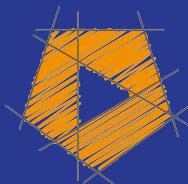


SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>



Exam Released May 2021



Latest Update November 2022



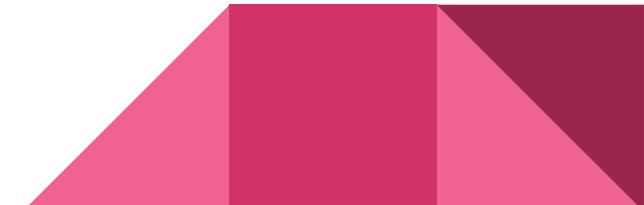
SCI -
Security,
Compliance,
Identity

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

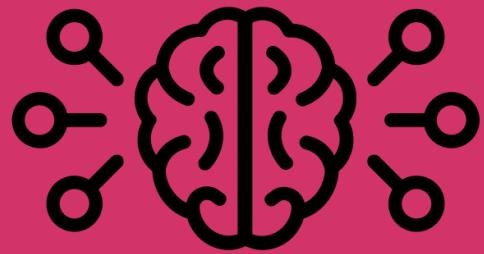
- Describe the concepts of security, compliance, and identity
- Describe the capabilities of Microsoft identity and access management solutions
 - Describe the capabilities of Microsoft security solutions
 - Describe the capabilities of Microsoft compliance solutions

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)



Created by Timofei Rostilov
from Noun Project

What Azure Security Management Services Exist?

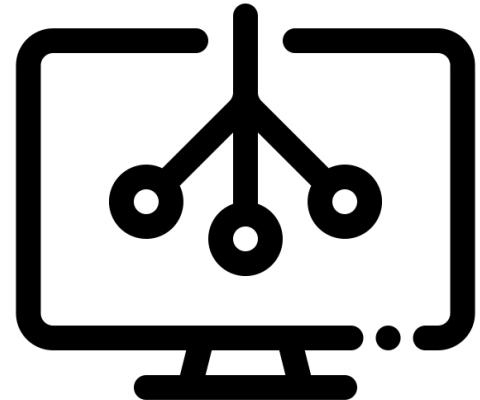
Microsoft Defender for Cloud

(was Azure Defender & Azure Security Center)

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 M365 Defender Capabilities Exist?

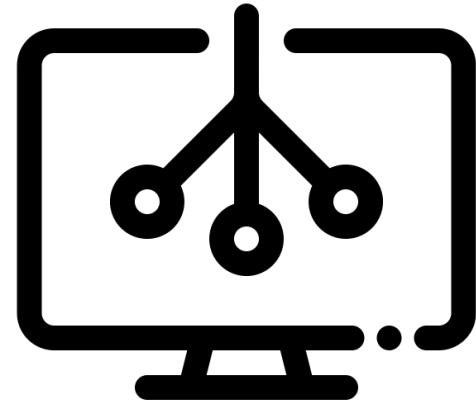
Microsoft 365 Defender

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)



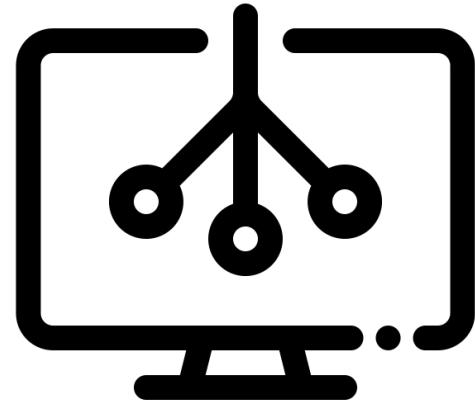
Created by Timofei Rostilov
from Noun Project

What M365 Security Management Capabilities Exist?

Microsoft 365 Defender Portal

Microsoft Secure Score

Intune



Created by Timofei Rostilov
from Noun Project

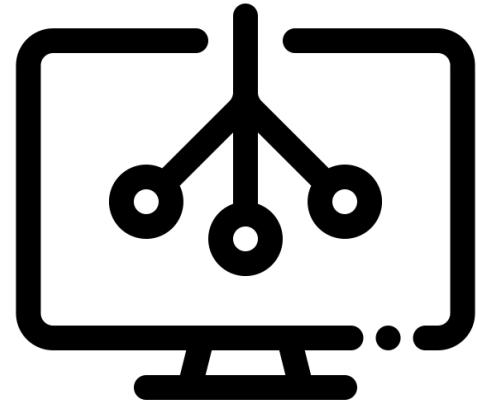
What Basic Azure Compliance Capabilities Exist?

Azure Policy

Azure Blueprints

Resource Locks

Cloud adoption framework



Created by Timofei Rostilov
from Noun Project

What M365 Compliance Capabilities Exist?

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?

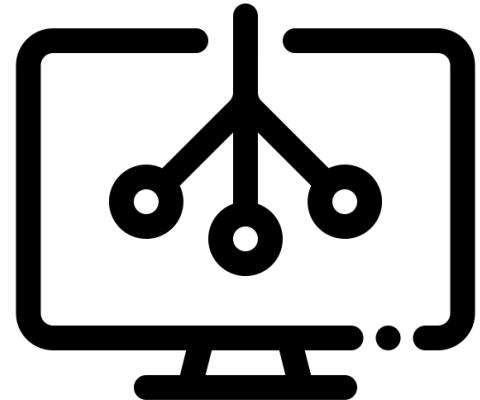
Active Directory

Azure Active Directory, part of Microsoft Entra

Windows Hello for Business

Azure AD Identity Protection

Privileged Identity Management (PIM)



Created by Timofei Rostilov
from Noun Project

Certifications

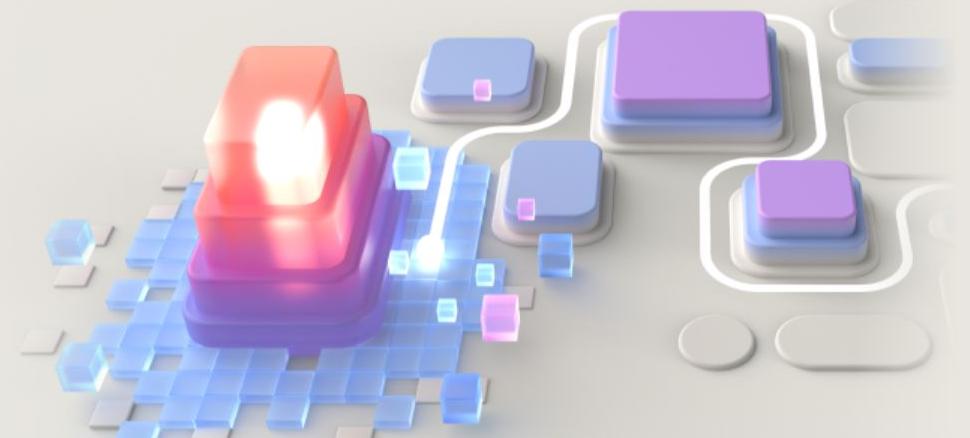
[Browse Certifications](#) [Certification Renewals](#) [FAQ & Help](#)

Docs / Certifications / [Browse Certifications](#) /



EXAMS

Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals

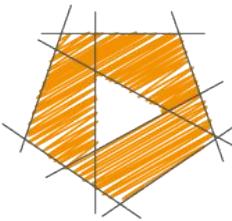


This exam is targeted to those looking to familiarize themselves with the fundamentals of security, compliance, and identity (SCI) across cloud-based and related Microsoft services.

This is a broad audience that may include business stakeholders, new or existing IT professionals, or students who have an interest in Microsoft Security, compliance, and identity solutions.

Candidates should be 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.

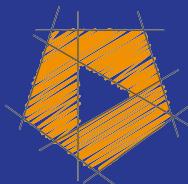
You may be eligible for ACE college credit if you pass this certification exam. See [ACE college credit for certification exams](#) for details.



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>



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
- Define defense in depth
- Describe the Zero-Trust model
- Describe encryption and hashing
- Describe compliance concepts

Security Methodologies

Zero-Trust Methodology



Don't assume
everything behind
the firewall is safe

Zero Trust Principles

- Verify explicitly
- Use least privileged access
- Assume breach



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



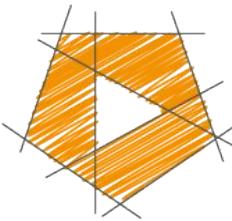
Data: data-driven
protection, encrypt
and restrict access



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



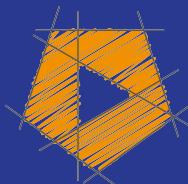
Network: encrypt all
communications



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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

Describe security and compliance concepts

- Describe the shared responsibility model
- Define defense in depth
- Describe the Zero-Trust model
- Describe encryption and hashing
- Describe compliance concepts

Security Concepts

Common Threats

- Data breach
- Dictionary attack
- Ransomware
- Denial of Service (Disruptive) attacks

Entry Points for Data Breach

Phishing attack

Spear phishing

Tech support scams

SQL injection

Malware, trojans, viruses

From: fraud@bankofamericans.com
To: targets@contoso.ltd
Date: Thu, 13 Jun 2019 09:35:31 -0700
Subject: Your Account Has Been Locked



Dear Online Banking Customer:

We are writing to inform you that there have been a number of invalid login attempts to access your account. As a result, we have temporarily locked your account and added an extra verification process intended to ensure your identity and protect the security of your account in the future.

Please [click here](#) to begin the account verification process. If you fail to update your account information in the next 24 hours, you will be required to go into our branch to reestablish your account.

Sincerely,
Bank of Americans Fraud Detection

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Prefer not to receive HTML mail? [Click here](#)

soft Support



Contact Microsoft
833-212-7212

SECURITY ALERT FROM MICROSOFT

DO NOT CLOSE THIS WINDOW OR RESTART YOUR COMPUTER

Your computer's registration key is Blocked.

Windows protected your PC

Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk. For technical support call on **+1-833-212-7212**.

Publisher: Unknown Publisher
App: windows10manager (1).exe

[Run anyway](#) [Don't run](#)

[Leave Page](#)

Enter Windows registration key to unblock.
ENTER KEY: [Submit](#)

[Ignore Alert](#)

[Chat Now](#)

[Close to ignore](#)

Microsoft Security Alert

Your System has Detected Some Unusual Activity.

It might harm your computer data and track your financial activities.

Please Report this activity to : **+1-833-212-7212** (Toll Free)



Dictionary Attack

Attempting to **brute force** gain entry into an account by guessing passwords from a large list of known popular passwords.

```
[*] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashish1' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashish1' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashish1' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashish1' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashish1' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashish1' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[+] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```

Ransomware

Locking a company from it's computer and data resources, and demanding payment in exchange for the key.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

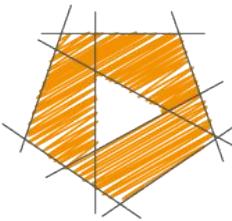
To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]

To pay the fine, you should enter the [REDACTED] digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

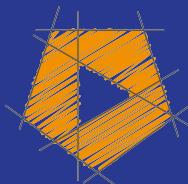




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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

Describe security and compliance concepts

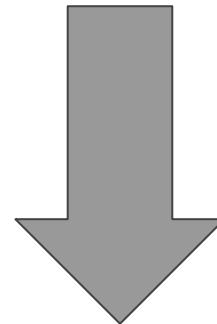
- Describe the shared responsibility model
- Define defense in depth
- Describe the Zero-Trust model
- Describe encryption and hashing
- Describe compliance concepts

Encryption and hashing

Encryption (n):

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

“Hello.”



f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

Types of Encryption

Symmetric and Asymmetric:

Symmetric - the same key is used for encryption and decryption

Asymmetric - the concept of a key pair - a public key and a private key; public used to encrypt and private used to decrypt

Hashing - a method of creating a digital signature, a one-way function, but is not technically encryption



A Brief Word on Hashing

A one-way function

Can take a long message, of any length, and make it a short code

32 or 64 characters

Hashes are not unique - hash collision

Rainbow tables

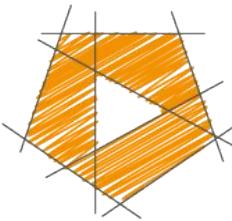
Should be used with a salt for passwords

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

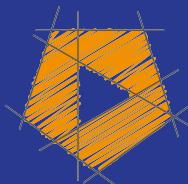
- RSA
 - Encryption used by HTTPS/SSL
- Diffie-Hellman
- ECC
 - Encryption used by Bitcoin
- ElGamal
 - Used in recent versions of PGP
- DSA
 - US Government FIPS standard for signing messages



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe 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

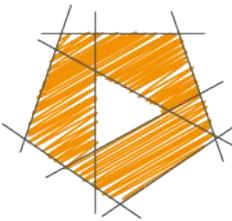
More granular security + logging

Intelligent monitoring that detects strange behavior

More granular security on data and documents

Restrict unrequired and unwanted lateral movement of traffic

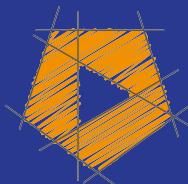
Least privilege / default deny



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe Active Directory
- Describe the concept of Federation

Define Authentication (AuthN)



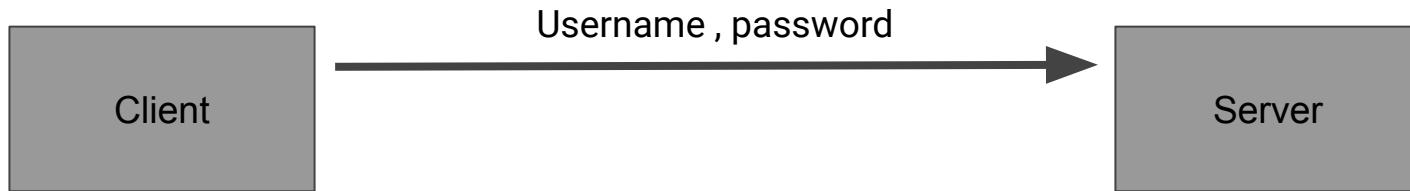
How much proof do
you need for me to
prove my identity to
you?

“Modern Authentication”

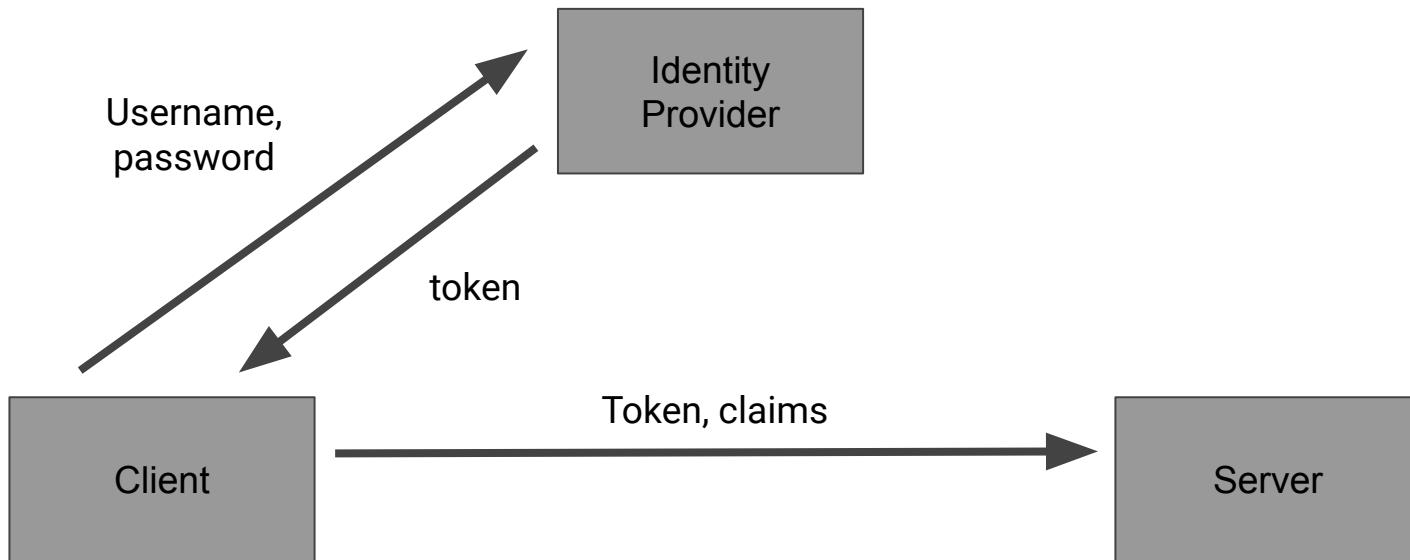


Server should use
an identity provider
to validate identity

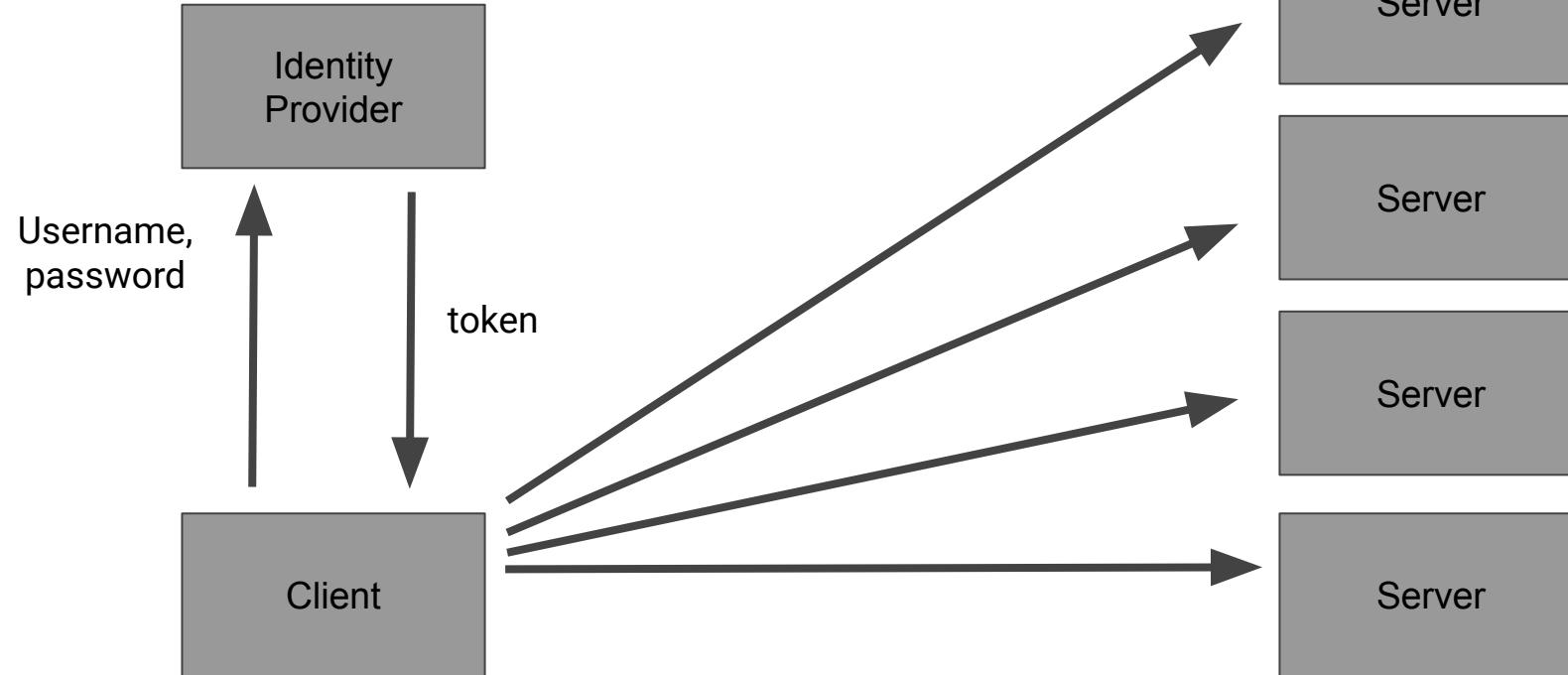
The Old Way



The New Way



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



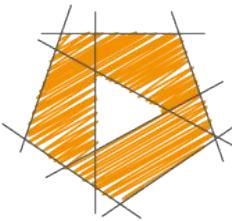
A ~~user~~ role
is granted a set of
permissions to
perform some
tasks



What role do you
have?



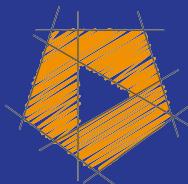
Users can have
multiple roles



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



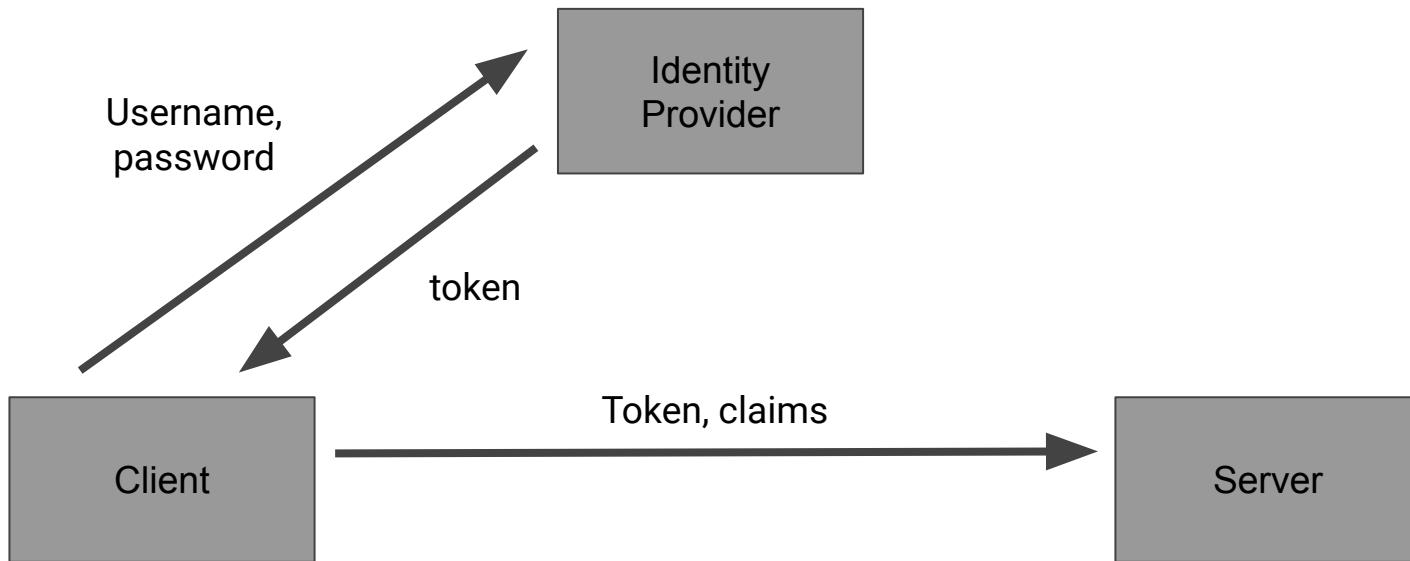
© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe 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

Azure Active Directory (Azure AD)

Active Directory



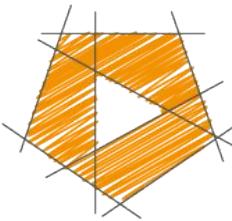
Google

Facebook

Twitter

LinkedIn

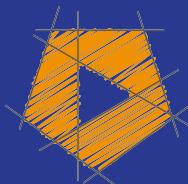
GitHub



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe Active Directory
- Describe the concept of Federation

Active Directory



A set of directory services developed by Microsoft as part of Windows 2000

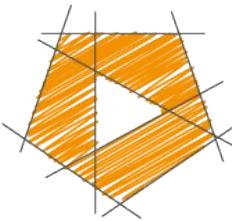
Managed on-prem identity



“Domain controller”



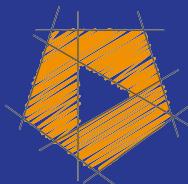
Uses protocols that
do not work over
the Internet



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Define identity concepts

- Define identity as the primary security perimeter
- Define authentication
- Define authorization
- Describe identity providers
- Describe 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



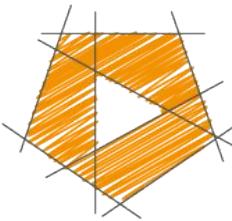
User from
Company B
can log in to
Company A app



Trust isn't always
bi-directional



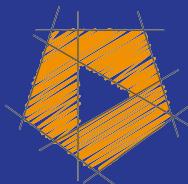
Azure AD B2C
can be configured
to use social media
sites for identity



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the basic identity services and identity types of Azure AD

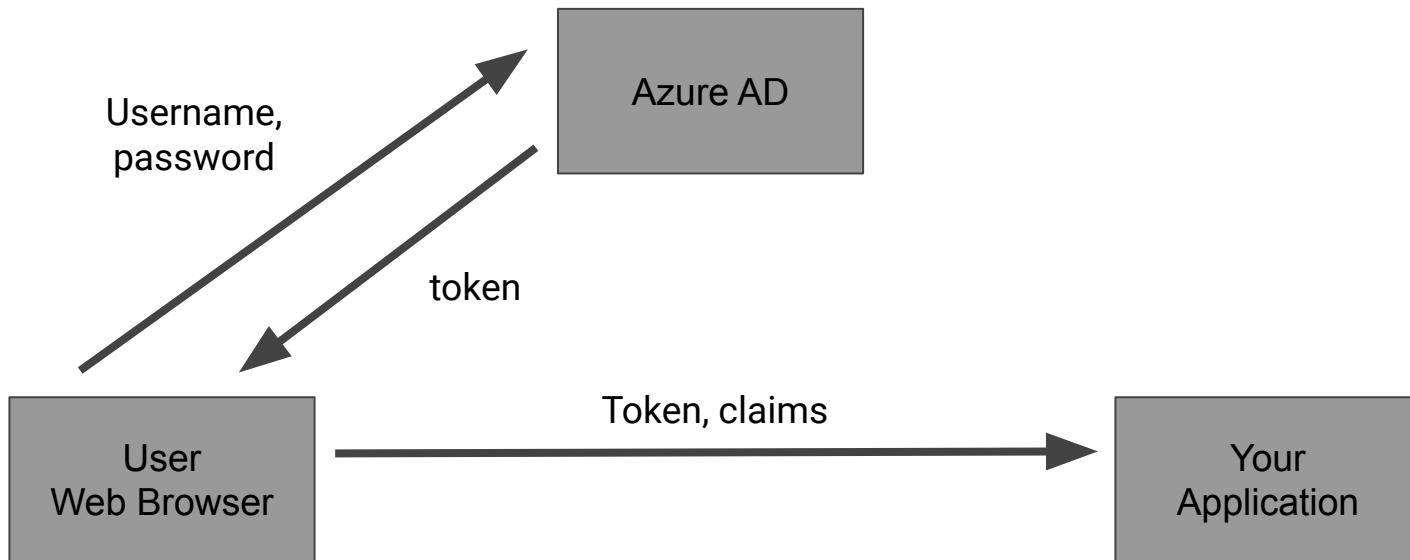
- describe what Azure Active Directory is
- describe Azure AD identities (users, devices, groups, service principals/applications)
- describe what hybrid identity is
- describe the different external identity types (Guest Users)



Azure Active Directory,
part of Microsoft Entra

Identity as a Service in Azure

Azure AD





A Tenant =
An Organization

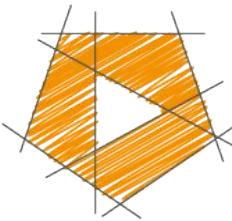


A tenant can have a subscription to enable compute resources to be created



Applications can
register with
Azure AD

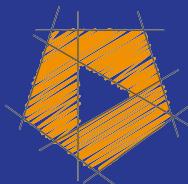
Demo of Azure AD



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

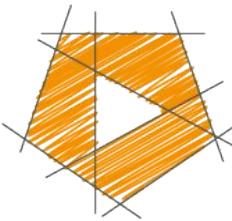
Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the basic identity services and identity types of Azure AD

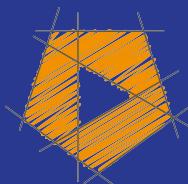
- describe what Azure Active Directory is
- describe Azure AD identities (users, devices, groups, service principals/applications)
- describe what hybrid identity is
- describe the different external identity types (Guest Users)



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the authentication capabilities of Azure AD

- Describe the authentication methods available in Azure AD
- Describe Multi-factor Authentication
- Describe self-service password reset
- Describe password protection and management capabilities available in Azure AD

Azure AD Password Protection

Global Banned Password List

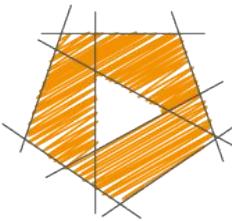
Custom Banned Password List



Bad password
attempts and
lockout duration



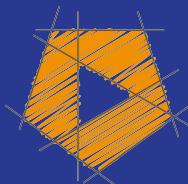
Can also protect
Windows Server
Active Directory



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the authentication capabilities of Azure AD

- Describe the authentication methods available in Azure AD
- Describe Multi-factor Authentication
- Describe self-service password reset
- Describe password protection and management capabilities available in Azure AD



Something you are
Something you have
Something you know



Authenticator app
OATH Hardware token
SMS
Voice call



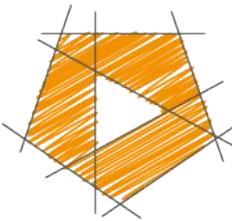
Enabled by
administrators



Signed up by users

Conditional access

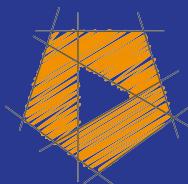
Session lifetime



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

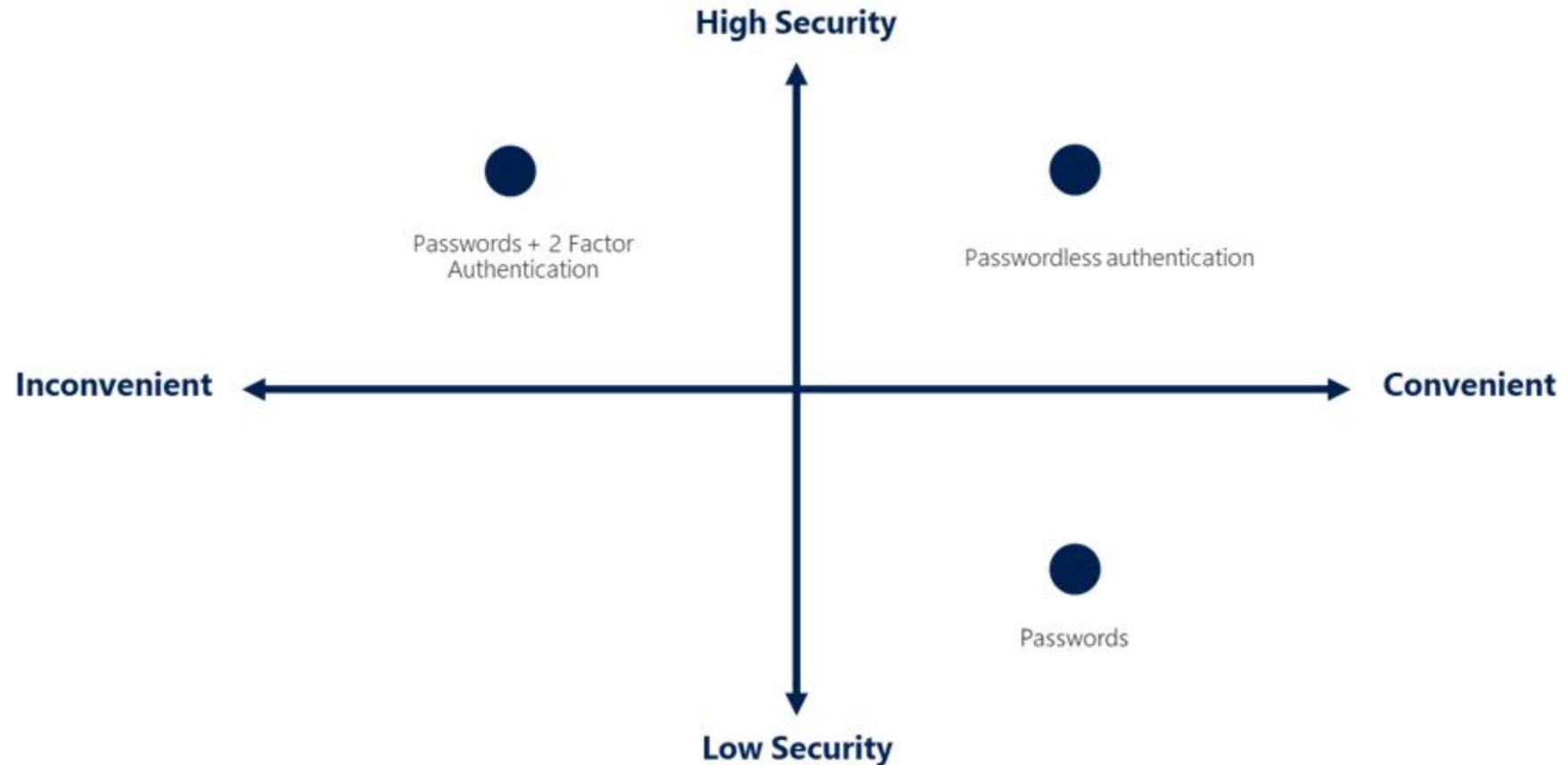
Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the authentication capabilities of Azure AD

- Describe the authentication methods available in Azure AD
- Describe Multi-factor Authentication
- Describe self-service password reset
- Describe password protection and management capabilities available in Azure AD



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?”

InPrivate Sign in to Microsoft Azu +

https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3a%2f%21

Microsoft Azure

 Microsoft

← bala@consoto.com

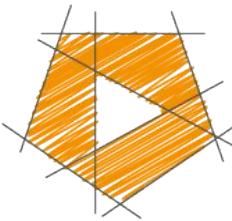
Approve sign in

To sign in with balas@identityitpro.com, please follow the instructions on your phone and enter the number you see below.

80

Other ways to sign in

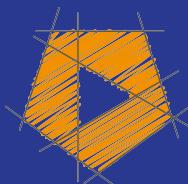
Terms of use Privacy & cookies ...



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe access management capabilities of Azure AD

- describe what conditional access is
- describe uses and benefits of conditional access
- describe the benefits of Azure AD roles

Conditional Access



Using signals to make decisions and enforce policies



User and location
Device
Application
Risk



Allow access

Require MFA

Deny access



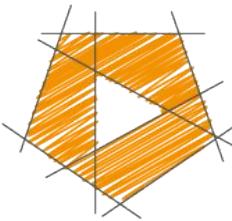
Require MFA for all
Admin users



Require MFA signup
from trusted
locations



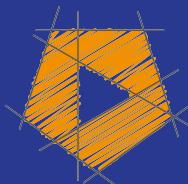
Some minimum
standard for device,
location, or risk



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the identity protection & governance capabilities of Azure AD

- describe what identity governance is
- describe what entitlement management and access reviews is
- describe the capabilities of PIM
- describe Azure AD Identity Protection

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

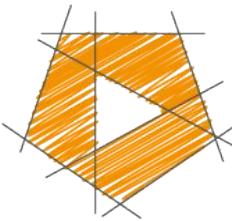
Conditional Access can enforce terms of use acceptance

Privileged Access Lifecycle

Azure AD Privileged Identity Management (PIM)

Just-in-time access

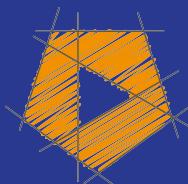
Access reviews



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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

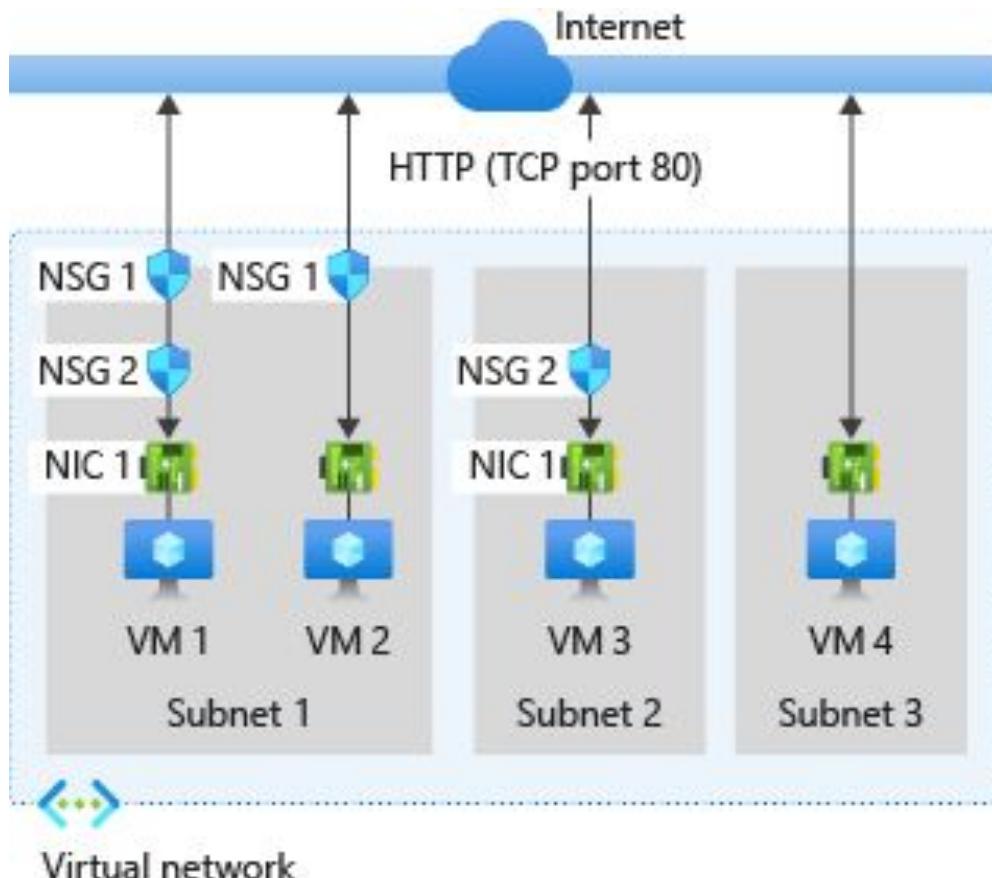
Network Security Group

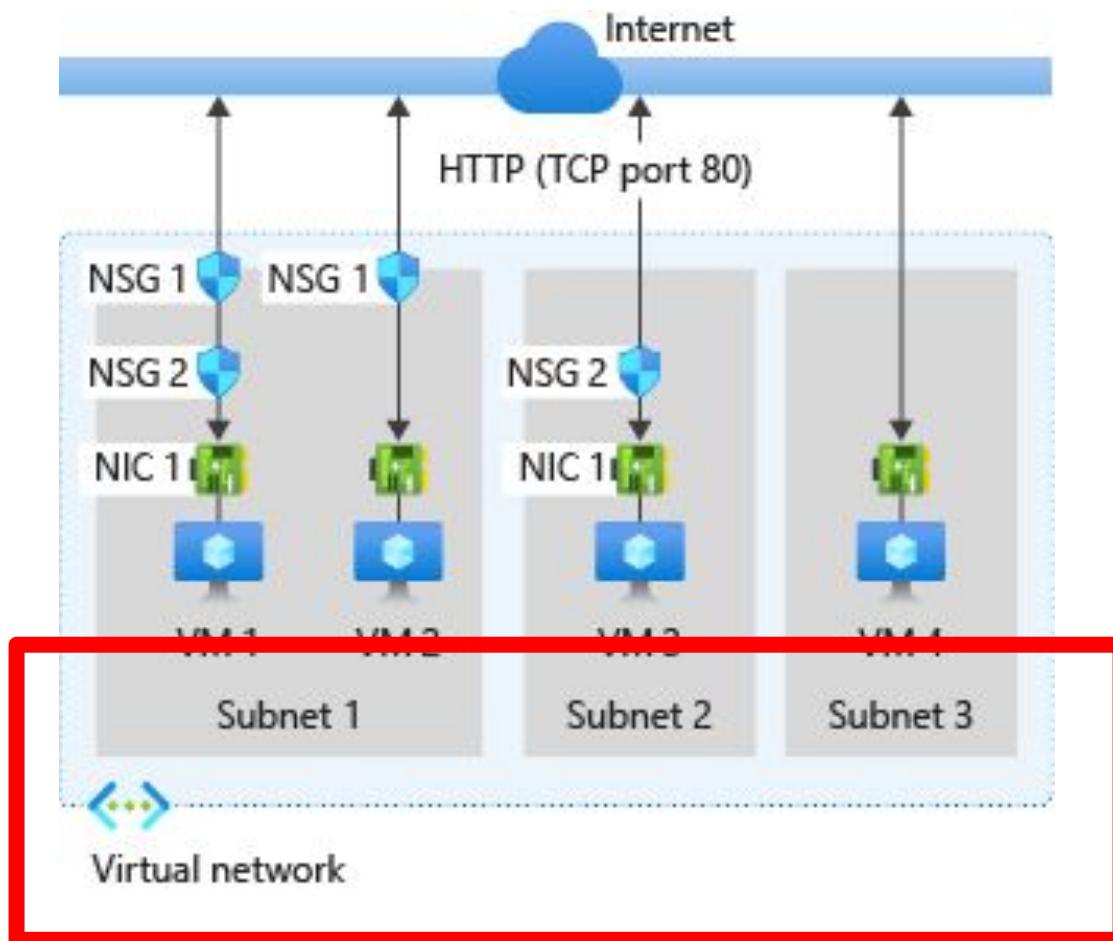
Simple, rules-based control that allows or denies traffic travelling over a network boundary

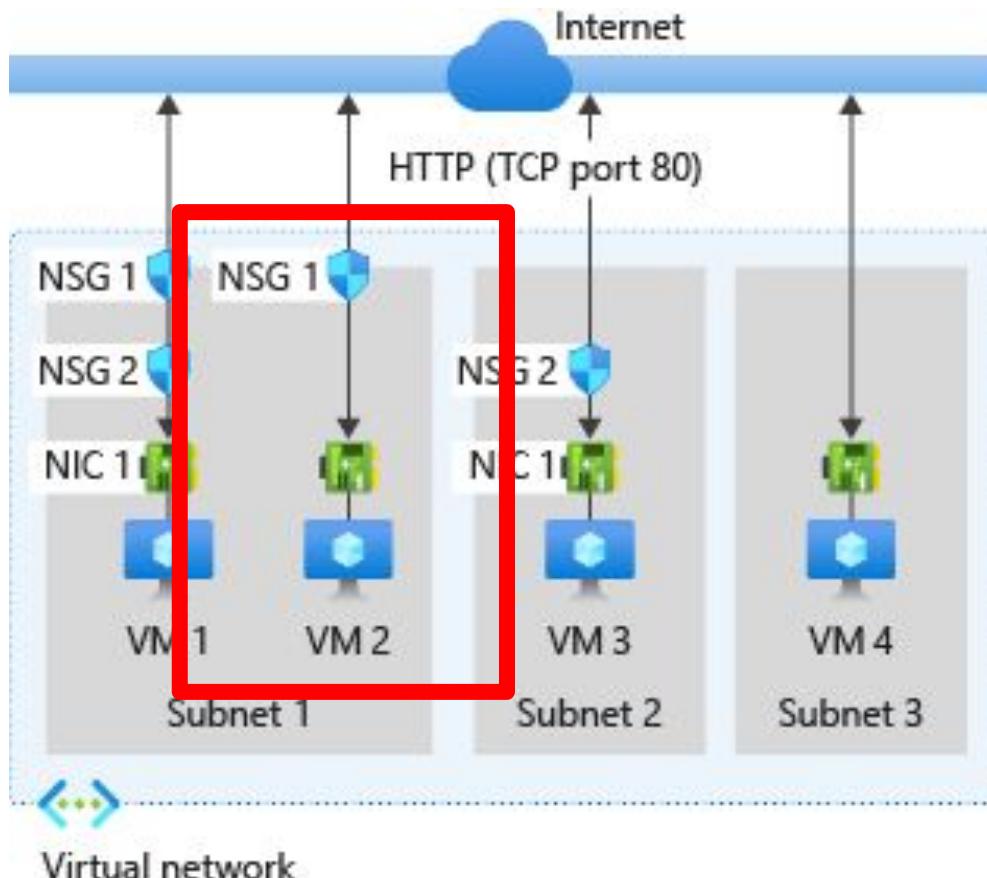
Inbound and outbound can have separate rules

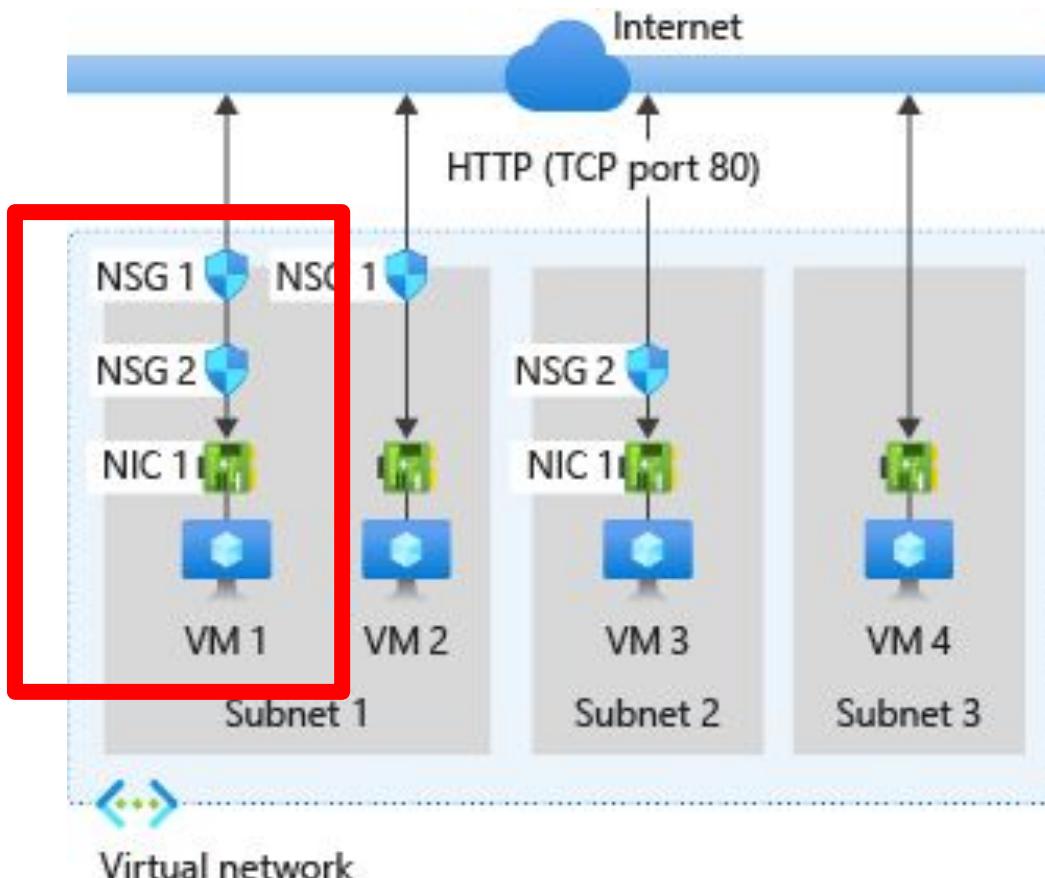
Two network boundaries - the subnet and a network interface card (NIC)

Deny by default

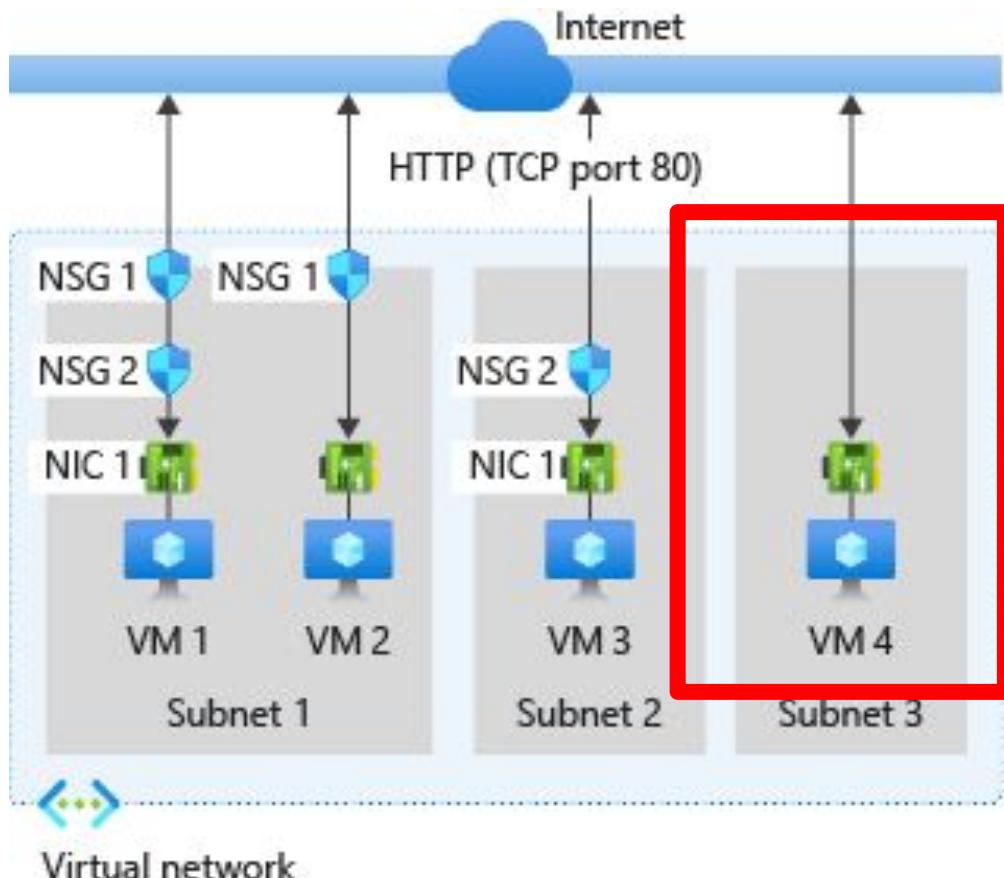


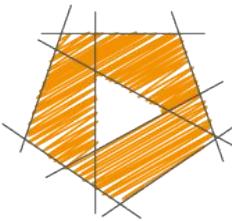






Virtual network

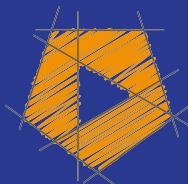




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

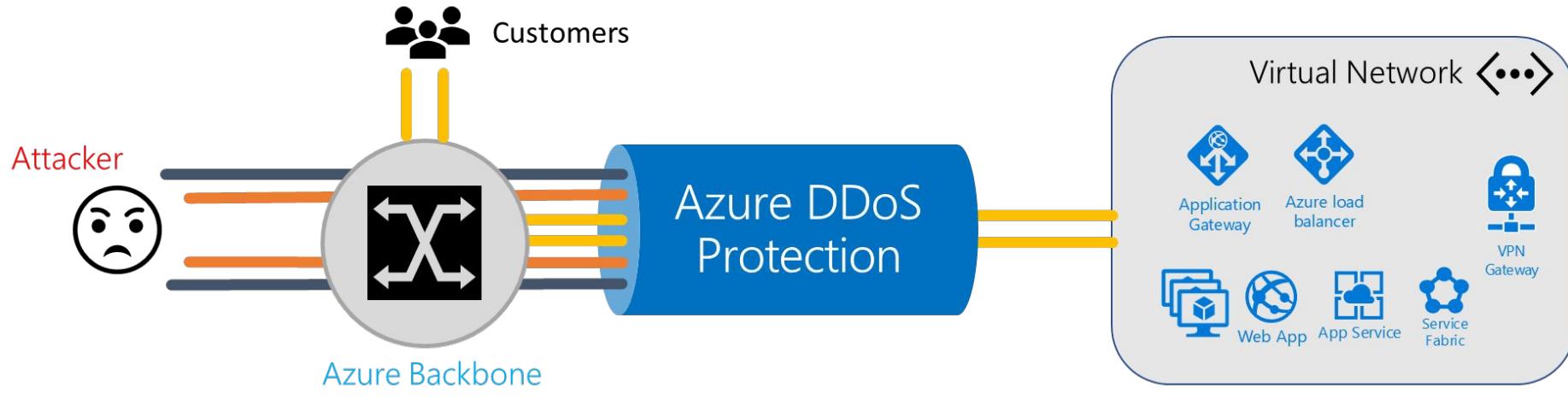


© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

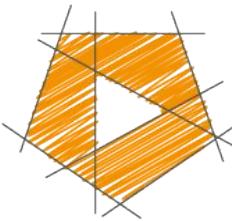
Describe the capabilities of Microsoft Security solutions (25—30%)

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



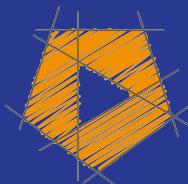
Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee	○	●
Cost Protection	○	●
Mitigation policies tuned to customers application	○	●
Metrics & alerts	○	●
Mitigation reports	○	●
Mitigation flow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



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

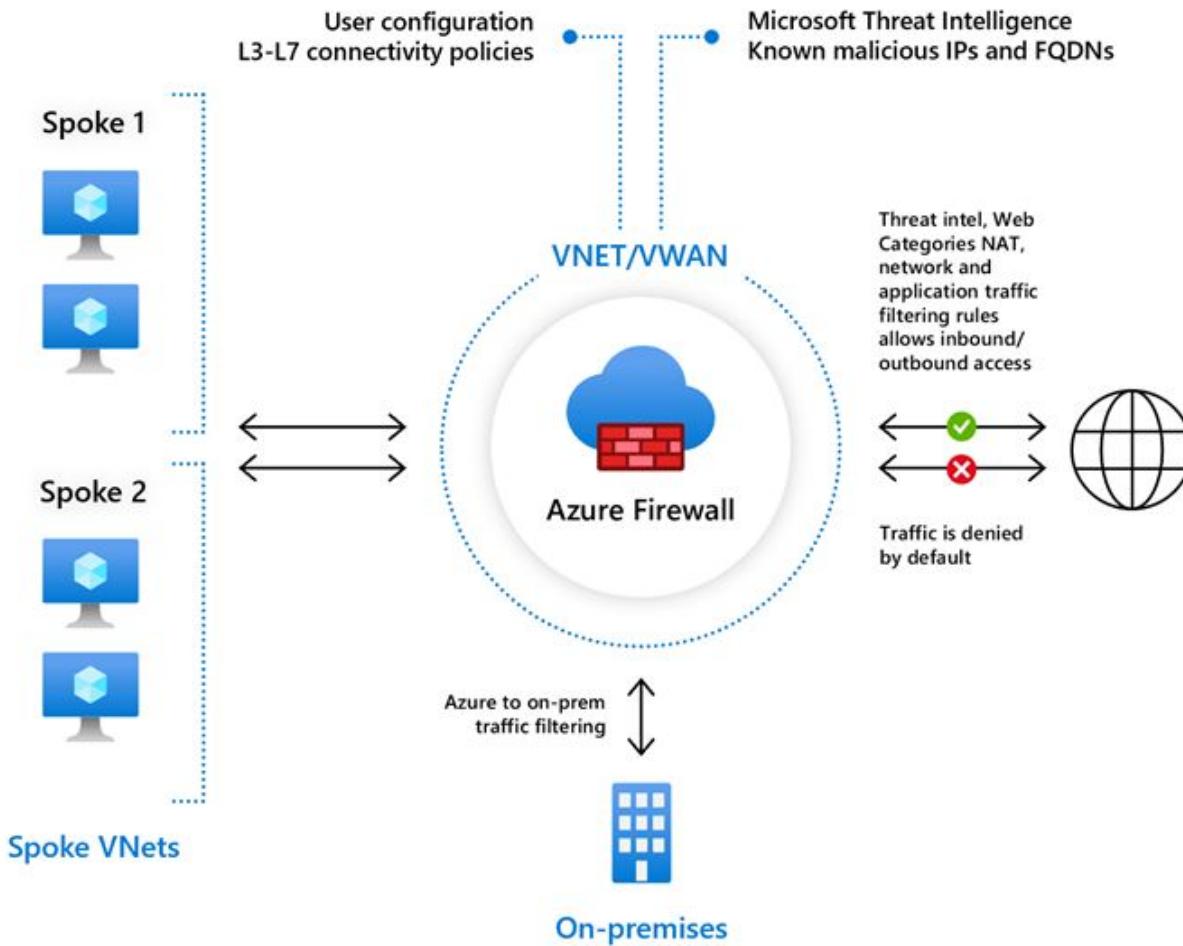


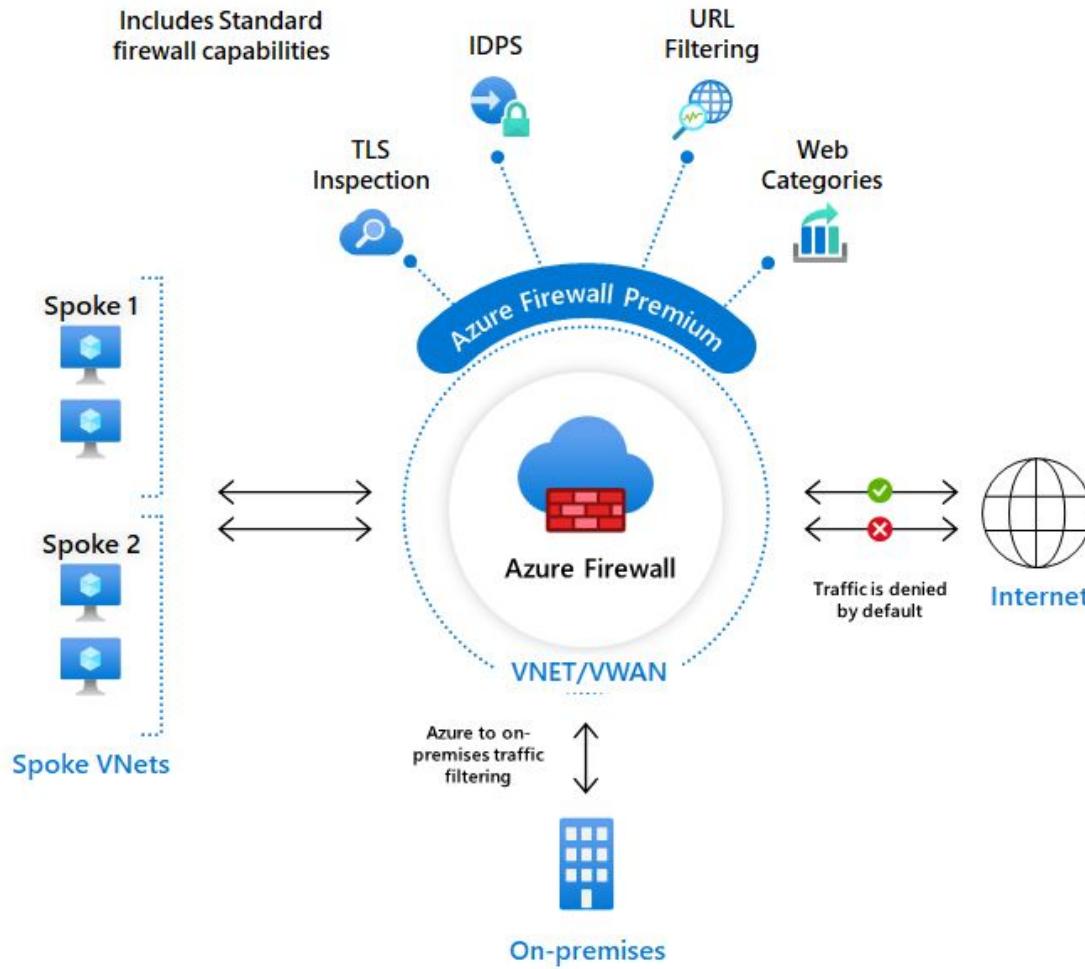
© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

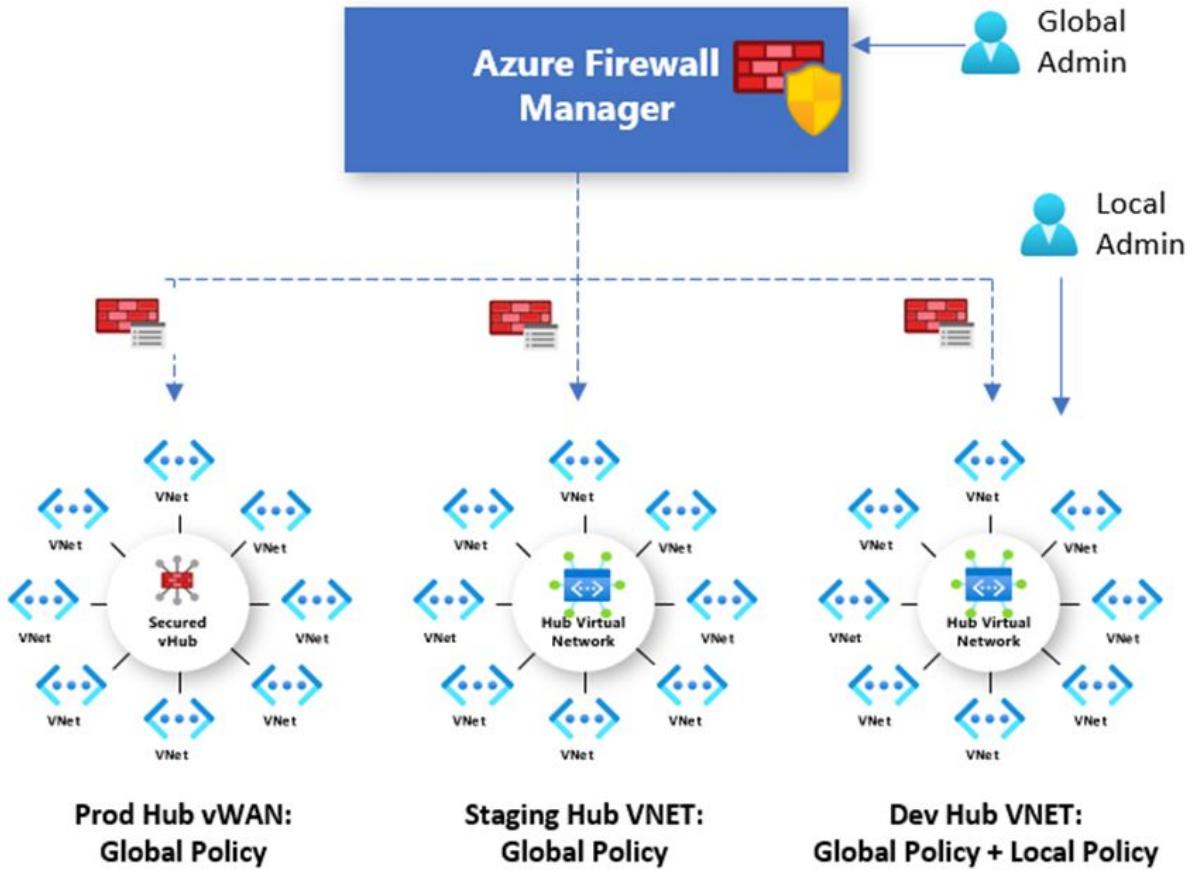
Describe the capabilities of Microsoft Security solutions (25—30%)

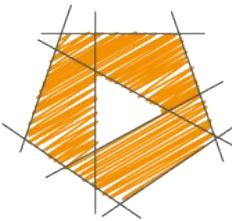
Describe basic security capabilities in Azure

- 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





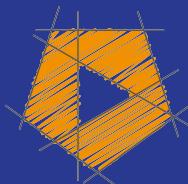




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

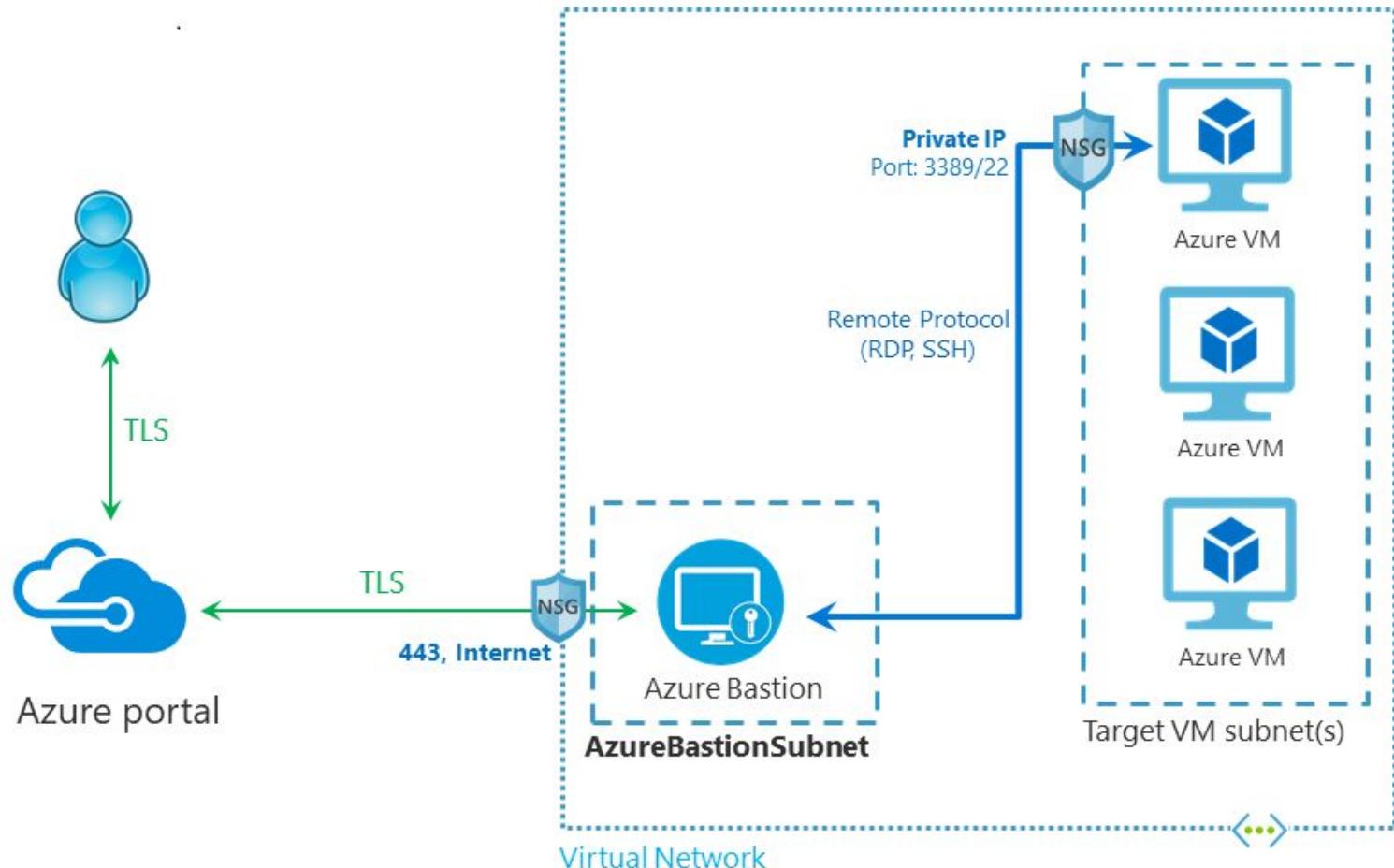


© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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



 Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Windows Admin Center (preview)

Disks

Size



This VM has a just-in-time access policy. Select "Request access" before co

[RDP](#) [SSH](#) [Bastion](#)

Connect with RDP

You need to request access to connect to your virtual machine. Select an IP number, and select "Request access". [Learn more](#)

IP address *

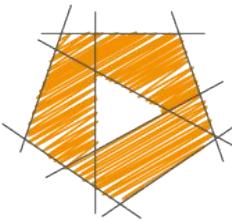
 Public IP address (20.224.194.134)

Port number *

 3389

Source IP

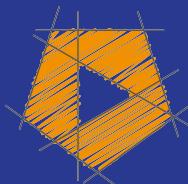
[My IP](#) [Other IP/ IPs](#) [All configured IPs](#)[Request access](#)[Download RDP file anyway](#)



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor

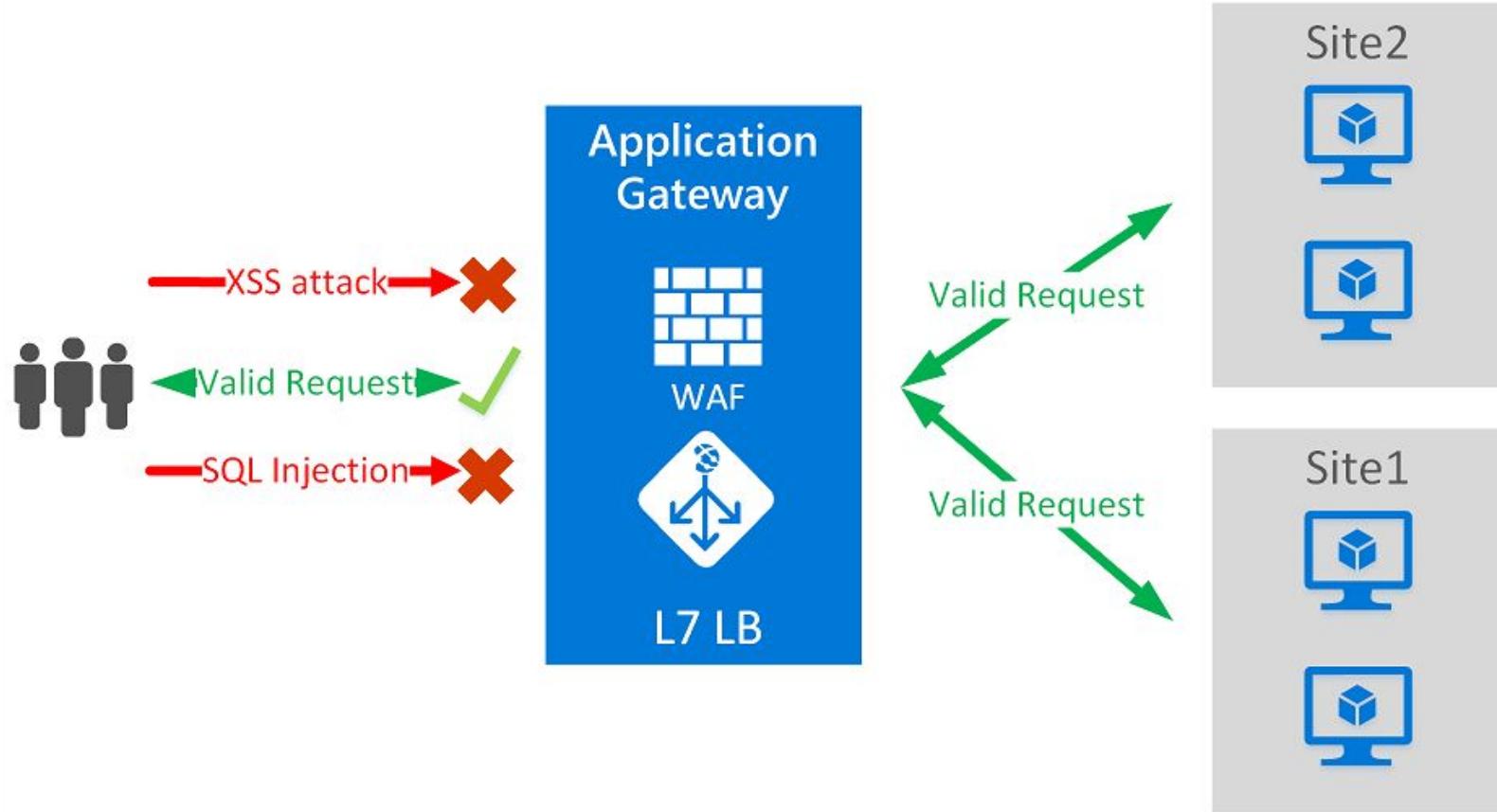


© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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)

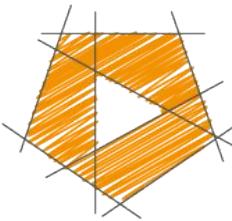
OWASP Rule Sets

Core Rule Sets 3.1, 3.0, and 2.2.9

Custom Rules

Geomatch Rules

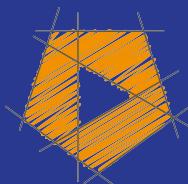




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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)

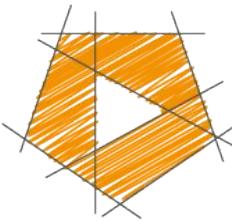
Azure Key Vault

Designed to securely store secrets, certifications and keys

Requires authenticated and authorized access to get key

Removes keys from common storage, code, source control

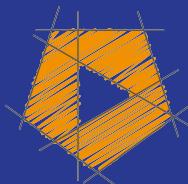
Can expire keys, generate new keys, etc.



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe security management capabilities of Azure

- Describe Cloud security posture management (CSPM)
- Describe Microsoft Defender for Cloud
- Describe the enhanced security features of Microsoft Defender for Cloud
- Describe security baselines for Azure

Azure Security Center

Infrastructure Security Management

Security Center | Overview

X

Showing 41 subscriptions

Subscriptions What's new

41
Azure subscriptions

1
AWS accounts

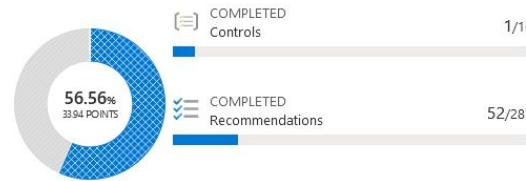
3
GCP projects

235
Active recommendations

112
Security alerts

Secure score

Current secure score



[Improve your secure score >](#)

Compliance

Current compliance by passed controls

HIPAA HITRUST	0/22
SOC TSP	1/13
ISO 27001	2/20
NIST SP 800 5...	3/29
PCI DSS 3.2.1	5/45

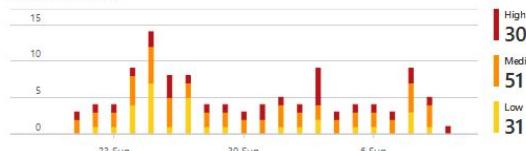
[Improve your compliance >](#)

Azure Defender

Resource Coverage

93% For full coverage turn on 8 resource bundles

Alerts by severity



[Enhance your threat protection capabilities >](#)

Inventory

Unmonitored vms

43 For a better protection of your org we recommend to install agents

Total Resources

2921

Unhealthy (1477) Healthy (1167) Not applicable (277)

[Explore your resources >](#)

Insights

Most prevalent recommendations (by resources)

Audit diagnostic setting	686
Disk encryption should be applied on virt...	118
A vulnerability assessment solution shou...	117
Secure transfer to storage accounts shou...	102

Controls with the highest potential increase

Remediate vulnerabilities	+11% (6pt)
Remediate security configurations	+6% (4pt)
Enable encryption at rest	+6% (4pt)

[View controls >](#)

Azure Security Center community

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback, and share knowledge about Security Center.

[View Azure Community >](#)

Security Center

Cloud Security Posture Management - assessments and recommendations

Cloud Workload Protection - protection

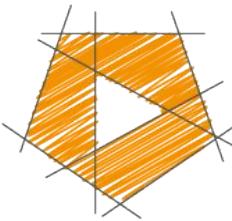
Supports PaaS Workloads like App Service Plans, Storage and SQL Servers



Free and paid
versions



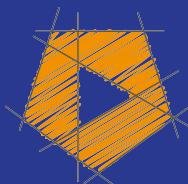
Protects Azure and
non-Azure
resources



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



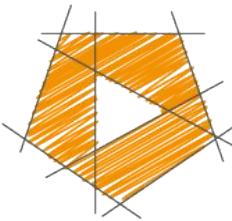
© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe security capabilities of Microsoft Sentinel

- Define the concepts of SIEM and SOAR
- Describe how Microsoft Sentinel provides integrated threat management

SIEM SOAR

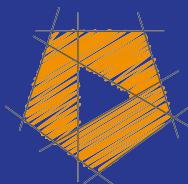
Collecting Data



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal



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 365 Defender services

Integrated Microsoft 365 Defender experience



Identity

Microsoft Defender
for Identity

+



Endpoints

Microsoft Defender
for Endpoint

+



Apps

Microsoft Cloud
App Security

+



Email/Collaboration

Microsoft Defender
for Office 365

Microsoft Cloud App Security
SaaS apps and data

Microsoft Defender for Endpoint
Devices

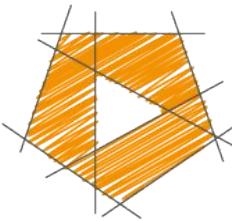
Microsoft Defender for Office 365
Microsoft 365 cloud apps and data

Identity

On-premises

Microsoft
Defender for
Identity

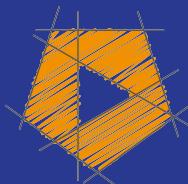
MFA
Conditional Access
Azure AD Identity Protection



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal

Formerly Advanced Threat Protection (ATP)

Azure AD Signals

Microsoft 365 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

License plans:

- 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

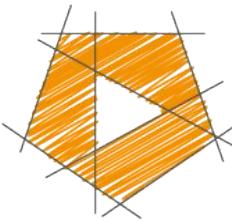
Atypical travel

Malware linked IP address

Leaked credentials

Password spray

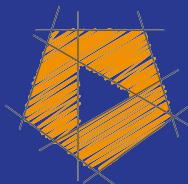
Inbox forwarding



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal



Formerly Office 365
Advanced Threat
Protection (ATP)

Microsoft 365 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

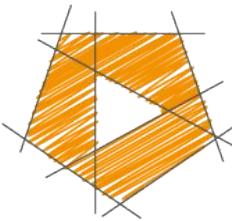
Plan 1

- 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...

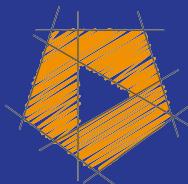
- Threat Trackers
- Threat Explorer
- Automated investigation and response (AIR)
- Attack Simulator



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal

Formerly Microsoft Defender Advanced Threat Protection (ATP)

Microsoft 365 Defender for Endpoint

Endpoints are “devices”

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

Microsoft Defender for Endpoint



Threat and
Vulnerability
Management



Attack surface
reduction



Next
generation
protection



Endpoint
detection
and response



Automated
investigation and
remediation

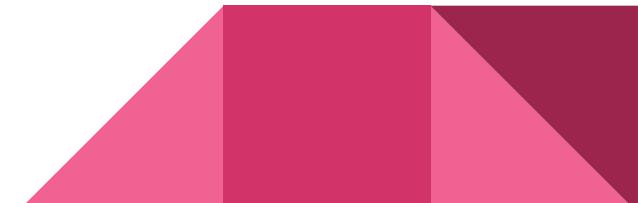


Microsoft
Threat Expert

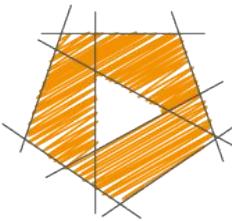
Centralized configuration, administration, and APIs

M365 Defender for Endpoint

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



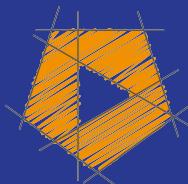
Microsoft Secure Score for Devices



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

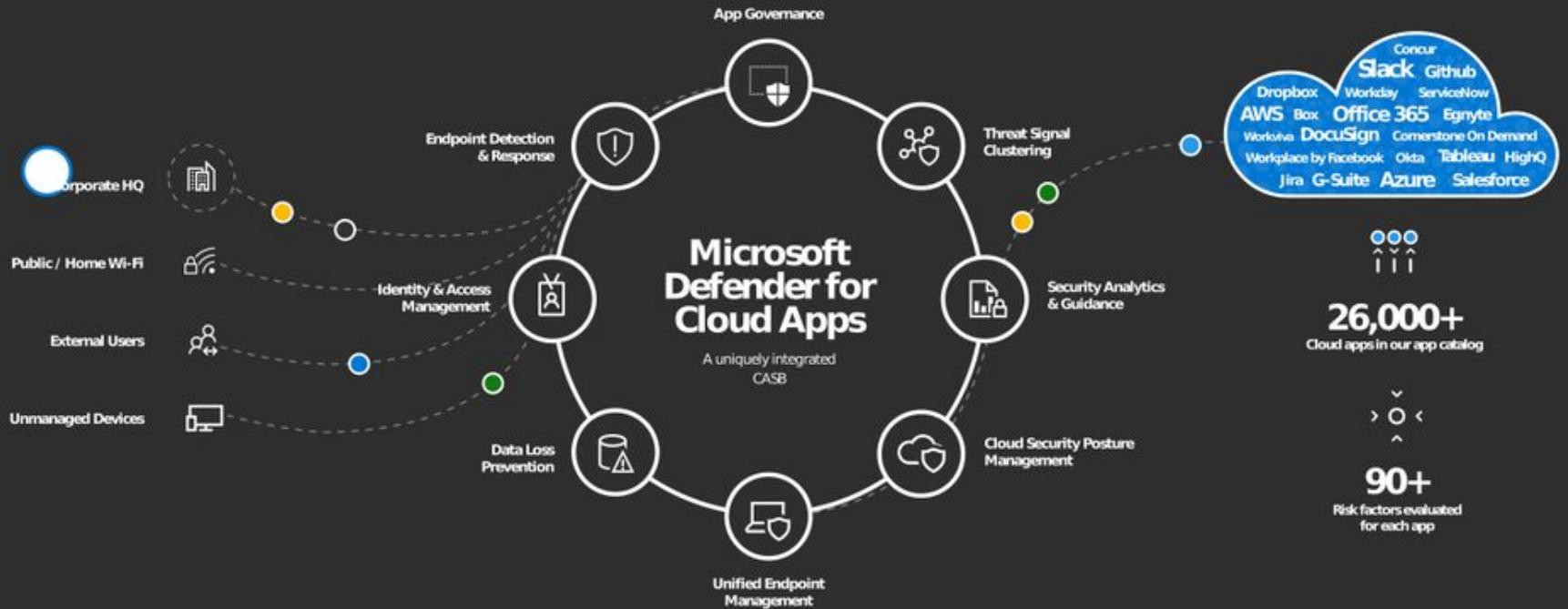
Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal



Microsoft Defender for Cloud Apps (CASB)

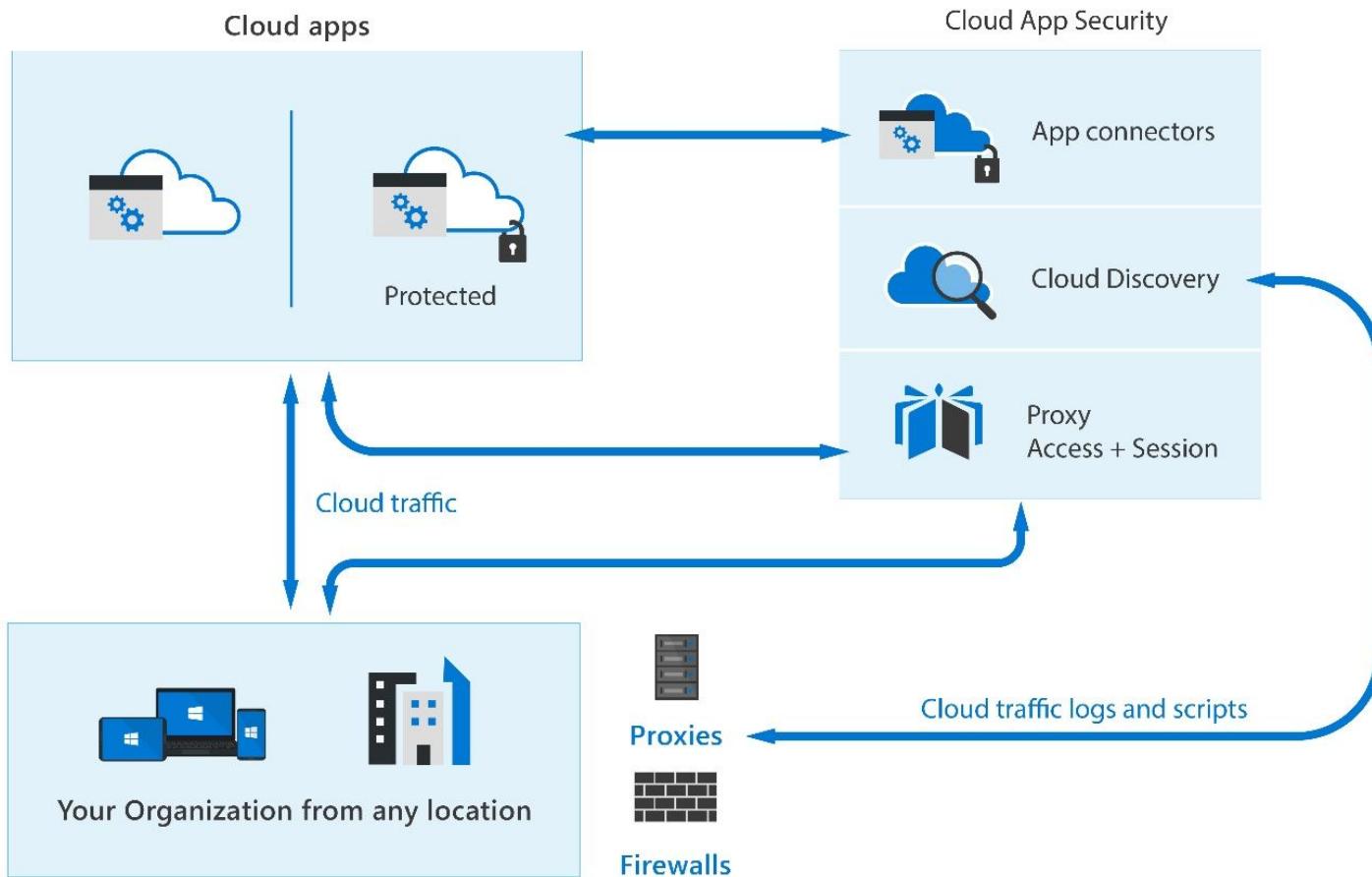
CAS Security Framework

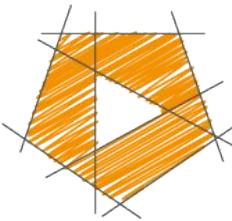
0365 CAS

Enhanced Cloud App Discovery in AAD

CAS architecture

Discover Shadow IT

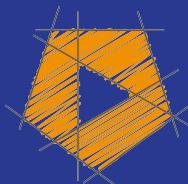




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe threat protection with Microsoft 365 Defender

- Describe Microsoft 365 Defender services
- Describe Microsoft Defender for Identity (formerly Azure ATP)
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
- Describe Microsoft Defender for Cloud Apps
- Describe the Microsoft 365 Defender portal

Microsoft 365 Defender Portal



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

Microsoft 365 Defender Portal

Microsoft Microsoft 365 Defender | contosohotels.com

Home

Incidents & alerts

Threat analytics

Secure score

Learning hub

Endpoints

Vulnerability management

Partners and APIs

Evaluation & controls

Email & collaboration

Investigations

Explorers

Submissions

Review

Campaigns

Threat tracker

Attack simulation training

Policies & rules

Cloud apps

Microsoft 365 Defender | contosohotels.com

Threat analytics

2 active threats

MOBILK/M mass email campaign (1)

Using off-the-shelf binaries (2)

Credentials Management API abuse (3)

Active alerts: 1 Recovered alerts: 0 No alert: 0

See more

Users at risk

88 users at risk

High Risk (1) Medium Risk (1) Low Risk (1)

View all users

Active incidents

112 active incidents

Newest for last 10 days

Unsuccessful cloud app access was blocked on multiple endpoint

Activity from infrequent country involving one user

'Minikatz' detected on multiple endpoints

Malicious credential theft tool execution detected on one endpoint

incident name Tag Severity Last activity Scope

Unsuccessful cloud app access was blocked on multiple endpoint #000000; background-color: #ff0000;">High Immediate Dec 15, 2021 12:22... A2 R1 G1

Activity from infrequent country involving one user #000000; background-color: #ff0000;">High Medium Dec 16, 2021 12:08... A3 R1 G1

'Minikatz' detected on multiple endpoints #000000; background-color: #ff0000;">High High Dec 16, 2021 12:08... A2 R6 G1

Malicious credential theft tool execution detected on one endpoint #000000; background-color: #ff0000;">High High Dec 16, 2021 12:08... A1 R1 G1

View all incidents

Device health

Active Devices: 682

Device health state

Misconfigured (0) Invalid (12,602)

Devices at risk

10 device(s) at risk

Device Risk level

Not prioritized (1) Moderate (1) High (3)

Discovered devices

Total discovered devices: 14.1k

IoT devices (1) Endpoints (14,085) High value devices (3)

Microsoft 365 Defender

A hub for threat intelligence, product news, security intelligence, and threat research.

Microsoft Security Intelligence

We updated our blog on the CVE-2021-44229 Log4j vulnerability with details about reconnaissance attacks on non-Microsoft-hosted Minecraft servers, as well as additional product guidance, including Threat and Vulnerability Management insight. #0015221UV

[Updated 12/16/2021] Guidance for preventing, detecting, and responding to attacks on non-Microsoft-hosted Minecraft servers, as well as additional product guidance, including Threat and Vulnerability Management insight. #0015221UV

View

- 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



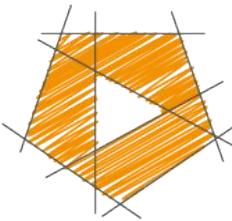
Incidents

[Create a notification rule](#)

Most recent incidents and alerts

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

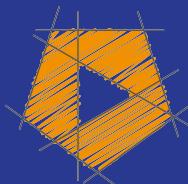
✓	Incident name	Tags	Severity	Investigation state
>	Multi-stage incident involving Initial access & Exfiltration on one endpoint ...	asdf tag test02	High	2 investigation states
>	Multi-stage incident involving Initial access & Exfiltration on multiple endp...	asdf tag test02 IT Team +3	High	2 investigation 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



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe endpoint security with Microsoft Intune

- describe what Intune is
- describe endpoint security with Intune
- describe the endpoint security with the Microsoft Endpoint Manager admin center

Intune

Microsoft Intune - device management

How phones, tablets, laptops connect to your environment

- MDM (company-owned)
- MAM (personal devices)

Endpoint Security with Intune

Manage devices

Security baselines - predefined settings for applications

Policies - device security

Device compliance - when a device is allowed (or not allowed)

Conditional access - risk factors

Integration with Microsoft Defender for Endpoint - Android, iOS, Windows 10+

RBAC

Endpoint Security with admin center

Security tasks for at-risk devices

Microsoft Endpoint Manager admin center

Home > Endpoint security | Overview

Search (Ctrl + /)

Overview

All devices

Security baselines

Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Setup

Microsoft Defender for Endpoint

Help and support

View Security Baselines

Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender for Endpoint to help prevent security breaches and gain visibility into your organization's security posture



Microsoft recommended security settings
Assign baselines quickly and securely using our recommended settings.

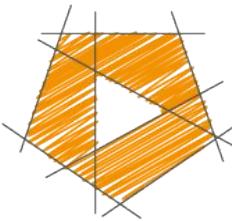
Simplified security policies
Select any of the following categories to jump right in and start securing your devices.

Remediate endpoint weaknesses
Remediate endpoint vulnerabilities reported by Microsoft Defender for Endpoint and Threat and Vulnerability Management.

View security tasks

Microsoft Defender for Endpoint

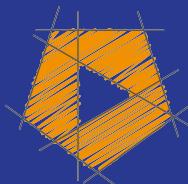
Antivirus
Disk encryption
Firewall
Attack surface reduction
Endpoint detection and response
Account protection



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft compliance solutions (25–30%)

Describe Microsoft's Service Trust Portal and privacy principles

- Describe the offerings of the Service Trust portal
- Describe Microsoft's privacy principles

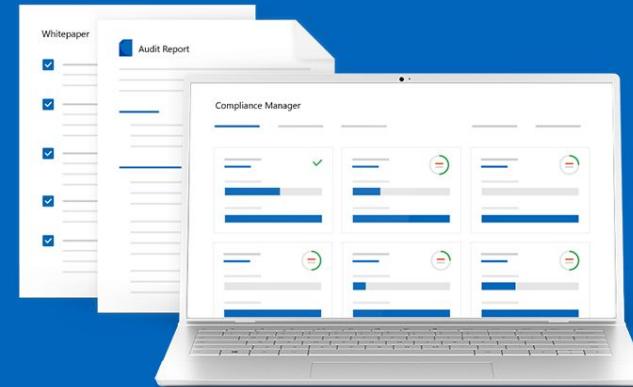
Service Trust Portal



<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 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.

[More Documents & Resources >](#)

Pen Tests & Security Assessments

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

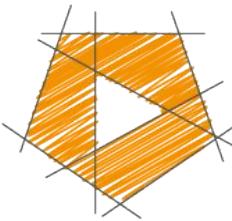
Azure Blueprints

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

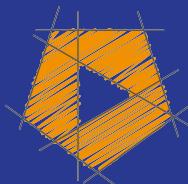




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe the capabilities of Microsoft compliance solutions (25–30%)

Describe Microsoft's Service Trust Portal and privacy principles

- Describe the offerings of the Service Trust portal
- Describe Microsoft's privacy principles

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



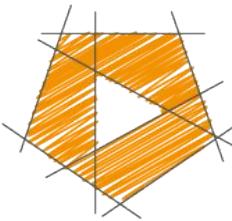
Respecting local
privacy laws and
fighting for privacy



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



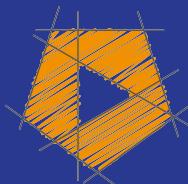
They only collect
data to make your
experience better



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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



“a unified data governance service that helps you manage your on-premises, multi-cloud, and software-as-a-service (SaaS) data.”

Purview Features:

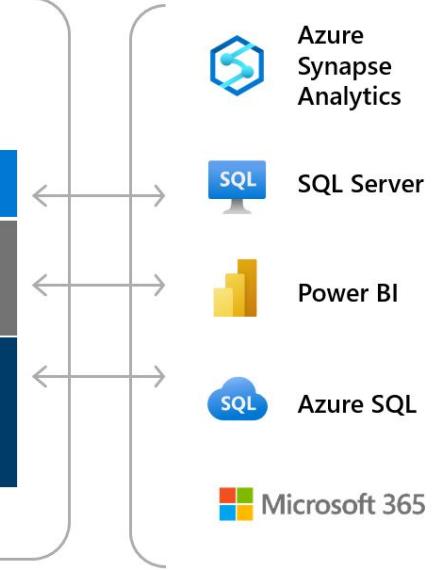
- Up-to-date map of your data landscape
 - Data discovery
 - Sensitive data classification
 - End-to-end data lineage
- Enable data curators to manage and secure data
- Empower data consumers to find valuable, trustworthy data



Microsoft Purview governance portal

On-premises
Cloud
SaaS Applications

Data Producers and Consumers		Data Officers	
Data Catalog Enable effortless data discovery	Data Sharing Share data within and between organizations	Data Estate Insights Access data estate health	Data Policy Govern access to data
Data Map Automate and manage metadata at scale			



Generally Available

Preview

Compliance Portal



Help understand
and manage an
organization's
compliance needs

Compliance center

Compliance score

Solution catalog

Active alerts

The screenshot shows the Microsoft 365 Compliance Center homepage. At the top right, there's a navigation bar with icons for Home, Back, Forward, Stop, Refresh, and a search bar. The URL https://compliance.microsoft.com/homepage is visible. The main header reads "Welcome to the Microsoft 365 compliance center". Below the header, there's a "Cloud icon" graphic with a key and a checkmark. A sidebar on the left lists various compliance-related sections: Home, Compliance Manager, Data classification, Data connectors, Alerts, Reports, Policies, and Permissions. Under "Solutions", there are links for Catalog and Records management. At the bottom of the sidebar, there are "Settings" and "More resources" sections, along with a "Customize navigation" link. The main content area features a large "Compliance Manager" section with the heading "Your compliance score: 69%" and a brief description of what it does. It includes two progress bars: "Protect information" at 27 / 928 and "Govern information" at 0 / 144. To the right, there's a "Solution catalog" section with the heading "Discover solutions for your compliance needs" and a brief description. There are "Need help?" and "Give feedback" buttons at the bottom.

<https://compliance.microsoft.com/>



Helps to manage an organization's compliance requirements

Compliance manager

Prebuilt assessments

Workflow capabilities

Step-by-step improvement actions

Compliance score

The screenshot shows the Microsoft 365 Compliance Manager interface for Contoso Electronics. The left sidebar includes Home, Compliance Manager (selected), Data classification, Data connectors, Alerts, Reports, Policies, Permissions, Solutions, Catalog, Records management, Settings, More resources, and Customize navigation. The main content area is titled "Compliance Manager" and displays an overall compliance score of 69%. A gauge chart indicates 14370/20566 points achieved. Below the score, it says "Your compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards." It also shows "Your points achieved: 57" and "Microsoft managed points achieved: 14213". A table lists "Key improvement actions" with columns for Improvement action, Impact, Test status, Group, and Action type. Actions include: Enable self-service password reset, Create mail flow rules to encrypt messages, Automatically apply Client Side Sensitivity La..., Conceal information with lock screen, UseIRM for Exchange Online, UseIRM for OneDrive for Business, Implement DMARC for outbound mail, Set up Sender Policy Framework to prevent s..., and Use boundary protection devices for unclassi... The total count is 496 actions, with 3 completed and 0 out of scope.

Compliance score

Helps an organizations:

Understand its current compliance posture

Prioritize actions based on their potential to reduce risk

Compliance score

Overall compliance score

Your compliance score: 69%



14370/20566 points achieved

Your points achieved ⓘ

57/6253

Microsoft managed points achieved ⓘ

14313/14313

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Key improvement actions

Not completed | Completed | Out of scope

496

3

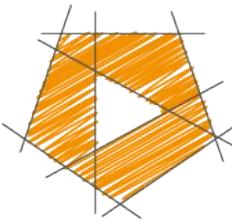
0

Improvement action

Impact

Enable self-service password reset	+27 points
Create mail flow rules to encrypt messages	+27 points
Automatically apply Client Side Sensitivity La...	+27 points
Conceal information with lock screen	+27 points
Use IRM for Exchange Online	+27 points
Use IRM for OneDrive for Business	+27 points
Implement DMARC for outbound mail	+27 points
Set up Sender Policy Framework to prevent s...	+27 points
Use boundary protection devices for unclassi...	+27 points

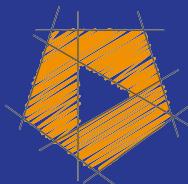
[View all improvement actions](#)



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



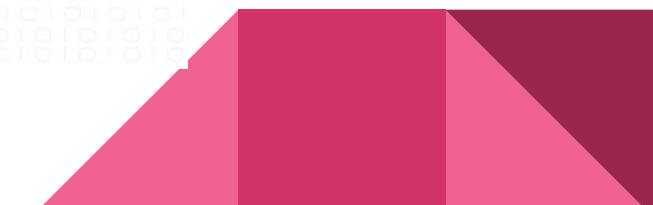
© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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 Policies 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

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

 Search for specific categories or labels

All locations > SharePoint Online > redmondhq.contoso.com >

Sensitive labels 

General 345

Confidential 344

MnA Legal Top Secret 34

 Manage label definition

  Name  Sensitive info types

 DLP test policy  Credit Card Number +6 more

  Contoso Ignite trip pla...  Credit Card Number +3 more

Activity Explorer

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

Activity Explorer

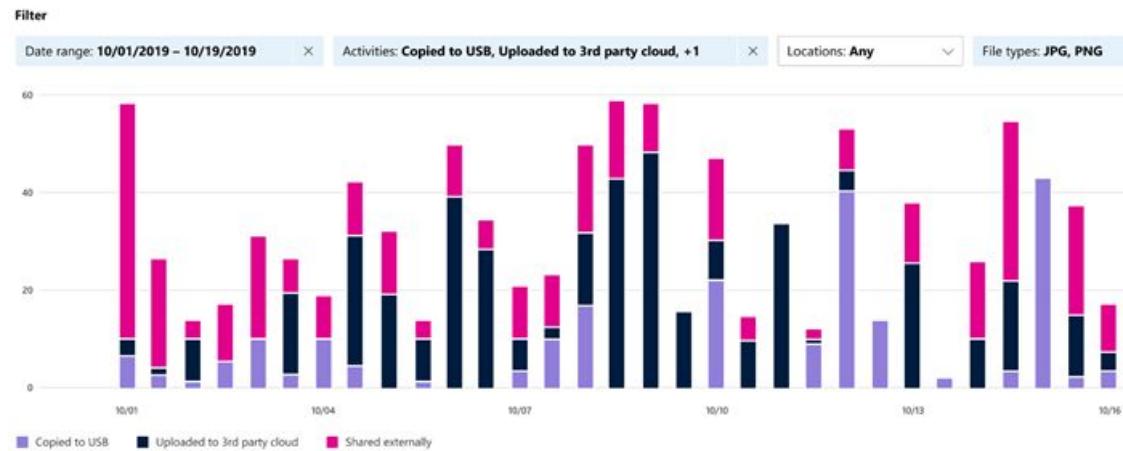
Some activity types that can be analyzed:

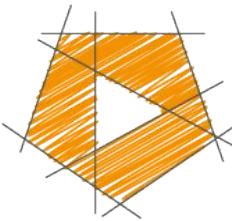
File copied to removable media

File copied to network share

Label applied

Label changed

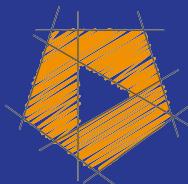




GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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 Policies and Retention Labels

Sensitivity labels

Sensitivity labels

Customizable

Clear text

Persistent

Try the Preview Search

Home Organize Tools

New Email New Items Delete Archive Reply Reply All Forward Move Junk Rules OneNote Tags Filter Email Find a Contact Address Book Send & Receive Store MyAnalytics

Inbox Drafts Archive Sent Groups Trash Junk Clutter Conversation History Smart Folders

Focused Other By: Conversations

Today

Marketing material 1:17 PM
Hi Kartik & Mas, Please publish the following mes...

Marketing material Wednesday, September 19, 2018 at 1:17 PM [Show Details](#)

Public [Learn more](#)

Please publish the following message to our public blog:

Sensitivity Labels

You can apply a sensitivity label to your documents and emails to keep them compliant with your organization's information protection policies.

1. In the Home tab, select **Sensitivity**.
2. Choose the sensitivity label that applies to your document or email.

AutoSave OFF

FinancialReport

Search Sheet

Home Insert Draw Page Layout Formulas Data Review Tell me what you want to do Share

Paste Cut Copy Undo Redo Find & Select Conditional Formatting Format as Table Cells Editing

D12 fx 80083

A B C D E F

	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						

Sheet1 +

Ready Highly Confidential

120%

Public
General
Confidential
 Highly Confidential
Learn More...

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

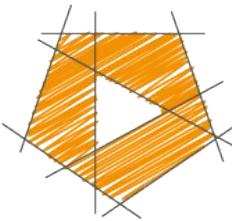
Choose the users and groups that can see labels

Apply a default label to all new emails and documents

Require justifications for label changes

Require users to apply a label (mandatory labeling)

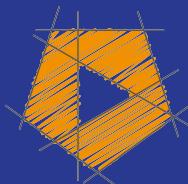
Link users to custom help pages



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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 Policies 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

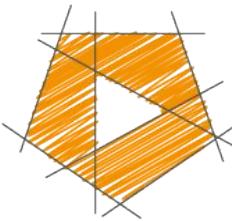
Retention policies

Applied at site or mailbox level

Applied to multiple locations, specific locations or users

Items inherit the retention settings from their container

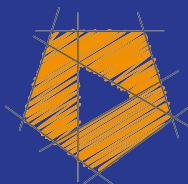
If an item is moved, the retention setting doesn't travel to new location



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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 Policies 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

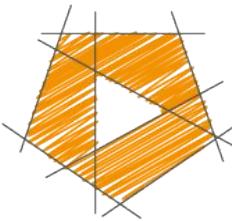
Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. [Learn more](#)

Mark items as a regulatory record

At the end of the retention period

Delete items automatically

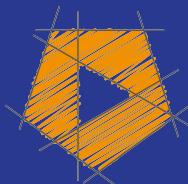
We'll delete items from where they're currently stored.



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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 Policies 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

Data loss prevention policy

Locations
to apply
the policy

Rule 1

Conditions

Actions

Rule 2

Conditions

Actions

Rule n...

Conditions

Actions

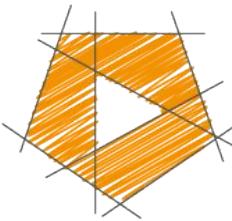
Endpoint Data Loss Prevention

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

Creating an item

Renaming an item

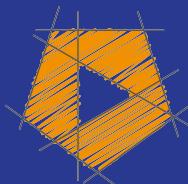
Copying items to removable media



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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

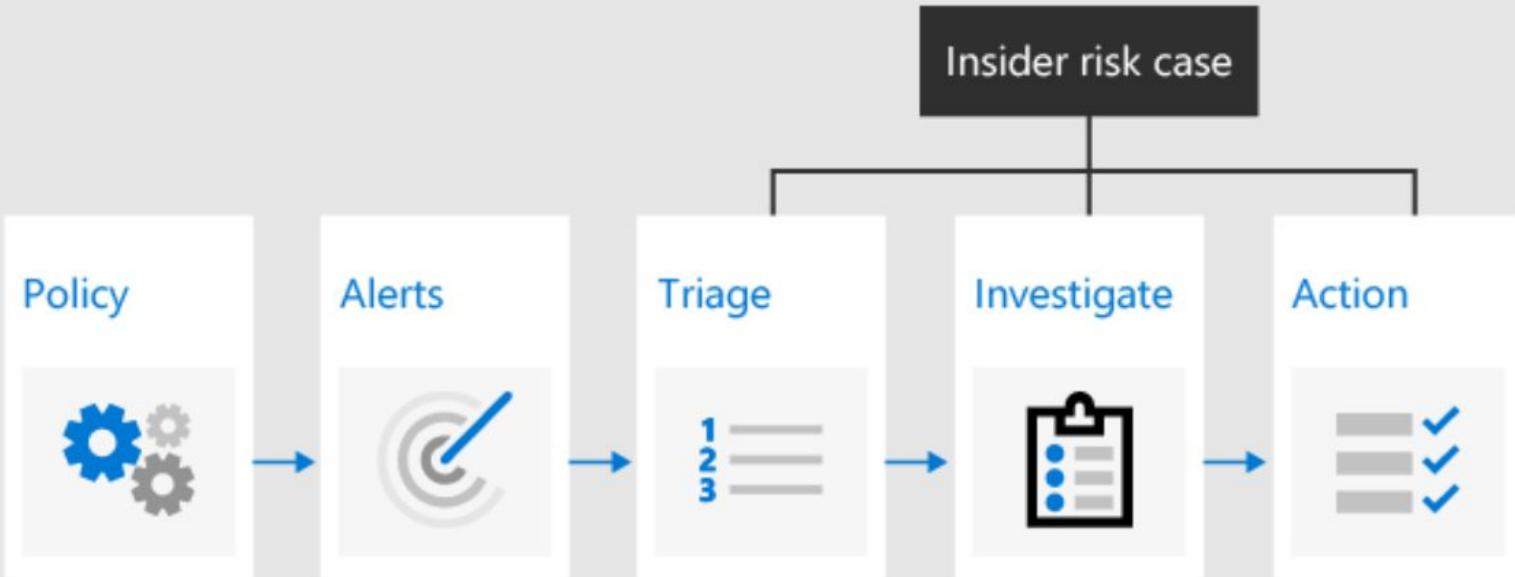


Leaks of sensitive data and data spillage

Confidentiality violations

Intellectual property (IP) theft



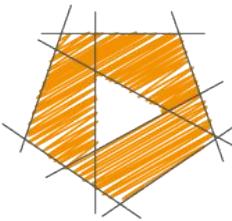


Insider risk case

Collaboration
Compliance, Human Resources, Legal, Security

Four Insider Risk solutions in M365:

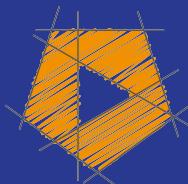
- Communication compliance
- Insider risk management
- Information barriers
- Privileged access management



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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

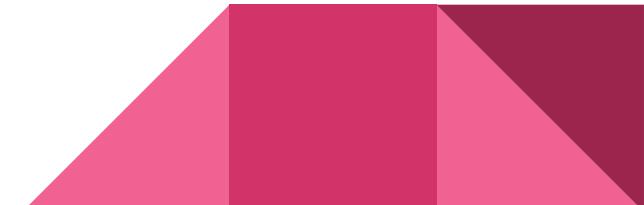
Inappropriate Communications

Profanity

Threats

Harassment

Sharing sensitive information inside and outside your organization





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



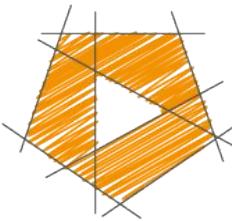


Configure

Investigate

Remediate

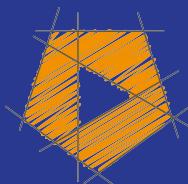
Monitor



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

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

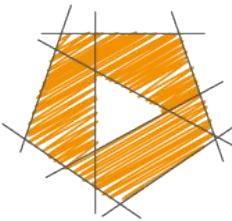
Can prevent the following in Teams:

Searching for a user

Adding a member to a team

Starting a chat session with someone

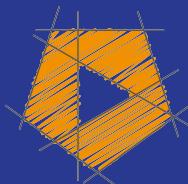
And more..



GetCloudSkills
.com

SC-900 Microsoft Security, Compliance, and Identity Fundamentals

Scott Duffy, Instructor



© 2022-2023 Scott Duffy, getcloudskills.com... get the course for these slides at:
<http://sjd.ca/sc900>

Describe resource governance capabilities in Azure

- describe the use of Azure Resource locks
- describe what Azure Blueprints is
- define Azure Policy and describe its use cases



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

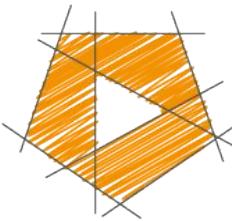
Azure Policy responses

Deny a change to a resource

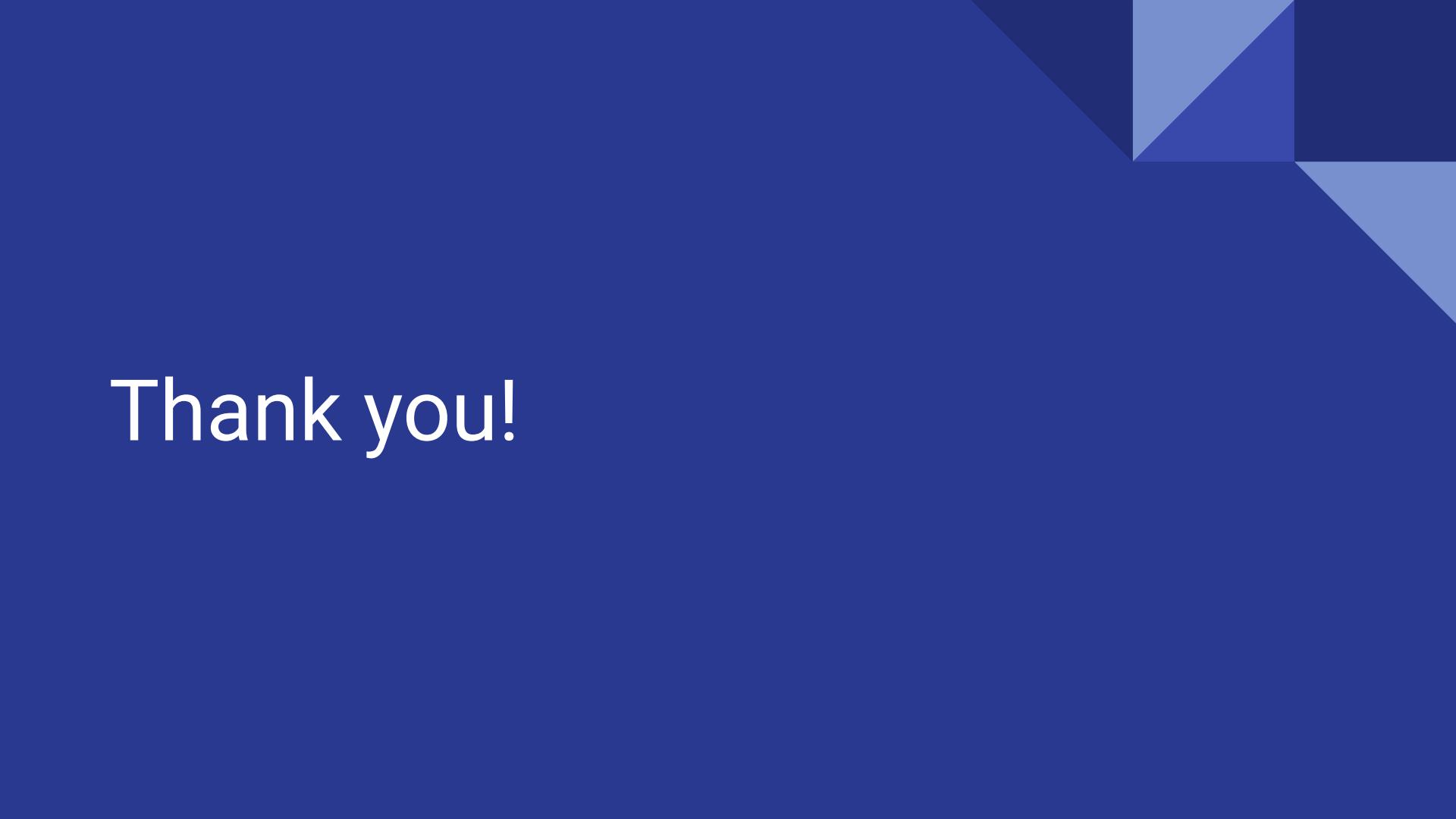
Log changes to a resource

Alter a resource before or after a change

Deploy related compliant resources



GetCloudSkills
.com

The background of the slide features a large, solid dark blue rectangle. Overlaid on the bottom right corner is a smaller, light blue triangle pointing upwards and to the left. Above it is a dark blue triangle pointing downwards and to the right. To the right of the light blue triangle is a dark blue rectangle. The overall effect is a minimalist, modern graphic.

Thank you!