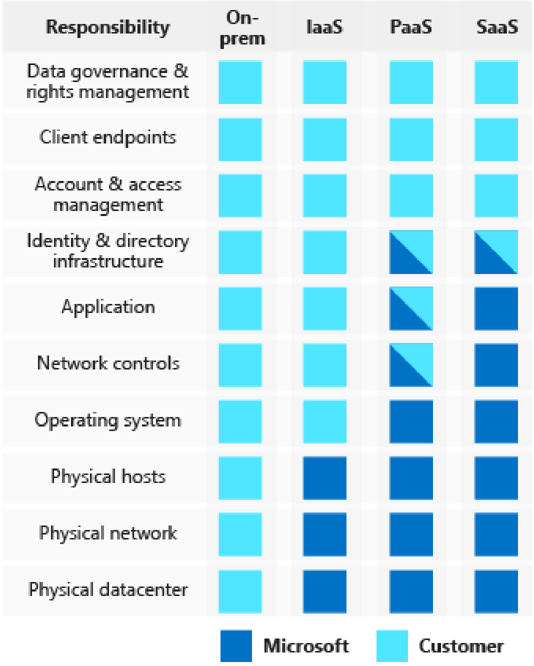
Security, responsibility and trust in Azure

1 Shared responsibility of cloud security



Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management	◻	◻	◻	◻
Client endpoints	◻	◻	◻	◻
Account & access management	◻	◻	◻	◻
Identity & directory infrastructure	◻	◻	◪	◪
Application	◻	◻	◪	◼
Network controls	◻	◻	◪	◼
Operating system	◻	◻	◼	◼
Physical hosts	◻	◼	◼	◼
Physical network	◻	◼	◼	◼
Physical datacenter	◻	◼	◼	◼

◼ Microsoft ◻ Customer

Regardless of the deployment type, you always retain responsibility for:

- Data
- Endpoints
- Accounts
- Access Management

1.1 Layered approach to security

1.1.1 Data

It is the responsibility of those storing and controlling access to the data to ensure that it's properly secured. There are often regulatory requirements for the CIA of this data

1.1.2 Application

- Ensure applications are secure and free of vulnerabilities
- Store sensitive application secrets in a secure storage medium
- Make security a design requirement for all application development

1.1.3 Compute

- Secure access to virtual machines
- Implement endpoint protection and keep systems patched and current

1.1.4 Networking

- Limit communication between resources
- Deny by default
- Restrict inbound internet access and limit outbound, where appropriate
- Implement secure connectivity to on-premises networks

1.2 Perimeter

- Use DDoS protection
- Use perimeter firewalls to identify and alert on malicious attacks against your network

1.3 Identity and access

- Control access to infrastructure and change control
- Use single sign on and multi factor authentication
- Audit events and changes

1.4 Physical security

- Physical building security and controlling access to computing hardware within the data center is the first line of defence

2 Azure Security Center

Security Center can:

- Provide security recommendations based on your configurations, resources and networks
- Monitor security settings and automatically apply required security to new services
- Continuously monitor services to provide automatic security assessments
- Use machine learning to detect and block malware being installed
- Analyse and identify inbound attacks
- Provide just in time access control for ports

2.1 Pricing Tiers

- Free - Just assessments and recommendations of resources
- Standard - Including continuous monitoring, threat detection etc.

2.2 Usage scenarios

You can use security centre to:

- Detect - Review the first indication of an event investigation
- Assess - Perform the initial assessment to obtain more information about the suspicious activity
- Implement a recommended security policy

3 Identity and access

Definition: Authentication

Establish the identity of a person or service looking to access a resource

Definition: Authorization

Establish what level of access an authenticated person or service has

3.1 Azure Active Directory

Azure AD provides services such as:

- Authentication
- Single Sign On - One ID and password for multiple services
- Application management
- Business to Business identity services
- Business to Customer identity services
- Device management

3.2 Providing identities to services

3.2.1 Service Principals

Definition: Identity

A thing that can be authenticated

Definition: Principal

An identity acting with certain roles or claims

Definition: Service Principal

An identity that is used by a service or application

3.2.2 Managed identities for Azure services

This makes creating service principles easier. A managed identity can be instantly created for any azure service that supports it.

3.3 Role based access control

Roles are sets of permissions that users can be granted to access an Azure service instance.

Identities are mapped to roles directly or through group membership.

Roles can be granted at the individual service instance level, but they also flow down the Azure resource manager hierarchy.

3.3.1 Privileged Identity Management

This is an additional offering that provides oversight of role assignments to ensure people don't hav excess privileges.

4 Encryption

Definition: Symmetric encryption

Uses the same key to encrypt and decrypt the data

Definition: Asymmetric encryption

Uses a public and private key pair

Definition: Encryption at rest

Encrypting data that has been stored on a physical medium

Definition: Encryption in transit

Encrypting data that is actively moving from one location to another

4.1 Encryption on Azure

- Azure Storage Service Encryption - For data at rest
- Azure Disk Encryption - Encrypt virtual machine disks
- Transparent data encryption - Protect Azure SQL database and Azure data warehouse
- Azure key vault - encrypt secrets

Benefits of using key vault:

- Centralized application secrets
- Securely stored secrets and keys
- Monitor access and use
- Simplified administration of application secrets
- Integrate with other Azure services

5 Azure Certificates

Certificates in Azure are **x.509 v3** and can be signed by a CA or self signed

5.1 Service Certificates

These are attached to cloud services and enable secure communication to and from this service.

These are managed separately from the services.

5.2 Management certificates

These allow you to authenticate with the classic deployment model

6 Protect your network

Definition: Firewall

A service that grants server access based on the originating IP address of each request

To provide inbound protection at the perimeter, you have several choices:

- Azure firewall - Managed cloud based network security service
- Azure application gateway - Load balancer that includes a web application firewall
- Network virtual appliances (NVAs) - Ideal for non HTTP services or advanced configs

6.1 DDoS Protection

Basic:

- Automatically enabled
- Always on traffic monitoring and real time mitigation of common network level attcks

Standard:

- Can mitigate:
  - Volumetric attacks - Flooding network layer with traffic
  - Protocol attacks - Exploit weakness in layer 3 and layer 4 protocol stack
  - Resource layer attacks - Target web application packets to disrupt the transmission of data between hosts

6.2 Virtual network security

For communication between virtual machines, Network Security Groups are a critical piece to restrict unnecessary communication.

This allows you to filter network traffic to and from Azure resources in an Azure virtual network

6.3 Network Integration

To provide a dedicated private network between your network and Azure, you can use Azure ExpressRoute.

7 Protecting shared documents

Azure information protection - A cloud based solution to help organizations classify and optionally protect documents by applying labels

8 Azure Advanced Threat Protection

This is a cloud based solution to identify, detect and help to investigate threats.

It has the following components:

- ATP portal - Allows you to monitor and respond to suspicious activity
- ATP sensor - Installed directly on domain controllers to monitor traffic
- ATP cloud service - Runs on Azure infrastructure and is connected to Microsoft's intelligent security graph

9 Security considerations for Application Lifecycle Management Solutions

- Provide training to ensure everyone knows the threats
- Define security requirements - Update continuously to address change in threat landscape.
- Define metrics and compliance reporting - Have minimum levels of security quality
- Perform threat modelling - Allows development teams to consider the security implications of designs
- Establish design requirements - Specific security features must be implemented
- Define and use cryptography standards
- Manage security risks from using third-party components - Keep an accurate inventory and plan to respond when new vulnerabilities are discovered
- Use approved tools - Define and publish a list of approved tools
- Perform Static Analysis Security Testing - Analyse source code prior to compilation
- Perform Dynamic Analysis Security Testing - Analyse fully compiled code
- Perform penetration testing
- Establish a standard incident response process