BAIT 3273 Cloud Computing

Week 11

Security, Responsibility, and Trust in Azure (Continued)

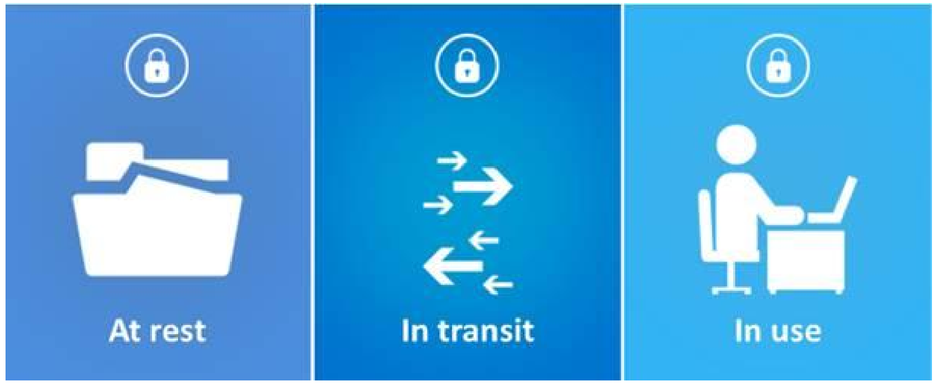
Lesson Objectives:

- To understand how encryption capabilities built into Azure can protect your data
- To study how to protect network and virtual networks
- To learn about advanced services and features provided by Azure to secure and safeguard the services and data

Encryption

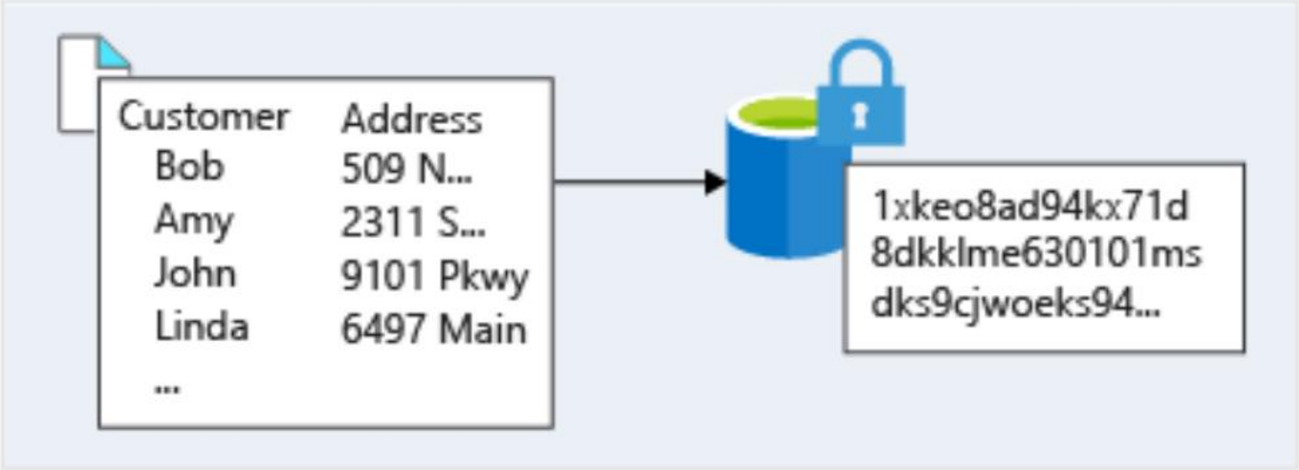
- The process of making data unreadable and unusable to users or services without authorized access.

- Two top-level types of encryption:
  - **Symmetric** – The same key is used to encrypt and decrypt data
  - **Asymmetric** – A public key and private key pair is used where both keys are required to decrypt data.
- Typically approached in two ways:
  1. Encryption at rest
  2. Encryption in transit



Encryption at rest

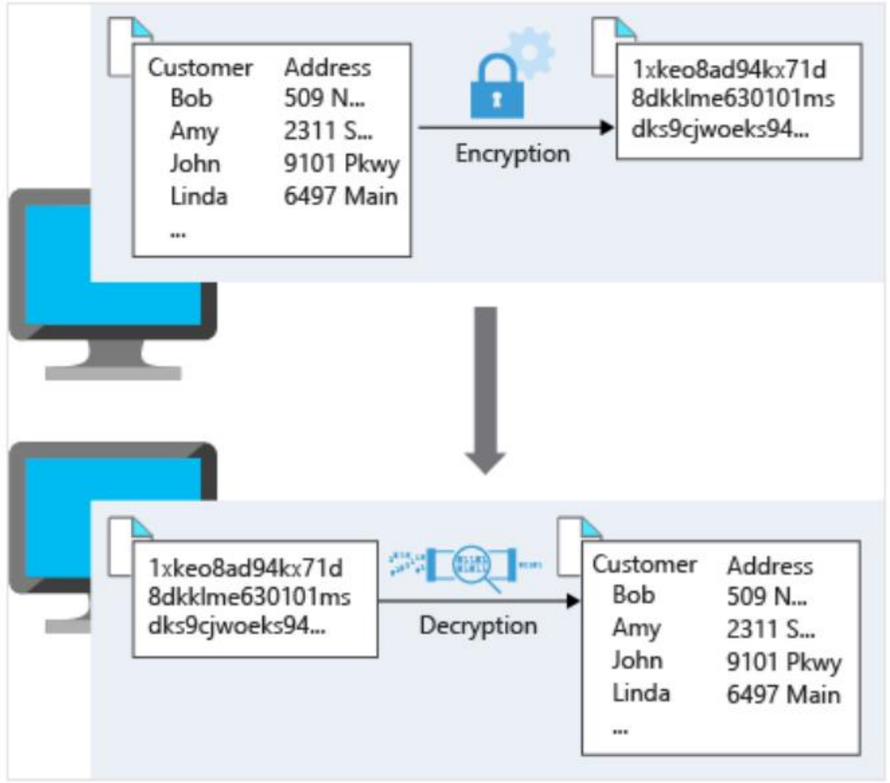
- Encrypt data stored such as on physical medium, disk of server or database.
- Ensure data stored is unreadable and unusable without the valid keys and secrets required to decrypt the data.



Encryption in transit

- Encrypt data that is moving from one location to another before sending the data over a network.
  - E.g. HTTPS

- Protects the data from outside observers and provides mechanism to limit the risk of exposure.



Encryption on Azure

- Encrypt raw storage
- Encrypt virtual machine disks
- Encrypt databases
- Encrypt secrets

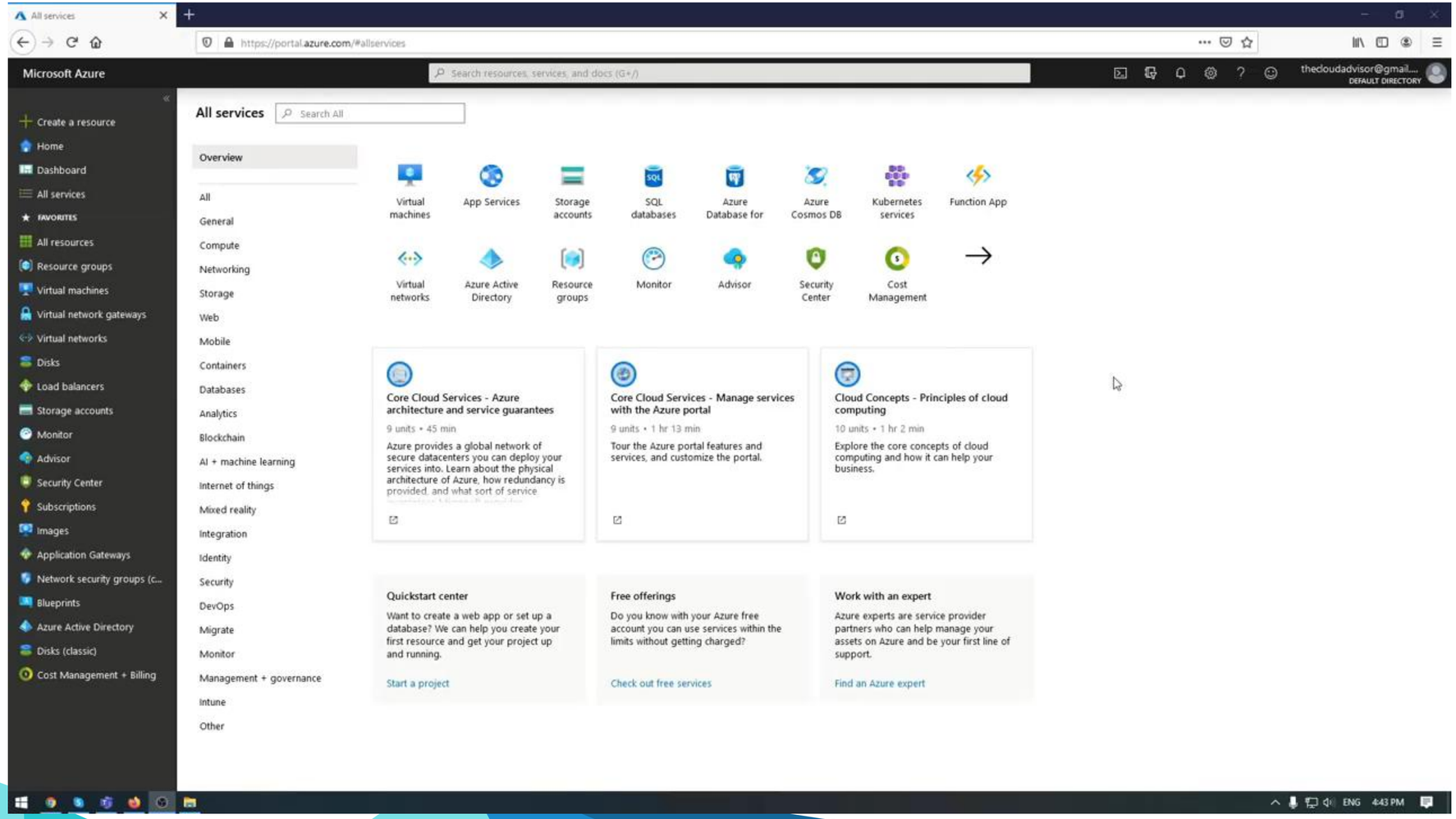
Encrypt raw storag

- Automatically encrypts data before persisting the data to Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage.
- Decrypts the data before retrieval.
- The process is transparent to applications using the services.

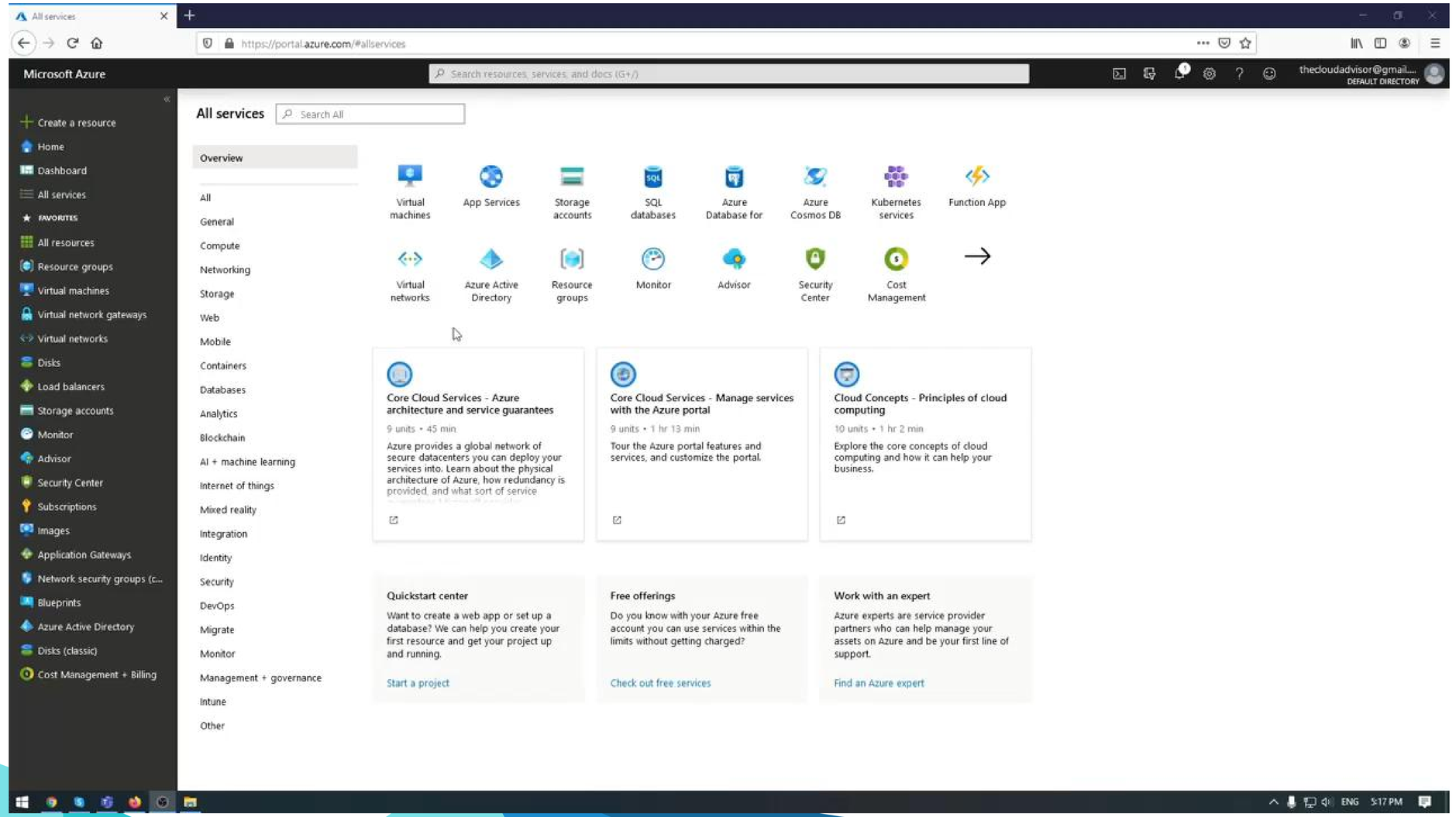
Encrypt virtual machine disks

- **Azure Disk Encryption** helps to encrypt Windows and Linux IaaS virtual machine disks.
- It provides volume encryption for OS and data disks.

Azure Disk Encryption



Azure Disk Encryption Demo



Encrypt databases

- **Transparent data encryption (TDE)** protects Azure SQL Database and Azure Data Warehouse against malicious attacks.
- It performs real-time encryption and decryption of the database.
- It encrypts the storage of an entire database by using database encryption key.

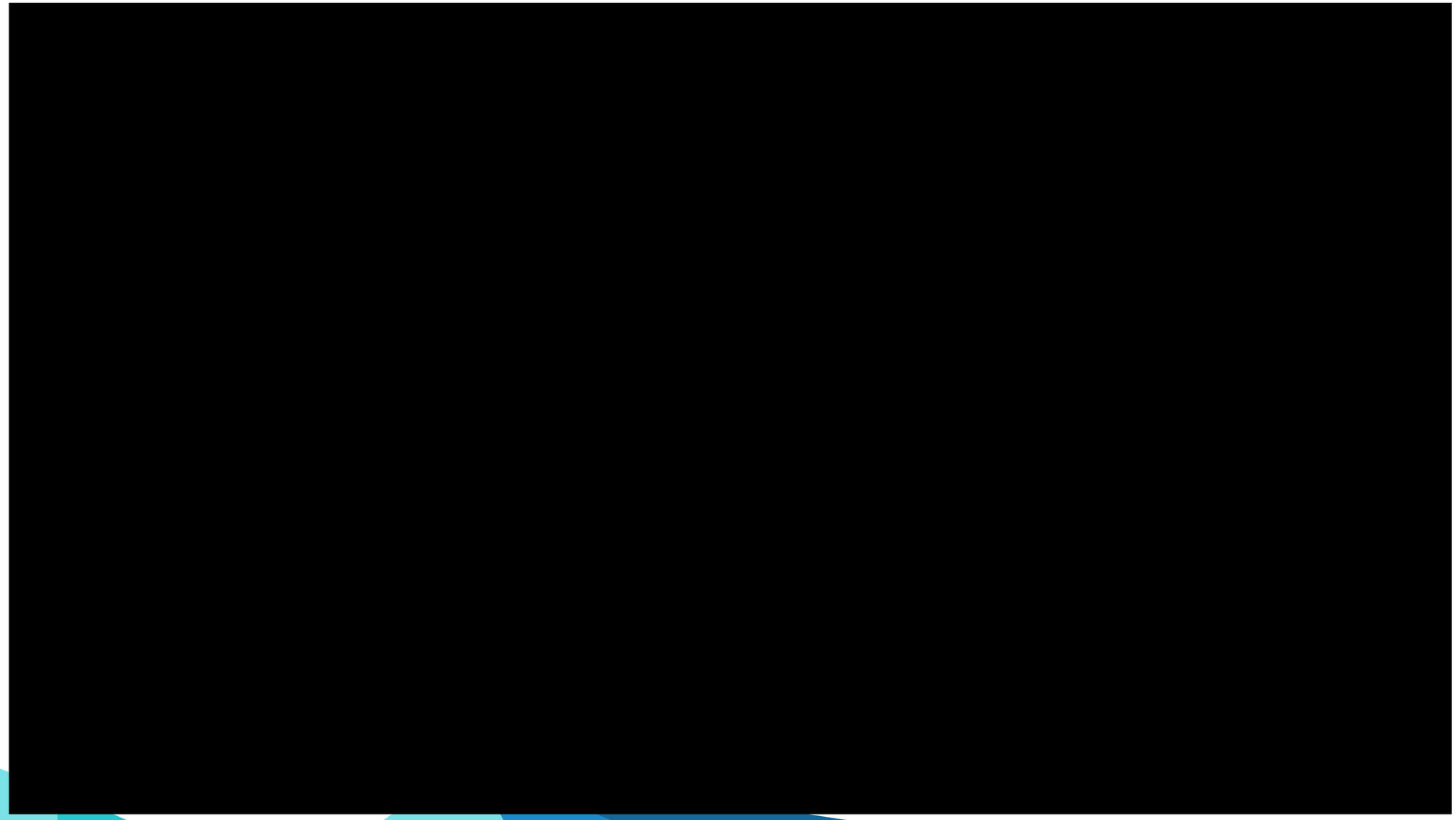
Encrypt secrets

- **Azure Key Vault** is a centralized cloud service used in Azure to protect customers' secrets.
- It is useful for a variety of scenarios:
  - Secrets management
  - Key management
  - Certificate management
  - Store secrets backed by hardware security modules (HSMs)

Encrypt secrets

- **Azure Key Vault** benefits:
  - Centralized application secrets
  - Securely stored secrets and keys
  - Monitor access and use
  - Simplified administration of application secrets
  - Integrate with other Azure services

Azure Key Vault



Summary on Encryption

- Encryption is usually the last line of defense and is important to secure your systems.
- Azure provides a variety of built-in capabilities and services to encrypt and protect data from n

Overview of Azure certificates

- Azure uses the certificates of **x.509 v3** which can be signed by trusted certificate authority or self-signed.
- These certificates can contain a private or public key and have a thumbprint that provides a means to identify a certificate in an unambiguous way.

Types of certificates

Service certificates

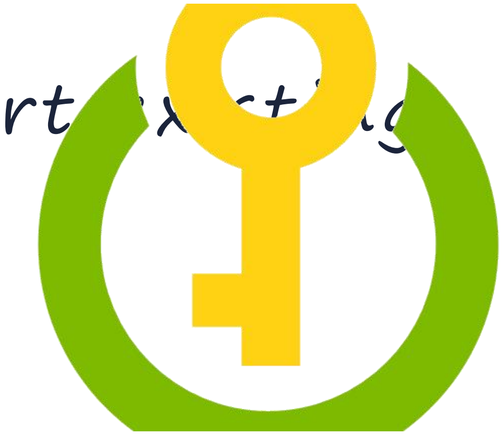
- Attached to cloud services that enables secure communication between service.
- Automatically deployed to the virtual machine
- Associated with a specific cloud service.

Management certificates

- Allows authentication with the classic deployment model.
- Used to automate configuration and deployment of various Azure services.
- Not related to cloud services.

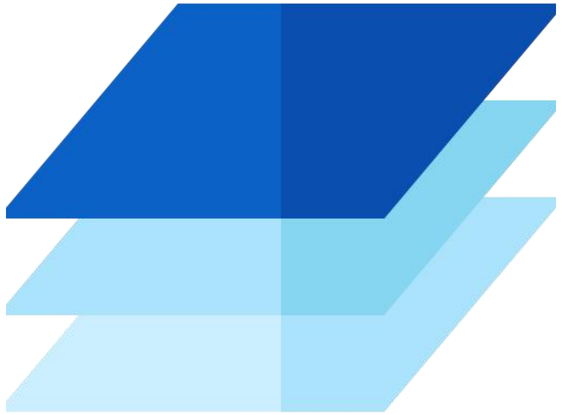
Using Azure Key Vault with certificates

- Certificates can be stored in Azure Key Vault
- Key Vault provides additional features:
  - Create certificates in Key Vault or import existing certificates
  - Securely store and manage certificates
  - Create a policy to manage the life cycle of a certificate
  - Provide contact information for the status of certificate
  - Automatically renew certificates



A layered approach to network security

- Layered approach provides multiple levels of protection to prevent attackers invade easily.
- Azure provide tools to secure network footprint via a layered approach.



Internet protection

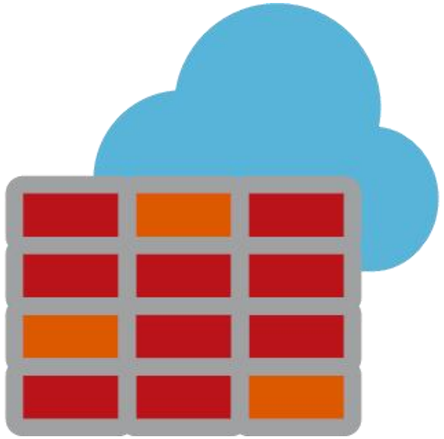
- Only allow inbound and outbound communication where necessary.
- Restrict inbound network traffic to ports and protocols required.

What is a Firewall?

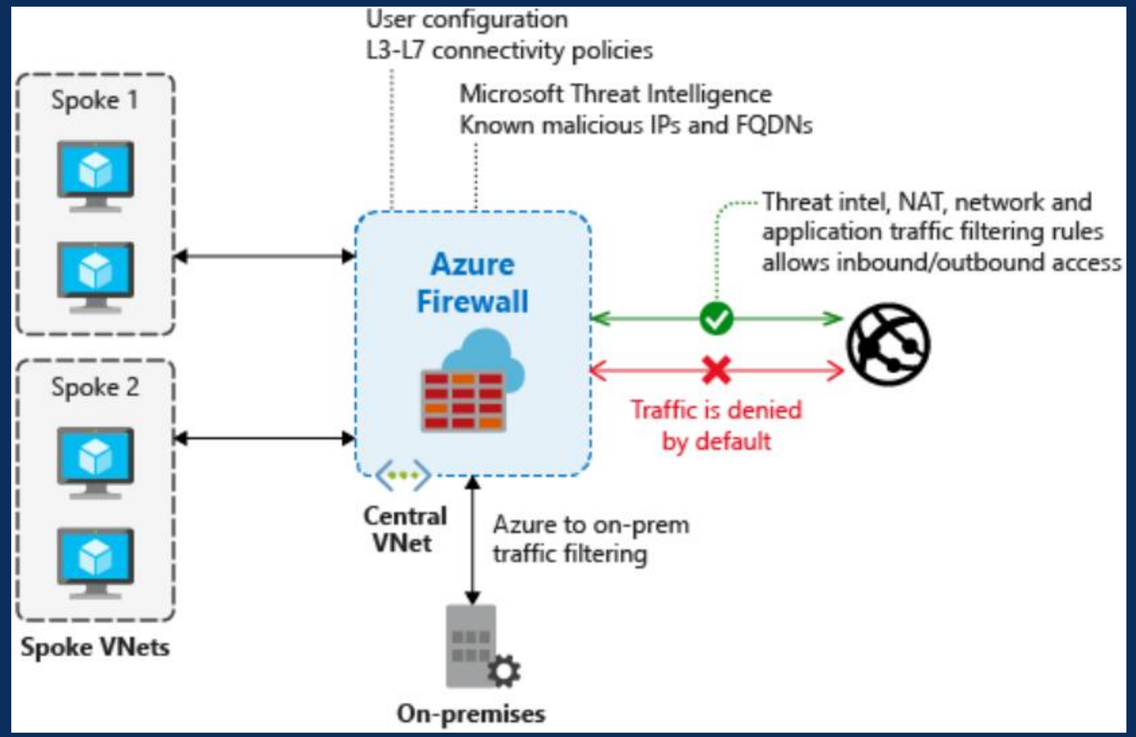
- A firewall is a service that grants server access based on the originating IP address of each request.

To provide inbound protection at the perimeter, there are several choices:

- **Azure Firewall**
- **Azure Application Gateway**
- **Network virtual appliances (NVAs)**



Azure Firewall



- A network security service that protects the Azure Virtual Network resources.
- Provides inbound protection for non-HTTP/S protocols and outbound protection for all ports and protocols, and application-level protection for outbound HTTP/S.

Azure Firewall

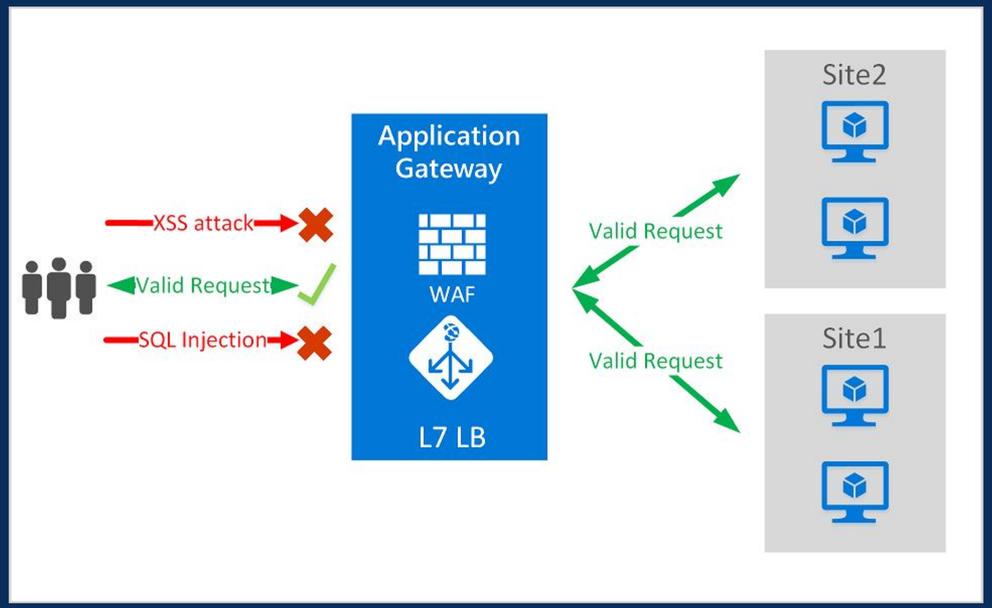
Azure Firewall Demo

Azure Firewall

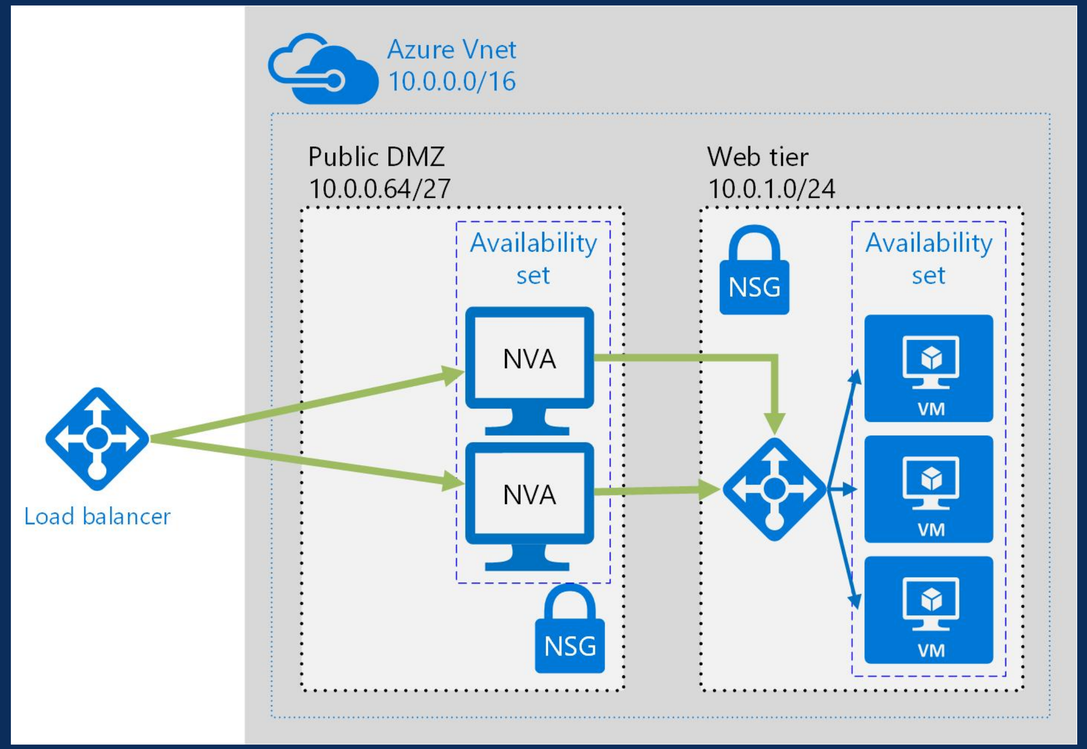
- Stateful packet inspection firewall managed by Microsoft
  - Low hassle factor
- Hyper scale, highly available
  - No NVA scaling troubles
- Native integration with Azure services
  - Service tags, RBAC, policy, etc

Azure Application Gateway

- A load balancer that protects common and known vulnerabilities in websites.
- Designed to protect HTTP traffic.



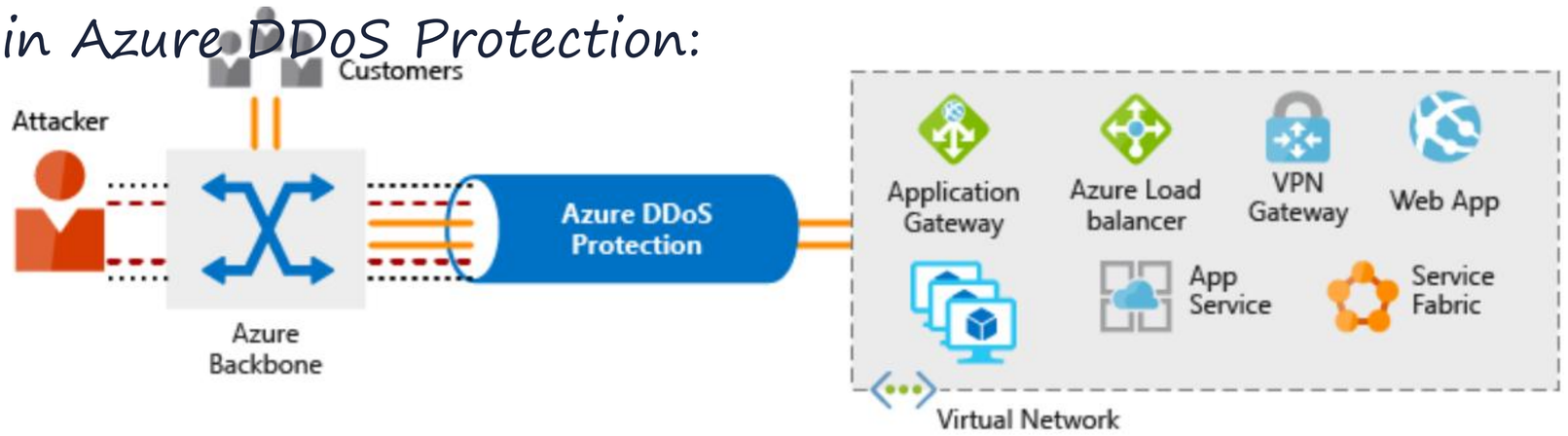
Network virtual appliances (NVAs)



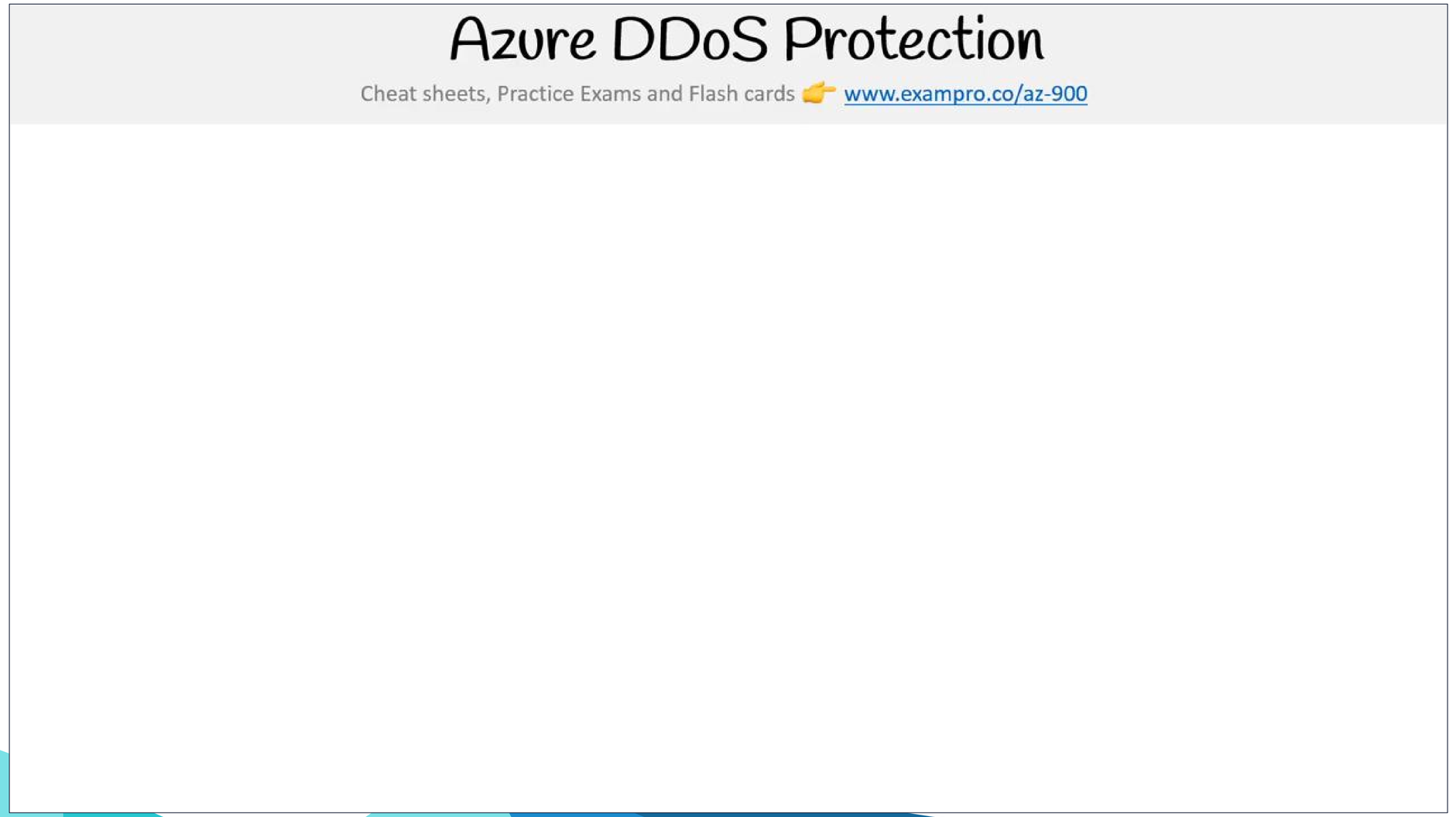
- Options for non-HTTP services or advanced configurations.
- Identical to hardware firewall appliances.

Stopping Distributed Denial of Service (DDoS) attacks

- **Azure DDoS Protection** service is able to protect Azure applications from DDoS attacks.
- When an attempt to overwhelm the network, Azure DDoS protection will blocks the traffic.
- There are two tiers in Azure DDoS Protection:
  - Basic
  - Standard



Azure DDoS Protection



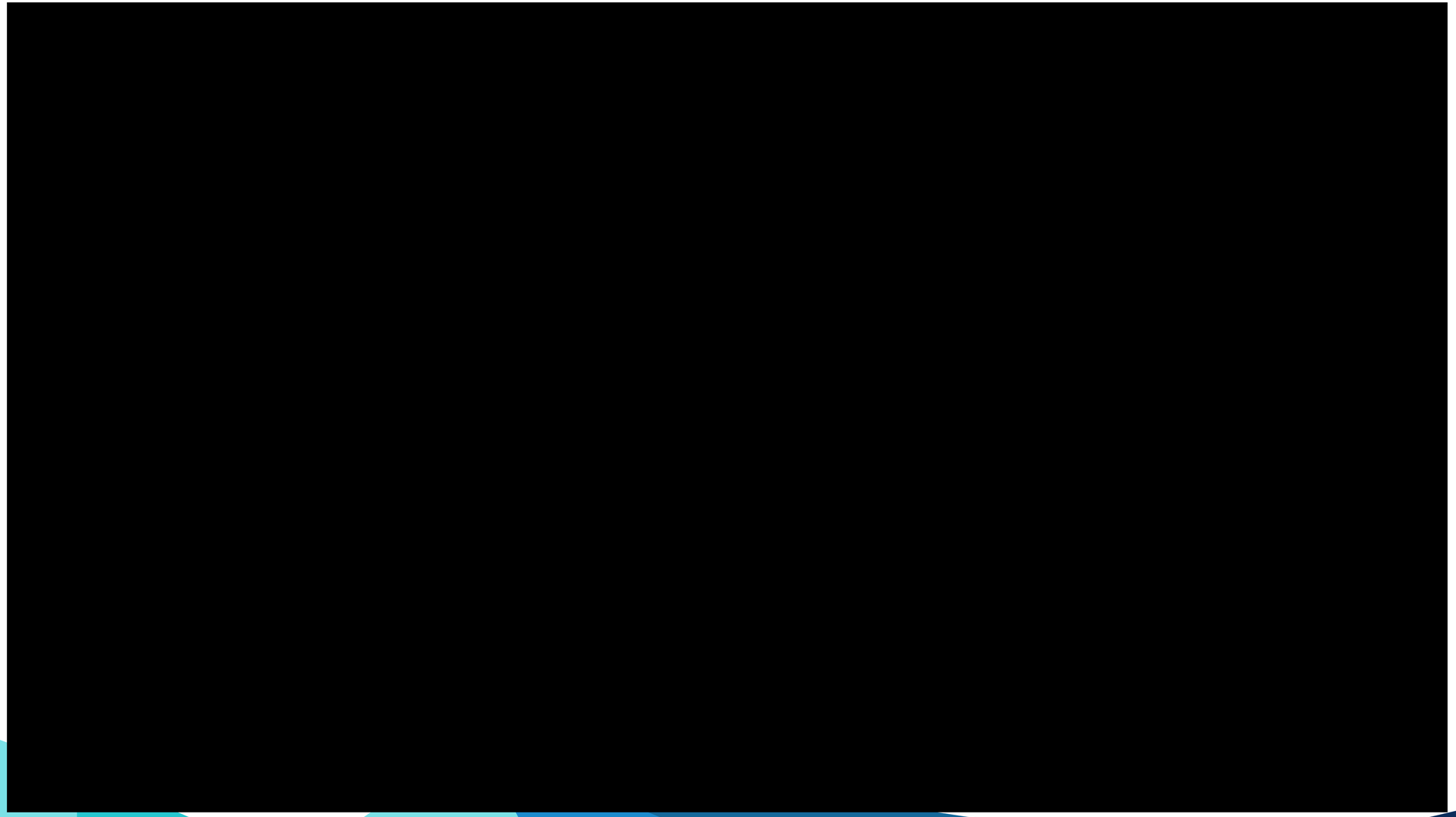
Controlling the traffic inside your virtual network

Virtual network security

- *Network Security Groups* (NSGs) are critical in restricting unnecessary communication between virtual machines.

- NSGs is capable of filtering network traffic to and from the Azure resources in an Azure virtual network.

Network Security Groups (NSGs)



Network integration

- Virtual private network (VPN) connections are one of the way to establish secure communication channels between networks.

- Connections between Azure Virtual Network and an on-premises VPN device are a great way to provide secure communication between your network and your virtual network on Azure.

Summary on Protect your network

- A layered approach to network security is able to reduce risk from being attacked.
- Azure provides several services and capabilities to create secure solutions on th

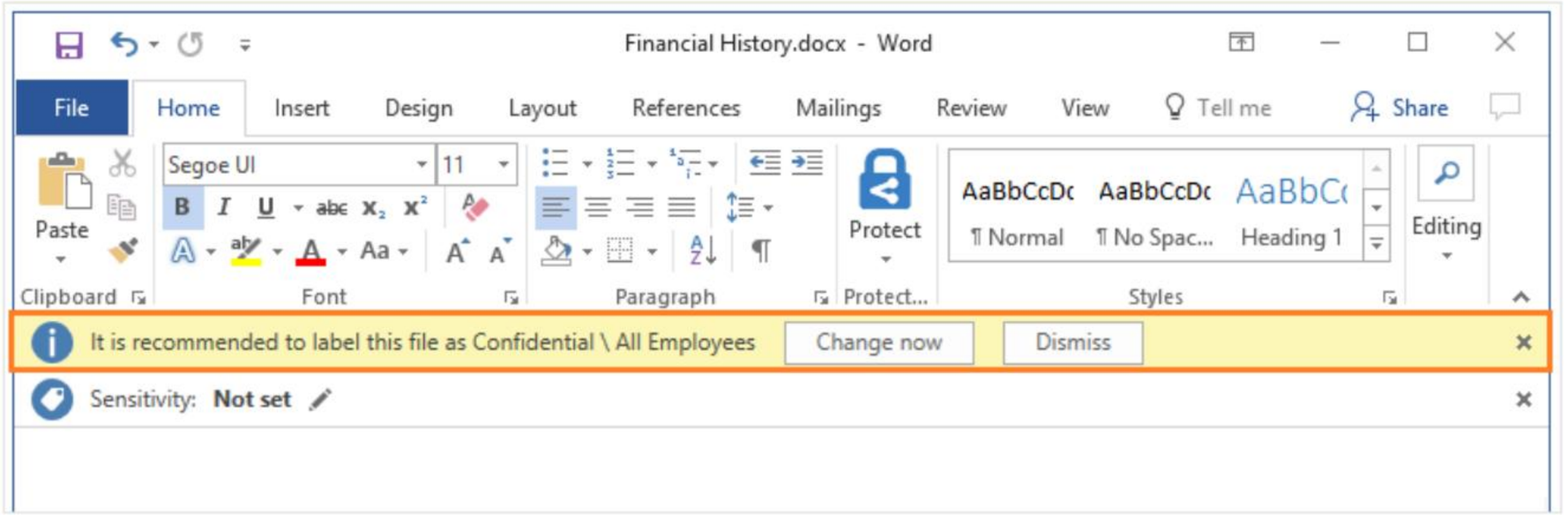
Protect your shared documents

Microsoft Azure Information Protection (AIP)

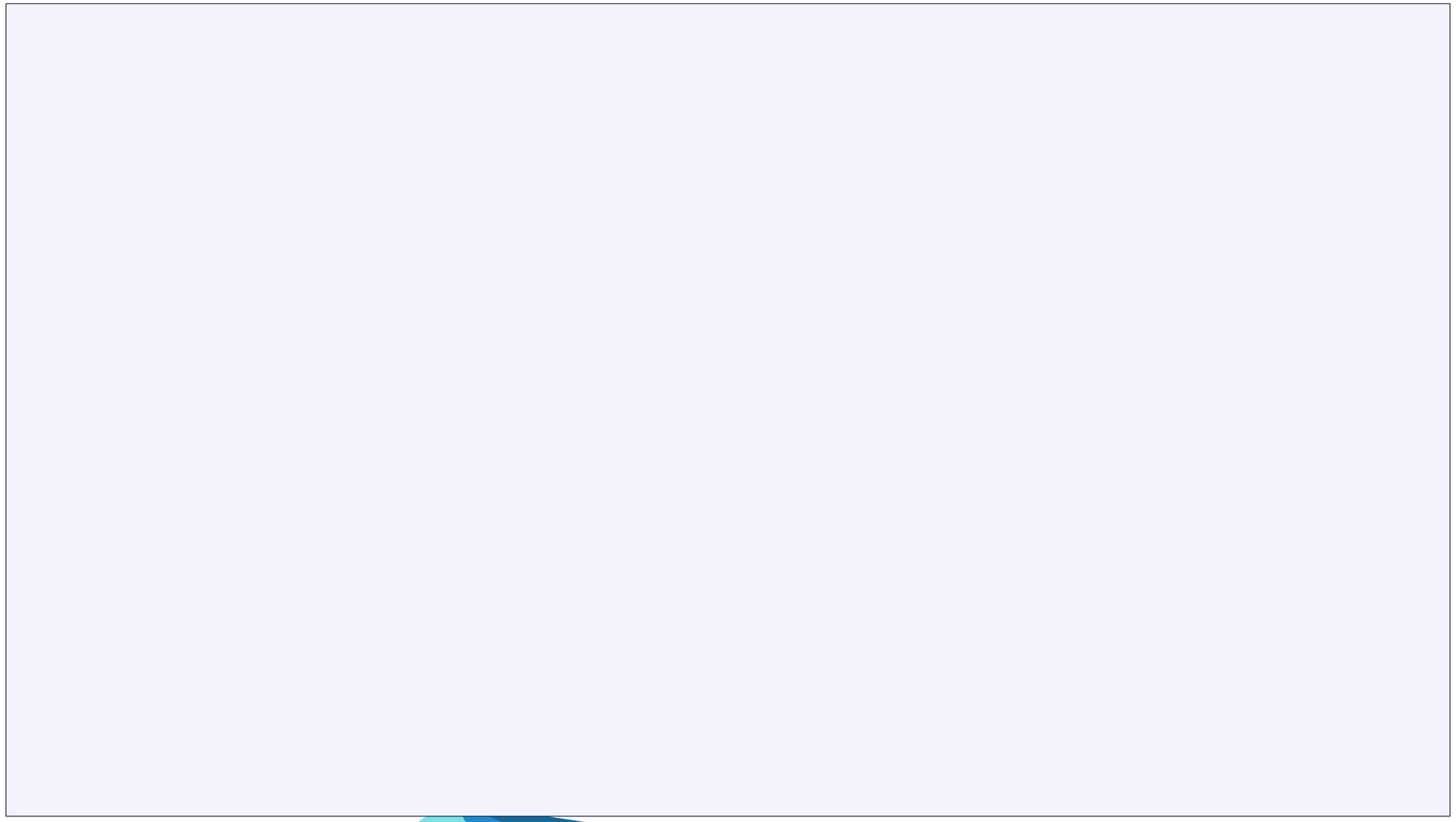
- A cloud-based solution that helps organizations to classify and protect documents and emails through labels.
- Labels can be applied both automatically or manually.

Example of AIP in action

In this example, the administrator has configured a label with rules that detect sensitive data. When a user saves a Microsoft Word document containing a credit card number, a custom tooltip is displayed. The tooltip recommends labelling the file as *Confidential \ All Employees*. This label is configured by the administrator. Using this label classifies the document and protects it

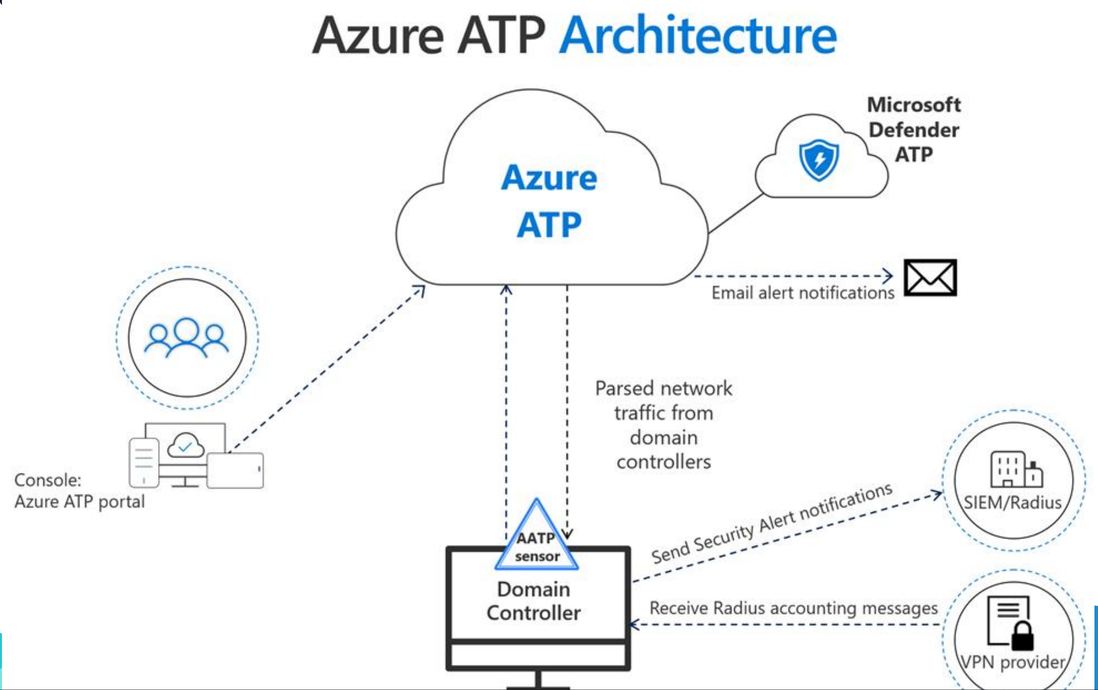


Azure Information Protection (AIP)



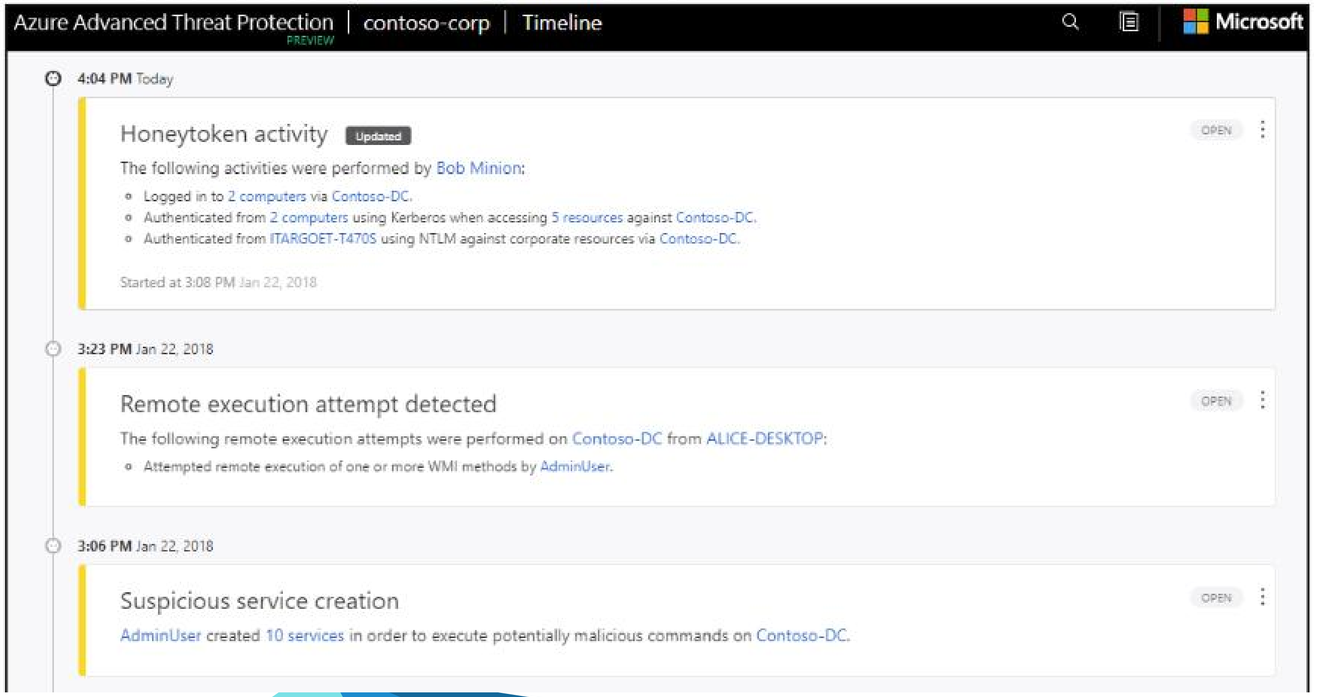
Azure Advanced Threat Protection

- Azure Advanced Threat Protection (Azure ATP) is a cloud-based security solution.
- It is capable of detecting acknowledged malicious attacks and techniques, security issues, and risks against your network.
- Azure ATP consists of several components



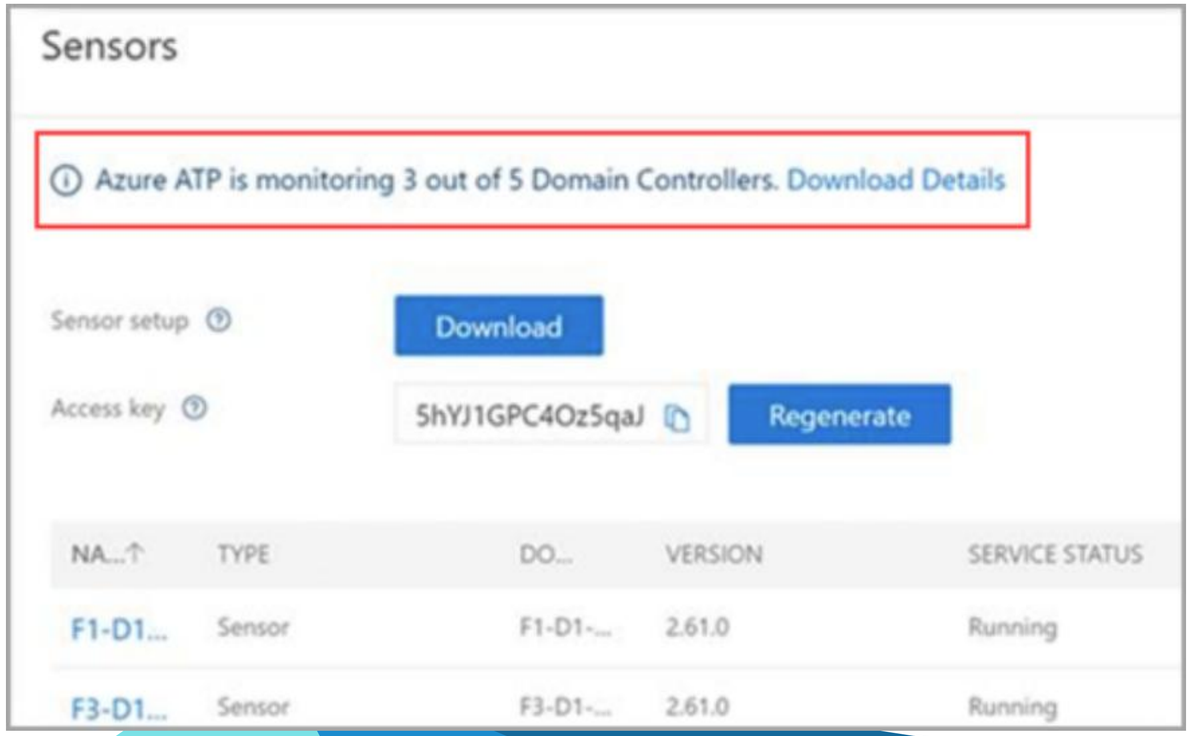
Azure ATP portal

- Azure ATP has its own portal for monitoring and respond to suspicious activities.
- The portal can be used to monitor, manage, and investigate threats towards your network environment.



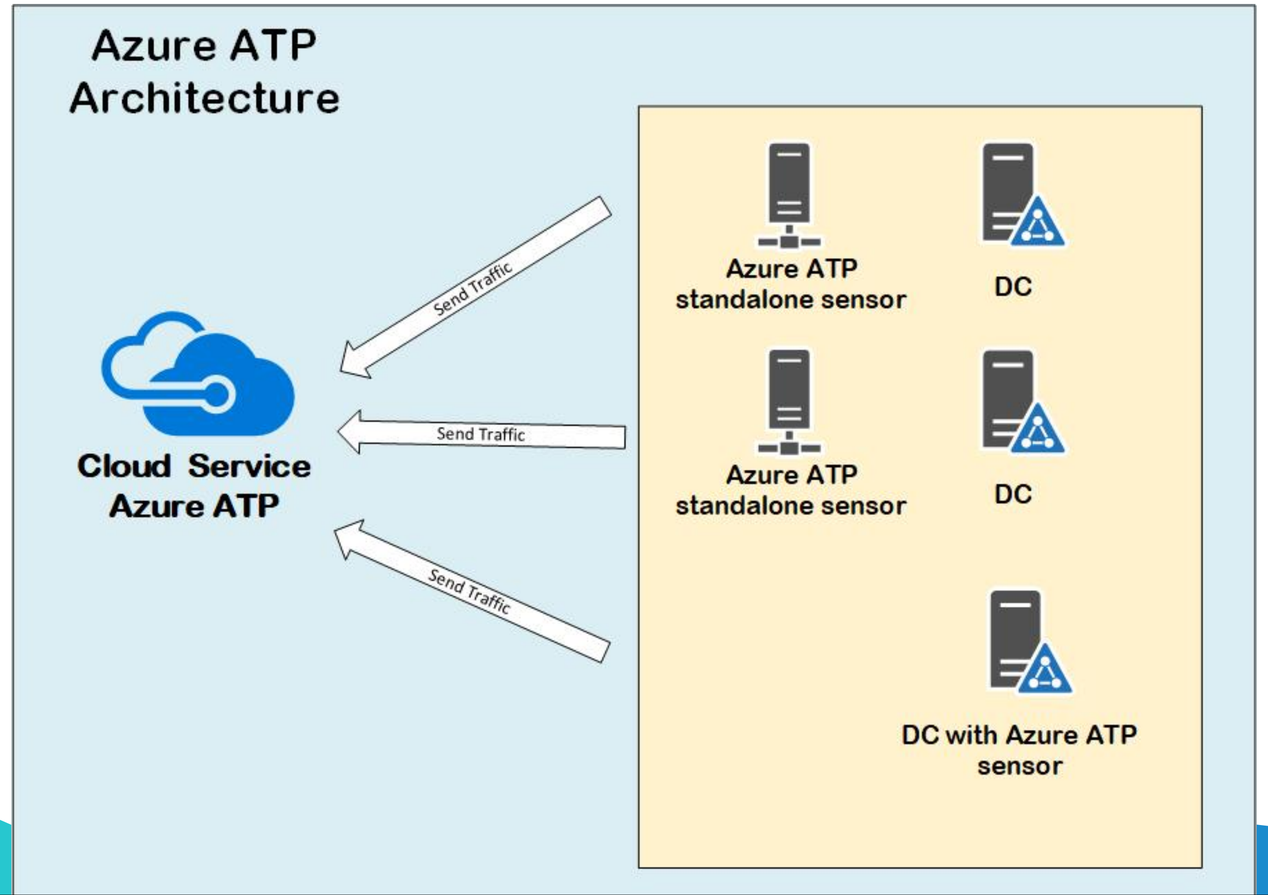
Azure ATP sensor

- The Azure ATP sensors monitors domain controller traffic without needing a dedicated server or configuring port mirroring.

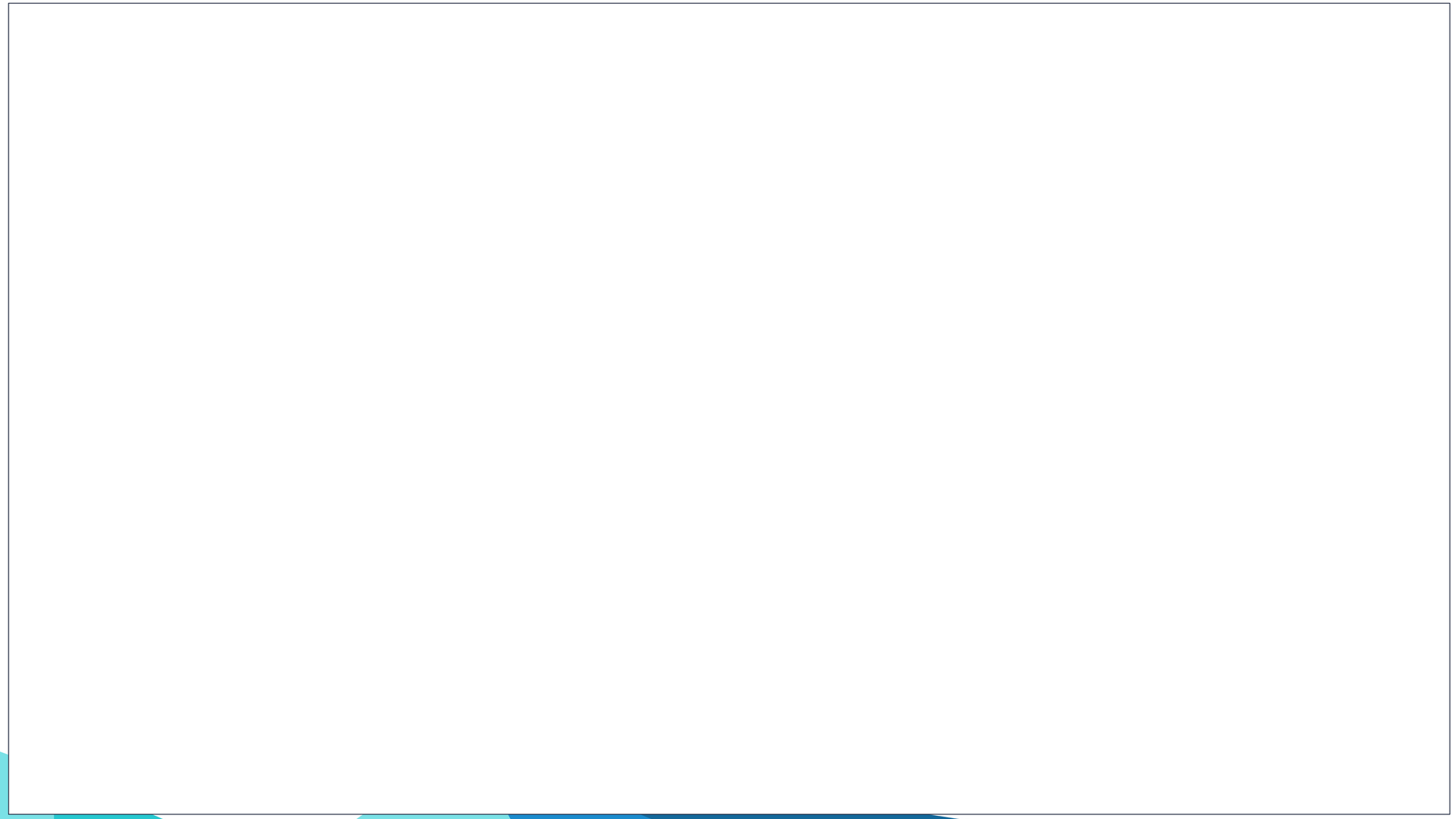


Azure ATP cloud service

- Azure ATP cloud service runs on Azure infrastructure and is connected to Microsoft's intelligent security graph.



zure Advanced Threat Protection (AT



Understand Security Considerations for Application Lifecycle Management Solutions

Provide training

- Security is everyone's job.
- IT experts should have fundamental knowledge about security.
- Effective training is able to enhance the knowledge regarding security such as SDL practices and security policies.

Define security requirements

- Security requirements shall be updated from time to time in order to address changes.

- Some of the factors that influence security requirements:
  - Legal and industry requirements
  - Internal standards and coding practices
  - Review of previous incidents
  - Known threats

Define metrics and compliance reporting

- Organization should define the minimum acceptable levels of security quality.
- Engineering teams working on the project are accountable to meet the criteria.
- Bug and/or work tracking mechanisms used should be able to label security clearly to allow accurate tracking and reporting of security

Perform threat modeling

- Allows development teams to acknowledge, document, and examine the security implications of designs.
- Helps a team to identify security vulnerabilities and determine potential risks.
- Make security feature selections and establish appropriate mitigations.

Establish design requirements

- Engineering team usually relies on features such as cryptography, logging and authentication for security.

- Design or implementations choices shall be applied consistently to reduce vulnerabilities.

Define and use cryptography standards

- It is essential to ensure all kinds of data are protected when being transmitted or stored.
- Clear encryption standards shall be developed to prevent disastrous events from happening.

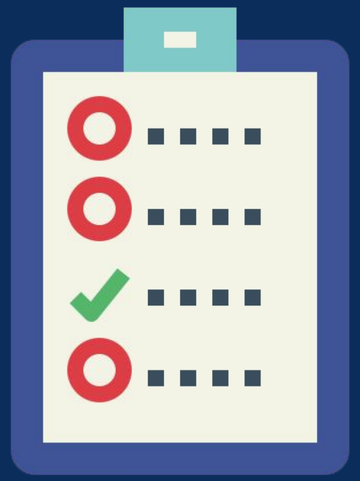
Manage security risks from using third-party components

- Most of software projects nowadays are built using third-party components.
- It is necessary to study the impact that would arise from the security vulnerability in these components.
- Ready a plan to respond whenever a new vulnerability is discovered.

Use approved tools

- Engineers should use the latest version of approved tools.
- Utilize new security analysis functionality and protections.

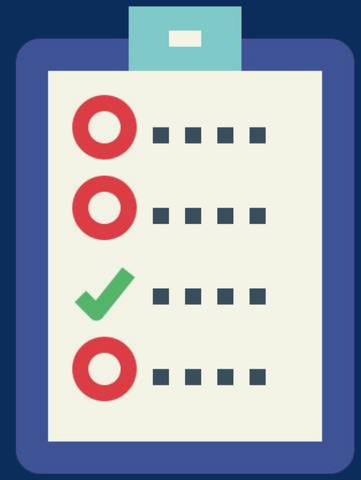
Perform Static Analysis Security Testing



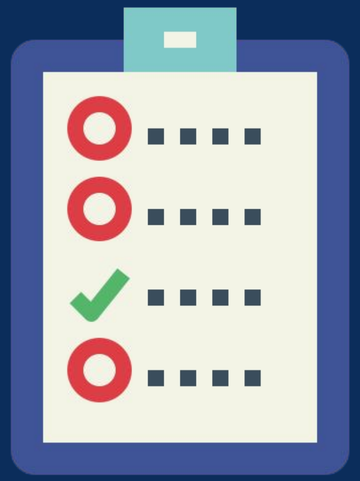
- Analyze the source code prior to compilation which can ensure the secure coding policies are being followed.
- The development teams should decide the frequency of performing Static Analysis Security Testing (SAST).

Perform Dynamic Analysis Security Testing

- Perform run-time verification of compiled or packaged software.
- Achieved by using a tool, a suit of pre-built attacks, or tools that specifically monitor application behavior.



Perform penetration testing



- A security analysis of a software system that is carried out by security professionals who simulate the actions that will be performed by hacker.

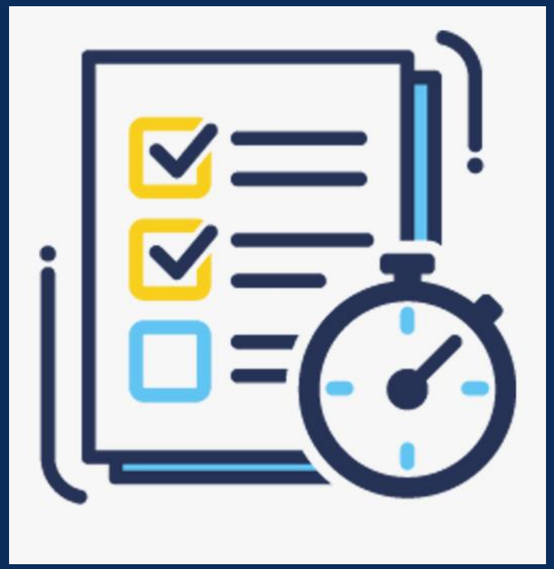
- The objective is to uncover potential vulnerabilities of the software system.

- Typically identify an extensive amount of vulnerabilities.

Establish a standard incident response process

- An incident response plan is important for addressing new threats that could emerge over time.

- Incident response plan should:
  - Include the person to contact in case a security emergency occurs
  - Establish the protocol for security servicing
  - Be tested before it is needed



Summary

- **Defense in depth** is the overriding theme – think about security as a multi-layer concern.
- Azure has radical help for a plenty of security issues we face.
- Azure Security Center centralizes the help offered by Azure which helps organization to mitigate threats

Check your knowledge

1. Cloud security is a shared responsibility between you and your cloud provider. Which category of cloud services requires the greatest security effort on your part?

- ○ Infrastructure as a service (IaaS)
- ○ Platform as a service (PaaS)
- ○ Software as a service (SaaS)

2. Which of these options helps you most easily disable an account when an employee leaves your company?

- ○ Enforce multi-factor authentication (MFA)
- ○ Monitor sign-on attempts
- ○ Use single sign-on (SSO)

3. Which of these approaches is the *strongest* way to protect sensitive customer data?

- ○ Encrypt data as it sits in your database
- ○ Encrypt data as it travels over the network
- ○ Encrypt data both as it sits in your database and as it travels over the network

Check your knowledg

4. There has been an attack on your public-facing website, and 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?

- ○ DDoS protection
- ○ Azure Firewall
- ○ Network Security Group
- ○ Application Gateway

5. You want to store certificates in Azure to centrally manage them for your services. Which Azure service should you use?

- ○ AIP
- ○ Azure AD
- ○ Azure Key Vault
- ○ Azure ATP

Answer

1. Cloud security is a shared responsibility between you and your cloud provider. Which category of cloud services requires the greatest security effort on your part?

- (•) Infrastructure as a service (IaaS) ✓

  At this level, the cloud provider provides physical security to compute resources. However, it's your responsibility to patch and secure your operating systems and software, as well as configure your network to be secure.

- ( ) Platform as a service (PaaS)
- ( ) Software as a service (SaaS)

2. Which of these options helps you most easily disable an account when an employee leaves your company?

- ( ) Enforce multi-factor authentication (MFA)
- ( ) Monitor sign-on attempts
- (•) Use single sign-on (SSO) ✓

  SSO centralizes user identity, so you can disable an inactive account in a single step.

3. Which of these approaches is the *strongest* way to protect sensitive customer data?

- ( ) Encrypt data as it sits in your database
- ( ) Encrypt data as it travels over the network
- (•) Encrypt data both as it sits in your database and as it travels over the network ✓

  Encrypting your data at all times, both as it sits in your database and as it travels over the network, minimizes the opportunity for an attacker to access your data in plain text.

Answer

4. There has been an attack on your public-facing website, and 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?

- (●) DDoS protection ✓

  DDoS protection is the correct answer, because it will help prevent DDoS attacks.

- ( ) Azure Firewall
- ( ) Network Security Group
- ( ) Application Gateway

5. You want to store certificates in Azure to centrally manage them for your services. Which Azure service should you use?

- ( ) AIP
- ( ) Azure AD
- (●) Azure Key Vault ✓

  Azure Key Vault is the correct answer, because it is a centralized cloud service for storing application secrets, referred to as a secret store.

- ( ) Azure ATP

Thanks!