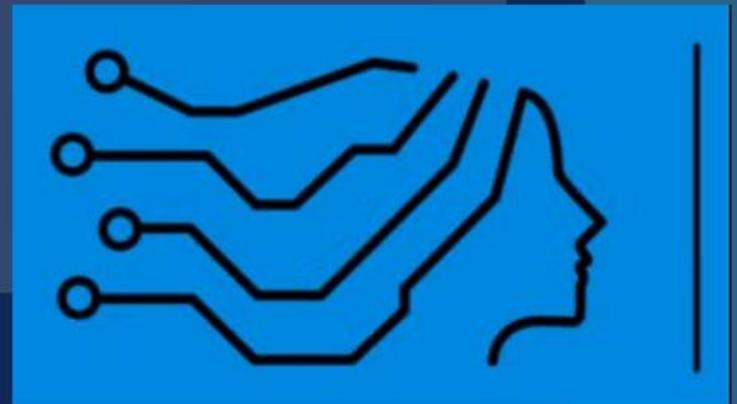


ANOTHER BRICK IN THE FIREWALL

How to Secure your Azure Data Platform

Grace O'Halloran





INTRODUCTION

- Grace O'Halloran
- Principal Data Engineering Consultant
@ Advancing Analytics
- Microsoft Data Platform MVP
- 8+ yrs working with Azure Data Platforms
- Microsoft Certified Azure Developer & Administrator



 Grace O'Halloran (grace-o-halloran)
 @graceaohalloran

 grace@advancinganalytics.co.uk
 www.thinkingacloud.co.uk



<https://github.com/gracedev94/GraceOH-CommunityContent>

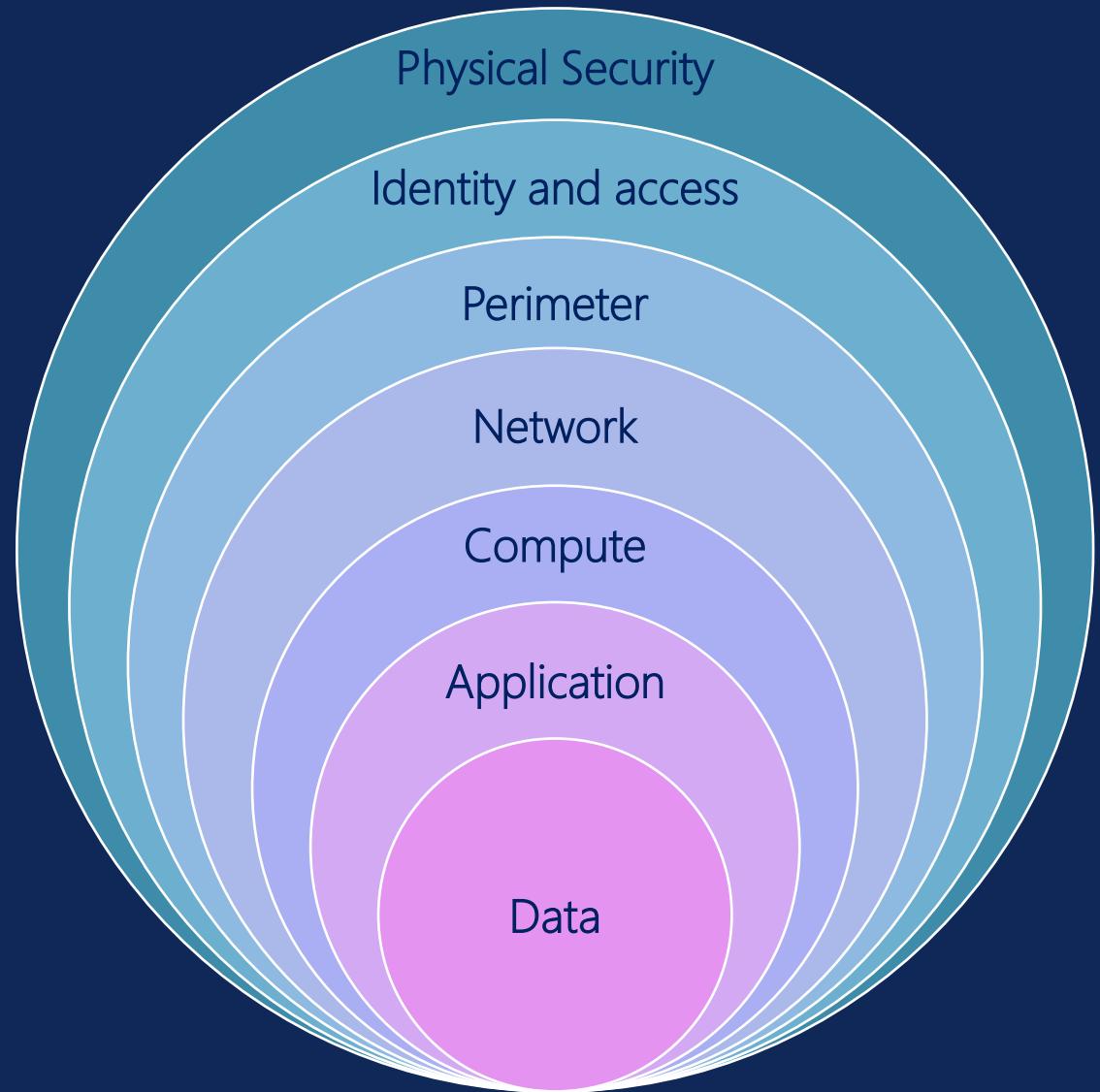
ANOTHER BRICK IN THE FIREWALL

Why care about Network Security	Networks	Ingress & Egress	Azure Private Link	Data Platform Components
<ul style="list-style-type: none">I do data – why is this relevant to me?	<ul style="list-style-type: none">Hub-and-spoke TopologyAddress Space Considerations	<ul style="list-style-type: none">Firewalls & UDRsNetwork Security GroupsSecure Development Access	<ul style="list-style-type: none">Private EndpointsAzure Private DNS	<ul style="list-style-type: none">Azure Data FactoryFabricAzure DevOpsDatabricks

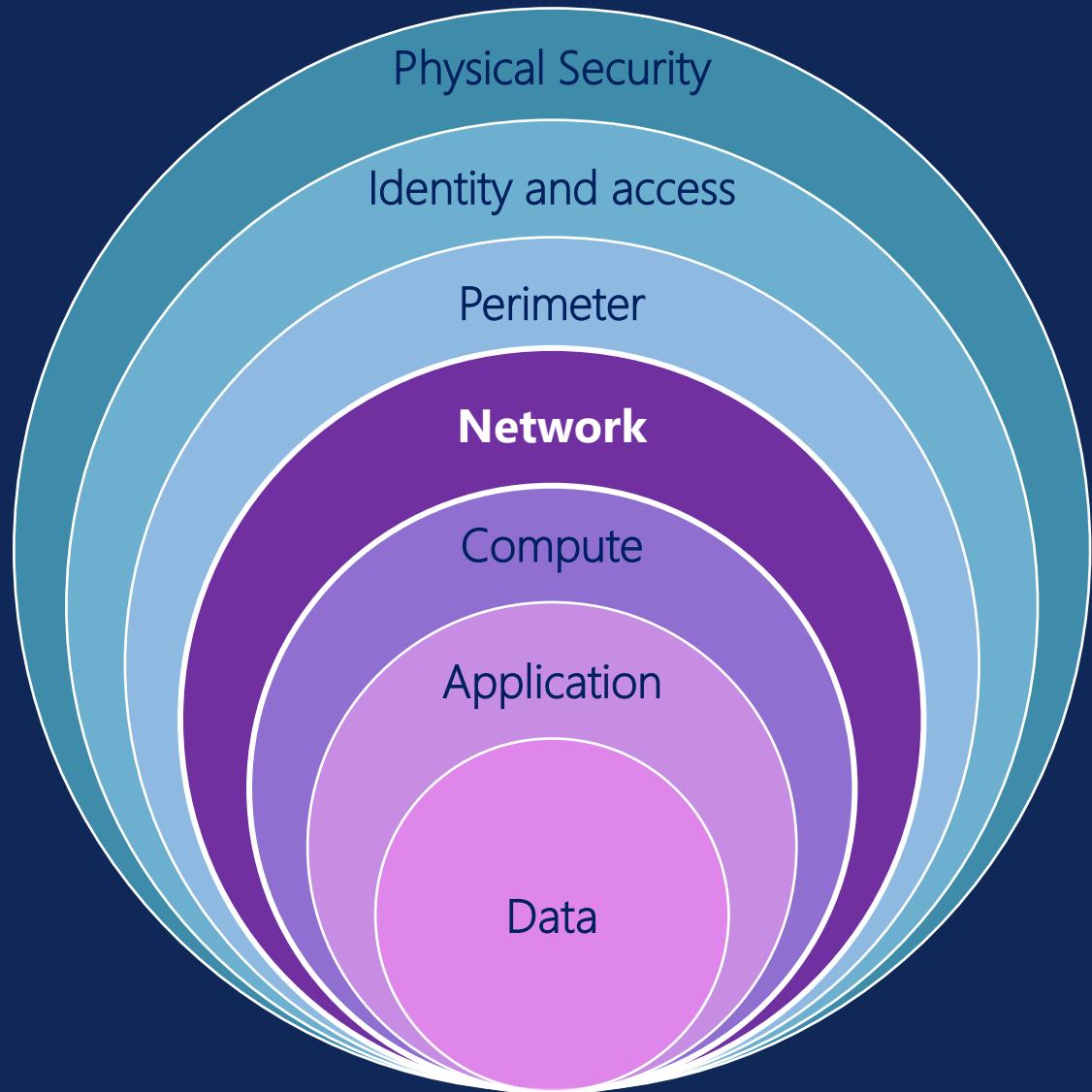
WHY CARE ABOUT NETWORK SECURITY

I do data – why is this relevant to me?

DEFENSE IN DEPTH



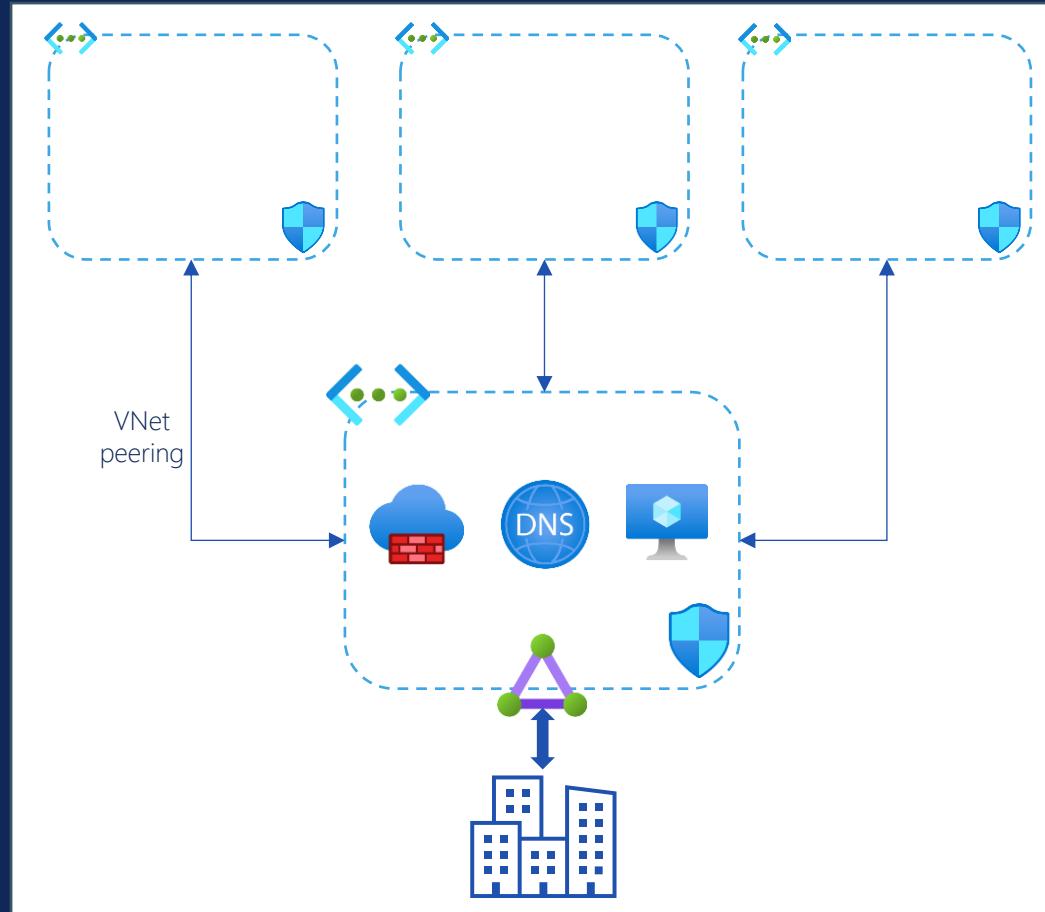
DEFENSE IN DEPTH



NETWORKS

Hub-and-Spoke Topology

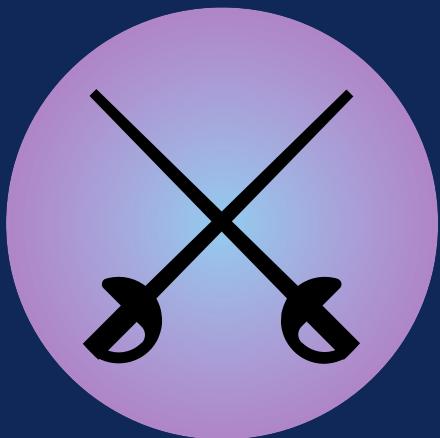
HUB-AND-SPOKE TOPOLOGY



NETWORKS

Address Space Considerations

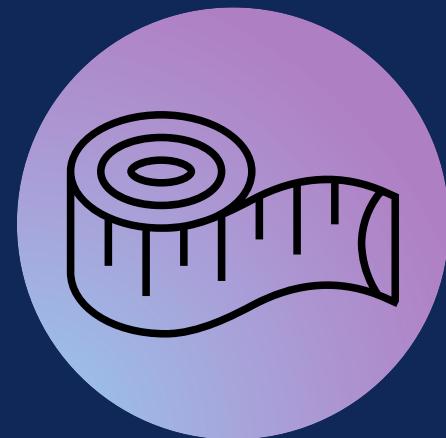
ADDRESS SPACE CONSIDERATIONS



Avoid Conflicts



Use IPAM



Size Requirements



Allow for Growth

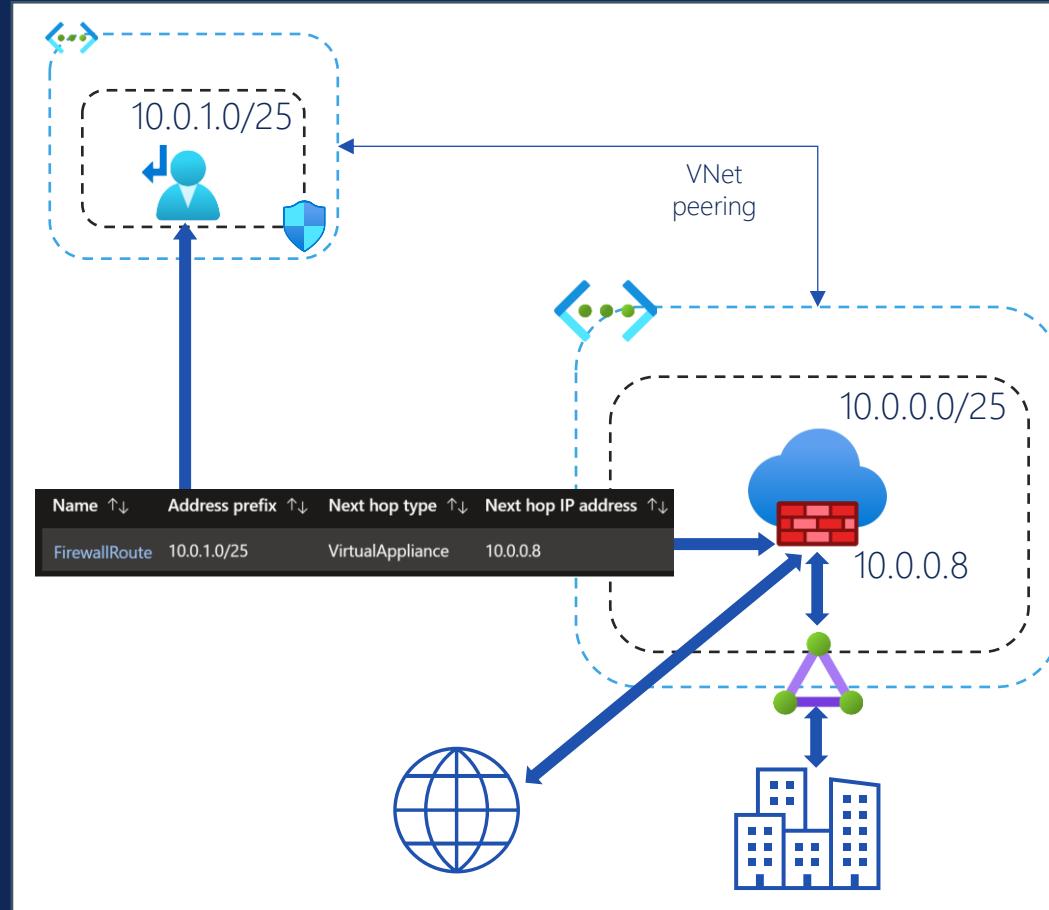
INGRESS & EGRESS

Firewalls & UDRs

"Ingress and Egress are fancy
words for Inbound and Outbound."

- Grace O'Halloran, now.

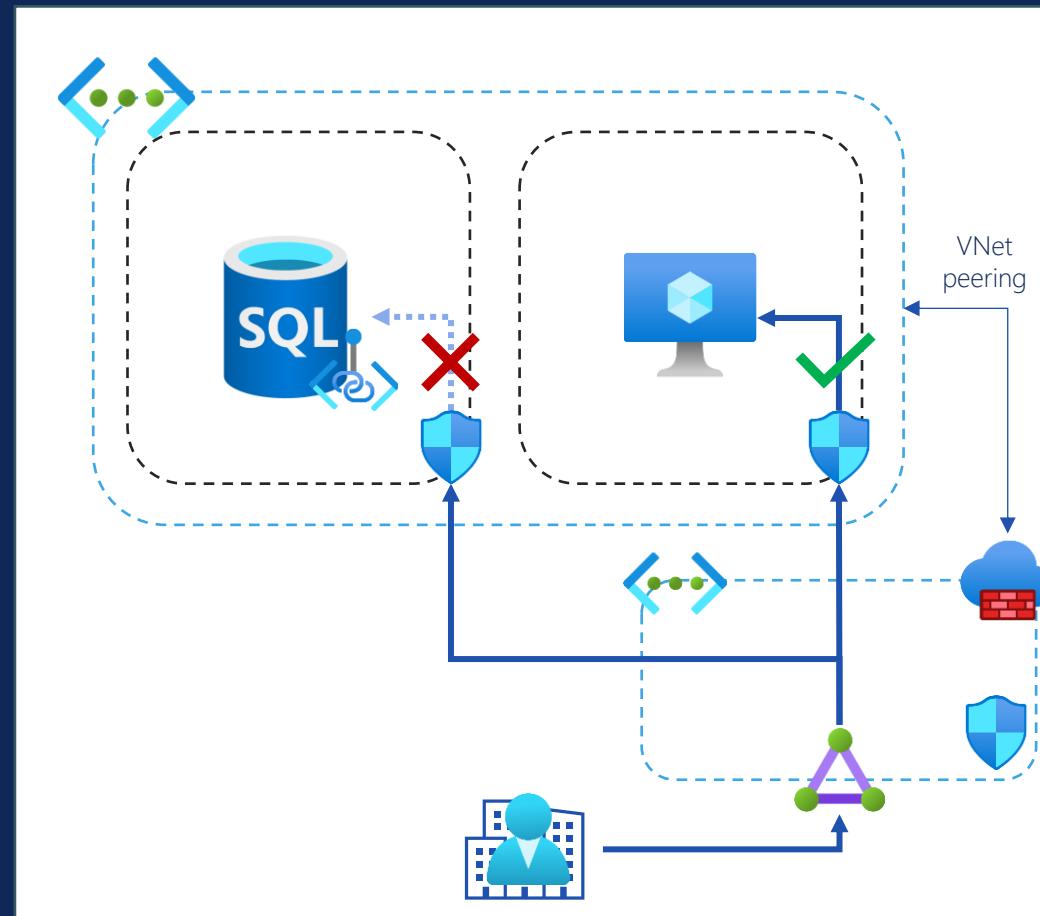
FIREWALLS & USER DEFINED ROUTES



INGRESS & EGRESS

Network Security Groups

NETWORK SECURITY GROUPS



INGRESS & EGRESS

Secure Development Access

SECURE DEVELOPMENT ACCESS



Virtualisation Tool

- Azure Virtual Desktop
- Windows Cloud PC
- Citrix
- VMWare



Microsoft DevBox

- DevBox provides preconfigured cloud-based developer workstations



Azure Bastion

- Azure Bastion provides a host for users to securely connect to Azure VMs.



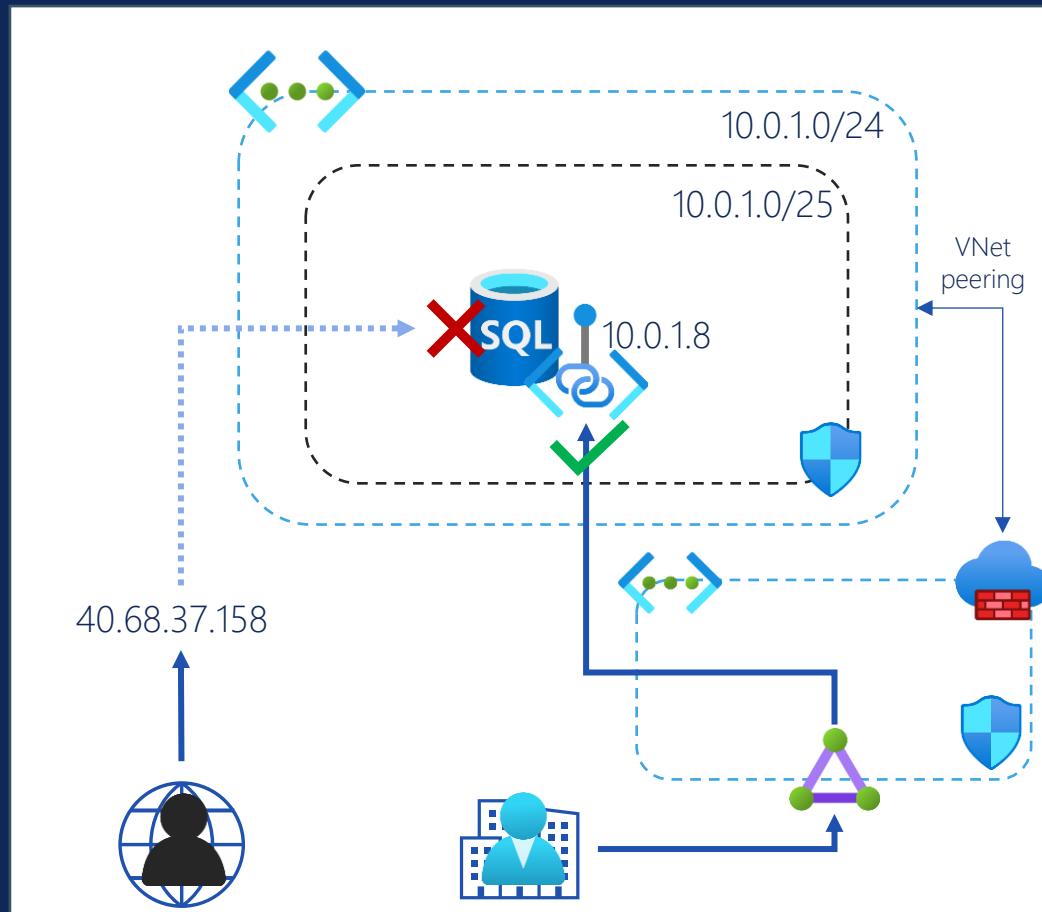
Jump Box

- Infra is responsible for maintaining the security of the jump box.

AZURE PRIVATE LINK

Private Endpoints

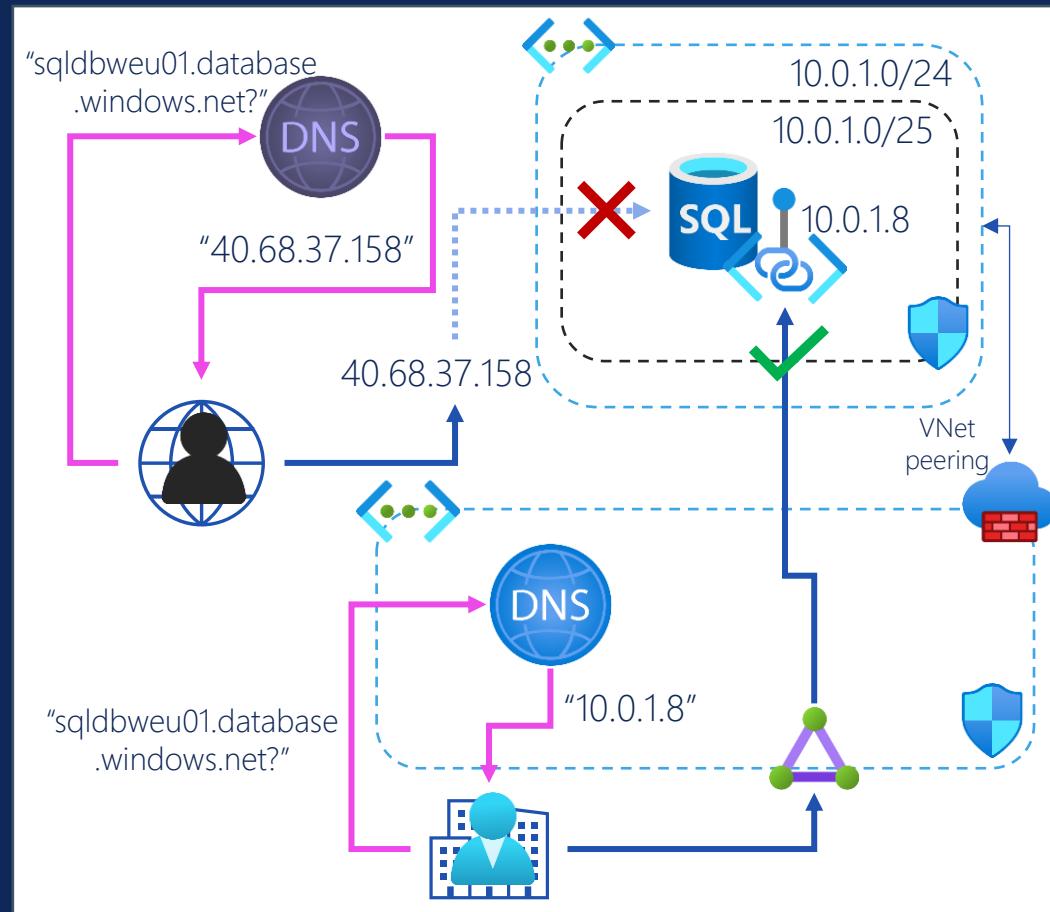
AZURE PRIVATE LINK



AZURE PRIVATE LINK

Azure Private DNS

AZURE PRIVATE DNS



PRIVATE DNS ZONES



Central

Private DNS Zones should be part of a central DNS solution



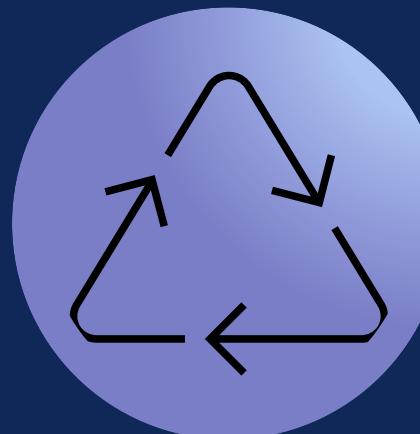
One per Domain

One Private DNS Zone required per Azure domain



Naming

Private DNS Zones used for Private Link must have specific names



Reusable

Resources part of the same domain can reuse the same Private DNS Zone

PRIVATE DNS ZONES

Azure SQL Server resource name:	sqlbweu01
Azure SQL Server public endpoint:	sqlbweu01.database.windows.net
Domain:	database.windows.net
Azure Private DNS Zone required:	privatelink.database.windows.net

A RECORDS

The screenshot shows the Azure portal interface for managing a Private DNS zone named `privatelink.database.windows.net`. The left sidebar includes navigation links for Home, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Virtual network links, Properties, Locks), Monitoring (Alerts), and Metrics.

The main content area displays the **Essentials** section with resource group, subscription, and tag information. It also features a search bar for record sets and a table listing existing records.

Name	Type	TTL	Value
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1
sqldbweu01	A	3600	10.0.1.8

A RECORDS

Home > privatelink.database.windows.net >

sqlbweu01

privatelink.database.windows.net

Save Discard Delete Access Control (IAM) Metadata

Name
sqlbweu01.privatelink.database.windows.net.

Type
A

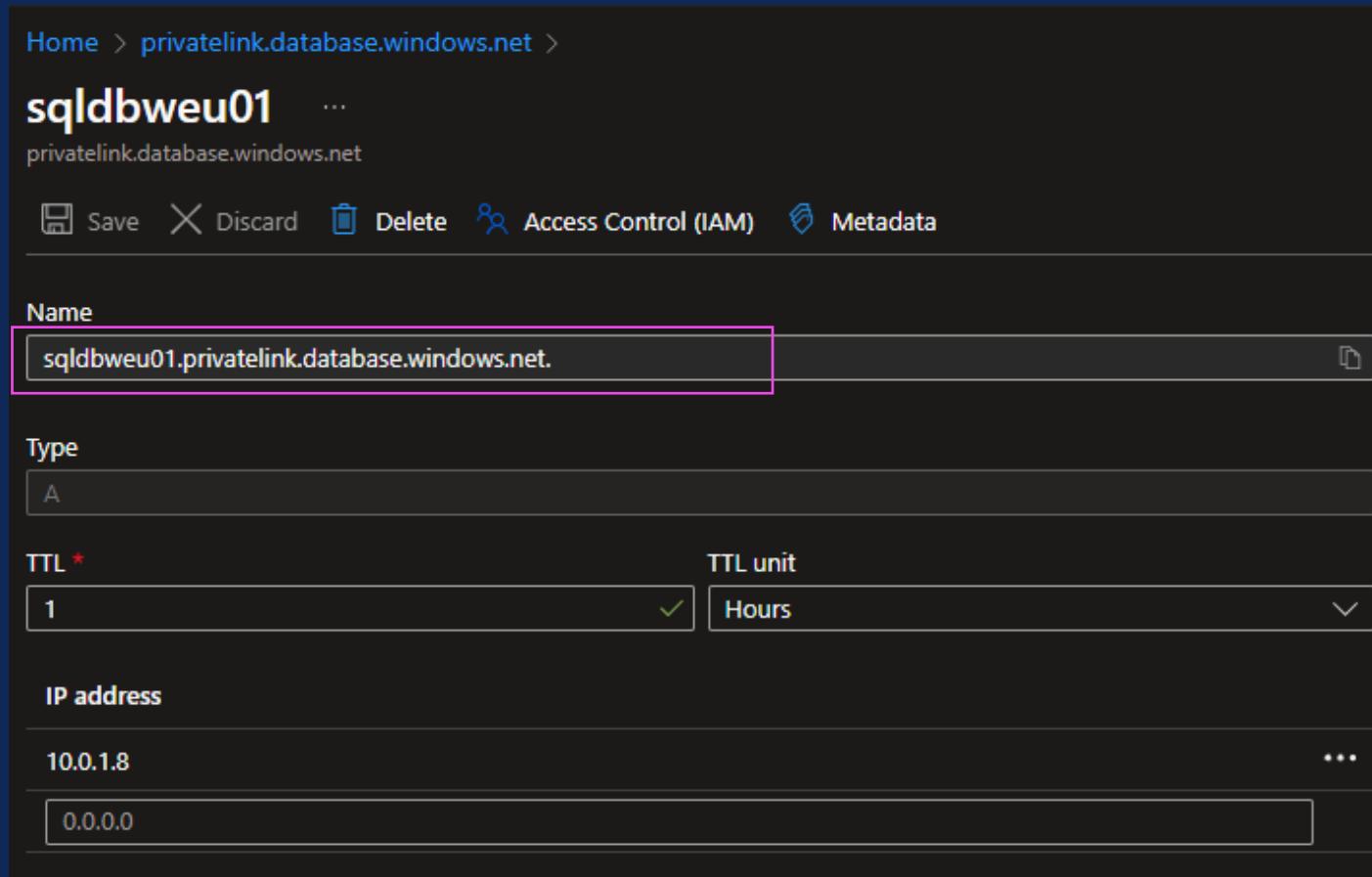
TTL *
1

TTL unit
Hours

IP address
10.0.1.8

0.0.0.0

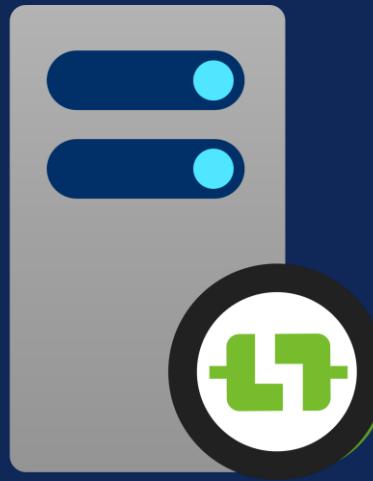
...



DATA PLATFORM COMPONENTS

Azure Data Factory: Integration Runtimes

ADF: INTEGRATION RUNTIMES



ADF: INTEGRATION RUNTIMES

Azure IR with Managed VNet

Use the Azure-hosted IR with the Managed VNet enabled in order to secure the compute inside a private network.

You must use Managed Private Endpoints to allow your IR access to your protected resources.

Self-hosted IR (SHIR)

SHIRs are created by installing an IR application on your own machine, this can be an on-prem server or an Azure VM.

The SHIR server will utilise existing Private Endpoints to securely connect to your protected resources.

ADF: INTEGRATION RUNTIMES

Pros	Azure IR with Managed VNet	Self-hosted IR (SHIR)
Cons	<ul style="list-style-type: none">💡 Fully managed and serverless⚡ Elastic scaling🧱 No maintaining of firewall rules	<ul style="list-style-type: none">💻 High Availability options💰 Runtime costs are cheaper🌐 Allows for easy connectivity to on-prem data sources
	<ul style="list-style-type: none">❓ No control over address space🏃 Requires additional private endpoints💰 Can increase cost🔗 Doesn't work easily with on-prem connectivity	<ul style="list-style-type: none">🏗 Requires pre-existing infrastructure🔧 Responsible for providing and maintaining the server🧱 Maintenance of firewall rules💻 Pay for compute resource

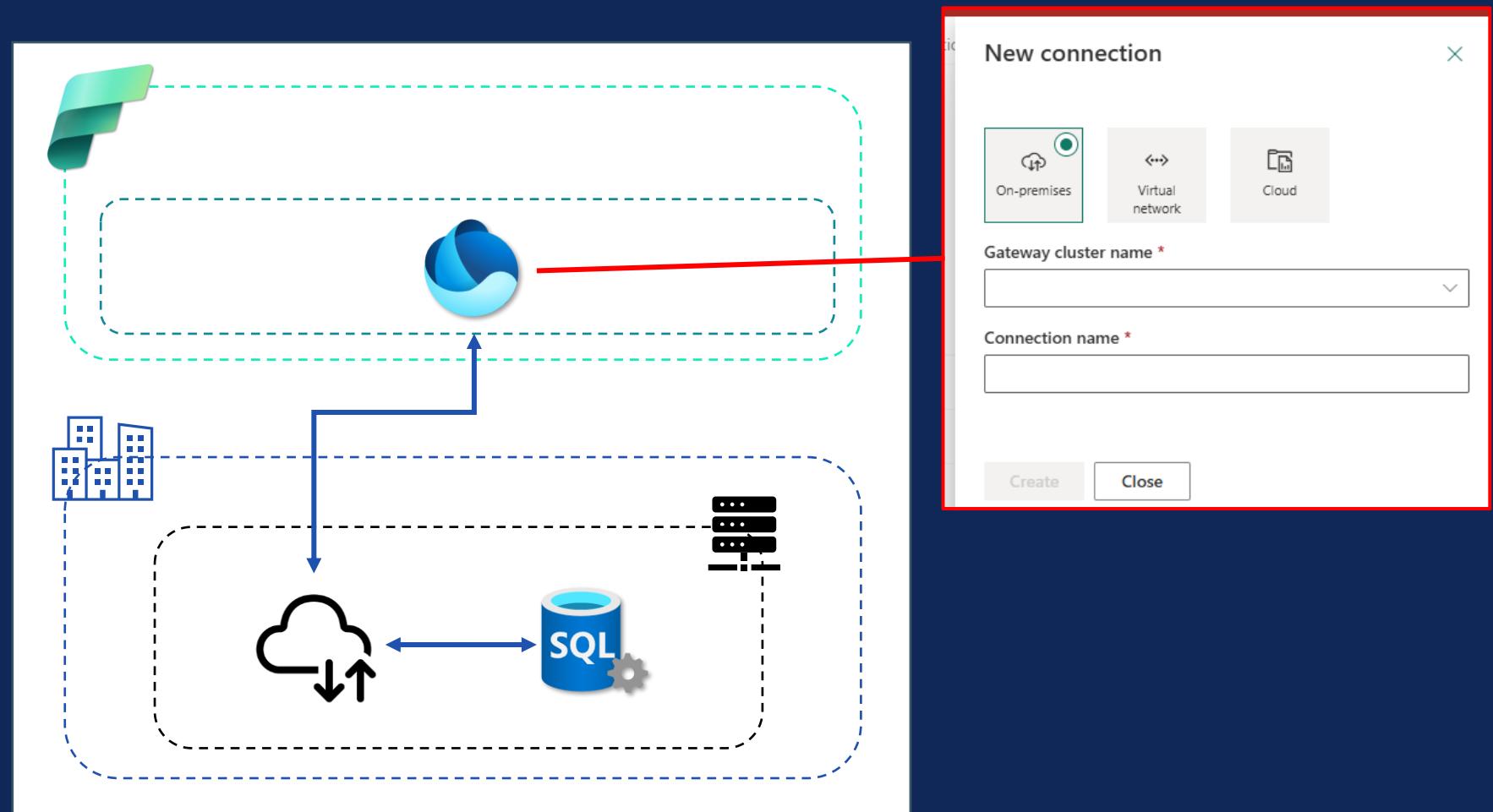
DATA PLATFORM COMPONENTS

Fabric: Data Gateways

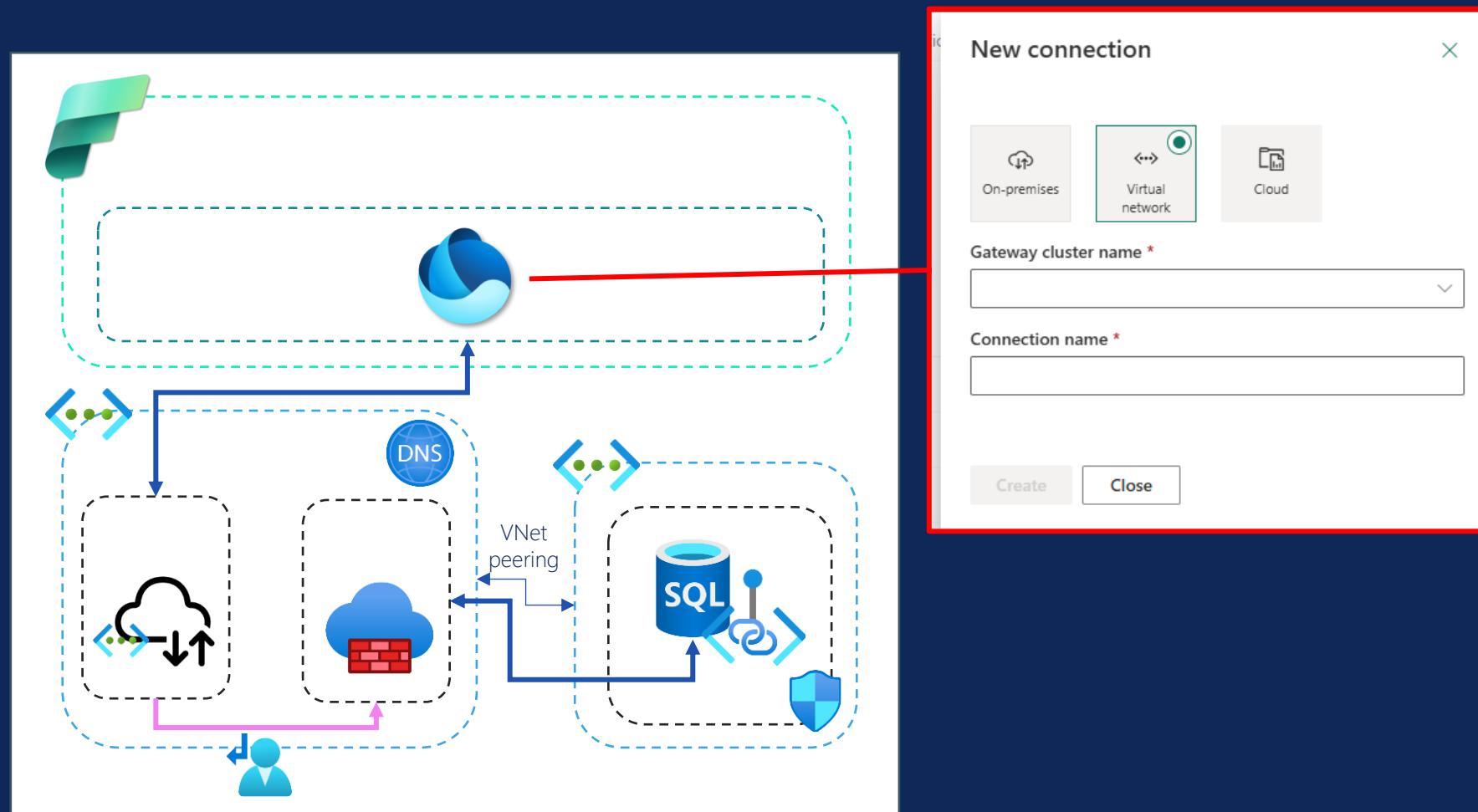
FABRIC: DATA GATEWAYS



FABRIC: ON-PREM DATA GATEWAY



FABRIC: VNET DATA GATEWAY



DATA PLATFORM COMPONENTS

Azure DevOps: Self-hosted Build Agents

AZURE DEVOPS: BUILD AGENTS

Get the agent X

Windows **macOS** **Linux**

x64 **x86**

System prerequisites
Configure your account
Configure your account by following the steps outlined [here](#).

Download the agent [Download](#)

Create the agent

```
PS C:\> mkdir agent ; cd agent
PS C:\agent> Add-Type -AssemblyName System.IO.Compression.FileSystem ;
[System.IO.Compression.ZipFile]::ExtractToDirectory("$HOME\Downloads\vsts-
agent-win-x64-3.225.0.zip", "$PWD")
```

Configure the agent [Detailed instructions](#)

```
PS C:\agent> .\config.cmd
```

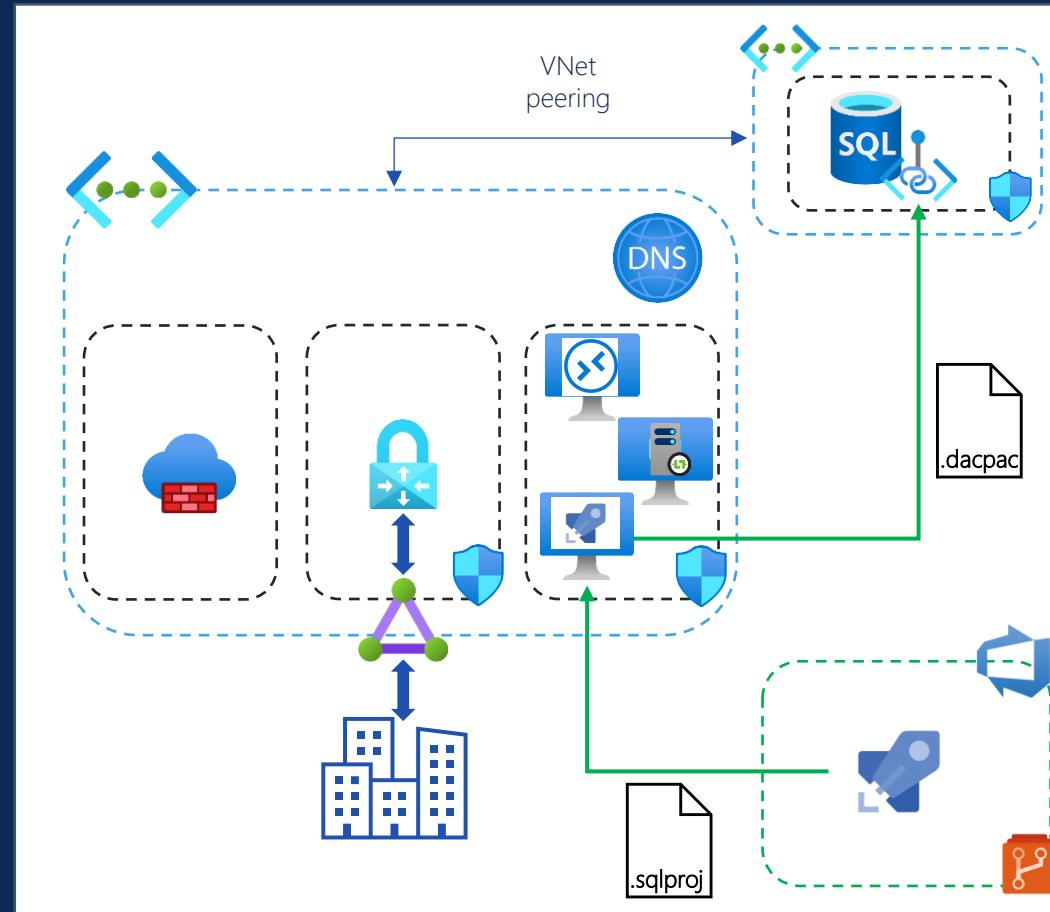
Optionally run the agent interactively
If you didn't run as a service above:

```
PS C:\agent> .\run.cmd
```

That's it!

[More Information](#)

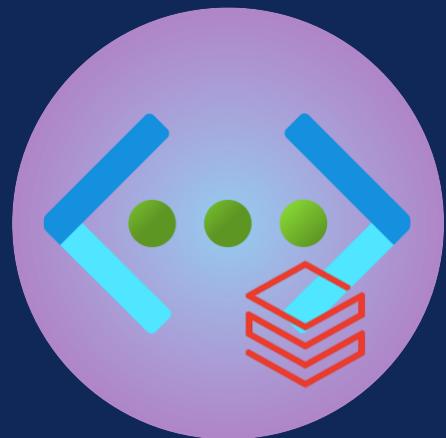
AZURE DEVOPS: BUILD AGENTS



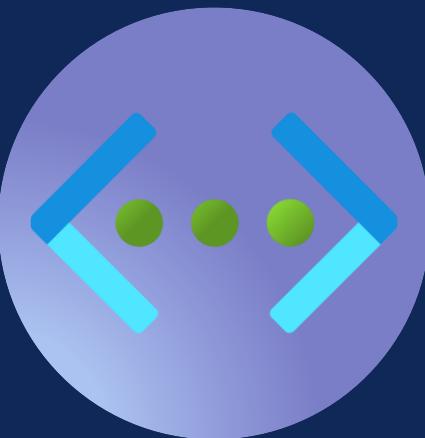
DATA PLATFORM COMPONENTS

Databricks: VNet Injection, Secure Cluster
Connectivity, Private Link, Network Connectivity,
Configurations.

DATA BRICKS



Managed VNet



VNet Injection

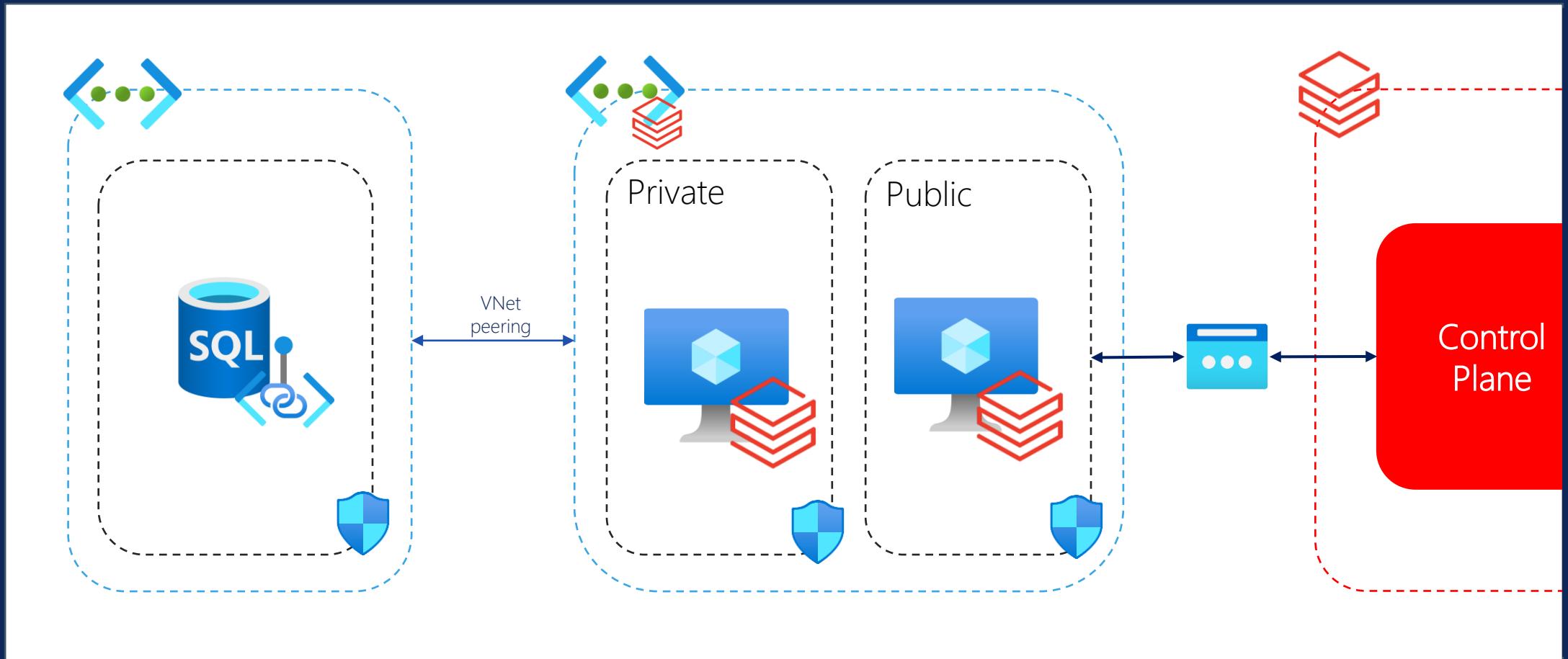


**Secure Cluster
Connectivity**

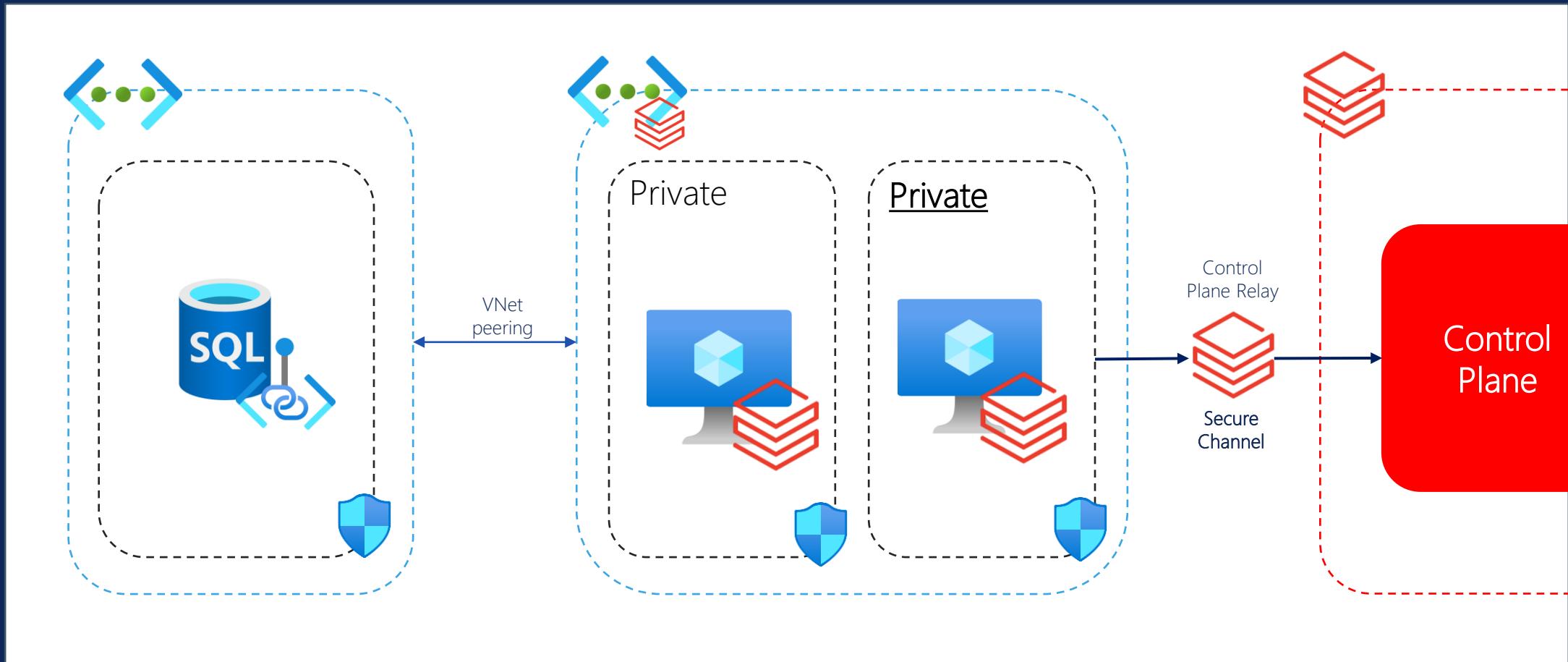


Private Link

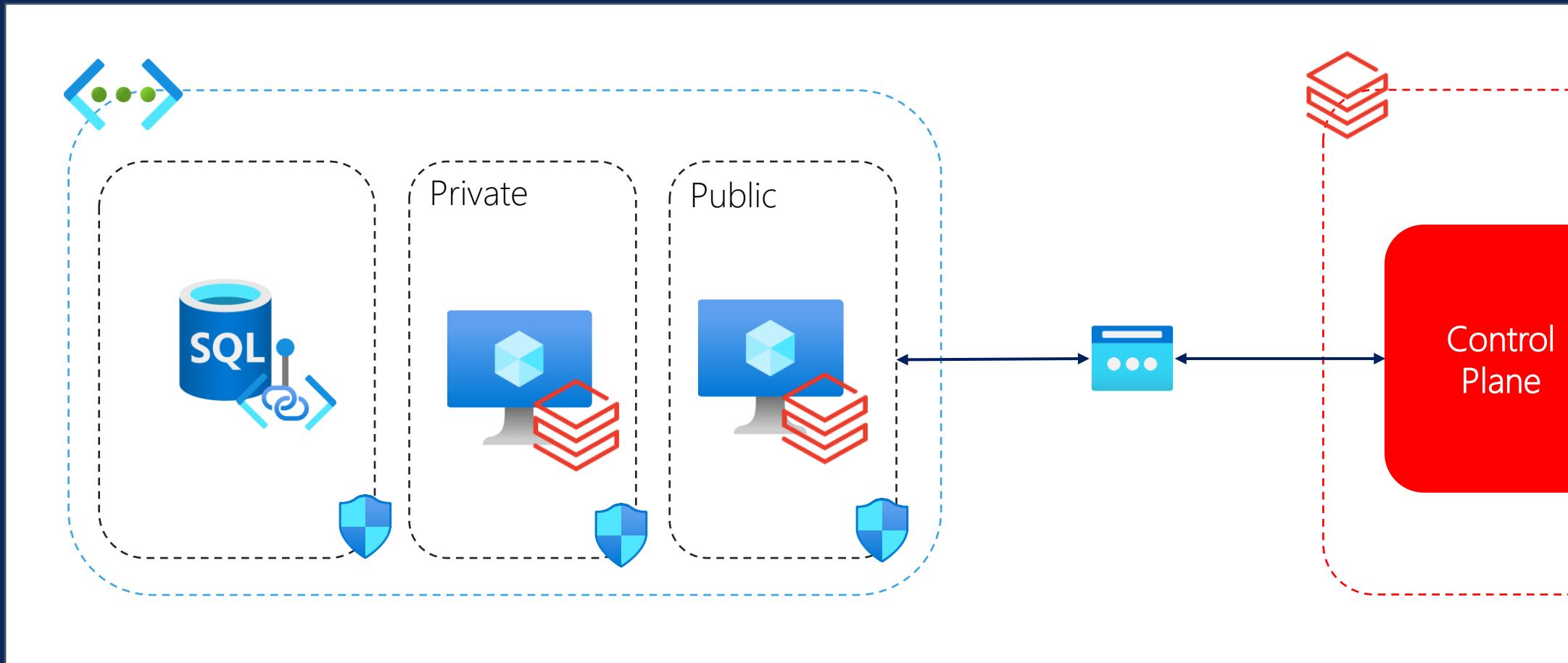
DATA BRICKS: MANAGED VNET



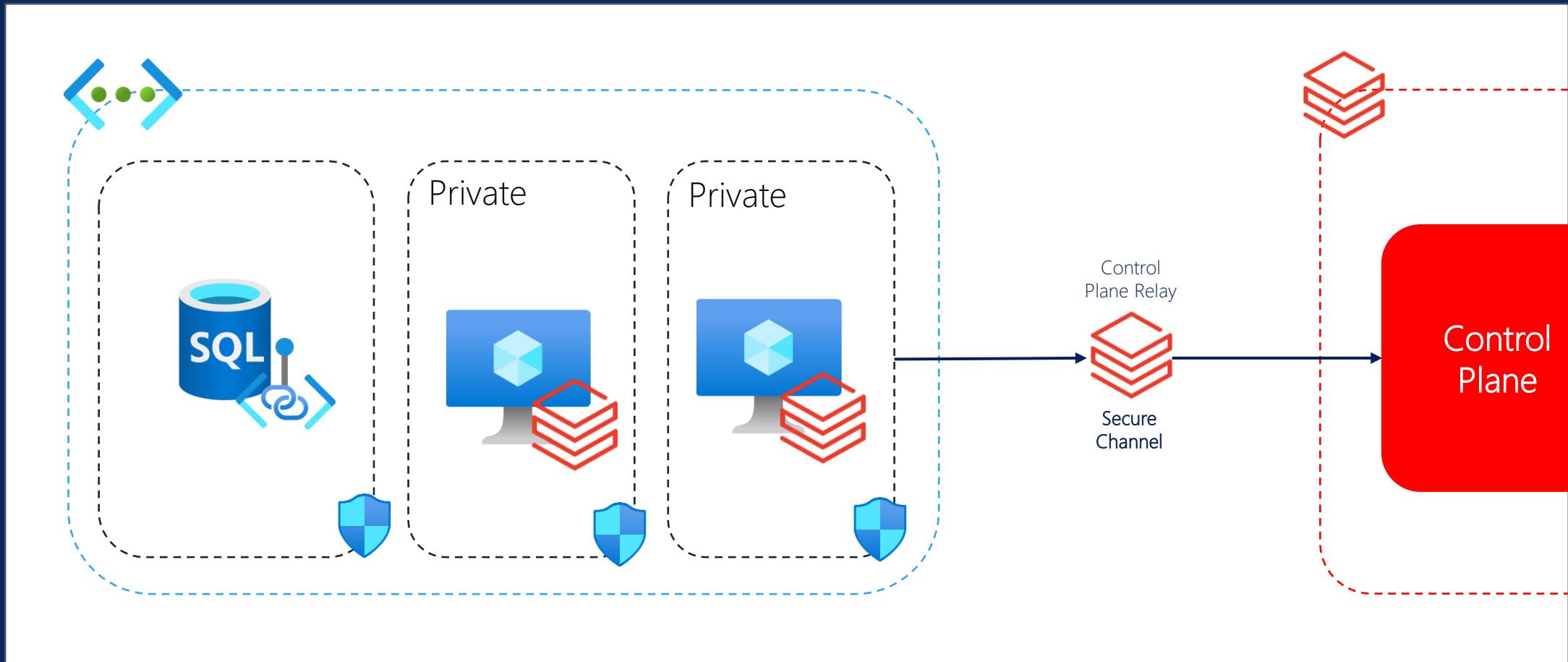
DATA BRICKS: MANAGED VNET & SCC



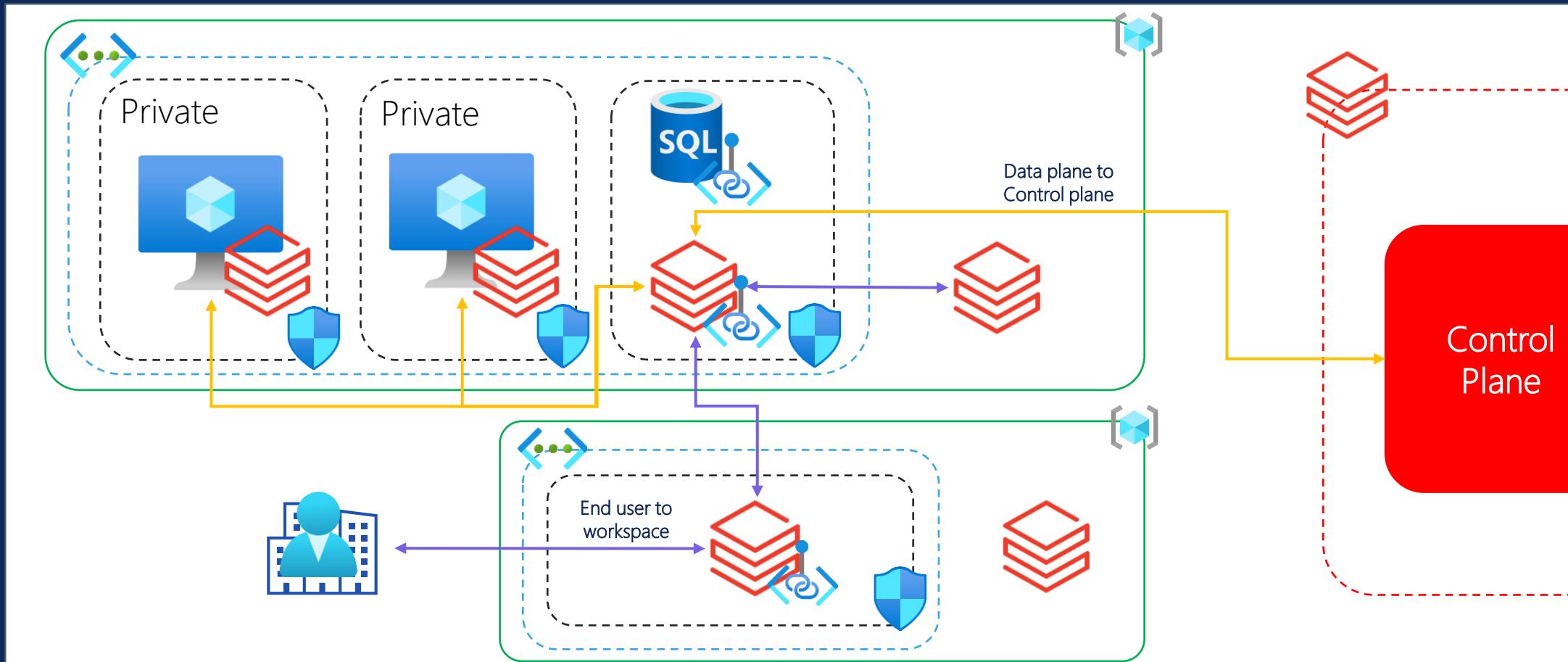
DATABRICKS: VNET INJECTION



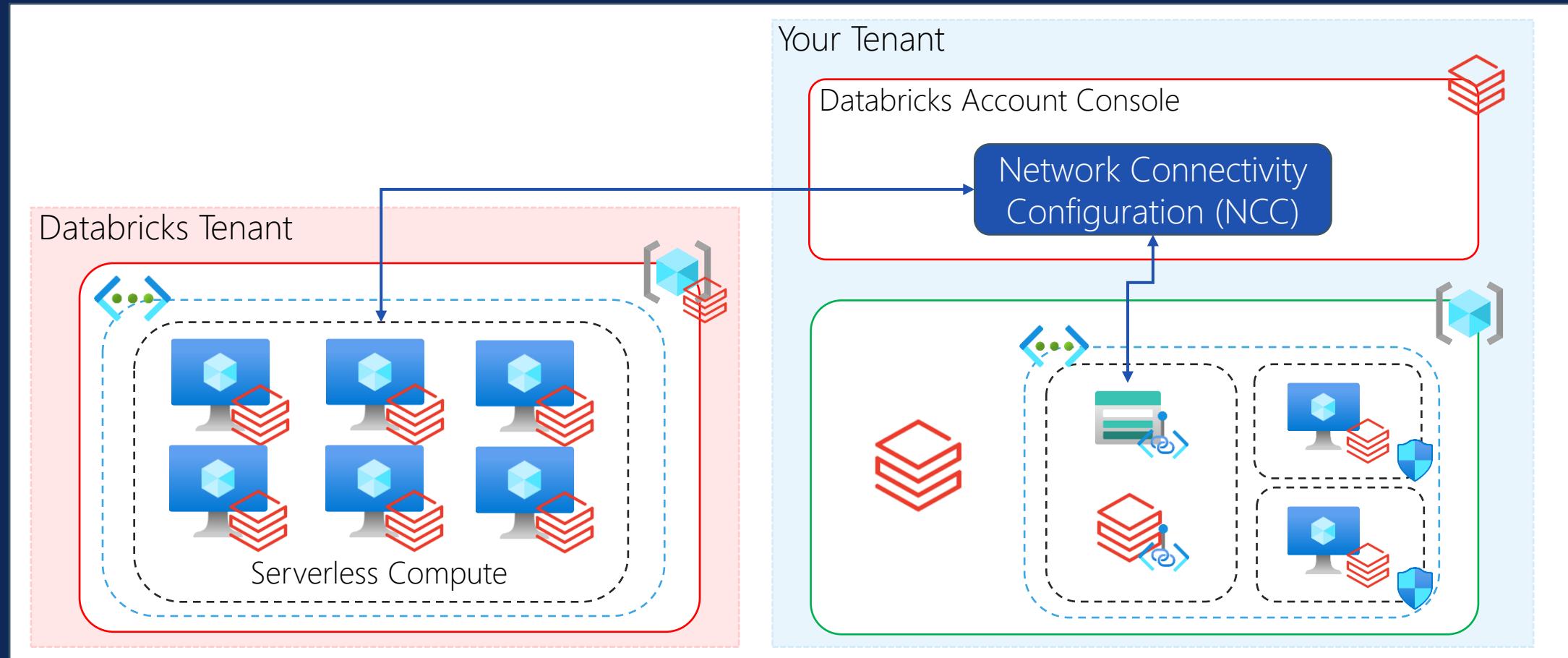
DATABRICKS: VNET INJECTION & SCC



DATABRICKS: VNET INJECTION & PRIVATE LINK



DATABRICKS: NCCS





Private Endpoints -
YouTube



ADF IRs - Blog



Community Content
- Github

THANK YOU

Any questions?



Another Brick in the Firewall: How to Secure your Azure Data Platform

- Grace O'Halloran (grace-o-halloran)
- @graceaohalloran
- grace@advancinganalytics.co.uk
- www.thinkingacloud.co.uk
- <https://github.com/gracedev94/GraceOH-CommunityContent>