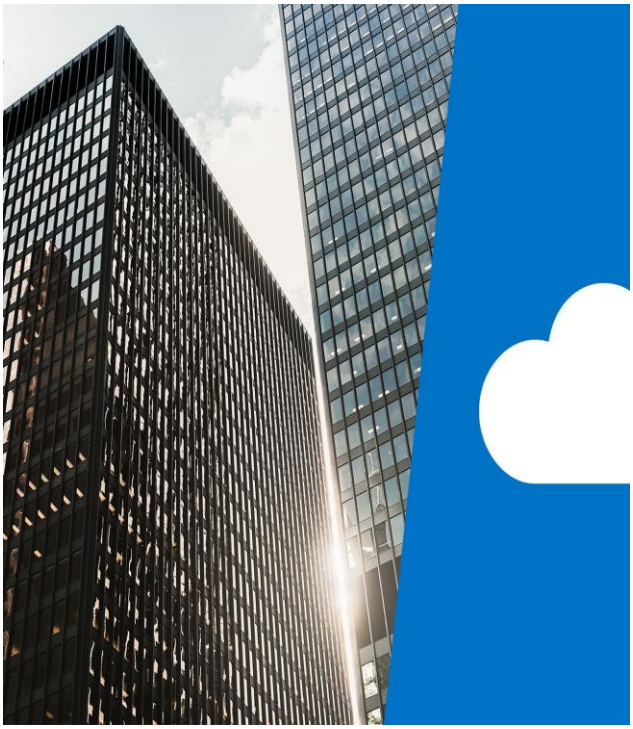
Microsoft

AZ-900T01: Module 03: Security, privacy, compliance, and trust



1

Lesson 01: Learning objectives

2

Module 3 – Learning objectives

- Understand and describe how to secure network connectivity in Microsoft Azure.
- Understand and describe core Azure identity services.
- Understand and describe security tools and features.
- Understand and describe Azure governance methodologies.
- Understand and describe monitoring and reporting in Azure.
- Understand and describe privacy, compliance, and data protection standards in Azure.

3

Lesson 02: Securing network connectivity in Azure

4

Azure Firewall

- A *firewall* is a service that grants server access based on the originating IP address of each request
- *Azure Firewall* is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.
- Azure Firewall includes many features, including:
  - Built-in high availability
  - Unrestricted cloud scalability
  - Inbound and outbound filtering rules
  - Azure Monitor logging

5

Azure DDoS protection

- *Distributed denial of service* (DDoS) *attacks* attempt to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users.
- Azure DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability.
- Azure DDoS Protection provides the following service tiers:
  - Basic. The Basic service tier is automatically enabled as part of the Azure platform.
  - Standard. The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources.

6

Network security groups

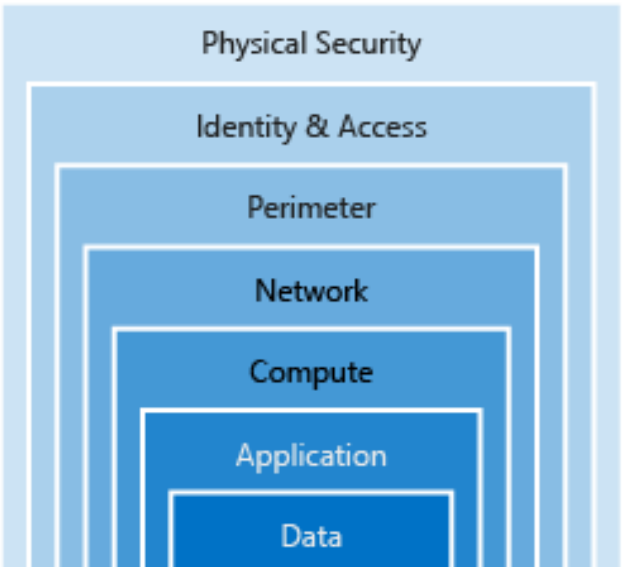
- *Network Security Groups* (NSGs) allow you to filter network traffic to and from Azure resources in an Azure virtual network. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.
- Network security rule properties:
  - A network security group can contain as many rules as you want within Azure subscription limits.
  - When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You cannot remove the default rules, but you can override them by creating new rules with higher priorities.

7

Choosing Azure network security solutions

Defense in Depth

A layered approach that provides multiple levels of protection so that if an attacker gets through one layer there are further protections in place. A common security concept that is applied to computing systems is *defense in depth*, which is essentially a layered approach to providing security.



8

Choosing Azure network security solutions - layers

- Perimeter layer. The network perimeter layer is about protecting organizations from network-based attacks against your resources. Some options are to use Azure DDoS Protection and Azure Firewall.
- Networking layer. At this layer, the focus is on limiting network connectivity across all your resources and only allowing what is required. Some options are deny by default, restrict inbound internet access, and limit outbound.
- Combining services. You can also combine multiple Azure networking and security services. Some examples are:
  - Network security groups and Azure Firewall
  - Application Gateway WAF and Azure Firewall.

9

Choosing Azure network security solutions - layers

Shared responsibility

As computing environments move from customer-controlled datacenters to cloud datacenters, the responsibility for security also shifts. Security is now a concern shared by cloud providers and customers.

Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory Infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

10

Lesson 03: Core Azure identity services

11

Authentication and authorization

Two fundamental concepts that should be understood when talking about identity and access are authentication and authorization:

- *Authentication* is the process of establishing the identity of a person or service looking to access a resource. It involves the act of challenging a party for legitimate credentials, and provides the basis for creating a security principal for identity and access control use. It establishes if they are who they say they are.
- *Authorization* is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

12

Azure Active Directory

- *Azure Active Directory (Azure AD)* is a Microsoft cloud-based identity and access management service. Azure AD helps employees of an organization sign in and access resources.
- Azure AD provides services such as:
  - Authentication
  - Single sign-on (SSO)
  - Application management
  - Business to business (B2B) identity services
  - Business-to-Customer (B2C) identity services

13

Azure Multi-Factor Authentication

Azure Multi-Factor Authentication (MFA) provides additional security for your identities by requiring two or more elements for full authentication. These elements fall into three categories:

- *Something you know:* This could be a password or the answer to a security question.
- *Something you possess:* This might be a mobile app that receives a notification, or a token-generating device.
- *Something you are:* This is typically some sort of biometric property, such as a fingerprint or face scan used on many mobile devices.

14

Lesson 04: Security tools and features

15

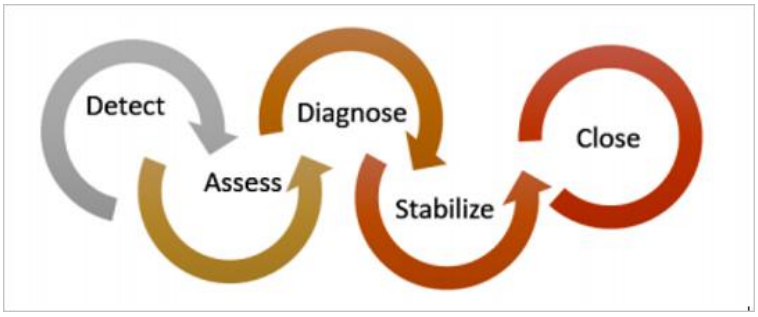
Azure Security Center

- *Azure Security Center* is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises.
- Azure Security Center can:
  - Provide security recommendations based on your configurations, resources, and networks.
  - Monitor security settings across on-premises and cloud workloads, and automatically apply required security to new services as they come online.

16

Azure Security Center usage scenarios

- You can use Security Center in the *detect*, *assess*, and *diagnose* stages of an incident response.



- Use Security Center recommendations to enhance security.

17

Azure Key Vault

- *Azure Key Vault* is a centralized cloud service that you use for storing application secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and providing secure access, permissions control, and access logging.
- Key Vault usage scenarios:
  - Secrets management
  - Key management
  - Certificate management
  - Store secrets backed by hardware security modules (HSMs)

18

Azure Information Protection

- *Microsoft Azure Information Protection* is a cloud-based solution that helps organizations classify and optionally help protect its documents and emails by applying labels. Labels can be applied:
  - Automatically by administrators who define rules and conditions
  - Manually by users
  - A combination of the two, where users are given recommendations
- Usage scenario:
  1. A user saves a Microsoft Word document containing a credit card number.
  2. A custom tooltip displays recommending that the file be labelled *Confidential\All Employees*, which is the label that the administrator has configured.
  3. This label classifies the document and protects it.

19

Azure Advanced Threat Protection

- *Azure Advanced Threat Protection* (Azure ATP) is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- Azure ATP consists of the following components:
  - Azure ATP portal. Azure ATP has it's own portal through which you monitor and respond to suspicious activity
  - Azure ATP sensor: Azure ATP sensors are installed directly on your domain controllers.
  - Azure ATP cloud service. Azure ATP cloud service runs on Azure infrastructure.

20

Lesson 05: Azure governance methodologies

21

Azure Policy

- *Azure Policy* is a service in Azure that you use to create, assign, and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements (SLAs).
- With *Azure Policy, provides the following:*
  - *Azure Policy* uses policies and initiatives to run evaluations of your resources and scans for those not compliant with the policies you have created.
  - *Azure Policy* comes with a number of built-in policy and initiative definitions that you can use, under categories such as Storage, Networking , Compute, Security Center, and Monitoring.

22

Policies

Applying a policy to your resources consist of the following steps:

1. Create a policy definition.
2. Assign a definition to a scope of resources.
3. View policy evaluation results.

23

Initiatives

- Initiatives work alongside policies in Azure Policy, and are made up of:
  - *Initiative definition*. A set of policy definitions to help track your compliance state for a larger goal, which simplify the process of managing and assigning policy definitions by grouping a set of policies as one single item.
    - Example. You could create an initiative named *Enable Monitoring in Azure Security Center*, with a goal to monitor all the available security recommendations in your Azure Security Center.
  - *Initiative assignments*. Initiative definitions assigned to a specific scope.

24

Role-based access control

- Role-based access control (RBAC) provides fine-grained access management for Azure resources:
  - Grant users only the rights they need to perform their jobs
  - Provided at no additional cost to all Azure subscribers
- Examples of when you might use RBAC include when you want to:
  - Allow one user to manage VMs in a subscription, and another user to manage virtual networks.
  - Allow a database administrator (DBA) group to manage Microsoft SQL Server databases in a subscription.
  - Allow a user to manage all resources in a resource group, such as VMs, websites, and subnets.

25

Locks

Locks help you prevent accidental deletion or modification of your Azure resources. You manage these locks from within the Azure portal.

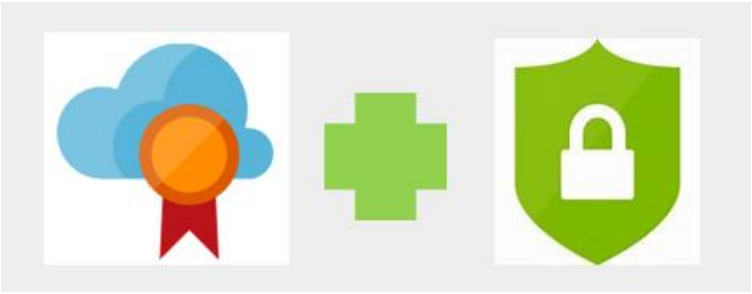
You may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to:

- CanNotDelete. Authorized users can still read and modify a resource, but they can't delete the resource.
- ReadOnly. Authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

26

Azure Advisor security assistance

- Azure Advisor provides security recommendation by integrating with Azure Security Center.
- View the security recommendations on the **Security** tab of the Advisor dashboard.
- Click deeper into the Security Center recommendations to improve and enhance your security governance.



27

Azure Blueprints

- *Azure Blueprints* enable cloud architects to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements.
- Usage Scenarios:
  - Use Azure Blueprints' artifacts and tools to help with auditing, traceability, and compliance with your deployments.
  - Use with Azure DevOps scenarios, where blueprints are associated with specific build artifacts and release pipelines, and require more rigorous tracking.

28

Lesson 06: Monitoring and reporting in Azure

29

Azure Monitor

- *Azure Monitor* maximizes the availability and performance of applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from cloud and on-premises environments.
- As soon as you create an Azure subscription and start adding resources, Azure Monitor starts collecting data:
  - Activity Logs. Record when resources are created or modified.
  - Metrics tell. Show how the resource is performing and the resources that it's consuming.
- You can extend the data you're collecting into the actual operation of the resources by enabling **Diagnostics** under the resource settings, and adding an agent to compute resources.

30

Azure Service health

- *Azure Service Health* is a suite of experiences that provide personalized guidance and support when issues with Azure services arise. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved.
- Azure Service Health is composed of:
  - Azure Status. Provides a global view of the health state of Azure services.
  - Service Health. A customizable dashboard that tracks the state of Azure services in the regions where you use them.
  - Azure Resource Health: Diagnose and obtain support when an Azure service issue affects your resources.

31

Monitoring applications and services

- Data monitoring is only useful if it can improve your visibility into the operations of your computing environment. Azure Monitor integrates with other Azure services to provide robust monitoring capabilities.
- You can loosely categorize monitoring into four categories:
  - Analyze. Use Azure Monitor for containers and virtual machines, and Azure Application Insights for applications.
  - Respond. Proactively respond to critical conditions identified in the data that it collects using Azure Alerts, or Auto-scale using Azure Monitor metrics.
  - Visualize: Visualize items such as charts and tables, or Power BI.
  - Integrate: Integrate Azure Monitor with other systems and build custom solutions.

32

Lesson 07: Privacy, compliance and data protection standards in Azure

33

Compliance Terms and Requirements

Microsoft provides the most comprehensive set of compliance offerings (including certifications and attestations) of any cloud service provider. Some compliance offering include:

CJIS (Criminal Justice Information Services)	**HIPAA** (Health Insurance Portability and Accountability Act)
CSA STAR Certification	**ISO/IEC 27018**
General Data Protection Regulation (GDPR)	**National Institute of Standards and Technology (NIST)**

You can view all the Microsoft compliance offerings at Microsoft Compliance Center - Compliance Offerings.

34

Microsoft privacy statement

- Explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.
- Applies to the interactions Microsoft has with users and Microsoft products such as Microsoft services, websites, apps, software, servers, and devices.
- Is intended to provide openness and honesty about how Microsoft deals with personal data in its products and services.

For more information, review the privacy statement at Microsoft Privacy Statement.

35

Trust Center

- *Trust Center* is a website resource containing information and details about how Microsoft implements and supports security, privacy, compliance, and transparency in all our cloud products and services.
- The Trust Center site provides:
  - In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
  - Recommended resources in the form of a curated list of the most applicable and widely-used resources for each topic.
  - Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.

36

Service Trust Portal

- The Service Trust Portal (STP) is the Microsoft public site for publishing audit reports and other compliance-related information related to Microsoft's cloud services.
- It also hosts the Compliance Manager service.
- STP is a companion feature to the **Trust Center**, and allows you to:
  - Access audit reports across Microsoft cloud services on a single page.
  - Access compliance guides to help you understand how can you use Microsoft cloud service features to manage compliance with various regulations.
  - Access trust documents to help you understand how Microsoft cloud services help protect your data.

37

Compliance Manager

- *Compliance Manager* is a workflow-based risk assessment in the Trust Portal that enables you to track, assign, and verify your organization's regulatory compliance activities
- It provide details related to Microsoft professional services and Microsoft cloud services such as Microsoft Office 365, Microsoft Dynamics 365, and Azure.
- *Compliance Manager* provides the following features:
  - Enables you to assign, track, and record compliance and assessment-related activities.
  - Provides a compliance score to help you track your progress and prioritize auditing.
  - Provides a secure repository in which to upload and manage evidence and other artifacts related to compliance activities.

38

Azure Government services

- Microsoft Azure Government addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers.
- Azure Government:
  - Is a separate instance of the Microsoft Azure service.
  - Offers physical isolation from non-US government deployments, and provides screened US personnel.
  - Handles data that is subject to certain government regulations and requirements, such as FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS.

39

Azure Germany services

- Microsoft Azure Germany is built on the Microsoft trusted cloud principles of security, privacy, compliance, and transparency.
- It brings data residency in transit and at rest in Germany, and data replication across German datacenters for business continuity.
- Customer data in the two datacenters is managed under the control of a data trustee, T-Systems International. This trustee is an independent German company and a subsidiary of Deutsche Telekom.
- Anyone who requires data to reside in Germany can use this service.

40

Azure China 21Vianet

- Microsoft Azure operated by 21Vianet (Azure China 21Vianet) is a physically separated instance of cloud services located in China.
- As the first foreign public cloud service provider offered in China in compliance with government regulations, Azure China 21Vianet provides world-class security as discussed in the Trust Center topic, as required by Chinese regulations for all systems and applications built on its architecture.

41

Lesson 08: Module 3 review questions

42

Module 3 review questions

1. There has been an attack on your public-facing website. The application's resources have been overwhelmed and exhausted, and are now unavailable to users. What service should you use to prevent this type of attack?
2. Azure AD is capable of providing which services?
3. Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?