Contents

[DEFENCE ON DEPTH 2](#_Toc159343390)

[COMPONENTS OF DEFENSE IN DEPTH 2](#_Toc159343391)

[SECURING NETWORK CONNECTIVITY 3](#_Toc159343392)

[TYPES OF ENDPOINTS 3](#_Toc159343393)

[PUBLIC ENDPOINT 3](#_Toc159343394)

[SERVICE ENDPOINT 4](#_Toc159343395)

[PRIVATE ENDPOINT 6](#_Toc159343396)

[MICROSOFT DEFENDER FOR CLOUD 9](#_Toc159343397)

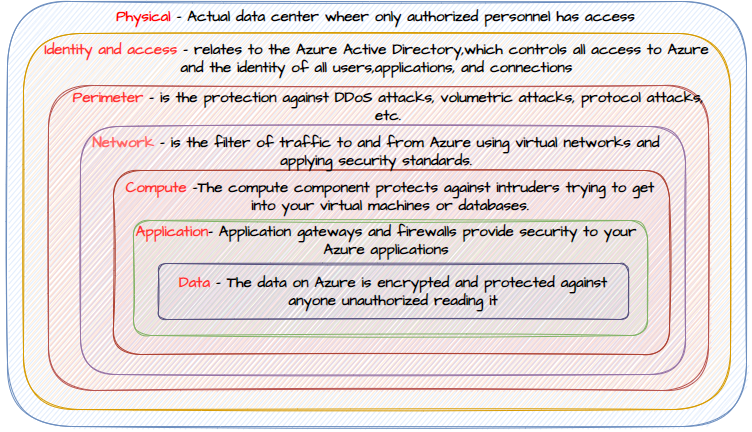
[MICROSOFT SENTINEL 10](#_Toc159343398)

[SETTING UP AZURE SENTINELS 10](#_Toc159343399)

# DEFENCE ON DEPTH

* **Defense in depth in Azure refers to the implementation of multiple layers of security controls and measures to protect Azure resources, data, and applications.**
* Azure provides a comprehensive set of security services and features that can be utilized to establish a strong defense in depth strategy.

**There are seven general layers of security in cloud computing**

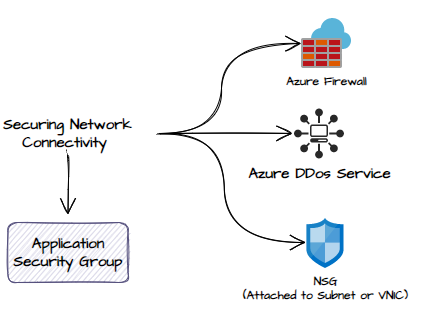


## COMPONENTS OF DEFENSE IN DEPTH

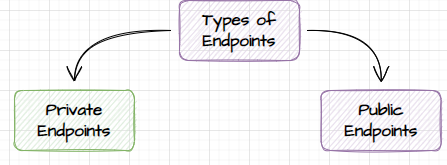
* IDENTITY AND ACCESS MANAGEMENT
  + Azure Active Directory (Azure AD) enables organizations to manage user identities, enforce strong authentication methods, and implement granular access control policies.
  + This helps ensure that only authorized users have access to Azure resources.
* NETWORK SECURITY
  + Azure Virtual Network (VNet) allows you to create isolated network environments within Azure.
  + You can implement Network Security Groups (NSGs), Azure Firewall, and Azure DDoS Protection to control inbound and outbound traffic, protect against network-based attacks, and mitigate distributed denial-of-service (DDoS) attacks.
* DATA ENCRYPTION
  + Azure offers various encryption capabilities to protect data at rest and in transit.
  + Azure Disk Encryption can be used to encrypt virtual machine disks, Azure Storage Service Encryption automatically encrypts data stored in Azure Storage, and Azure Key Vault provides a secure location to manage encryption keys and secrets.
* APPLICATION SECURITY
  + Azure provides services and tools to enhance application security, such as Azure Web Application Firewall (WAF) to protect web applications from common attacks, Azure Security Center to monitor and assess application security, and Azure Functions to securely run serverless applications.
* THREAT DETECTION AND MONITORING
  + Azure Security Center provides continuous monitoring and threat detection capabilities for Azure resources. It uses advanced analytics and machine learning to identify potential security threats, misconfigurations, and vulnerabilities. Azure Sentinel, a cloud-native security information and event management (SIEM) solution, helps organizations collect, analyze, and respond to security events across the Azure environment.
* INCIDENT RESPONSE AND RECOVERY
  + Azure provides features for incident response and recovery, such as Azure Backup for data protection and recovery, Azure Site Recovery for disaster recovery planning, and Azure Security Center's incident response capabilities to help organizations respond to and mitigate security incidents.

# SECURING NETWORK CONNECTIVITY

There are multiple ways to secure network connectivity which includes the following



## TYPES OF ENDPOINTS

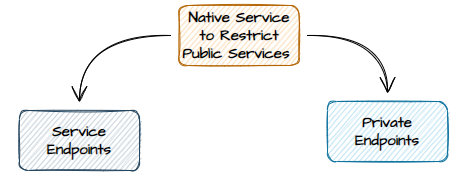


### PUBLIC ENDPOINT

* By default the PaaS service like Azure Storage, Azure SQL etc. These services are publicly reachable or or publicly exposed over the public internet.

|  |  |
| --- | --- |
| * When accessing these public services over a VNET (specifically from VM in the VNET) - **traffic from that virtual network to these managed services (like Azure Storage) traverses the public internet**. * **Additionally, these managed services end points are by default public endpoints, which are exposed to the public**.   *Note – Public endpoint - does not mean that the contents of those resources are accessible to the public. We still need proper authentication to grant access. However, these resources are still publicly exposed or publicly reachable,*  *which in scenarios in which your services contain sensitive content, this could be a little bit of a problem.* |  |

To limit the public exposure we have 2 native services and have private communication within Azure

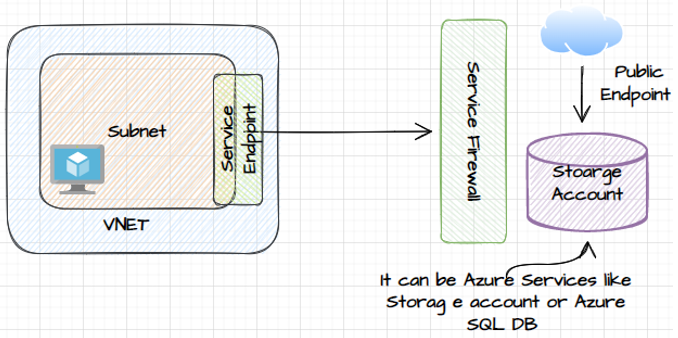


### SERVICE ENDPOINT

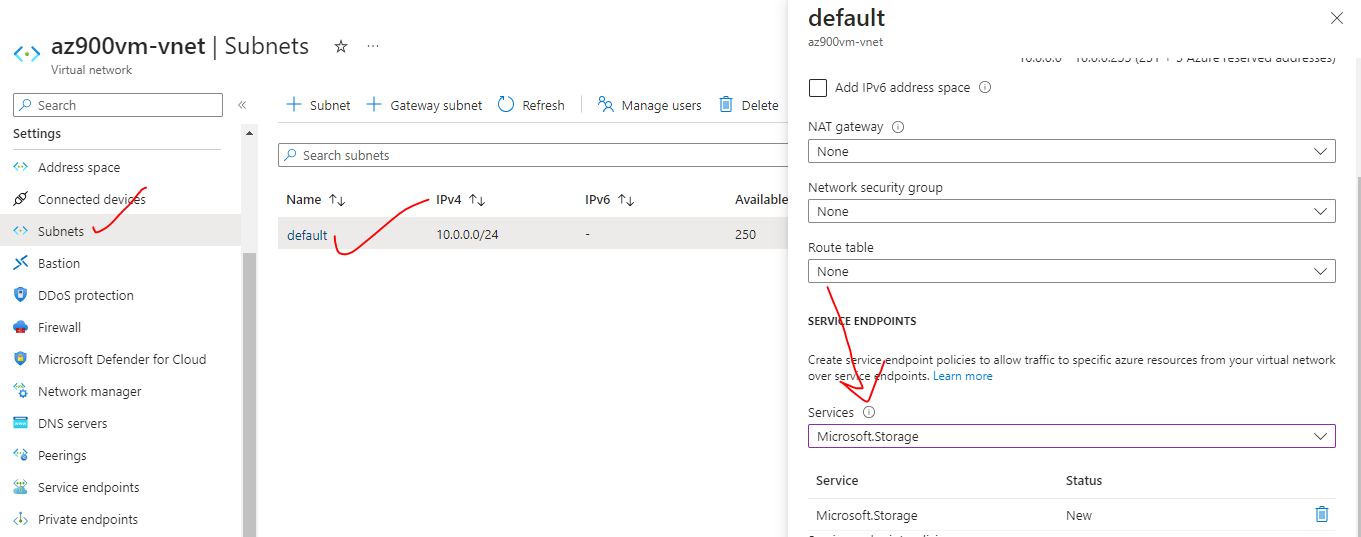
* Service endpoints allow **secure connectivity from Azure VMs that are part of Azure virtual network** to PaaS services such as Azure storage accounts or Azure Web apps, etc.
* There is no cost associated with service endpoint

EXAMPLE

* Let's say we have an Azure VM that is part of an Azure virtual network, that doesn't have a public IP address. The VM has an application that needs to connect onto an Azure storage account. Hence for private communication between them

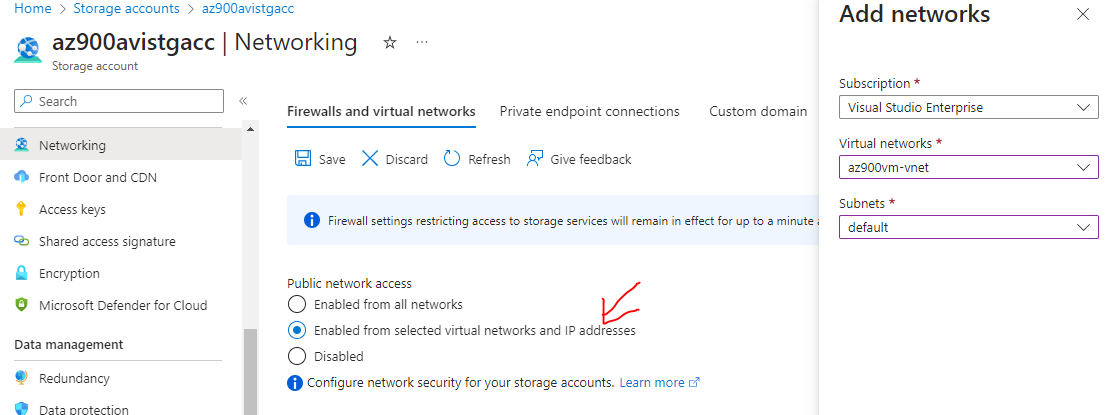


#### STEP 1: FROM VNET WE NEED TO ENABLE SERVICE ENDPOINT FOR STORAGE SERVICE



The Service endpoint has been created for the subnet of which the VM is part of.

#### STEP 2: FIREWALL SETTING IN STORAGE ACCOUNT

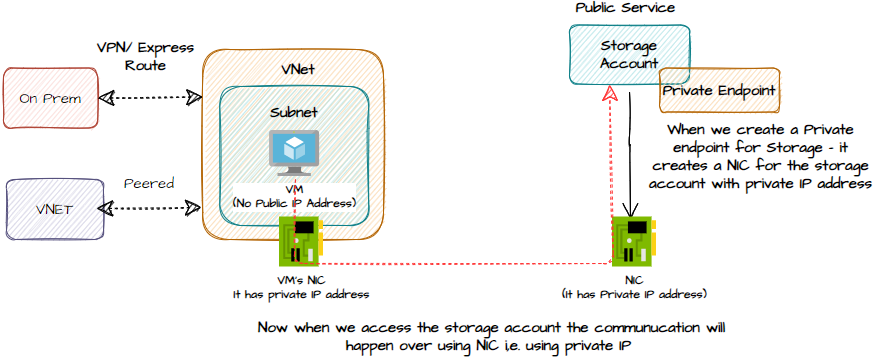




#### LIMITATIONS OF SERVICE ENDPOINTS

* Service Endpoints provides secure access to only Azure virtual networks. For non-Azure services or on-premises locations - the service endpoint provides private access over the public internet. However, we restrict to a small portion of public IPs only even though it is still going over the public internet. In other words, that connection is still not truly private, and there is still some public internet exposure.
* Service endpoints provide private access to the entirety of a managed service not a specific instance of a managed service. For example, when we set up service endpoints with a VNet subnet, it provides private access to the entirety of the Azure Storage service, not just to a single individual storage account.

### PRIVATE ENDPOINT



* The traffic between the virtual network and the PasS services goes via the Microsoft Backbone Network.

EXAMPLE

* *Let's say we have a storage account, which is a public service available on the Internet. When we implement private endpoint, it creates a Network interface card with a private IP*
* *When we access the storage account - the communication between this VM and the storage account will be done via this private IP address.*
* *Along with private IP – it also creates Azure private DNS zone. The private IP address of the VNIC mapped to the private DNS.*
* *The communication with the services like storage account can happen using private IP, (i.e., using DNS)*

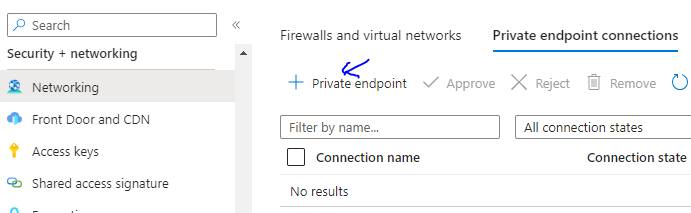
#### COMMUNICATION USING PRIVATE ENDPOINT

* *The Peered VNET can also do the communication with storage account using private endpoint.*
* *Similarly – from On-Prem environment which are connected using Site 2 Site VPN or Express route to the VNET/Subnet can also connect to storage account using Private endpoint.*
* *To validate the connectivity to a storage using private endpoint:* [*https://github.com/MicrosoftDocs/azure-docs/blob/main/articles/private-link/tutorial-private-endpoint-storage-portal.md*](https://github.com/MicrosoftDocs/azure-docs/blob/main/articles/private-link/tutorial-private-endpoint-storage-portal.md)

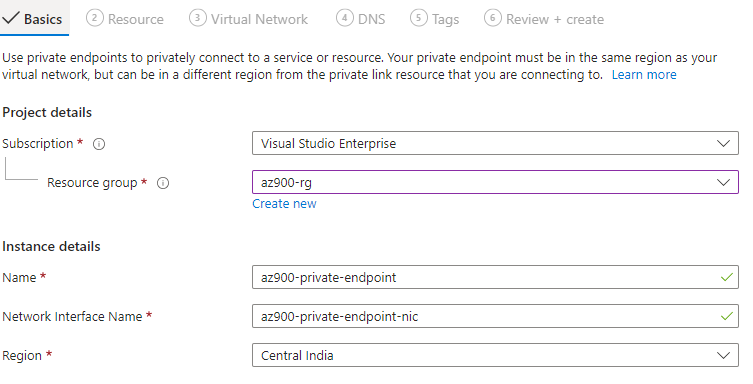
#### SETTING UP PRIVATE ENDPOINT (FOS STORAGE ACCOUNT)

*Step 1: Create a Storage Account*

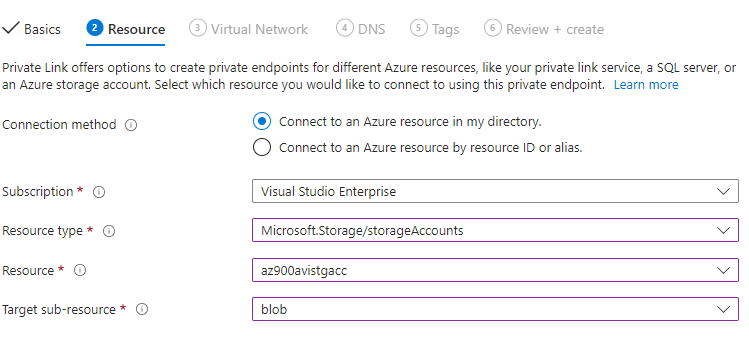
*Step 2: Set up private endpoint for Storage Account*

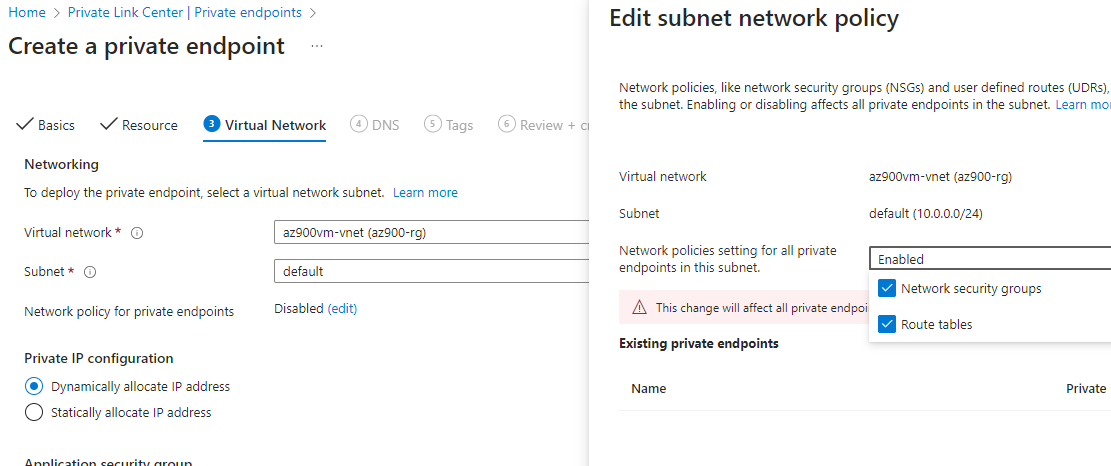


* The private endpoint a separate resource in Azure.
* The below wizard creates a Network interface Card

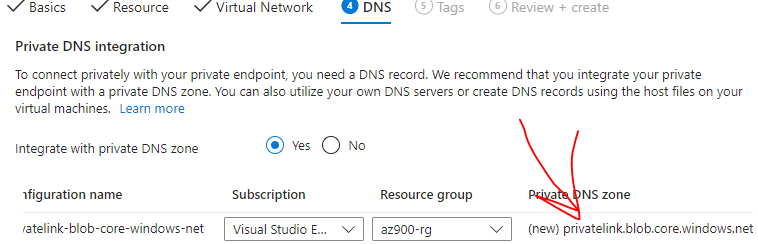


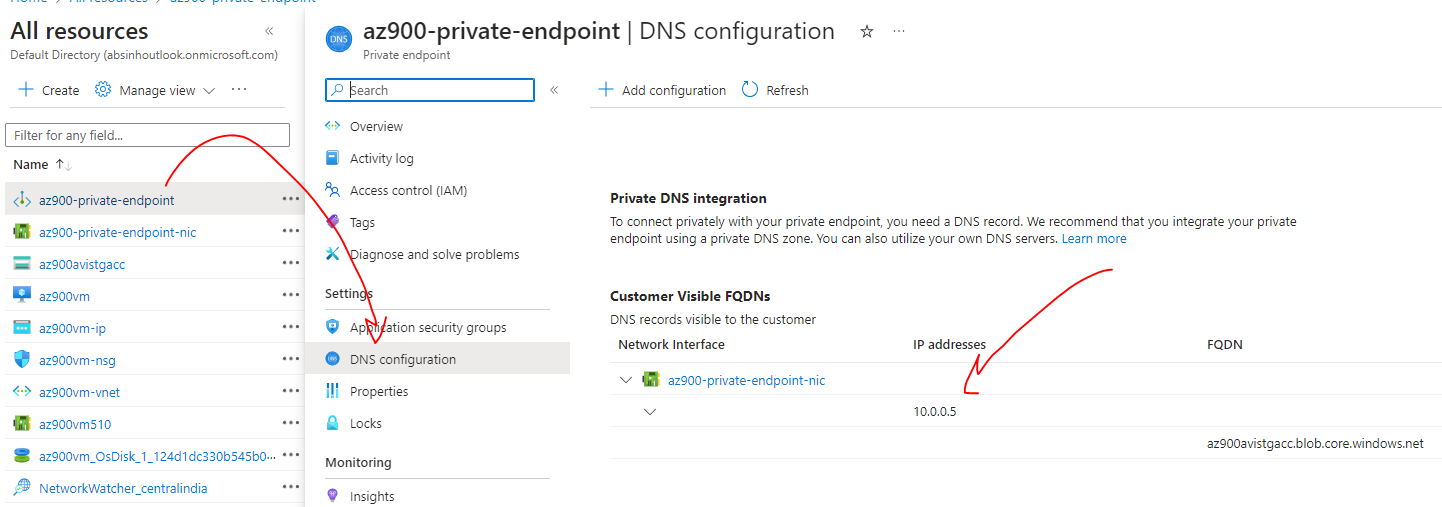
*Step 2: Select the Resource to which the endpoint will connect. Below private endpoint will target the ”blob” service*



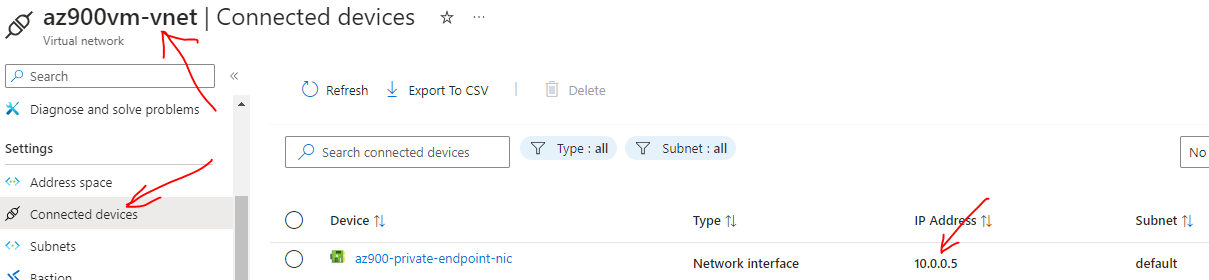


*Step 3: Azure provides the DNS name to the private endpoint(Private IP address)*

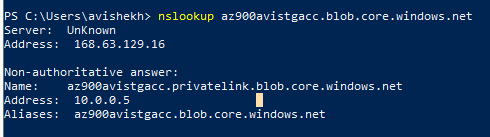




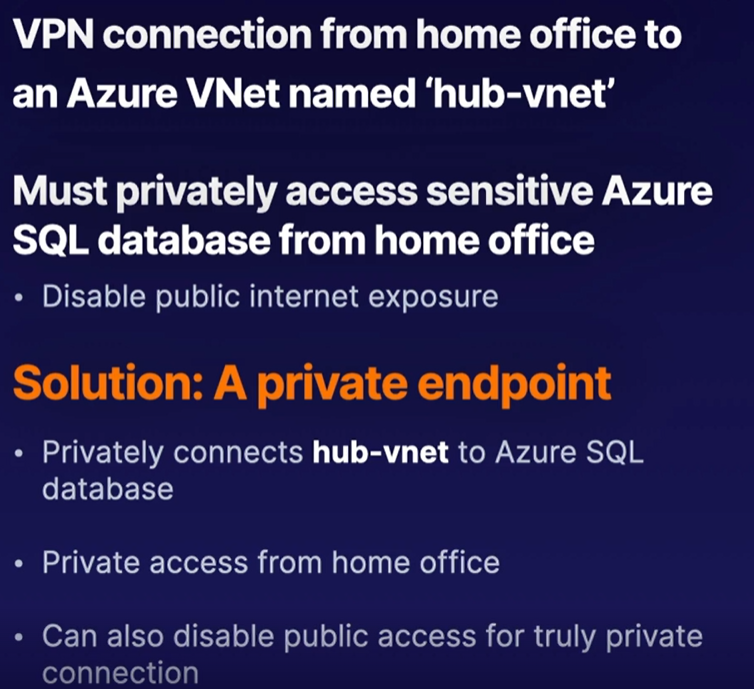
*View from VNET end (Connected devices will show the NIC attached to the private endpoint)*

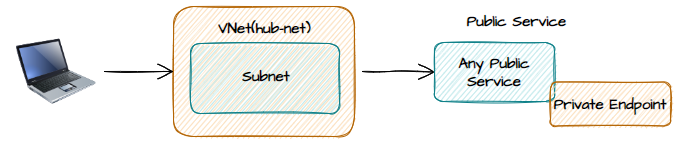


*To test the connection from the VM in the VNET*

**

#### USE CASE

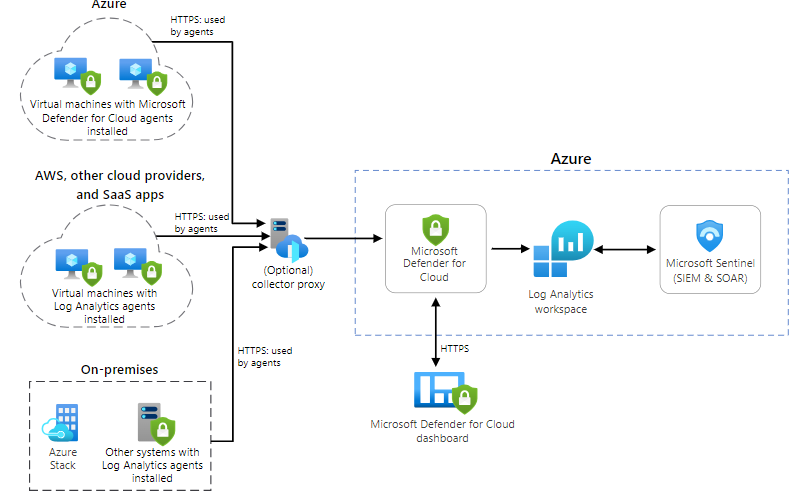




# MICROSOFT DEFENDER FOR CLOUD

* Microsoft Defender for Cloud is a cloud-based security solution provided by Microsoft.
* It is designed to help organizations detect and protect against advanced threats and potential breaches within their cloud and hybrid environments.
* It continually assessing the resources for security and provide recommendations to secure the Azure account.
* Based on the recommendations, we can implement certain steps to ensure that security is at the forefront
* We get a secure score to let us know - how secure our account is.

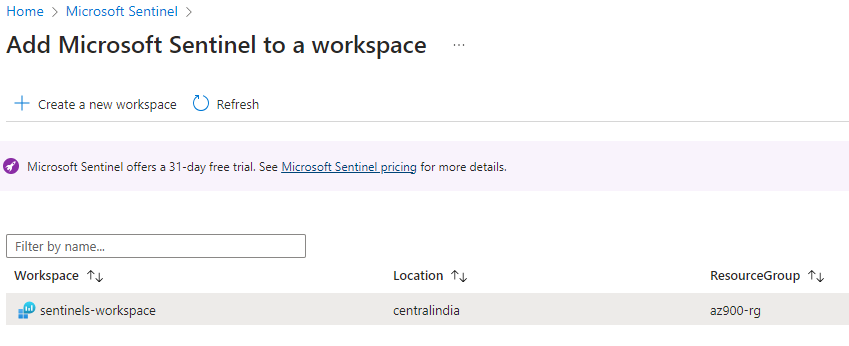
# MICROSOFT SENTINEL



* Microsoft Sentinel tool can be used for security information, event management, security orchestration, automation and response.
* When we host resources on a cloud platform, we can direct the logs to Log Analytics workspace. The logs can be for example, Azure Activity Log (for all the activities that are occurring in Azure account) or sign-in logs from AD.
* We can collect data not only from Azure based services but can also collect data from other third party services as well.
* **We can Microsoft Sentinel on top of the Log Analytics workspace which can look at the collected data from these different sources and detect any sort of threats**.
* Based on collected data it can provide data about the of threat patterns so that we can then respond and investigate threats.

## SETTING UP AZURE SENTINELS

1. Step 1: Create a Log Analytics Workspace
2. Step 2: Creating Azure Sentinels Service. Note – while creation itself it will ask for log analytics workspace.



* DATA CONNECTORS:
  + For the collection of data. Configuration 🡪 data connectors.
  + There are various connectors that allow us to collect data from various sources e.g. Azure Service and other third party services as well.
* ANALYTICS
  + Once the data is collected we can search for any sort of threat using in-built or custom rules from Analytics
  + Using Playbooks we can automate i.e. we automate the mitigation to the threats that are detected.

