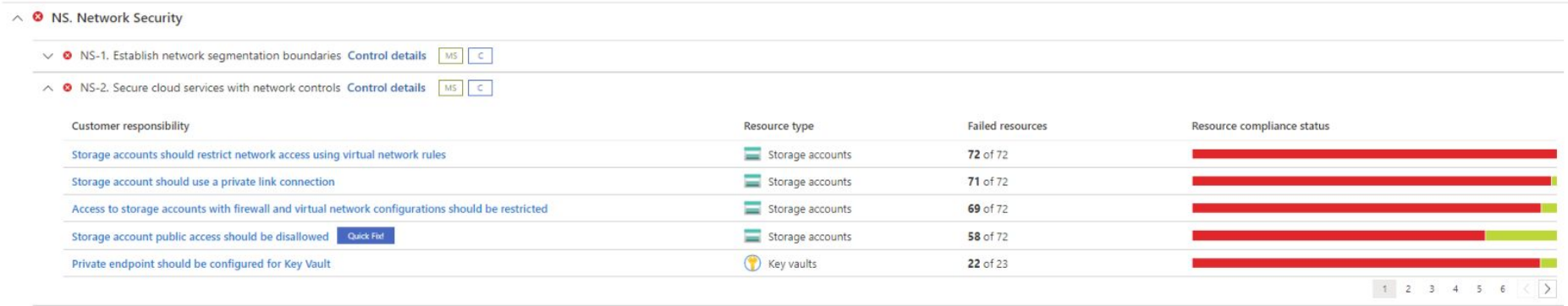
Severity	Alert title	Activity start time (UTC-7)	MITRE ATT&CK® tactics	Status
Medium	Suspected brute-force attack attempt	08/23/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	08/18/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	08/16/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	08/11/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	08/04/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	08/02/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	07/28/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	07/26/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	07/21/22, 09:00 PM	Pre-attack	Active
Medium	Suspected brute-force attack attempt	07/19/22, 09:00 PM	Pre-attack	Active

Compliance Posture

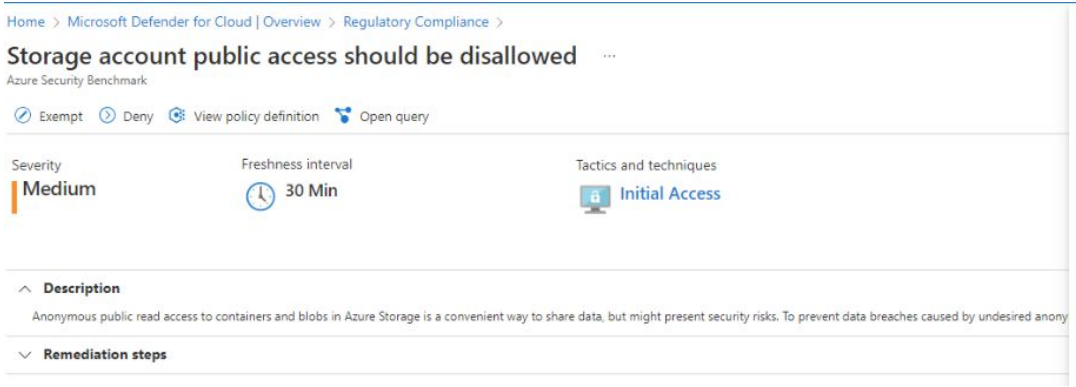
Regulatory Compliance

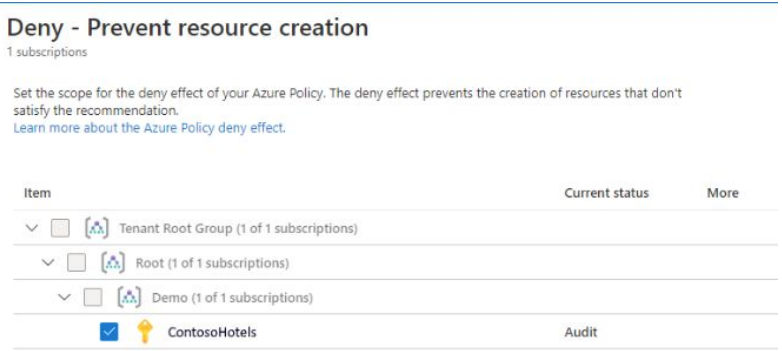


Where You Are Out of Compliance

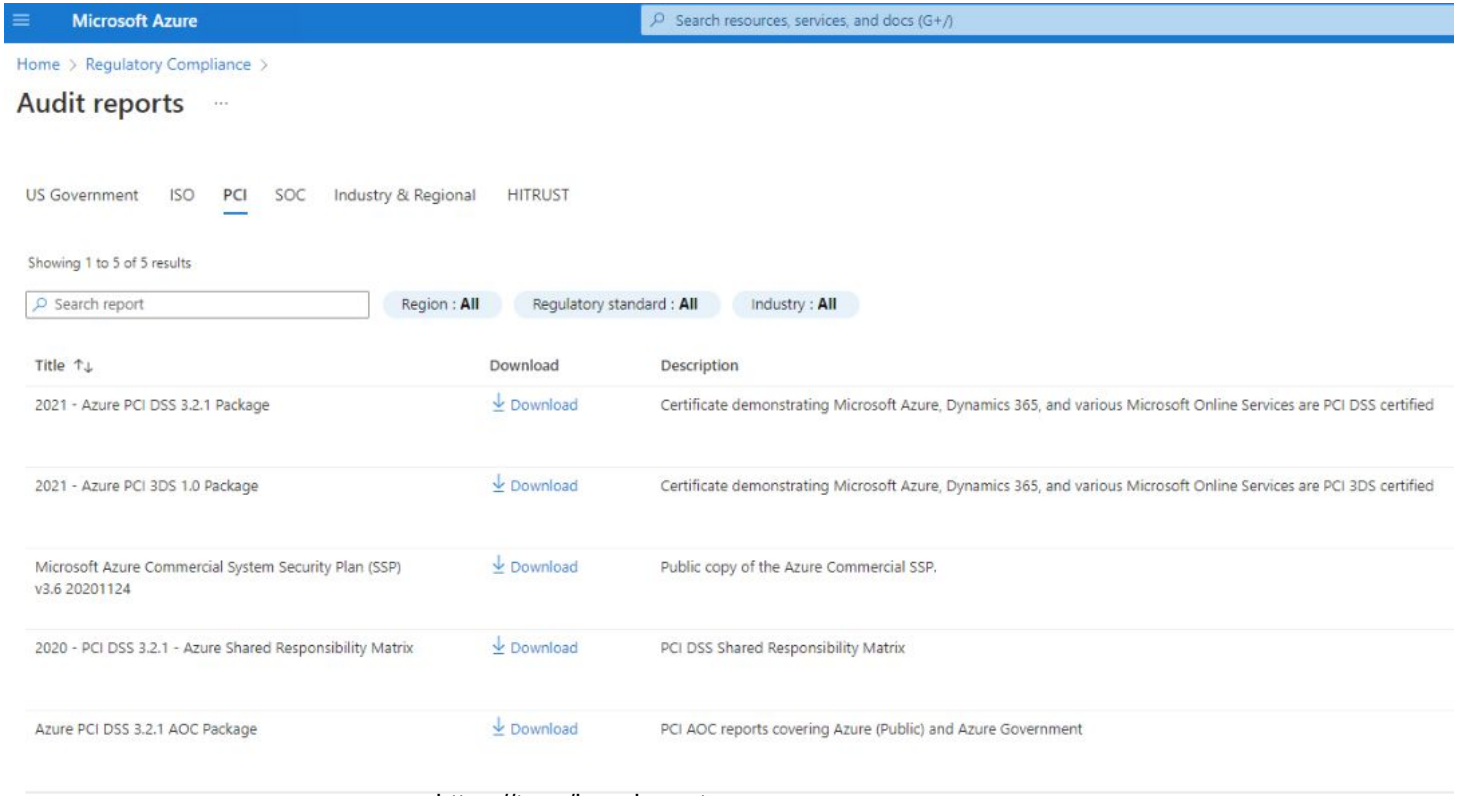


Implement Policies to Prevent Violations



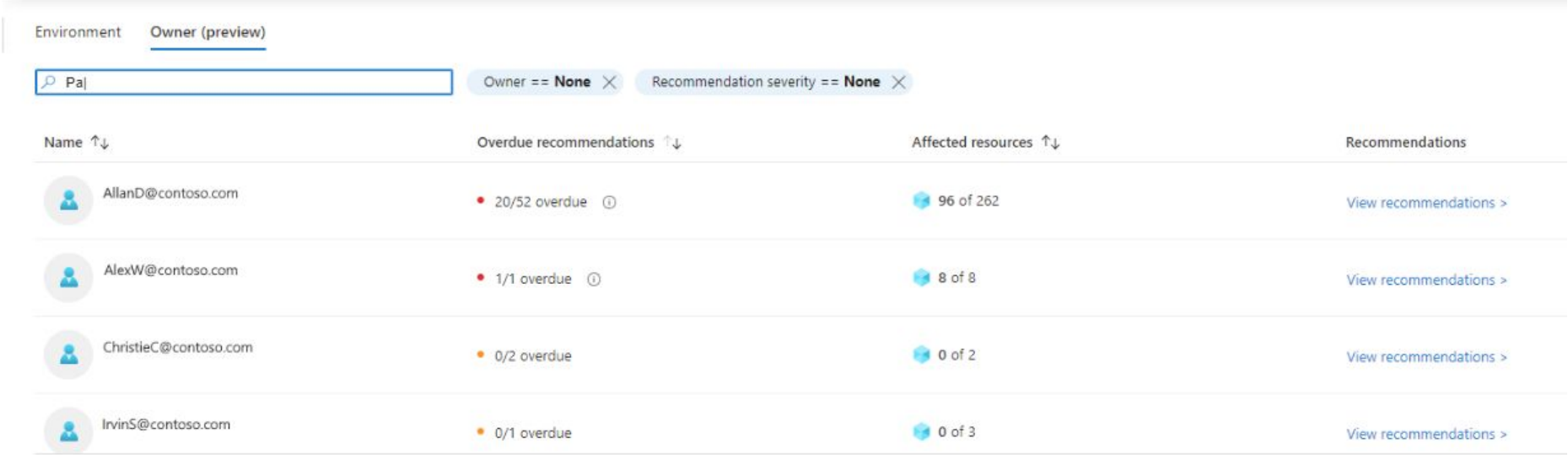


Audit Reports

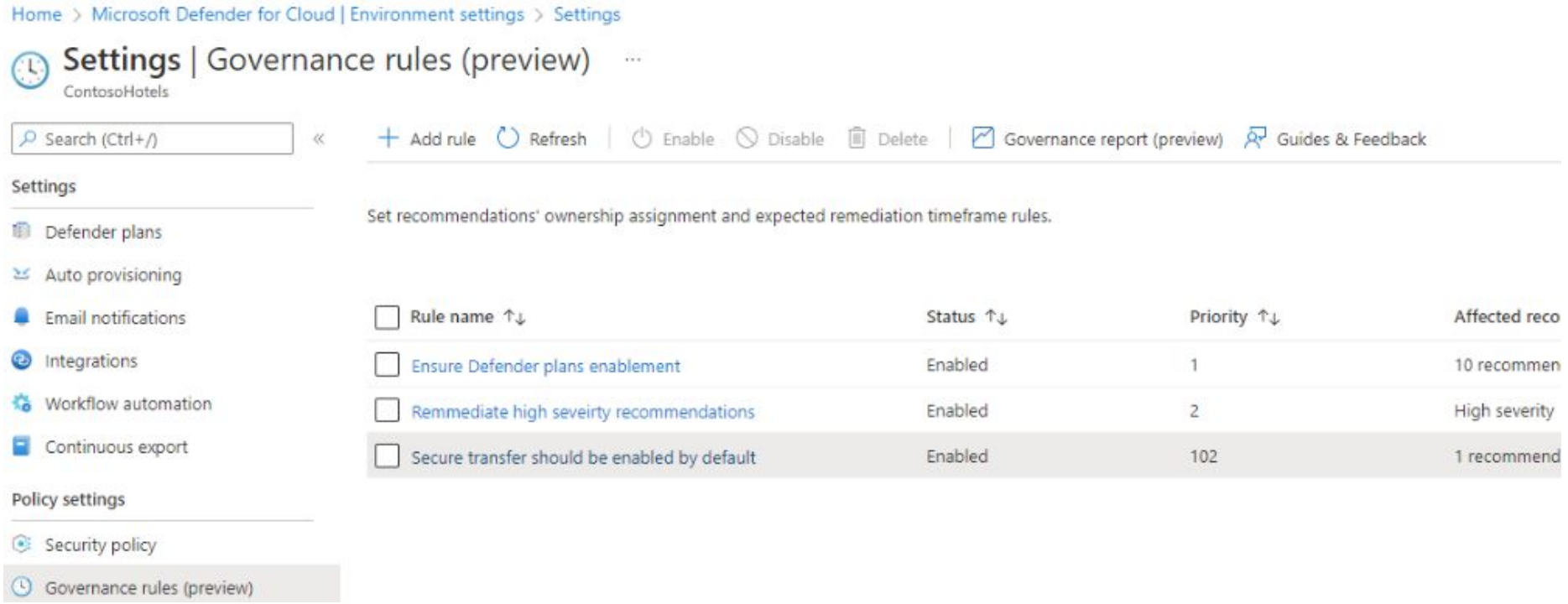


Security Governance

Overdue Recommendations



Governance Rules



Email Nag

Action required: Implement Microsoft Defender for Cloud recommendations

MD

Microsoft Defender for Cloud <DefenderCloudnoreply@microsoft.com>
To Christie Cline

Microsoft

Action required

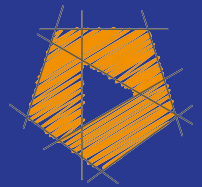
Implement active recommendations assigned to you in Microsoft Defender for Cloud

You're assigned as the owner of several active Microsoft Defender for Cloud security recommendations in subscription ContosoHotels (d1d8779d-38d7-4f06-91db-9cbc8de0176f).

Recommendation	Severity	Number of affected resources
Machines should have a vulnerability assessment solution	Medium	110 (0 overdue)
Windows Defender Exploit Guard should be enabled on machines	Medium	97 (0 overdue)

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe security management capabilities of Azure

- Describe Microsoft Defender for Cloud
- Describe Cloud Security Posture Management (CSPM)
- Describe how security policies and initiatives improve the cloud security posture
- Describe enhanced security features provided by cloud workload protection

Cloud security posture management (CSPM)

CSPM identifies and remediates risk

CSPM

- automating visibility
- uninterrupted monitoring
- threat detection
- remediation workflows

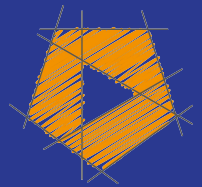
Highest percentage of errors still comes from cloud misconfigurations and human error

Defender for Cloud helps identify vulnerabilities and manage mitigations

CSPM continuously analyzes the security state of your entire cloud platform, not just individual apps or resources

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe capabilities of Microsoft Sentinel

- Define the concepts of security information and event management (SIEM) and security orchestration automated response (SOAR)
- Describe threat detection and mitigation capabilities in Microsoft Sentinel

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native, **security information and event management (SIEM)** and **security orchestration automated response (SOAR)** solution.

Intelligent security analytics and threat intelligence across an enterprise.

- alert detection
- threat visibility
- proactive hunting
- threat response

Key Capabilities (SIEM):

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously uncovered threats and minimize false positives.

Investigate threats with artificial intelligence (AI).

Respond to incidents rapidly.

Key Capabilities (SOAR):

Takes alerts from many sources including SIEM

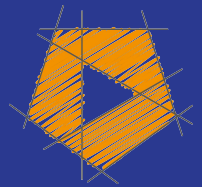
Triggers action-driven automated workflows and processes

Run security tasks that mitigate the issue

Security insights and security automation

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Security Products in Azure / M365

Microsoft Defender for Cloud - CSPM (security posture, configuration and settings)

Microsoft Sentinel - SIEM/SOAR (log ingestion)

Microsoft Defender XDR - XDR (unified pre- and post-breach enterprise defense suite)

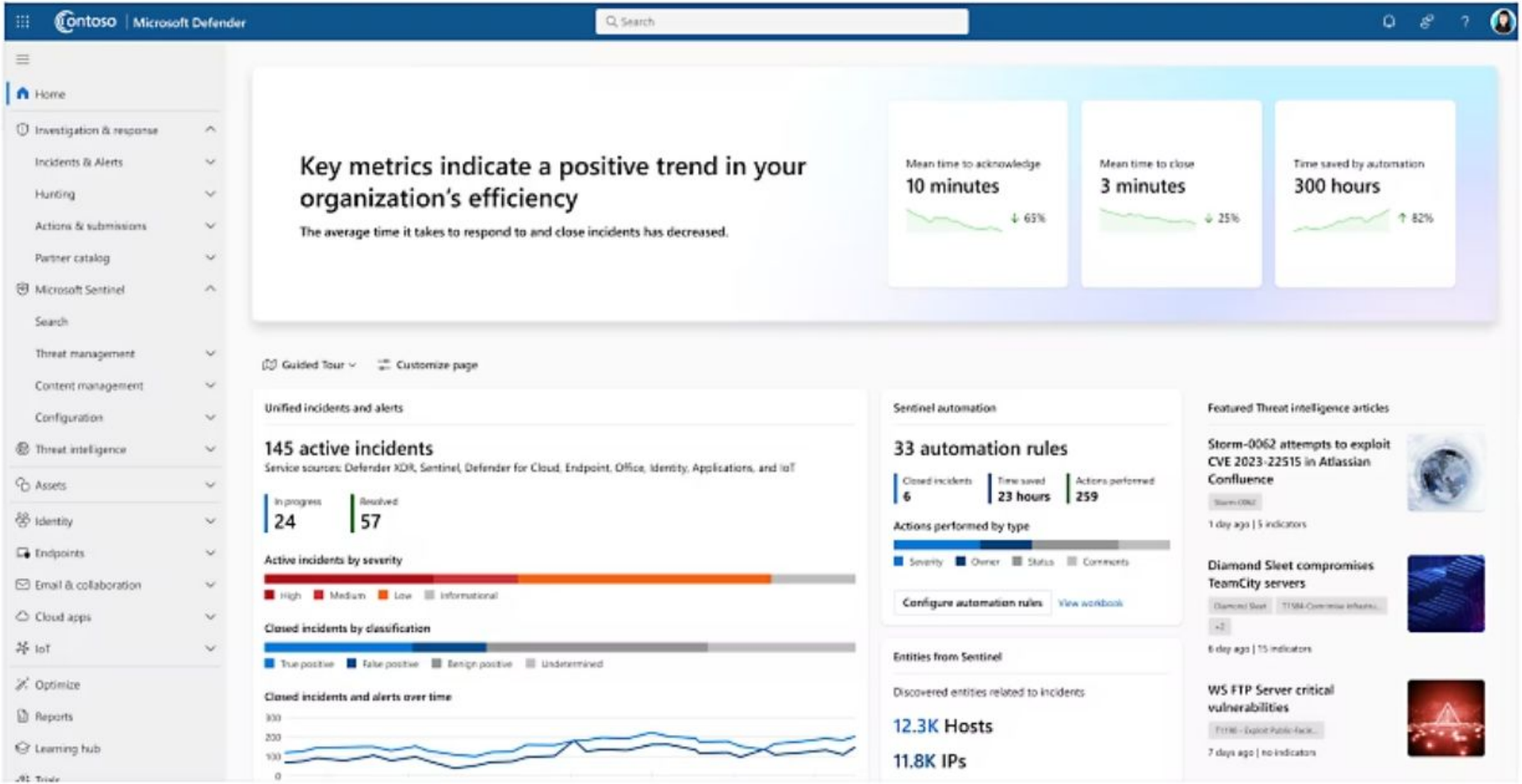
XDR - Extended Detection and Response

United suite of enterprise defense services

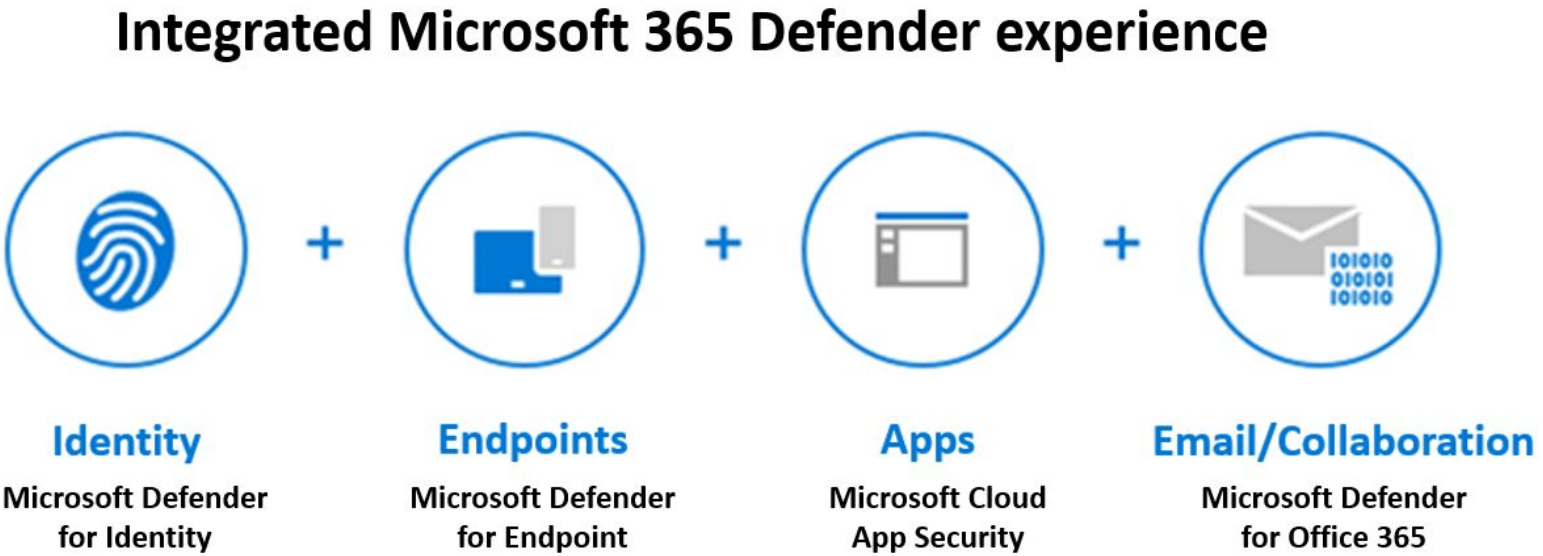
Detection
Prevention
Investigation
Response

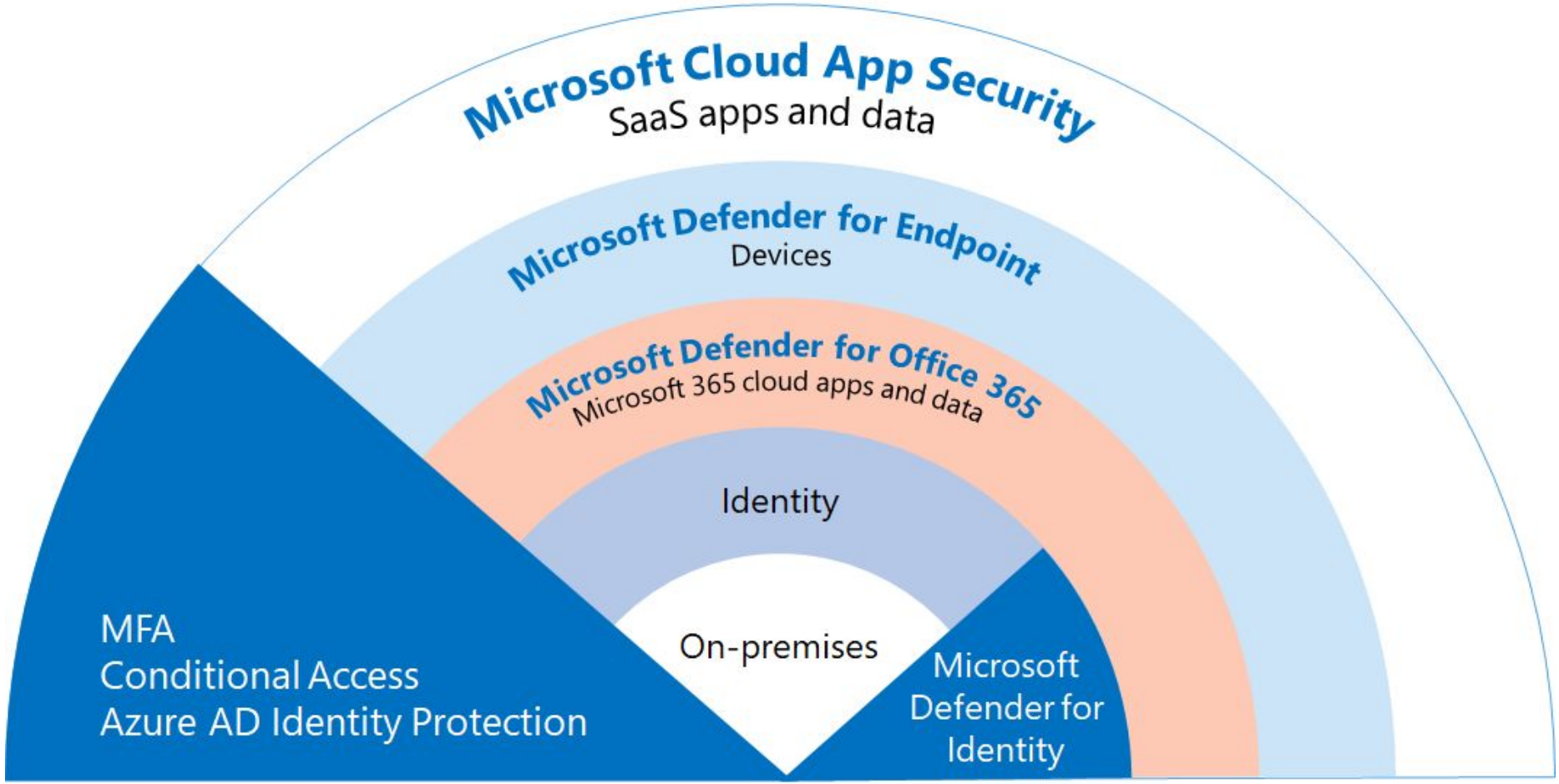
Not just network protection...

… apps and services that run on the network, the identities, devices, M365, etc



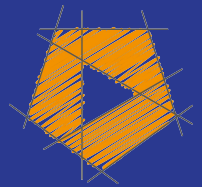
Microsoft Defender XDR services





SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Identity

Formerly Advanced Threat Protection (ATP)

Entra ID Signals

Microsoft Defender for Identity

Monitor user behavior and activities

Protect users identities and reduce attack surface

Identify suspicious activities and attacks across the kill-chain

Alerts

<u>License plans:</u>

- EMS E5 or stand alone

Understanding what is normal behavior for each user?

Identify behavior anomalies

Security reports and user profile analytics

Kill-chain: attacks start with low-hanging fruit

Then try to move over (lateral) or move up

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Identity Risks

Anonymous IP Address

Atypical travel

Malware linked IP address

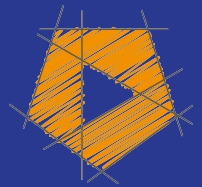
Leaked credentials

Password spray

Inbox forwarding

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Office 365

Formerly Office 365 Advanced Threat Protection (ATP)

Microsoft Defender for O365

E-mails

Links (URLs)

Collaboration tools (Teams, Sharepoint Online, OneDrive for Business, etc)

Licenses:

- O365 Plan 1, O365 Plan 2
- M365 E5, O365 E5/A5, and M365 Business Premium

Plan 1

- Safe Attachments
- Safe Links
- Protection for SharePoint, OneDrive, and Microsoft Teams
- Anti-phishing protection
- Real-time detections

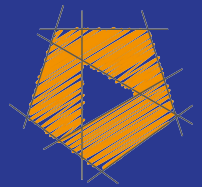
Plan 2

All features of Plan 1 plus…

- Threat Trackers
- Threat Explorer
- Automated investigation and response (AIR)
- Attack Simulator

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Endpoint

Formerly Microsoft Defender Advanced Threat Protection (ATP)

Microsoft Defender for Endpoint

Endpoints are “devices”

Think of your laptop, phone, tablet - regardless of operating system

Microsoft Defender for Endpoint

Expand table

					
Core Defender Vulnerability Management	Attack surface reduction	Next-generation protection	Endpoint detection and response	Automated investigation and remediation	Microsoft Threat Experts
Centralized configuration and administration, APIs					
Microsoft Defender XDR					

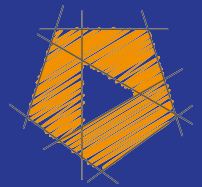
Microsoft Defender for Endpoint

- Threat and vulnerability management (core)
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Microsoft Threat Experts
- Management and APIs

Microsoft Secure Score for Devices

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

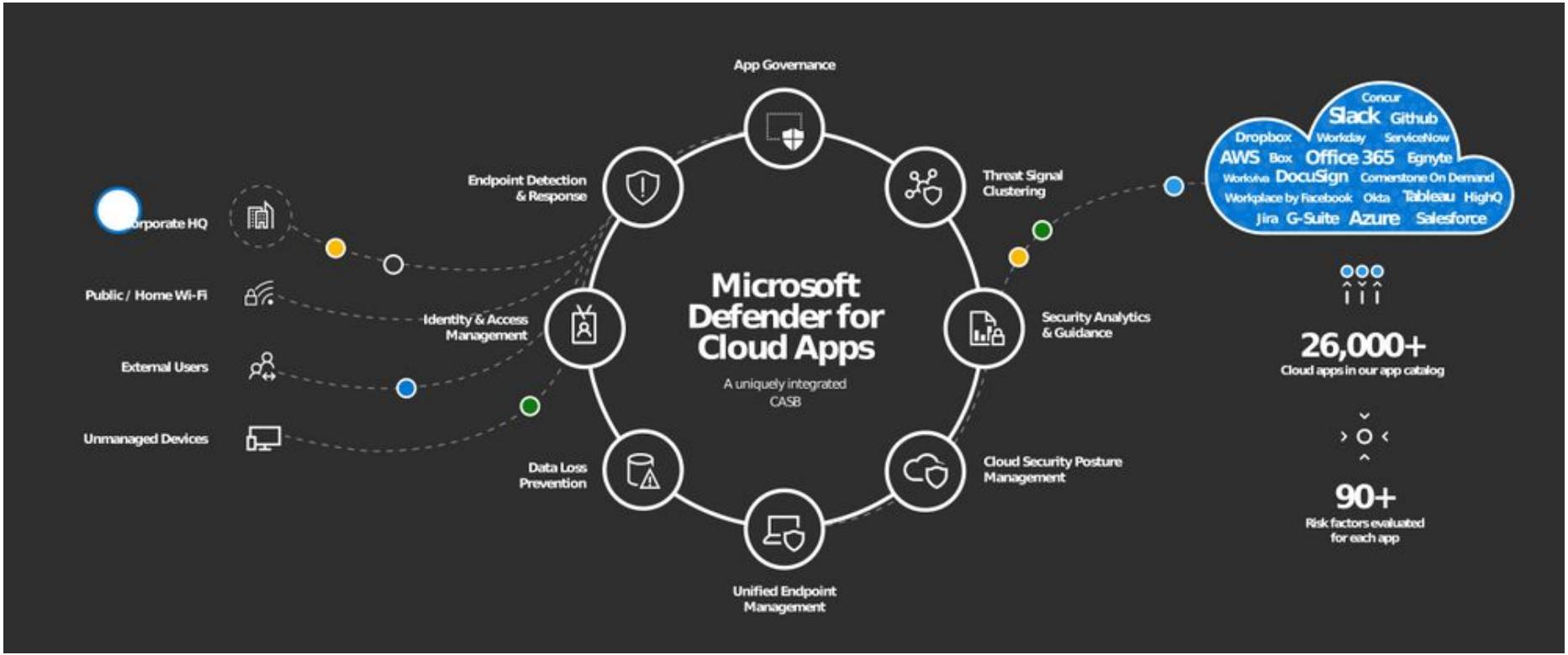
Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender for Cloud Apps



Microsoft Defender for Cloud Apps (CASB)

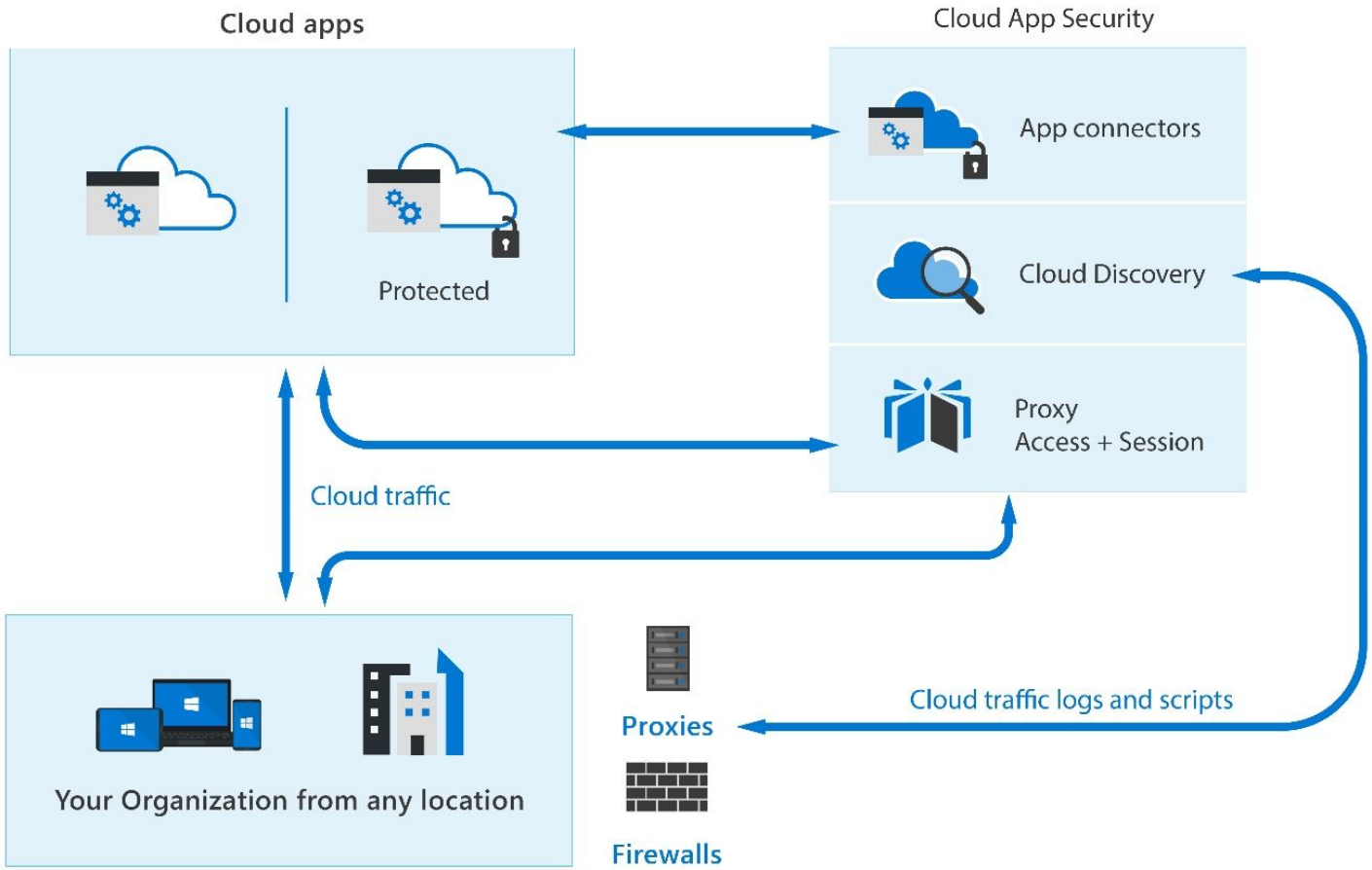
CAS Security Framework

O365 CAS

Enhanced Cloud App Discovery in AAD

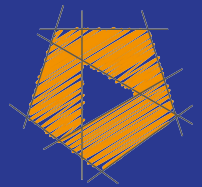
CAS architecture

Discover Shadow IT



SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

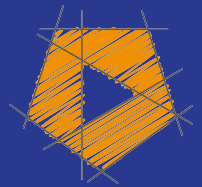
- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender Vulnerability Management

Add-on for Defender for Endpoint (Plan 2)

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



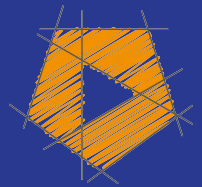
Describe threat protection with Microsoft Defender XDR

- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender Threat Intelligence

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe threat protection with Microsoft Defender XDR

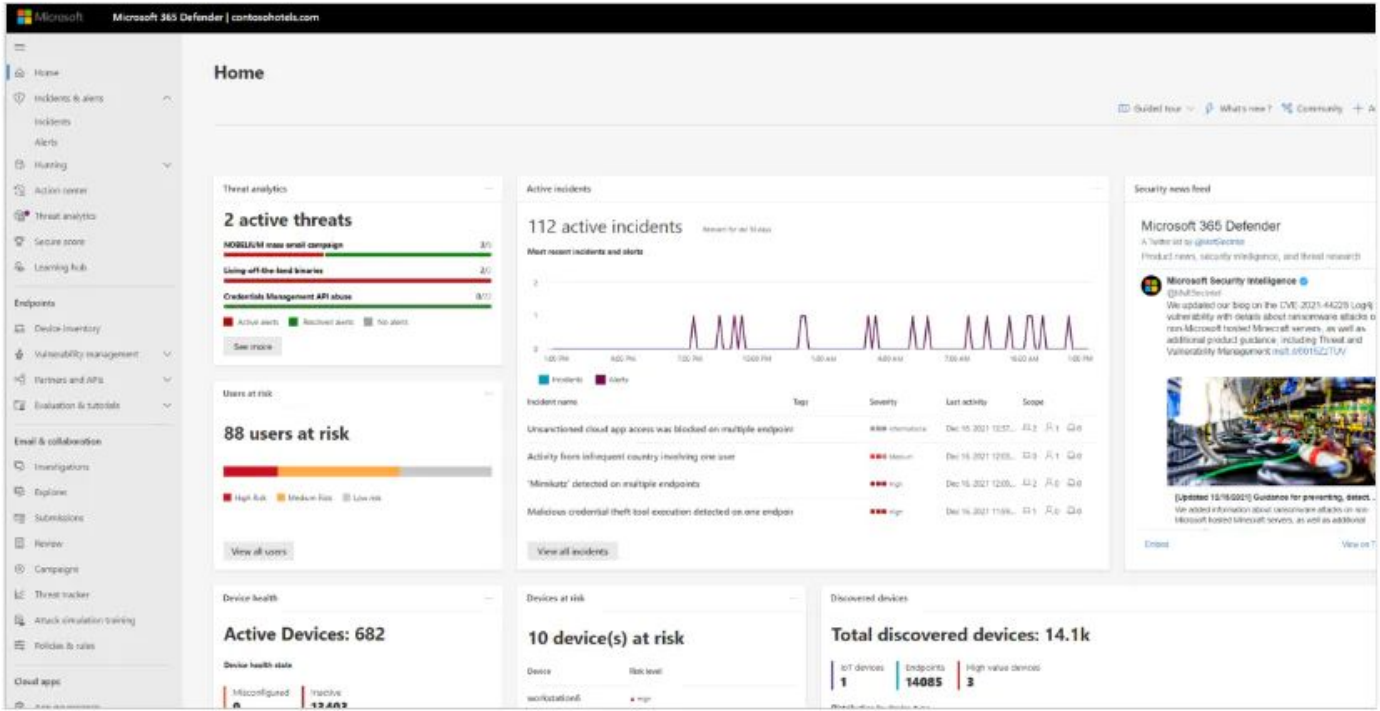
- Describe Microsoft Defender XDR services
- Describe Microsoft Defender for Office 365
- Describe Microsoft Defender for Endpoint
- Describe Microsoft Defender for Cloud Apps
- Describe Microsoft Defender for Identity
- Describe Microsoft Defender Vulnerability Management
- Describe Microsoft Defender Threat Intelligence (Defender TI)
- Describe the Microsoft Defender portal

Microsoft Defender Portal

https://security.microsoft.com

Manage security across identities, data, devices, apps, and infrastructure

Microsoft Defender Portal



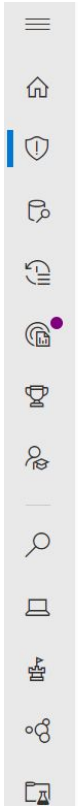
- Protection
- Detection
- Investigation
- Response

- Email
- Collaboration
- Identity
- Device
- Cloud App

- Defender for Office 365
- Defender for Endpoint
- Defender for Identity
- Defender for Cloud Apps

A Set of Unified Experiences For…

- Incidents & alerts
- Hunting
- Actions & submissions
- Threat analytics
- Secure score
- Learning hub
- Trials



Incidents

Create a notification rule

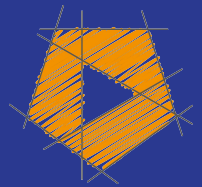
Most recent incidents and alerts

1-7 | 6 months | Choose columns | 30 items per page | Filters

Incident name	Tags	Severity	Investigation state
Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	asdf tag test02	High	2 investigation states
Multi-stage incident involving Initial access & Exfiltration on multiple endp...	asdf tag test02 IT Team +3	High	2 investigation states
Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	ar test01 asdf tag test02	High	4 investigation states
Multi-stage incident on one endpoint reported by multiple sources	asdf tag test02	Medium	2 investigation states
Multi-stage incident involving Persistence & Exfiltration on one endpoint r...	asdf tag test02	Medium	2 investigation states
Multi-stage incident involving Initial access & Discovery on multiple endpo...	test01 test02 test03 +7	High	4 investigation states

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft compliance solutions (20–25%)

Describe Microsoft Service Trust Portal and privacy principles

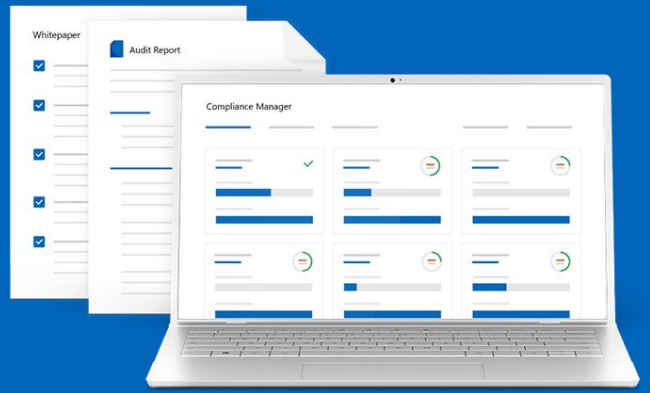
- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Priva

Service Trust Portal

https://servicetrust.microsoft.com/

https://aka.ms/STP

Built upon a foundation of trust, security and compliance

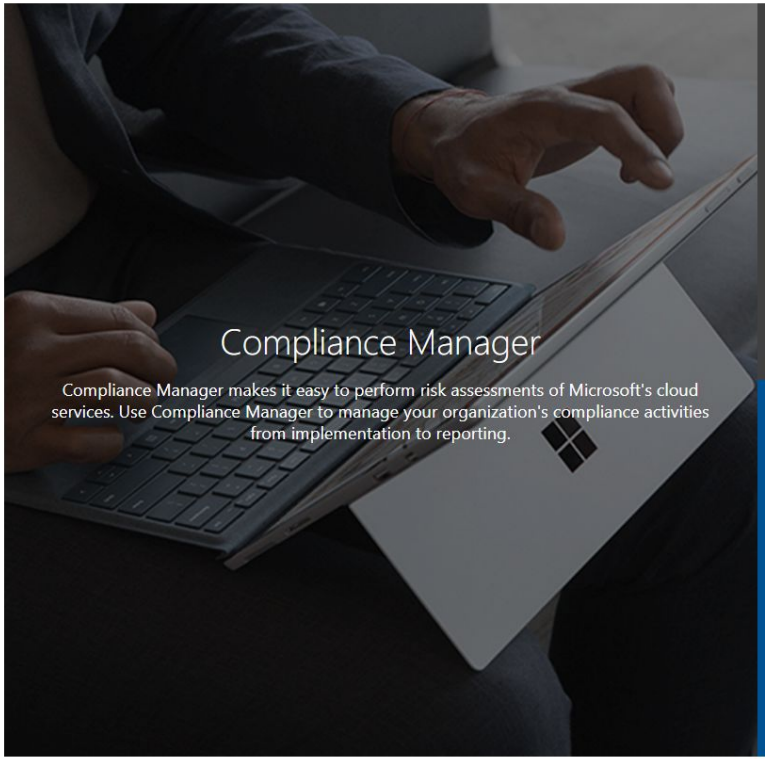


Audit Reports

Review the available independent audit reports for Microsoft's Cloud services, which provide information about compliance with data protection standards and regulatory requirements, such as International Organization for Standardization (ISO), Service Organization Controls (SOC), National Institute of Standards and Technology (NIST), Federal Risk and Authorization Management Program (FedRAMP), and the General Data Protection Regulation (GDPR)

SOC | FedRAMP | ISO 27001 | PCI/DSS

Documents & Resources



Compliance Manager

Compliance Manager makes it easy to perform risk assessments of Microsoft's cloud services. Use Compliance Manager to manage your organization's compliance activities from implementation to reporting.

Pen Tests & Security Assessments

View reports from independent third-party penetration tests and security assessments of Microsoft's cloud services

Azure Blueprints

Define a repeatable set of Azure resources that implement and adhere to your organization's standards, patterns, and requirements and rapidly build new environments with a set of built-in components to speed up development and delivery

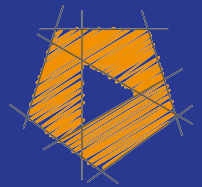
White Papers, FAQs, & Compliance Guides

Review the wealth of available security implementation and design information with the goal of making it easier for you to meet regulatory compliance objectives by understanding how Microsoft Cloud services keep your data secure

More Documents & Resources >

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft compliance solutions (20–25%)

Describe Microsoft Service Trust Portal and privacy principles

- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Priva

Privacy Principles

Microsoft’s Six Privacy Principles

- Control
- Transparency
- Security
- Strong legal protections
- No content-based targeting
- Benefits to you

You’re in control of your privacy with easy tools and clear choices.

Transparent about the data they collect

Strong security and the use of encryption

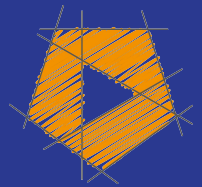
Respecting local privacy laws and fighting for privacy

They won’t use the content of documents and emails to target ads

They only collect data to make your experience better

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the capabilities of Microsoft compliance solutions (20–25%)

Describe Microsoft Service Trust Portal and privacy principles

- Describe the Service Trust Portal offerings
- Describe the privacy principles of Microsoft
- Describe Microsoft Priva

Microsoft Priva

Automate the management, definition, and tracking of privacy operations at scale

Consent Management (preview)

Privacy Assessments (preview)

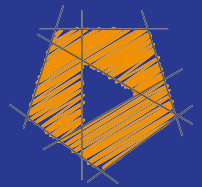
Privacy Risk Management

Subject Rights Requests

Tracker Scanning (preview)

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe the compliance management capabilities of Microsoft Purview

- Describe the Microsoft Purview compliance portal
- Describe compliance manager
- Describe the use and benefits of compliance score

Microsoft Purview

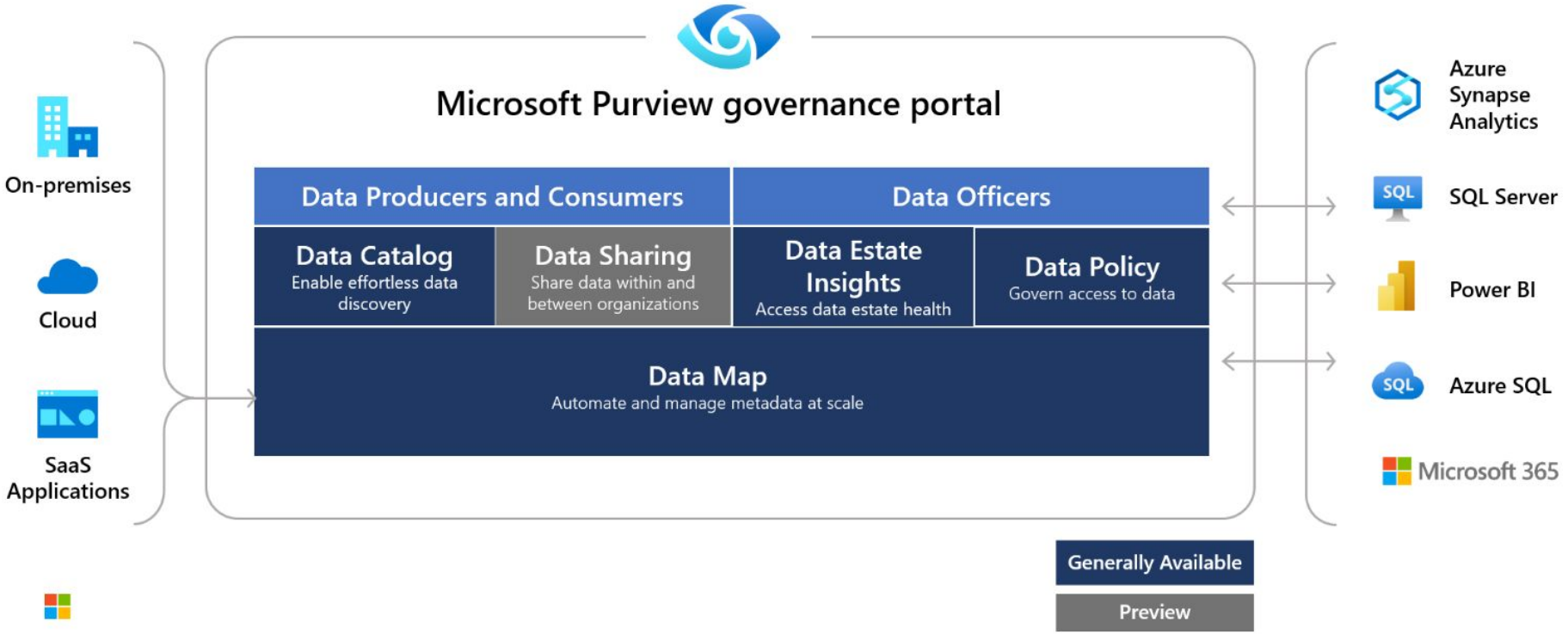
Microsoft Purview is a comprehensive data governance service offered by Microsoft.

It helps organizations manage their data across various environments including on-premises, multi-cloud, and SaaS.

The goal of **Microsoft Purview** is to provide a unified platform for governing, protecting, and managing data, regardless of where it resides.

Purview Features:

- Up-to-date map of your data landscape
  - Data discovery
  - Sensitive data classification
  - End-to-end data lineage
- Enable data curators to manage and secure data
- Empower data consumers to find valuable, trustworthy data



Microsoft Purview Compliance Portal

https://purview.microsoft.com/

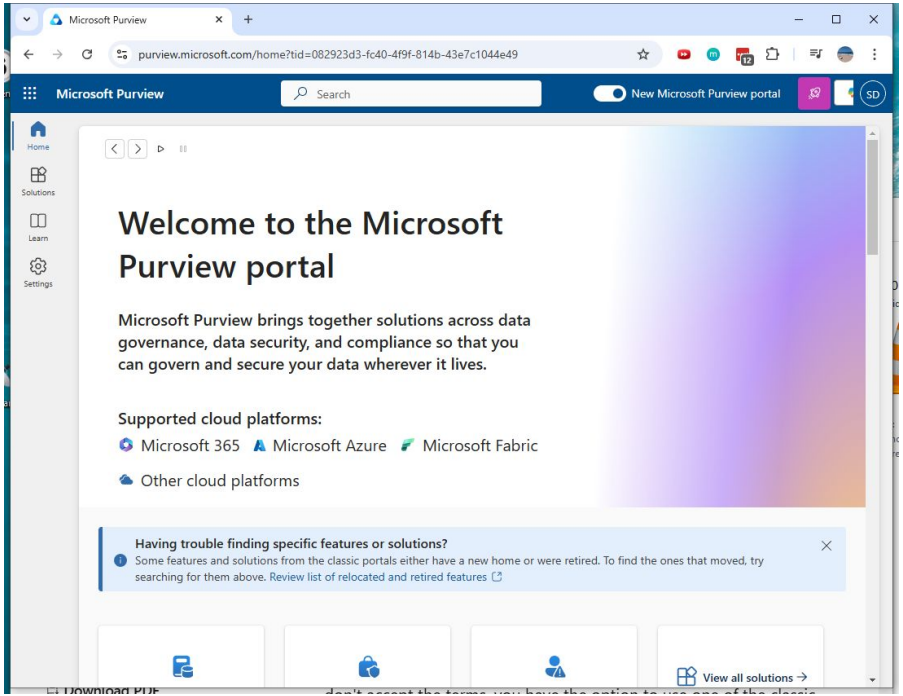
Help understand and manage an organization’s compliance needs

Microsoft Purview Compliance Portal

Compliance score

Solution catalog

Active alerts



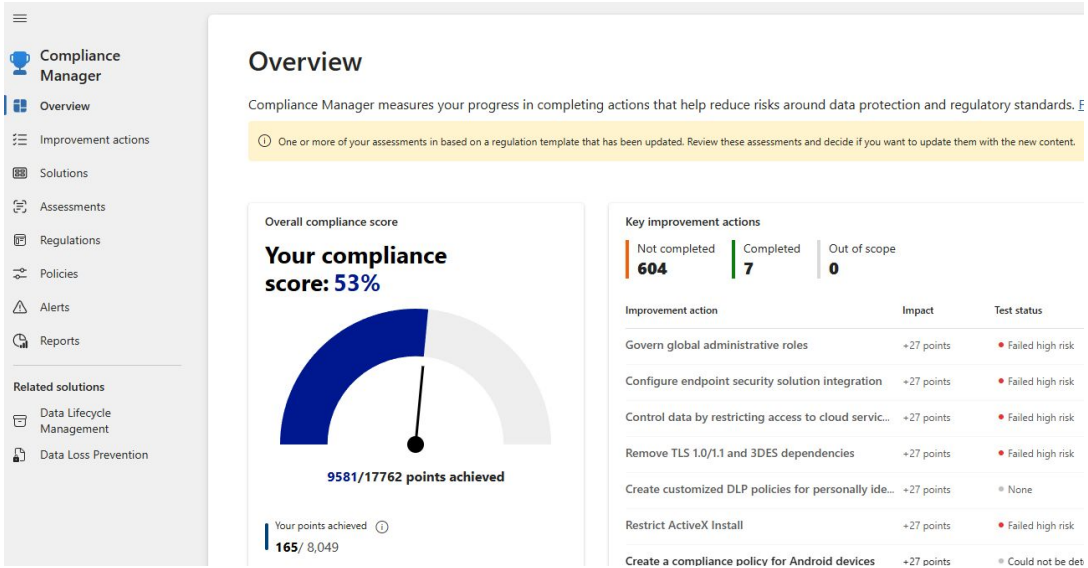
Compliance manager

Prebuilt assessments

Workflow capabilities

Step-by-step improvement actions

Compliance score

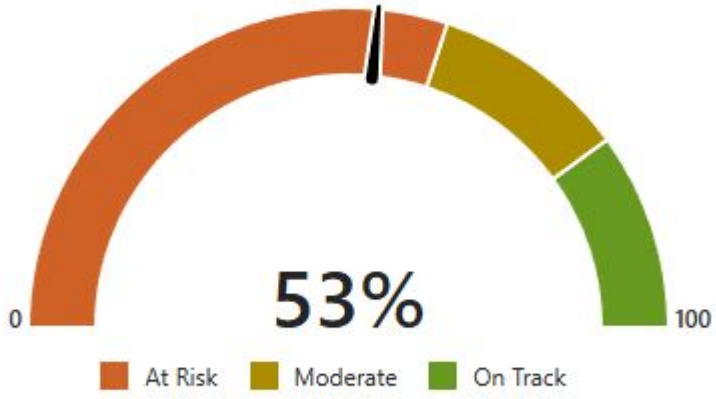


Compliance score

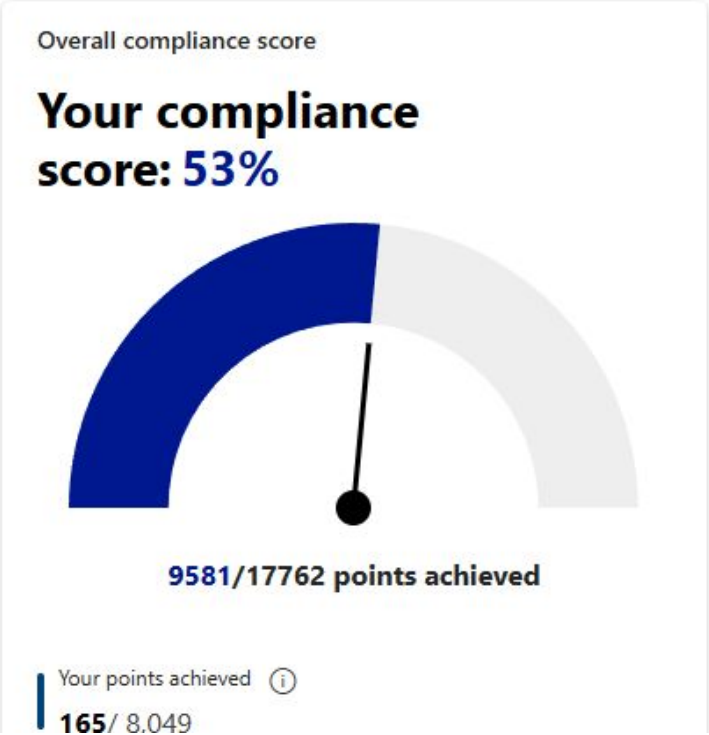
Helps an organizations:

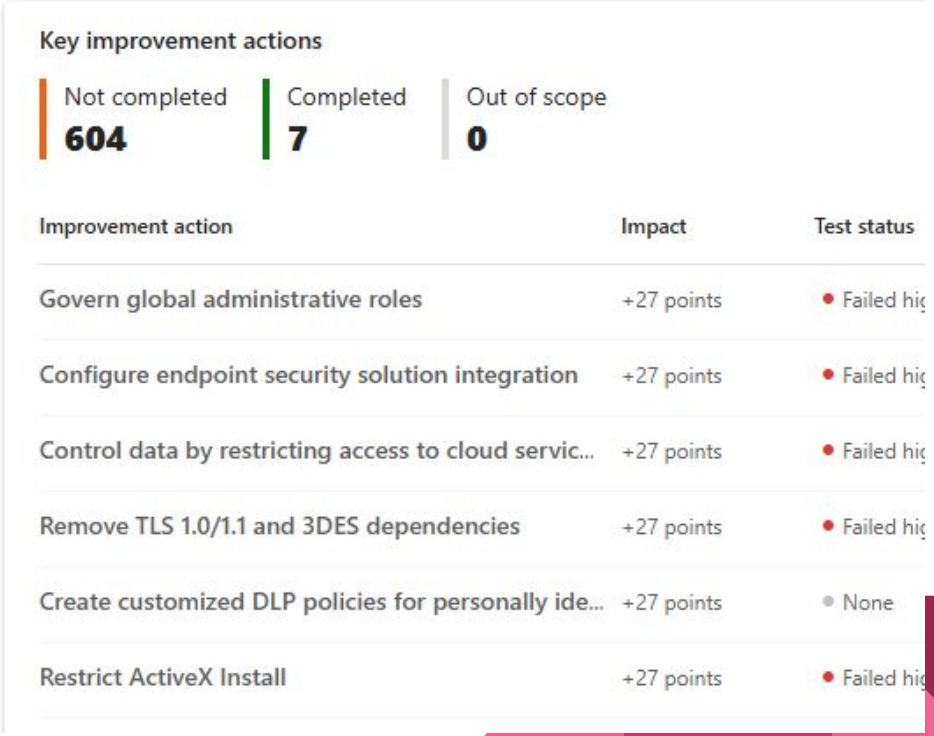
Understand its current compliance posture

Prioritize actions based on their potential to reduce risk



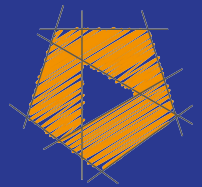
Compliance score





SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

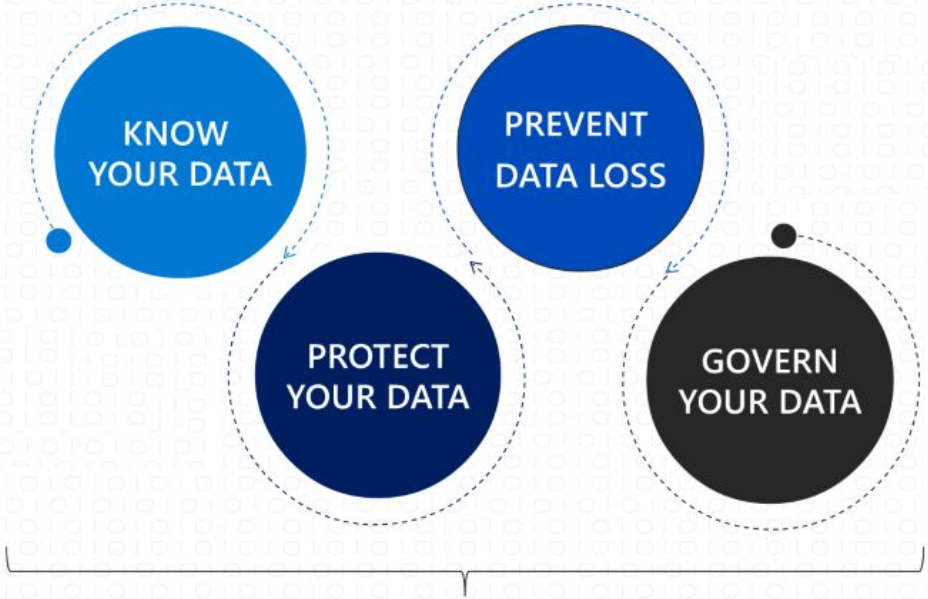


Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Polices and Retention Labels

Data Classification

Data classification



Sensitive information types

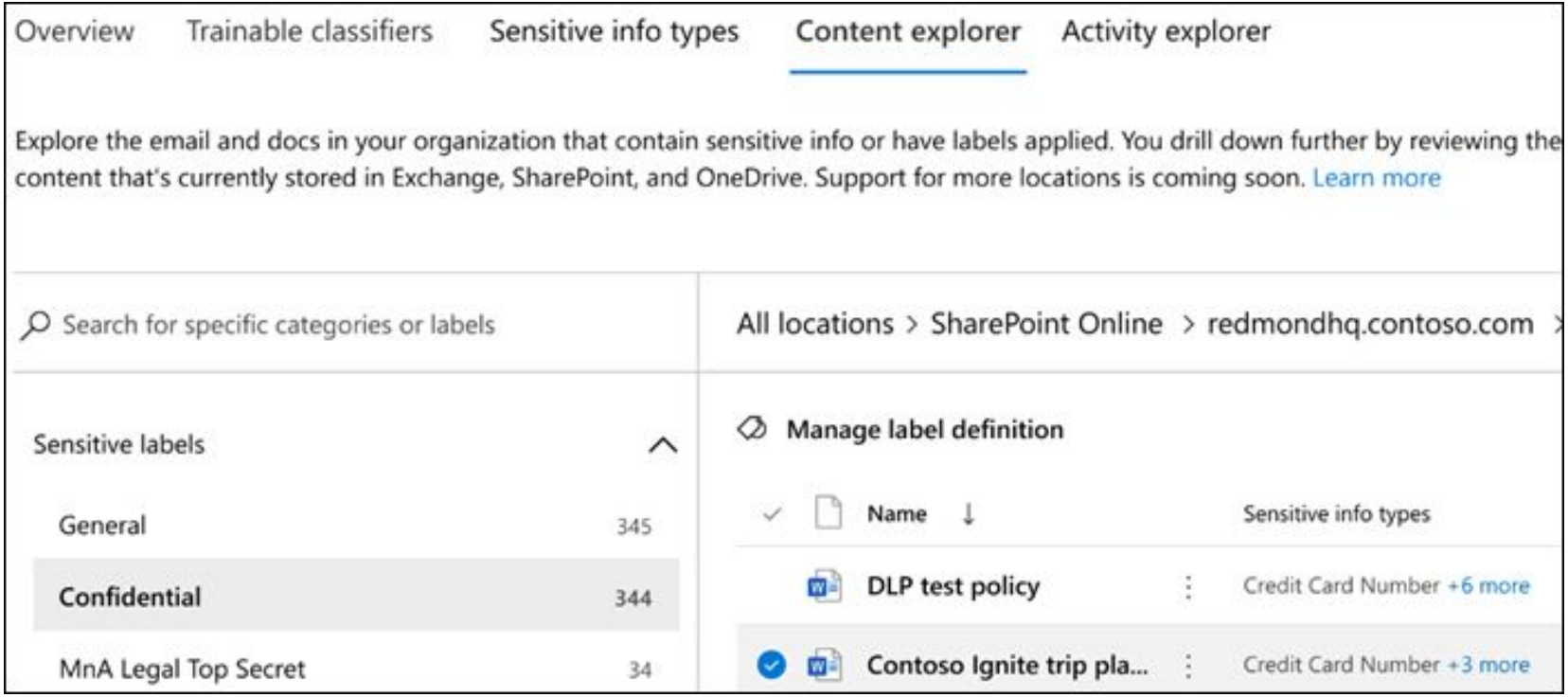
Trainable classifiers

Content explorer

Activity explorer

Content Explorer

A current snapshot of individual items that have been classified across the organization



Activity Explorer

Provides visibility into what content has been discovered, labeled, and where that content is

Activity Explorer

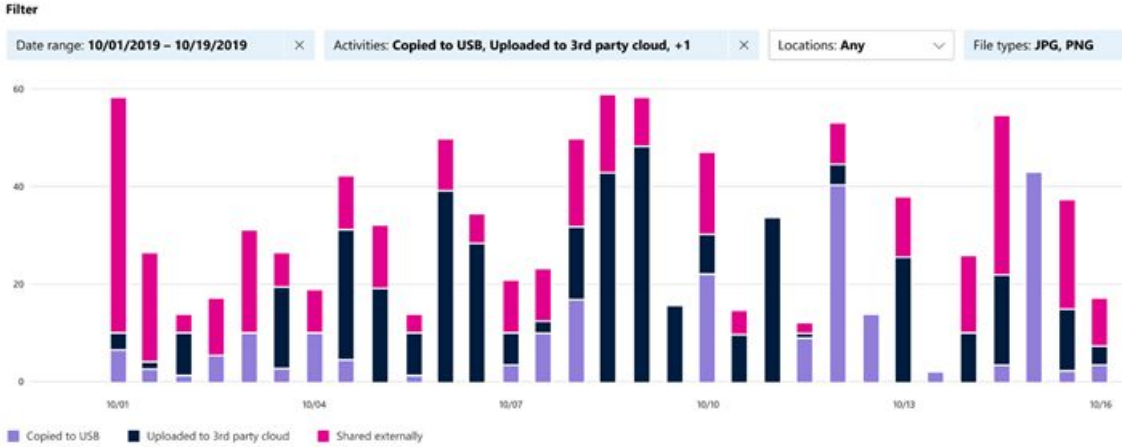
Some activity types that can be analyzed:

File copied to removable media

File copied to network share

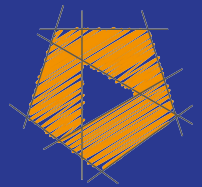
Label applied

Label changed



SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Polices and Retention Labels

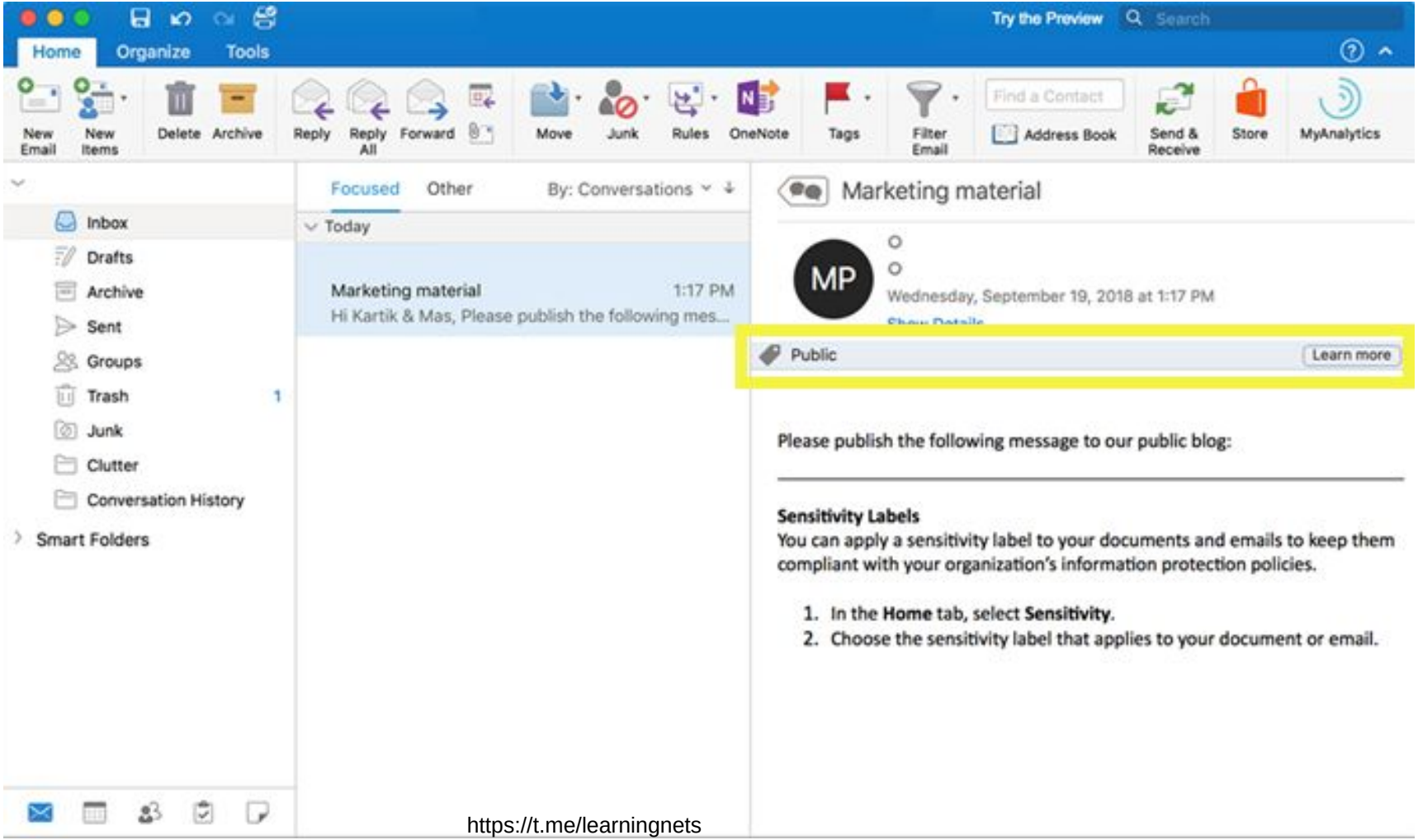
Sensitivity labels

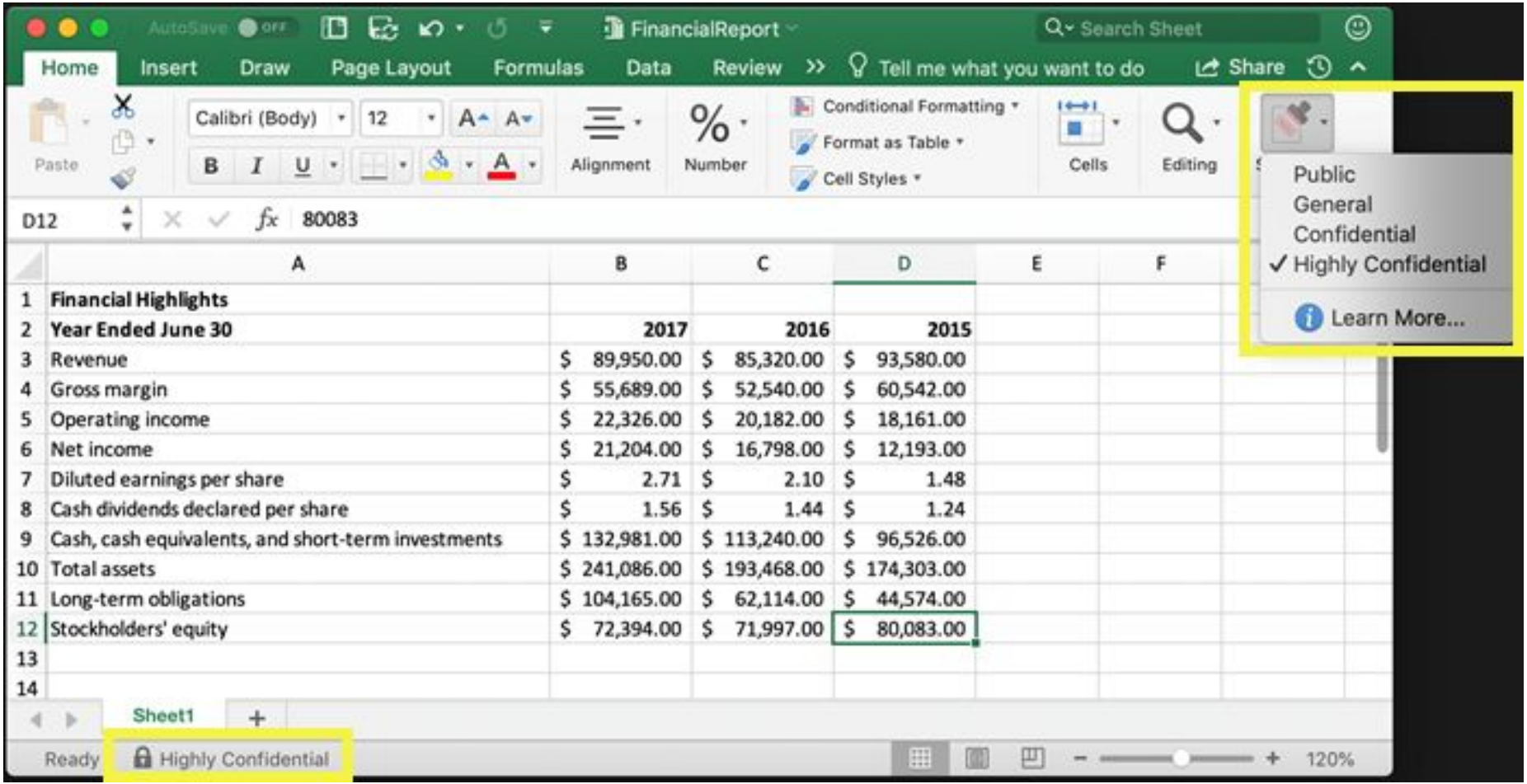
Sensitivity labels

Customizable

Clear text

Persistent





	A	B	C	D	E	F
1	**Financial Highlights**					
2	**Year Ended June 30**	**2017**	**2016**	**2015**		
3	Revenue	$ 89,950.00	$ 85,320.00	$ 93,580.00		
4	Gross margin	$ 55,689.00	$ 52,540.00	$ 60,542.00		
5	Operating income	$ 22,326.00	$ 20,182.00	$ 18,161.00		
6	Net income	$ 21,204.00	$ 16,798.00	$ 12,193.00		
7	Diluted earnings per share	$ 2.71	$ 2.10	$ 1.48		
8	Cash dividends declared per share	$ 1.56	$ 1.44	$ 1.24		
9	Cash, cash equivalents, and short-term investments	$ 132,981.00	$ 113,240.00	$ 96,526.00		
10	Total assets	$ 241,086.00	$ 193,468.00	$ 174,303.00		
11	Long-term obligations	$ 104,165.00	$ 62,114.00	$ 44,574.00		
12	Stockholders' equity	$ 72,394.00	$ 71,997.00	$ 80,083.00		
13						
14						

Sensitivity label usage

Encrypt email or both email and documents

Mark content

Apply a label automatically

Protect content in containers (sites and groups)

Extend sensitivity labels (third-party apps and services)

Classify content without protection settings

Labels need to be published to make them available to people and services

Sensitivity label policies

Choose the users and groups that can see labels

Apply a default label to all new emails and documents

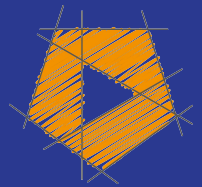
Require justifications for label changes

Require users to apply a label (mandatory labeling)

Link users to custom help pages

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Polices and Retention Labels

Retention policies and labels

Ensuring content is kept only for a required time, and then permanently deleted

Works with:

Sharepoint, OneDrive, Teams, Yammer and Exchange

Comply proactively with industry regulations and internal policies

Reduce risk when there's litigation or a security breach

Ensure users work only with content that's current and relevant to them

Retention labels

Applied at item level (file, doc, email)

Only 1 label supported

Labels travel with content if moved to a different location within your M365 tenant

Applied manually/automatically

Support disposition review: review content before permanent deletion

Retention policies

Applied at site or mailbox level

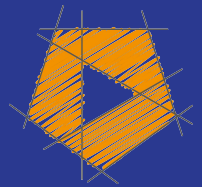
Applied to multiple locations, specific locations or users

Items inherit the retention settings from their container

If an item is moved, the retention setting doesn’t travel to new location

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Polices and Retention Labels

Records Management

Used to look after your companies legal obligations and helps to demonstrate compliance with regulations

Disposition of items that are:

No longer required to be kept, have no value or no business purpose

Three Types of Retention:

- Retention Label
- Record (locked / unlocked)
- Regulatory Record

Retention labels enable admins to mark items as records

Action	Retention label	Record - locked	Record - unlocked	Regulatory record
Edit contents	Allowed	**Blocked**	Allowed	**Blocked**
Edit properties, including rename	Allowed	Allowed	Allowed	**Blocked**
Delete	Allowed [1]	**Blocked**	**Blocked**	**Blocked**
Copy	Allowed	Allowed	Allowed	Allowed
Move within container [2]	Allowed	Allowed	Allowed	Allowed
Move across containers [2]	Allowed	Allowed if never unlocked	**Blocked**	**Blocked**

Action	Retention label	Record - locked	Record - unlocked	Regulatory record
Open/Read	Allowed	Allowed	Allowed	Allowed
Change label	Allowed	Allowed - container admin only	Allowed - container admin only	**Blocked**
Remove label	Allowed	Allowed - container admin only	Allowed - container admin only	**Blocked**

During the retention period

- ○ Retain items even if users delete
- ◉ Mark items as a record

  Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. Learn more
- ○ Mark items as a regulatory record

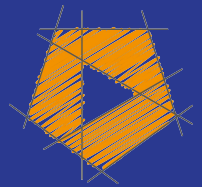
At the end of the retention period

- ◉ Delete items automatically

  We'll delete items from where they're currently stored.

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe information protection and data lifecycle management capabilities of Microsoft Purview

- Describe data classification capabilities
- Describe the benefits of content and activity explorer
- Describe sensitivity labels
- Describe Data Loss Prevention (DLP)
- Describe Records Management
- Describe Retention Polices and Retention Labels

Data Loss Prevention: Protect sensitive information and prevent its inadvertent disclosure

Data Loss Prevention (DLP)

Identify, monitor, and automatically protect sensitive information across M365:

OneDrive for Business, SharePoint Online, Microsoft Teams, Exchange Online

Help users learn how compliance works

View DLP reports

Data Loss Prevention (DLP)

DLP policies protect information by identifying and automatically protecting sensitive data, eg.:

Credit card number

Personal Information

Endpoint Data Loss Prevention

To audit and manage activities that users complete on sensitive content on Windows 10 devices, eg.:

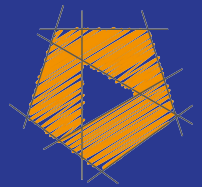
Creating an item

Renaming an item

Copying items to removable media

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe insider risk capabilities in Microsoft Purview

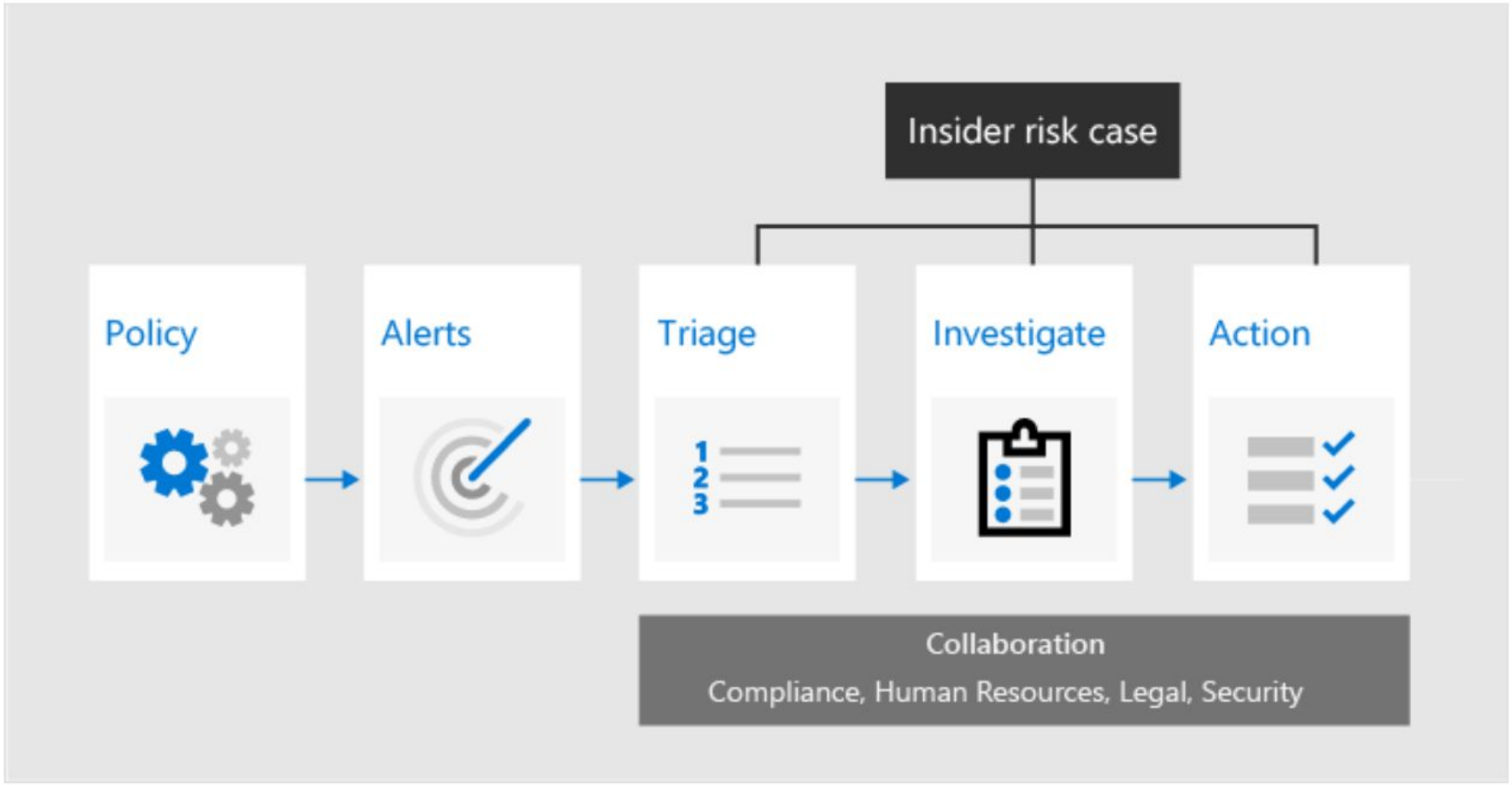
- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers

Insider Risk Management is used to minimize internal risks

Leaks of sensitive data and data spillage

Confidentiality violations

Intellectual property (IP) theft

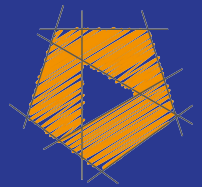


Four Insider Risk solutions in M365:

- Communication compliance
- Insider risk management
- Information barriers
- Privileged access management

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe insider risk capabilities in Microsoft Purview

- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers

Communication Compliance

Minimize communication risks by detecting, capturing, and take remediation actions for inappropriate messages

- Microsoft Teams
- Exchange Online
- Yammer
- Third-party communications

Monitoring email and chat for compliance risks

Inappropriate Communications

Profanity

Threats

Harassment

Sharing sensitive information inside and outside your organization

Contoso Electronics Microsoft 365 compliance

Communication compliance

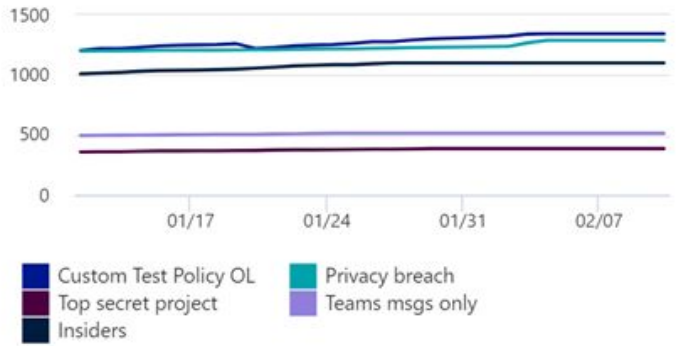
Communication compliance settings | Show in navigation

Policies | Alerts | Reports

Get quick insights into how your policies are performing, including recent activity, escalations, and user matches. Or view detailed reports to drill down more and export results for further analysis. Learn more

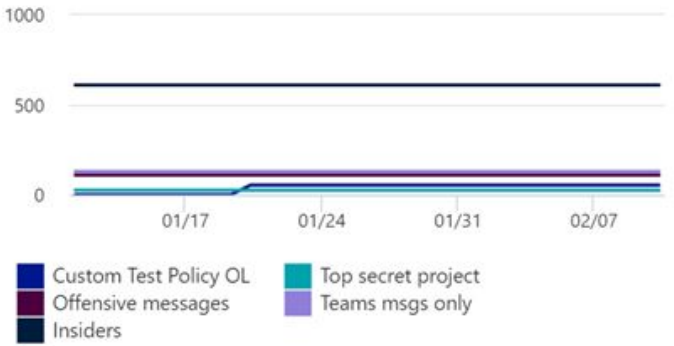
Recent policy matches

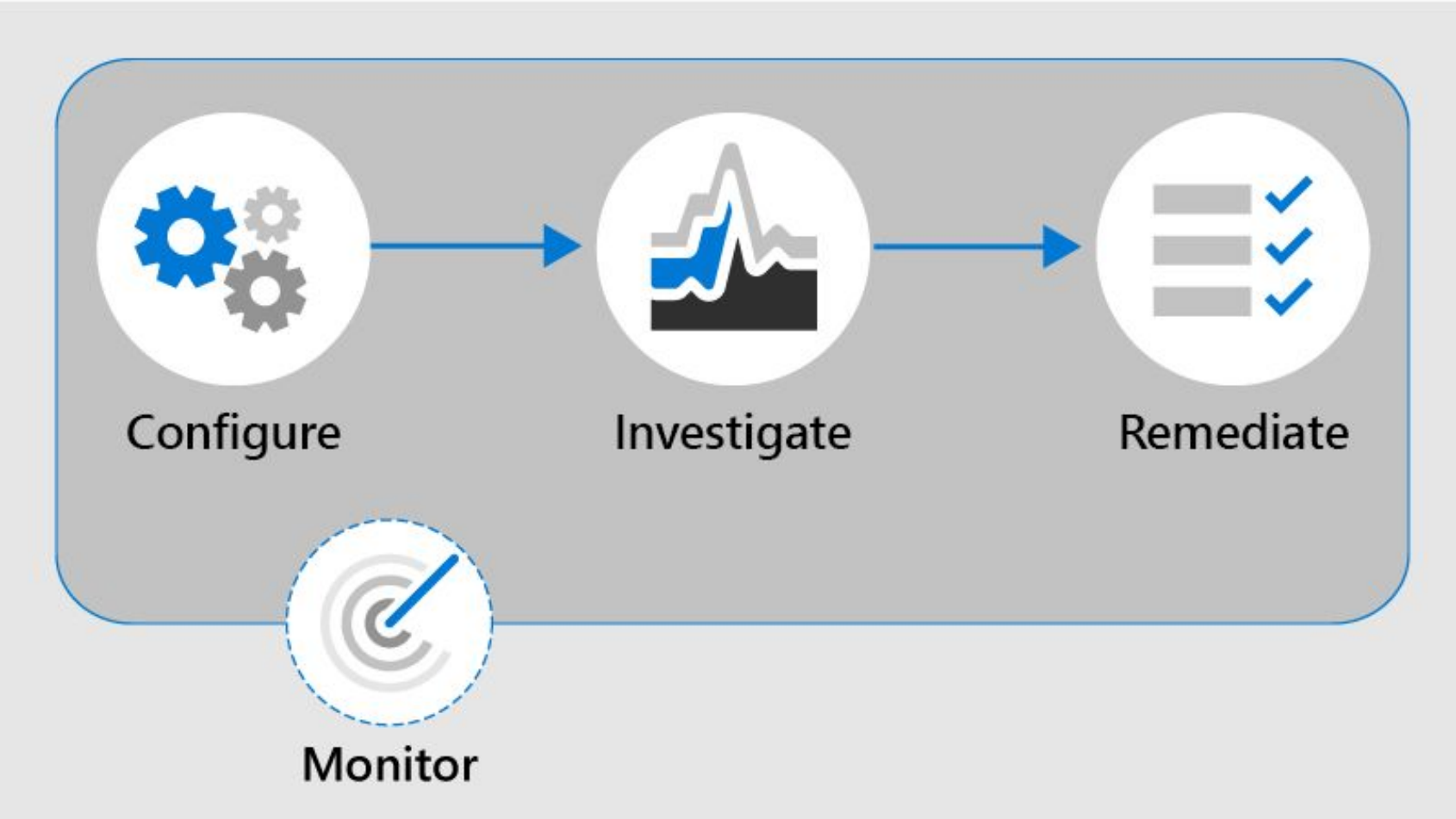
Last 30 days, updated 3:38 PM today



Resolved items by policy

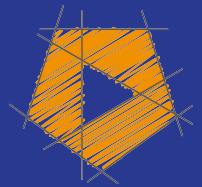
Last 30 days, updated 3:38 PM today





SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe insider risk capabilities in Microsoft Purview

- Describe Insider Risk Management
- Describe communication compliance
- Describe information barriers

Information barriers restrict communications among specific groups of users

I.e. User in the day trader group should not communicate or share files with the marketing team

Information barriers

Only support two-way restrictions

Can prevent the following in Teams:

Searching for a user

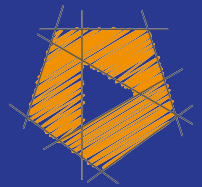
Adding a member to a team

Starting a chat session with someone

And more..

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



Describe resource governance capabilities in Azure

- Describe Azure Policy
- Describe Azure Blueprints
- Describe the Microsoft Purview unified data governance solution

Prevent resources from being accidentally deleted or changed

Azure Resource Locks

Apply a lock at a parent scope, all resources within that scope inherit that lock

Apply only to operations that happen in the management plane

Changes to the actual resource are restricted, but resource operations aren't restricted

CanNotDelete ReadOnly

A way to define a repeatable set of Azure resources

Azure Blueprints

Always in line with the organization’s compliance requirements

Provision Azure resources across several subscriptions simultaneously

Blueprint objects are replicated to multiple Azure regions

Azure Blueprints

Declarative way to orchestrate the deployment of various resource templates and artifacts, including:

- Role Assignments
- Policy Assignments
- ARM templates
- Resource Groups

Azure Policy is designed to help enforce standards and assess compliance

Azure Policy evaluates all resources in Azure and Arc enabled resources

Azure Policy uses cases

Implementing governance for resource consistency

Regulatory compliance

Security, cost, and management

Azure Policy responses

Deny a change to a resource

Log changes to a resource

Alter a resource before or after a change

Deploy related compliant resources

Thank you!