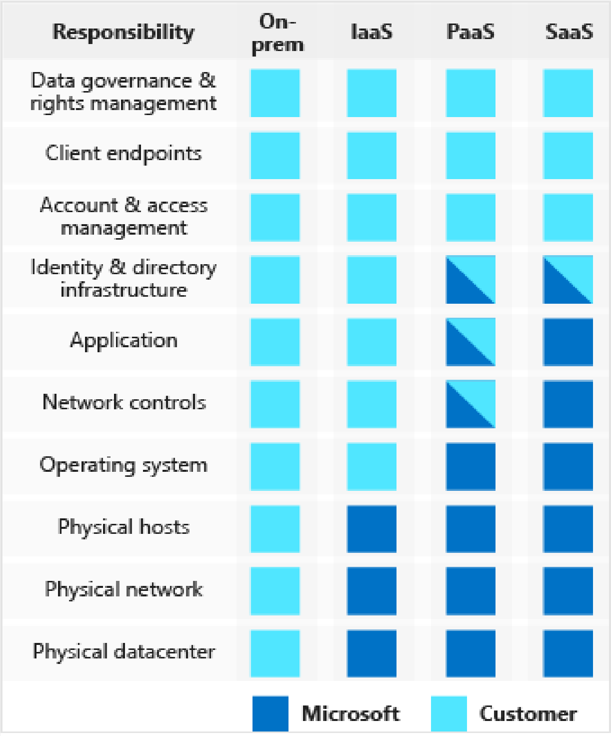
MICROSOFT AZURE SECURITY

Azure Security

Every system, architecture, and application needs to be designed with security in mind. There's too much at risk. For instance, a denial of service attack could prevent your customer from reaching your web site or services and block you from doing business. Defacement of your website damages your reputation. And a data breach could be even worse — as it can ruin hard-earned trust, while causing significant personal and financial harm. As administrators, developers, and IT management, we all must work to guarantee the security of our systems.

Cloud security is a shared responsibility

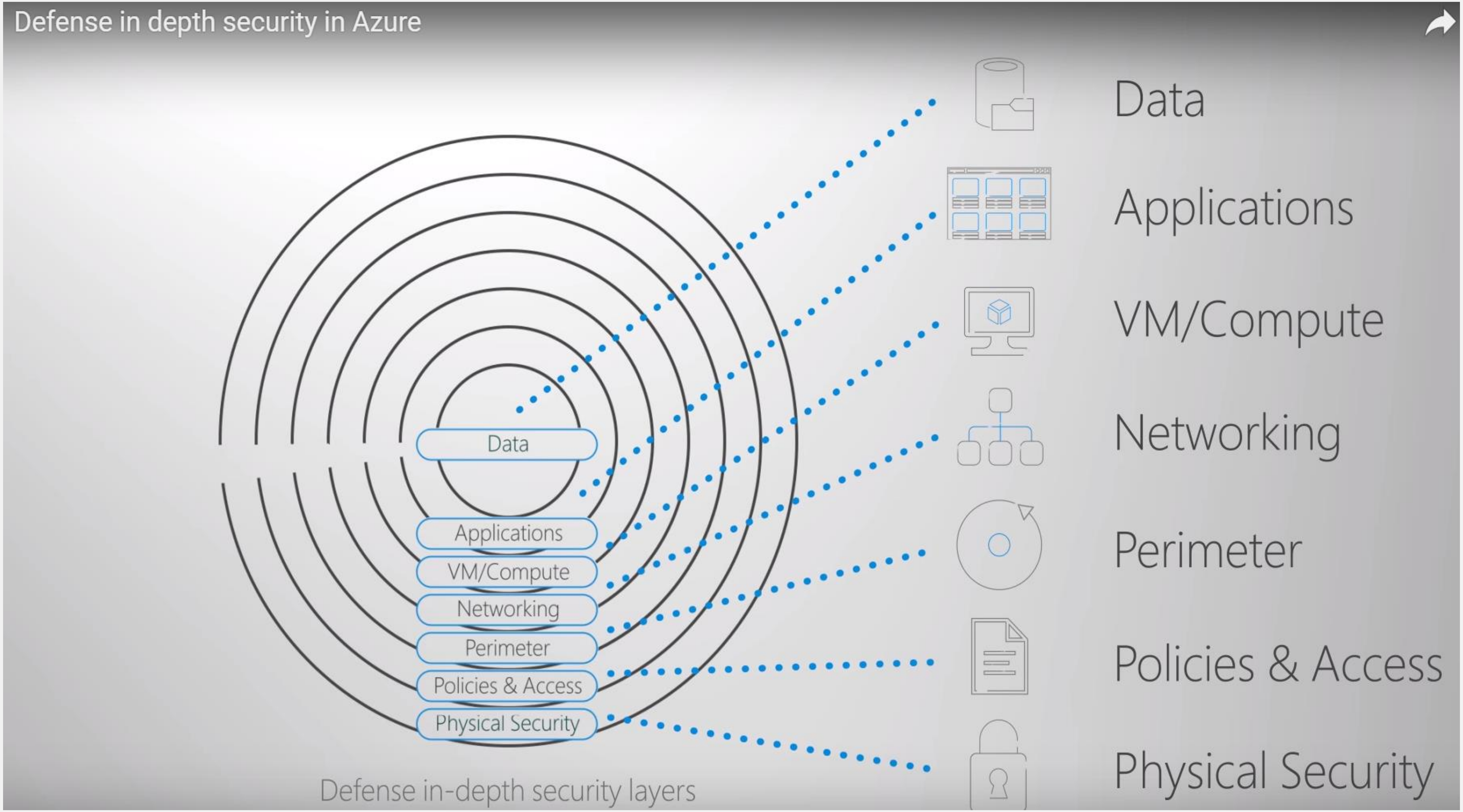
- As computing environments move from customer-controlled datacenters to the cloud, the responsibility of security also shifts.
- By shifting these responsibilities to a cloud service like Azure, organizations can reduce focus on activities that aren't core business competencies.
- Depending on the specific technology choices, some security protections will be built into the particular service, while addressing others will remain the customer's responsibility.
- The first shift you'll make is from on-premises data centers to infrastructure as a service (IaaS). you are taking advantage of IaaS when you start using Azure VMs instead of your on-premises physical servers.
- Moving to platform as a service (PaaS) outsources several security concerns. At this level, Azure is taking care of the operating system and of most foundational software like database management systems



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

Defense in depth security in Azure



Defense in-depth security layers

Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud environments.

Benefits of Security Center

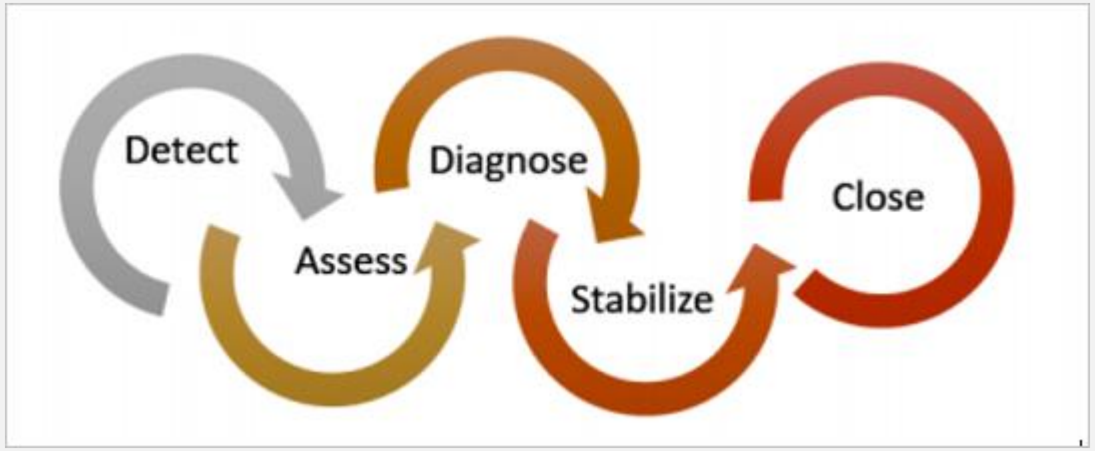
- Centralized Policy management - Ensure compliance with company or regulatory security requirements by centrally managing security policies across all hybrid cloud workloads.
- Continuous Security assessment - Monitor the security posture of the machine network storage devices and applications to discover potential threats.
- Actionable recommendations - Remediate security vulnerabilities before they can be exploited by attackers, with prioritized and actionable security recommendations.
- Prioritized alerts and incidents - Focus on most critical threats first with prioritized security alerts and incidents.
- Advanced cloud defenses - Reduce threats with just in time access to management ports and adaptive application controls running on the VM.
- Integrated Security Solutions - Collect search and analyze data from different sources including partner solutions.

Azure Security Center is available in two tiers:

- Free. Available as part of your Azure subscription, this tier is limited to assessments and recommendations of Azure resources only.
- Standard. This tier provides a full suite of security-related services including continuous monitoring, threat detection, just-in-time access control for ports, and more.

Usage scenarios

Use Security Center for incident response.
Many organizations learn how to respond to security incidents only after suffering an attack. To reduce costs and damage, it's important to have an incident response plan in place before an attack occurs.



Use Security Center recommendations to enhance security.

You can reduce the chances of a significant security event by configuring a security policy, and then implementing the recommendations provided by Azure Security Center.

- A *security policy* defines the set of controls that are recommended for resources within that specified subscription or resource group.
- Security Center analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates recommendations based on the controls set in the security policy.

Demo Security Center

Just in time VM access

- Reduce the network attack surface with just in time VM access.
- Specify rules for how users can access the VM ,when needed access can be requested from the security center or via PowerShell

Adaptive application controls

- Block malware and other unwanted applications by applying whitelisting recommendations adapted to your specific needs powered by machine learning.

Integrate your security solutions

- You can collect and analyze security data from various sources and including connected partner firewall solutions

Identity and access

Network perimeters, firewalls, and physical access controls used to be the primary protection for corporate data. But network perimeters have become increasingly porous with the explosion of bring your own device (BYOD), mobile apps, and cloud applications.

Identity has become the new primary security boundary. Therefore, proper authentication and assignment of privileges is critical to maintaining control of your data.

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.

What is Azure Active Directory?

Azure AD is a cloud-based identity service.

Authentication. This includes verifying identity to access applications and resources, and providing functionality such as self-service password reset, multi-factor authentication (MFA), a custom banned password list, and smart lockout services.
Single-Sign-On (SSO). SSO enables users to remember only one ID and one password to access multiple applications. A single identity is tied to a user, simplifying the security model. As users change roles or leave an organization, access modifications are tied to that identity, greatly reducing the effort needed to change or disable accounts.
Application management. You can manage your cloud and on-premises apps using Azure AD Application Proxy, SSO, the My apps portal (also referred to as Access panel), and SaaS apps.
Business to business (B2B) identity services. Manage your guest users and external partners while maintaining control over your own corporate data.
Business-to-Customer (B2C) identity services. Customize and control how users sign up, sign in, and manage their profiles when using your apps with services.
Device Management. Manage how your cloud or on-premises devices access your corporate data.

Single sign-on

The more identities a user has to manage, the greater the risk of a credential-related security incident. More identities mean more passwords to remember and change. Password policies can vary between applications and, as complexity requirements increase, it becomes increasingly difficult for users to remember them.

With single sign-on (SSO), users need to remember only one ID and one password. Access across applications is granted to a single identity tied to a user, simplifying the security model.

SSO with Azure Active Directory

By leveraging Azure AD for SSO you'll also have the ability to combine multiple data sources into an intelligent security graph. This security graph enables the ability to provide threat analysis and real-time identity protection to all accounts in Azure AD, including accounts that are synchronized from your on-premises AD. By using a centralized identity provider, you'll have centralized the security controls, reporting, alerting, and administration of your identity infrastructure.

Multi-factor authentication

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:

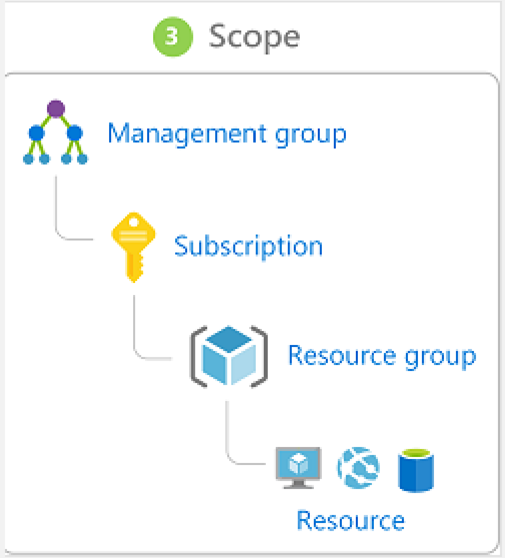
- *Something you know*
- *Something you possess*
- *Something you are*

Role-based access control

Roles are sets of permissions, like "Read-only" or "Contributor", that users can be granted to access an Azure service instance.

Identities are mapped to roles directly or through group membership. Separating security principals, access permissions, and resources provides simple access management and fine-grained control. Administrators are able to ensure the minimum necessary permissions are granted.

Here's a diagram that shows this relationship. Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.



Privileged Identity Management

In addition to managing Azure resource access with role-based access control (RBAC), a comprehensive approach to infrastructure protection should consider including the ongoing auditing of role members as their organization changes and evolves. Azure AD Privileged Identity Management (PIM) is an additional, paid-for offering that provides oversight of role assignments, self-service, and just-in-time role activation and Azure AD and Azure resource access reviews.

Encryption

Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read the encrypted data, it must be *decrypted*, which requires the use of a secret key. There are two top-level types of encryption: **symmetric** and **asymmetric**.

Symmetric encryption uses the same key to encrypt and decrypt the data.

Asymmetric encryption uses a public key and private key pair. Either key can encrypt but a single key can't decrypt its own encrypted data. To decrypt, you need the paired key

Encryption is typically approached in two ways:
1.Encryption at rest
2.Encryption in transit

Encryption on Azure

Azure Storage Service Encryption for data at rest helps you protect your data to meet your organizational security and compliance commitments. With this feature, the Azure storage platform automatically encrypts your data before persisting it to Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage, and decrypts the data before retrieval

Encrypt virtual machine disks

Storage Service Encryption provides low-level encryption protection for data written to physical disk, but how do you protect the virtual hard disks (VHDs) of virtual machines? If malicious attackers gained access to your Azure subscription and got the VHDs of your virtual machines, how would you ensure they would be unable to access the stored data?

Azure Disk Encryption is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption leverages the industry-standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and data disks.

Encrypt databases

Transparent data encryption (TDE) helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Encrypt secrets

We've seen that the encryption services all use keys to encrypt and decrypt data, so how do we ensure that the keys themselves are secure? Corporations may also have passwords, connection strings, or other sensitive pieces of information that they need to securely store. In Azure, we can use **Azure Key Vault** to protect our secrets.

Azure certificates

Certificates used in Azure are **x.509 v3** and can be signed by a trusted certificate authority, or they can be self-signed. A self-signed certificate is signed by its own creator; therefore, it is not trusted by default.

Types of certificates

Certificates are used in Azure for two primary purposes and are given a specific designation based on their intended use.

1. **Service certificates** are used for cloud services
2. **Management certificates** are used for authenticating with the management API

Service certificates

Service certificates are attached to cloud services and enable secure communication to and from the service. For example, if you deploy a web site, you would want to supply a certificate that can authenticate an exposed HTTPS endpoint. Service certificates, which are defined in your service definition, are automatically deployed to the VM that is running an instance of your role.

Management certificates

Management certificates allow you to authenticate with the classic deployment model. Many programs and tools (such as Visual Studio or the Azure SDK) use these certificates to automate configuration and deployment of various Azure services. However, these types of certificates are not related to cloud services.

Protect your network

Layered approach to network security is also recommended at the network layer. It's not enough to just focus on securing the network perimeter, or focusing on the network security between services inside a network. A layered approach provides multiple levels of protection, so that if an attacker gets through one layer, there are further protections in place to limit further attack.

Internet protection

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 provides inbound protection for non-HTTP/S protocols. Examples of non-HTTP/S protocols include: Remote Desktop Protocol (RDP), Secure Shell (SSH), and File Transfer Protocol (FTP). It also provides outbound, network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S.

Azure Application Gateway is a load balancer that includes a Web Application Firewall (WAF) that provides protection from common, known vulnerabilities in websites. It is designed to protect HTTP traffic.

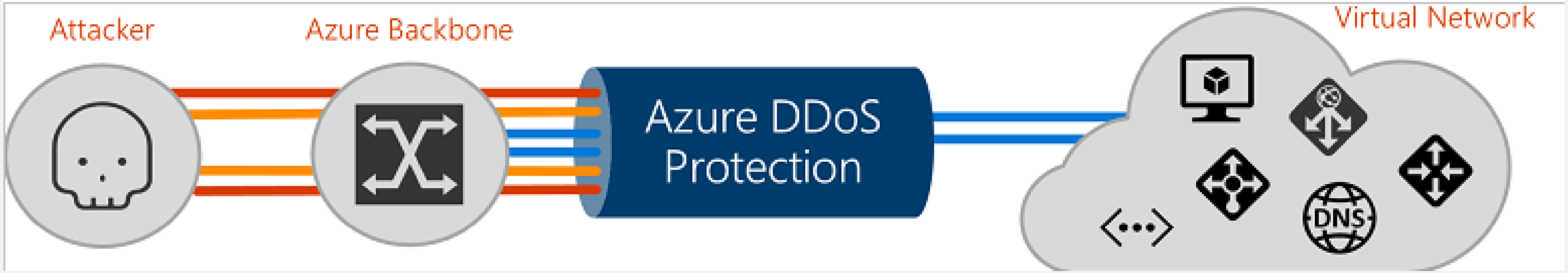
Network virtual appliances (NVAs) are ideal options for non-HTTP services or advanced configurations, and are similar to hardware firewall appliances.

Virtual network security

Once inside a virtual network (VNet), it's crucial that you limit communication between resources to only what is required.
For communication between virtual machines, *Network Security Groups* (NSGs) are a critical piece to restrict unnecessary communication.

DDoS protection

- Distributed Denial of service attack is one of the biggest security concerns which makes an application unavailable by exhausting the applications resources and making it unavailable to legitimate users.
- There are two tiers of service provided
  - Azure Ddos Basic - Automatically enabled as a part of azure platform.
  - Azure Ddos Standard - Provides additional capabilities such as protection policies which are tuned through dedicated traffic monitoring and machine learning algorithms, applied to Public IP associated with Virtual network
- Resources such as load balancers, application gateways and Service fabric instances. Real time telemetry is available through Azure monitor views during attack and for history.



Protect your shared documents

Microsoft Azure Information Protection (sometimes referred to as AIP) is a cloud-based solution that helps organizations classify and optionally protect documents and emails by applying labels.

Labels can be applied automatically based on rules and conditions. Labels can also be applied manually. You can also guide users to choose recommended labels with a combination of automatic and manual steps.

After your content is classified, you can track and control how the content is used. For example, you can:

- Analyze data flows to gain insight into your business
- Detect risky behaviors and take corrective measures
- Track access to documents
- Prevent data leakage or misuse of confidential information