Designing Data Architectures that InfoSec will actually approve

Craig Porteous

Principal Consultant

https://craigporteous.com

@cporteous

https://github.com/cporteou

databricks
PARTNER PROGRAM
SOLUTIONS ARCHITECT CHAMPION

MVP Microsoft® Most Valuable Professional

Designing Data Architectures that InfoSec will actually approve

Craig Porteous

Principal Consultant

⌂ https://craigporteous.com

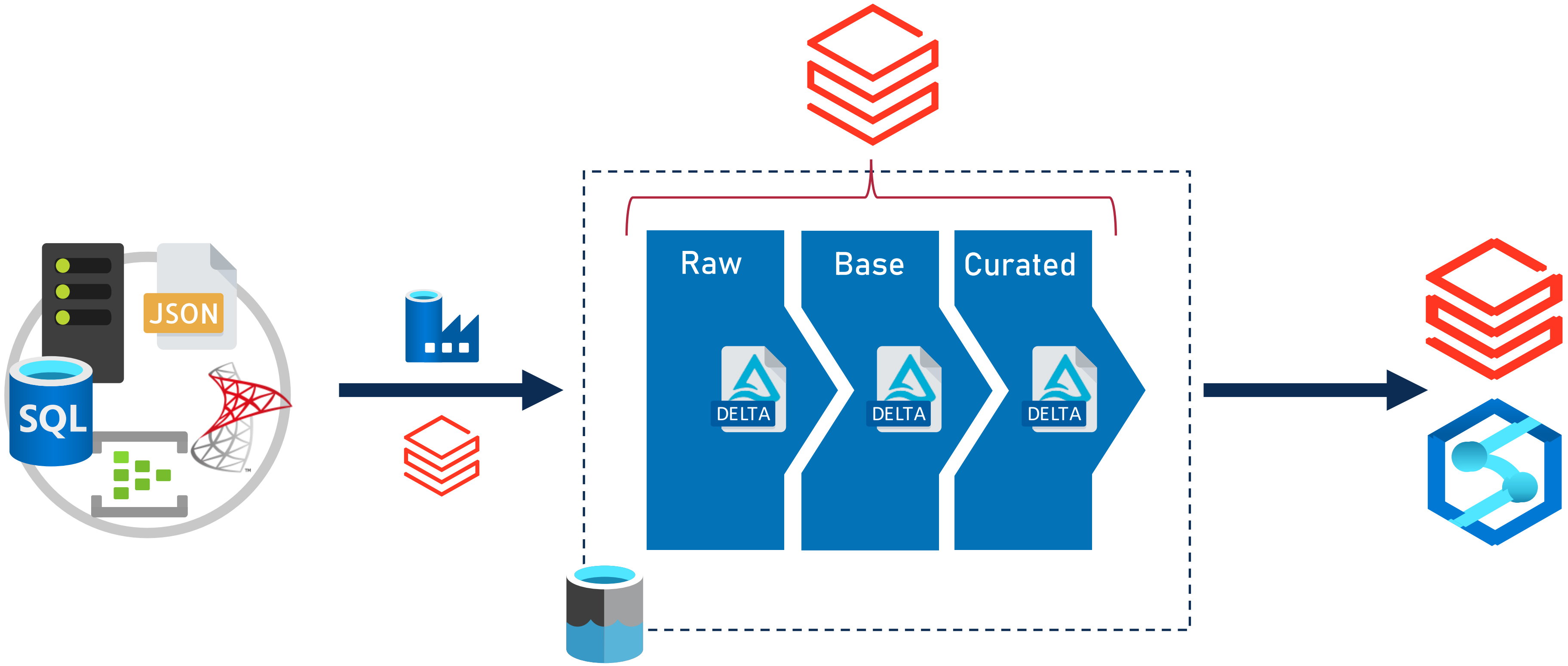
@cporteous

https://github.com/cporteou

databricks
PARTNER PROGRAM
SOLUTIONS ARCHITECT CHAMPION

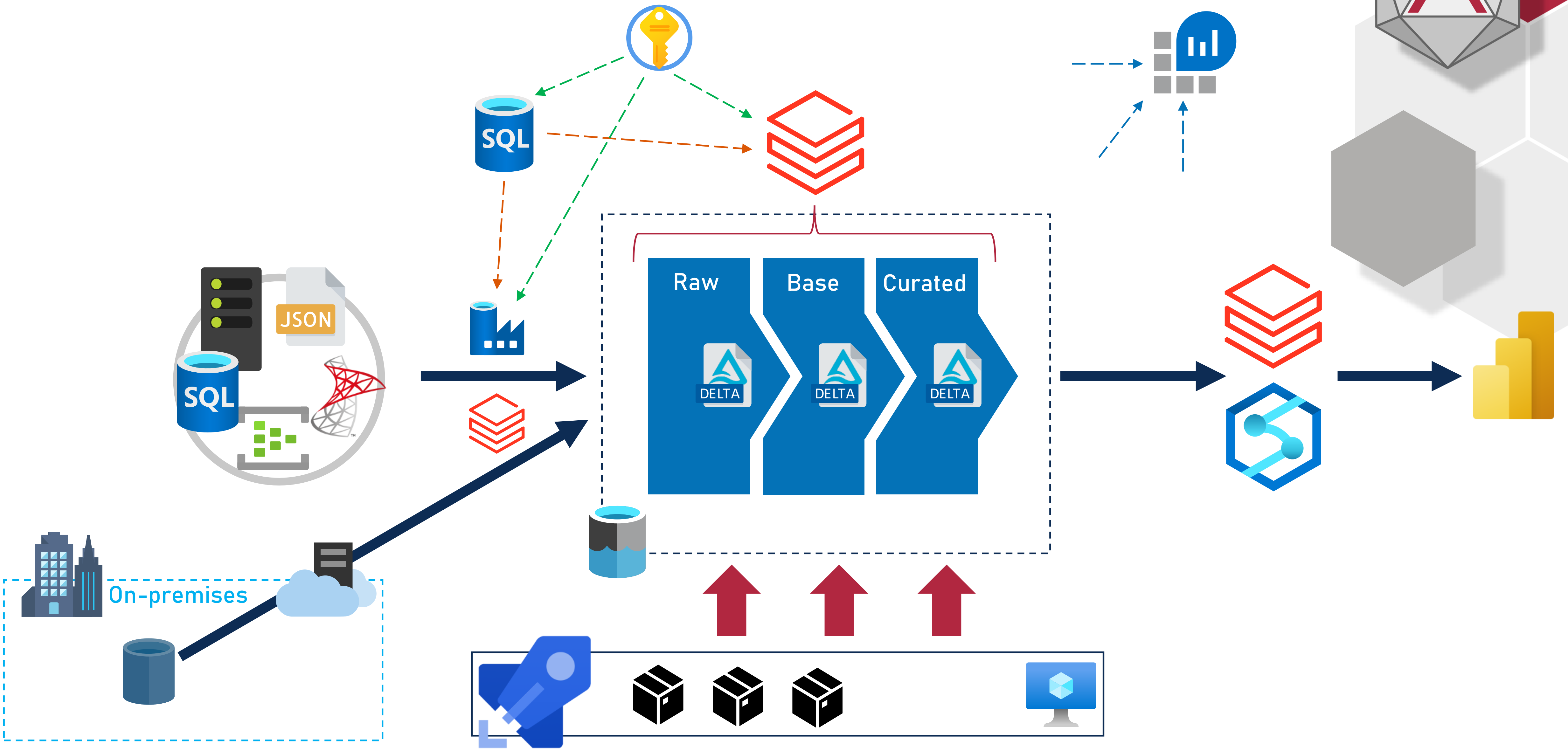
MVP Microsoft® Most Valuable Professional

THE DATA PLATFORM

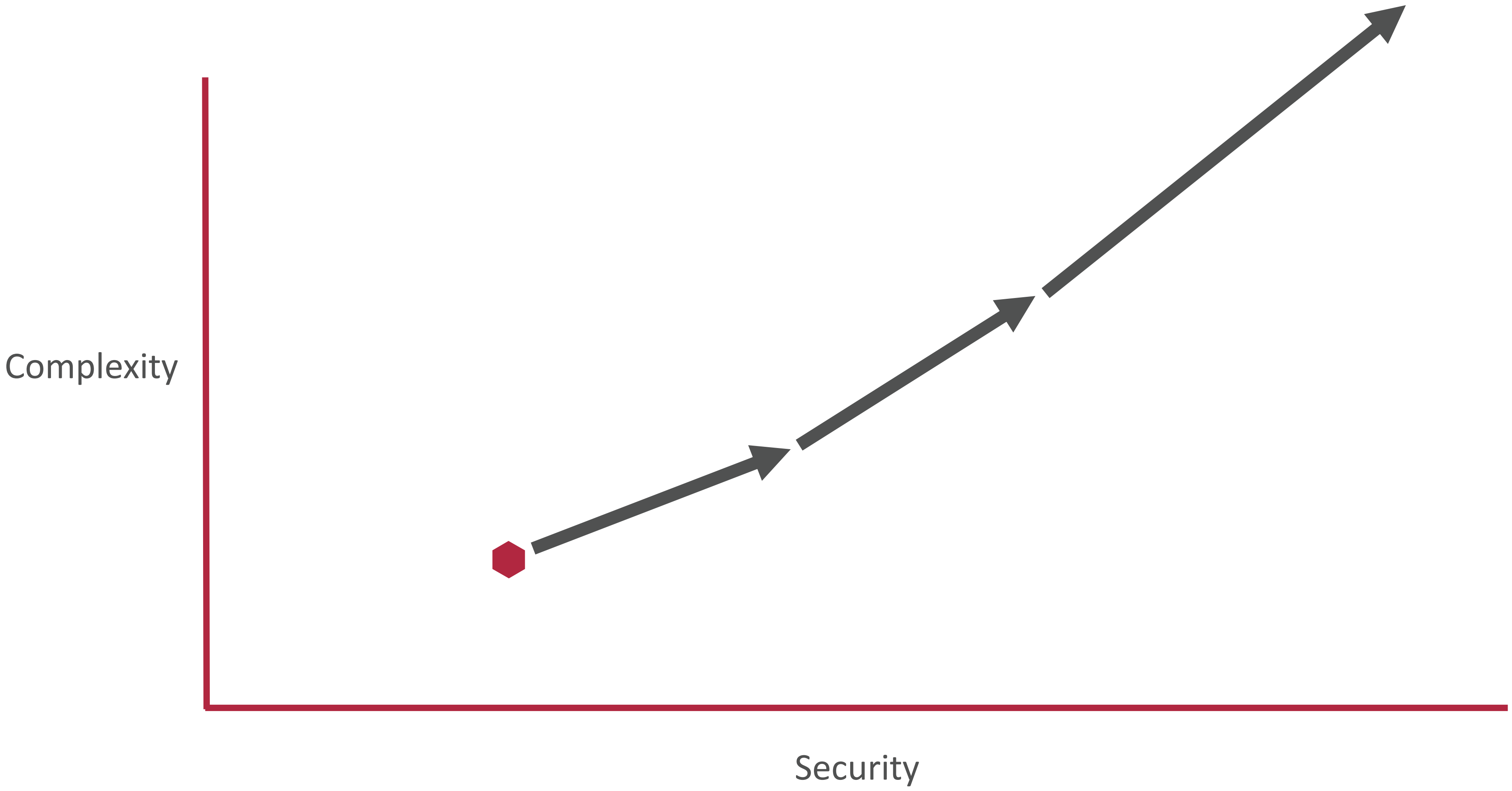


ADVANCING ANALYTICS

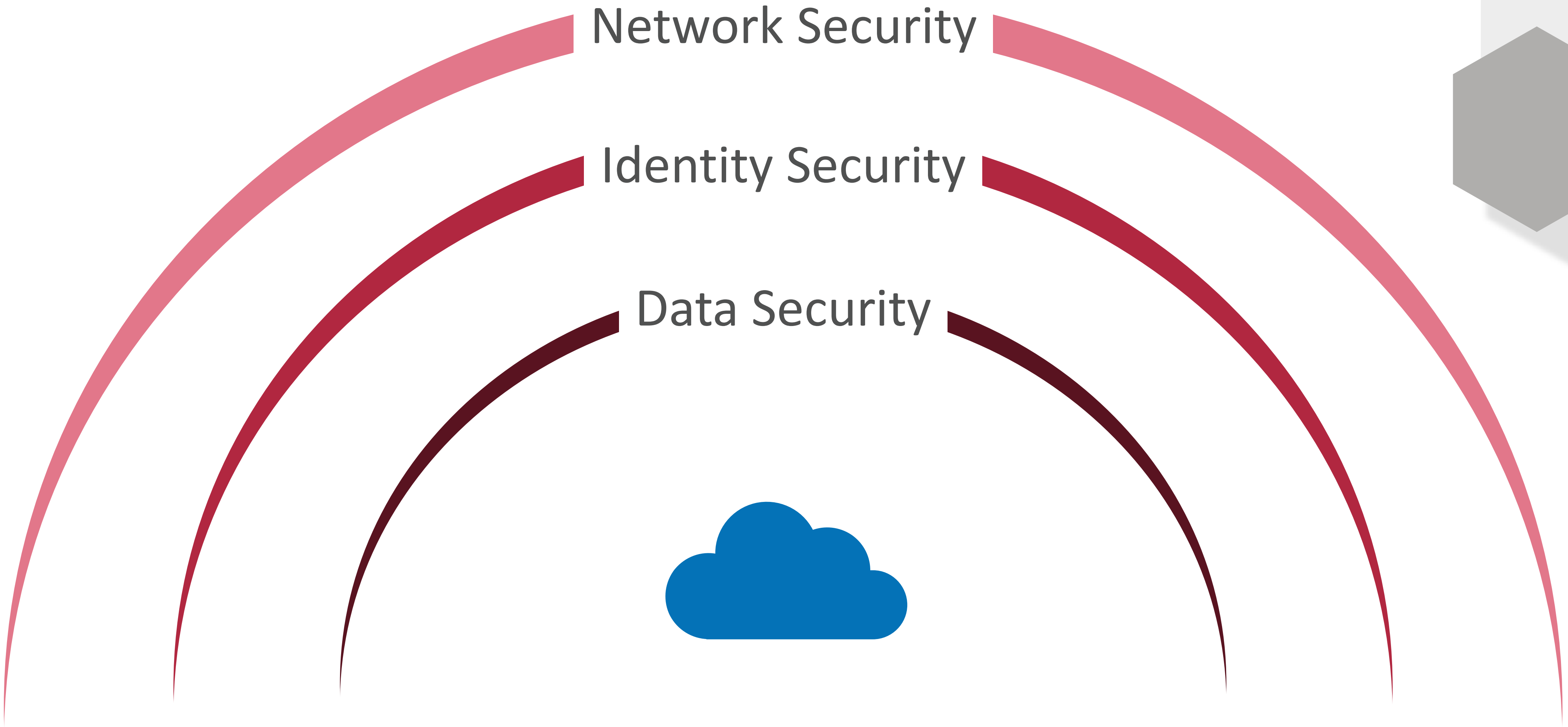
THE DETAIL



WHAT'S THE IMPACT



DEFENCE IN DEPTH



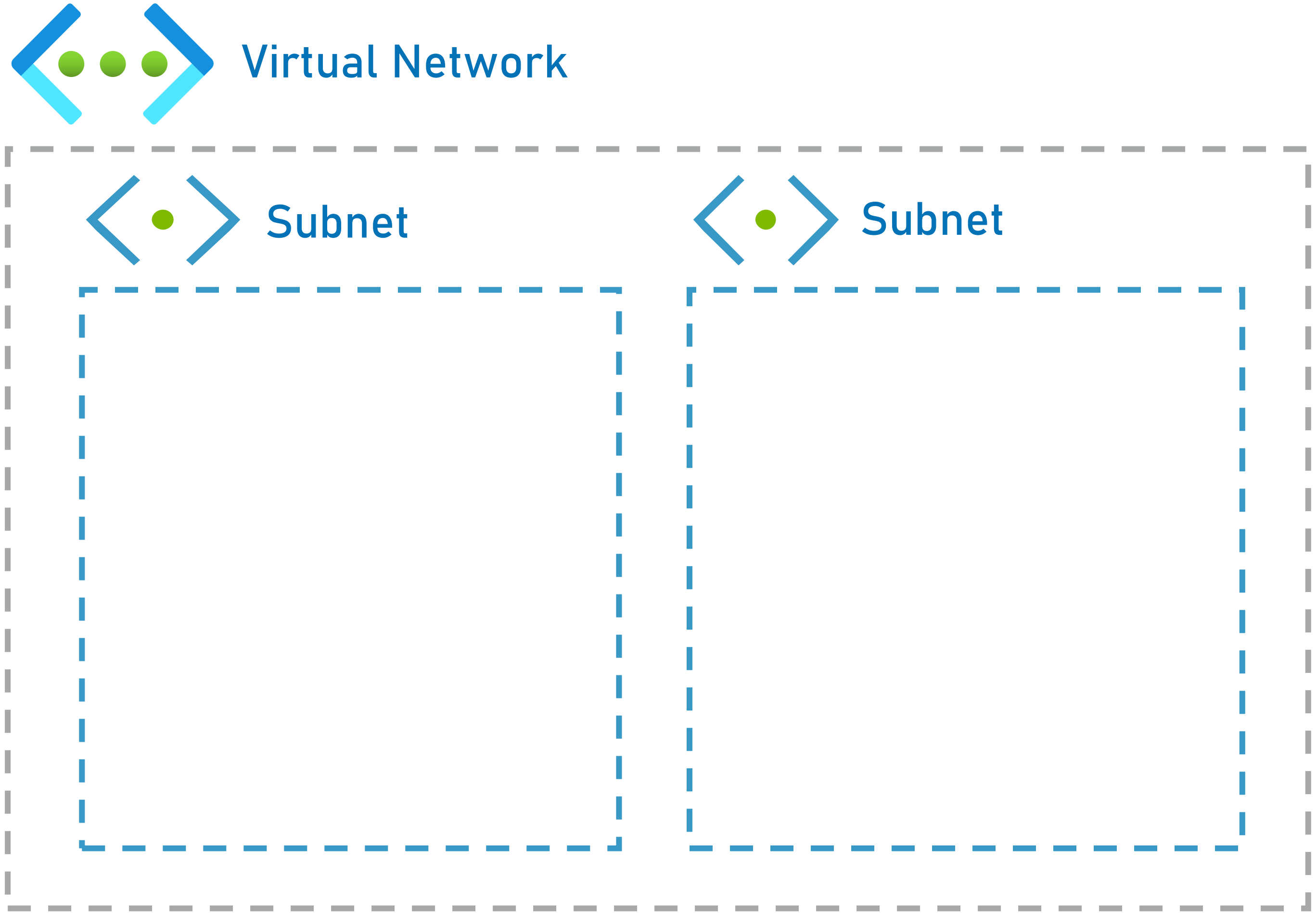
Network Security

Identity Security

Data Security

NETWORK SECURITY

THE FOUNDATIONS

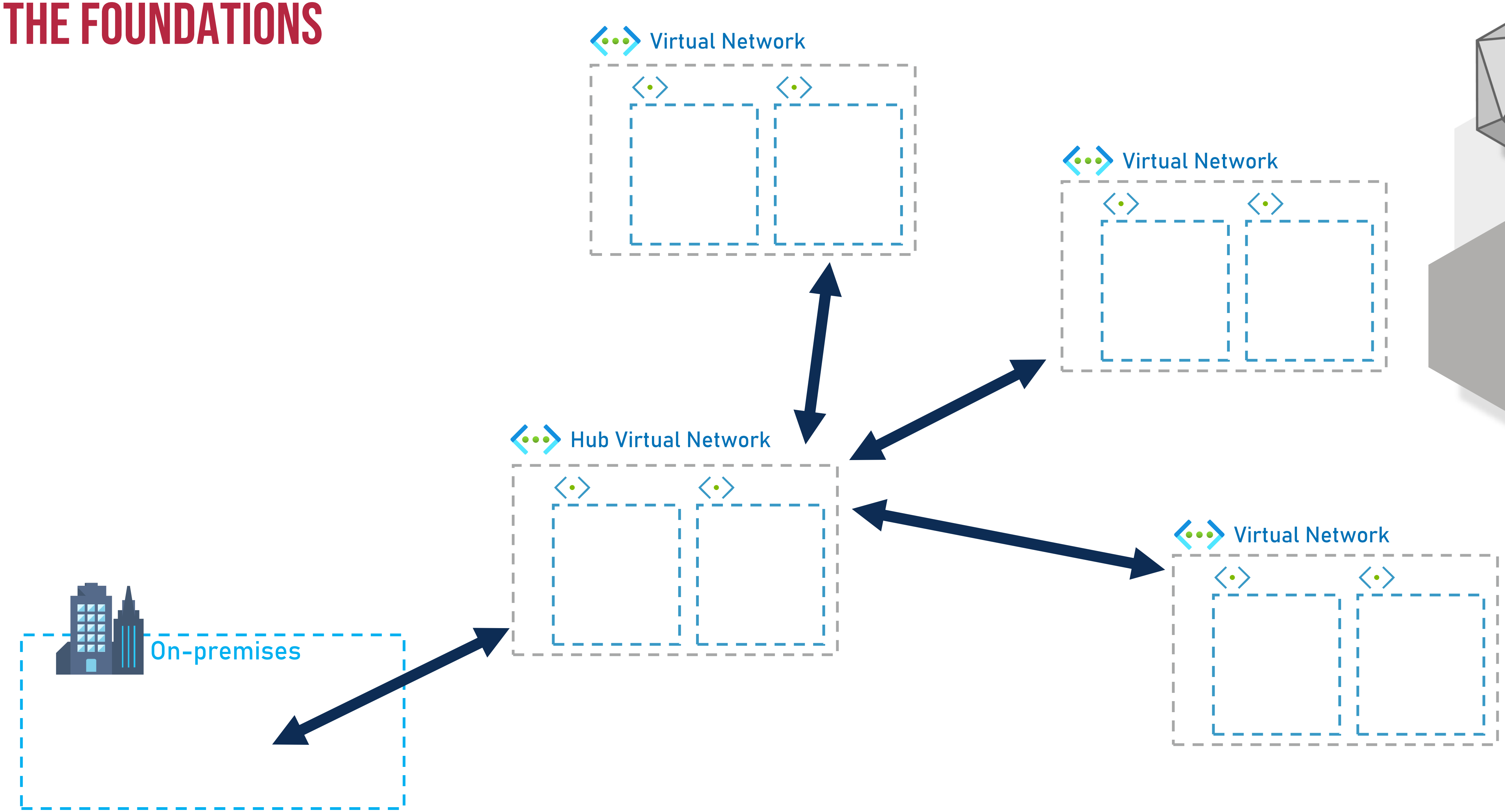


Virtual Network

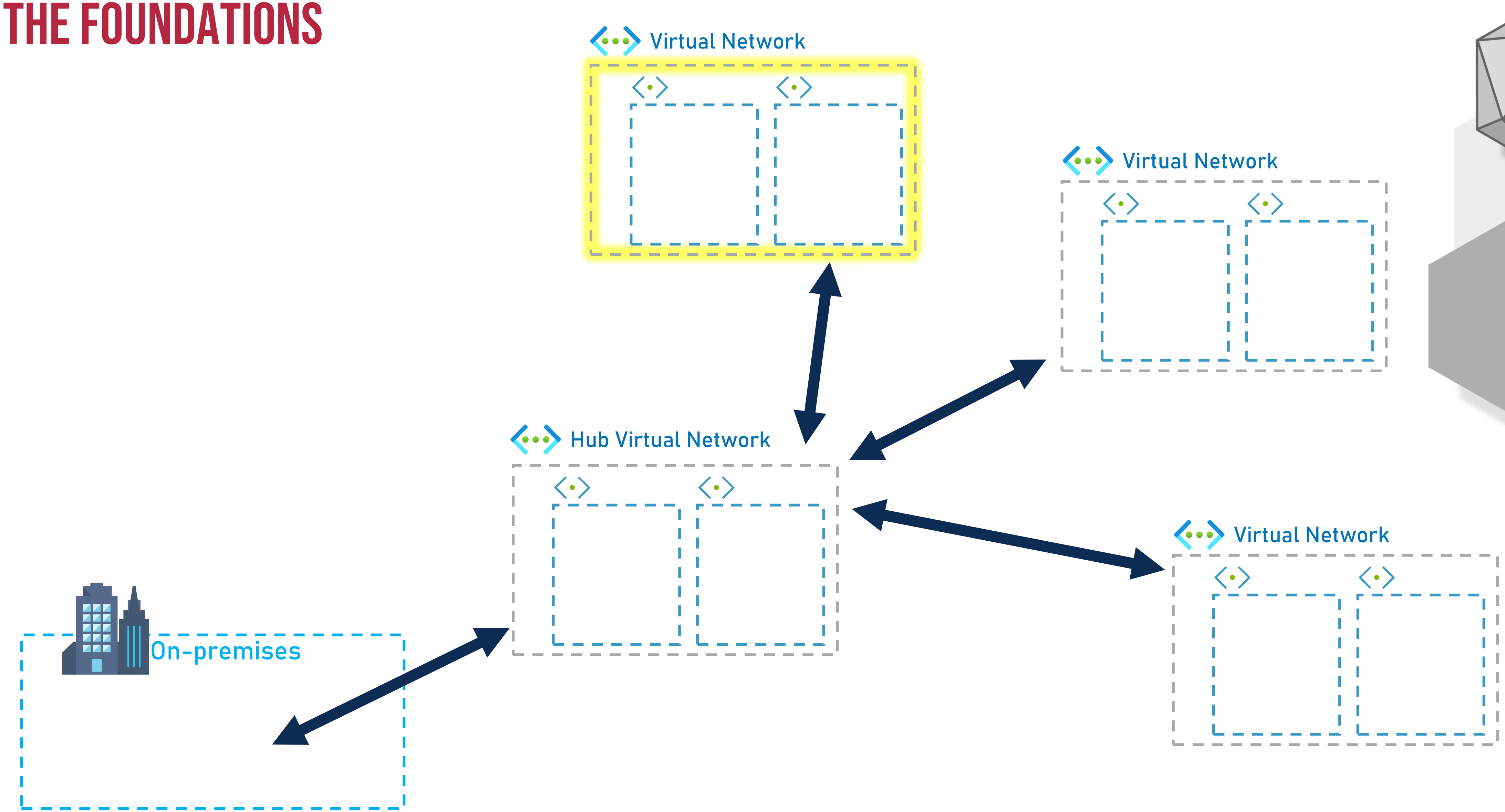
Subnet

Subnet

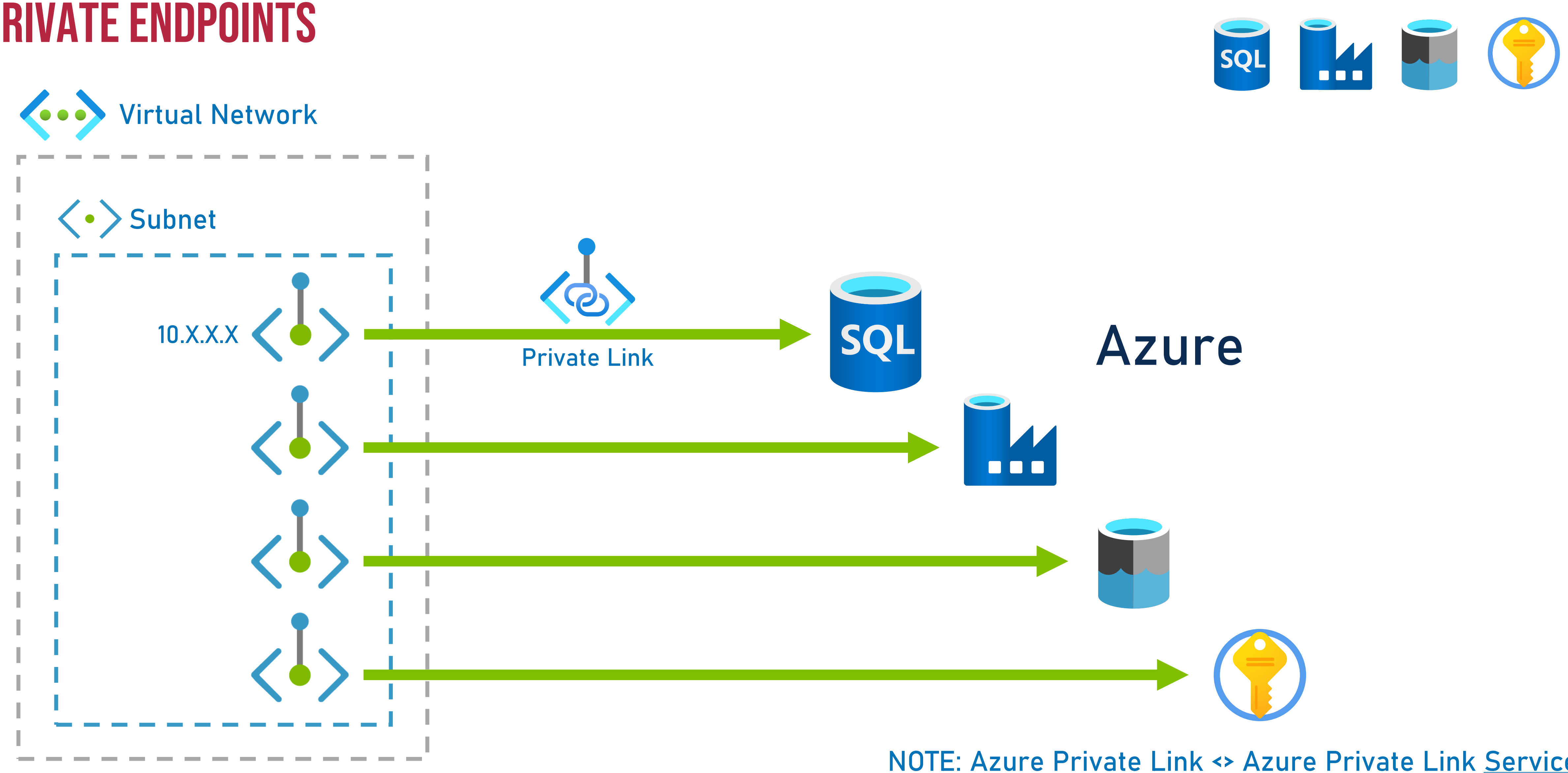
THE FOUNDATIONS



THE FOUNDATIONS



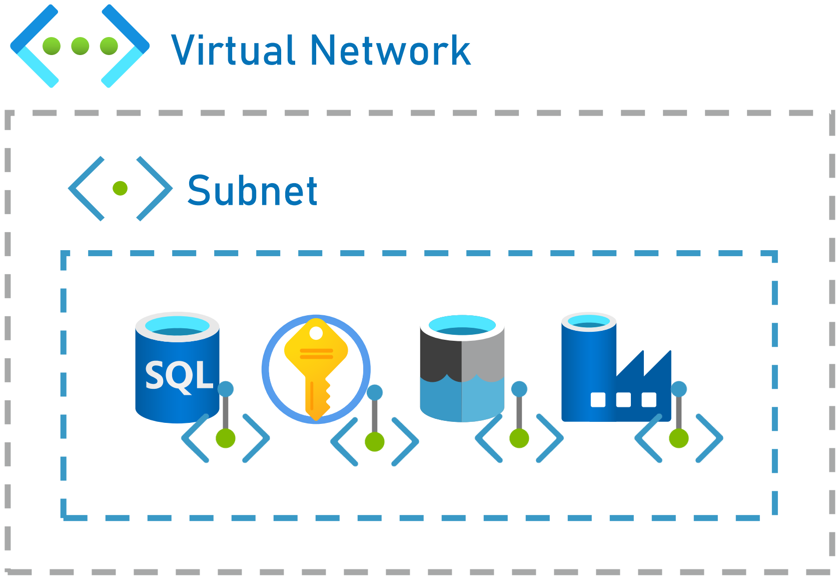
PRIVATE ENDPOINTS



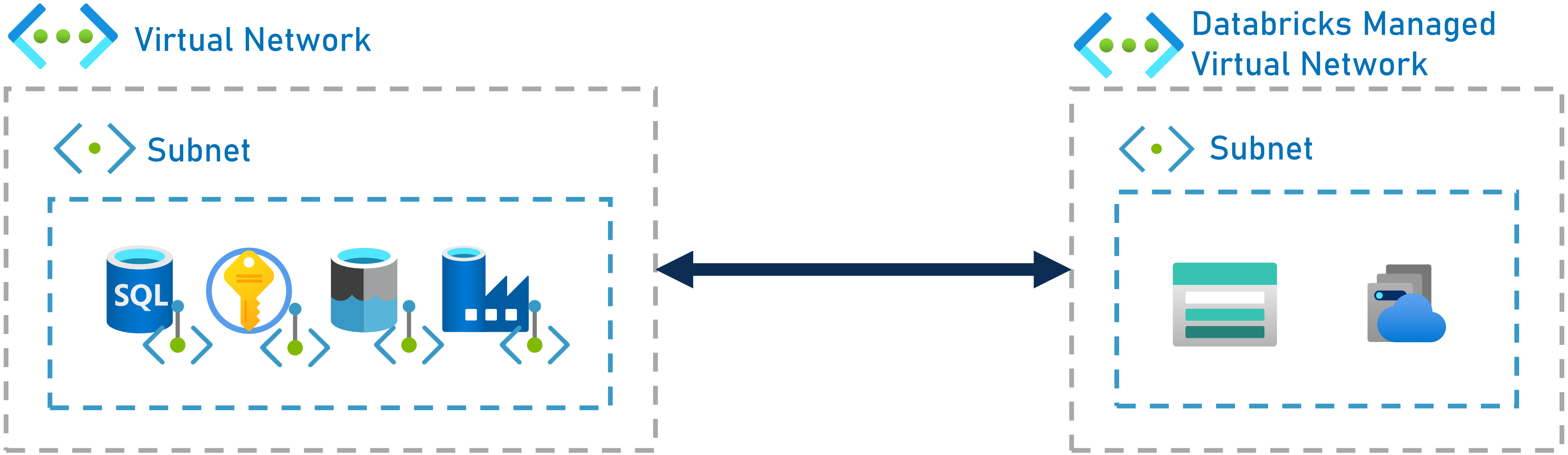
NOTE: Azure Private Link <> Azure Private Link Service

ADVANCING ANALYTICS

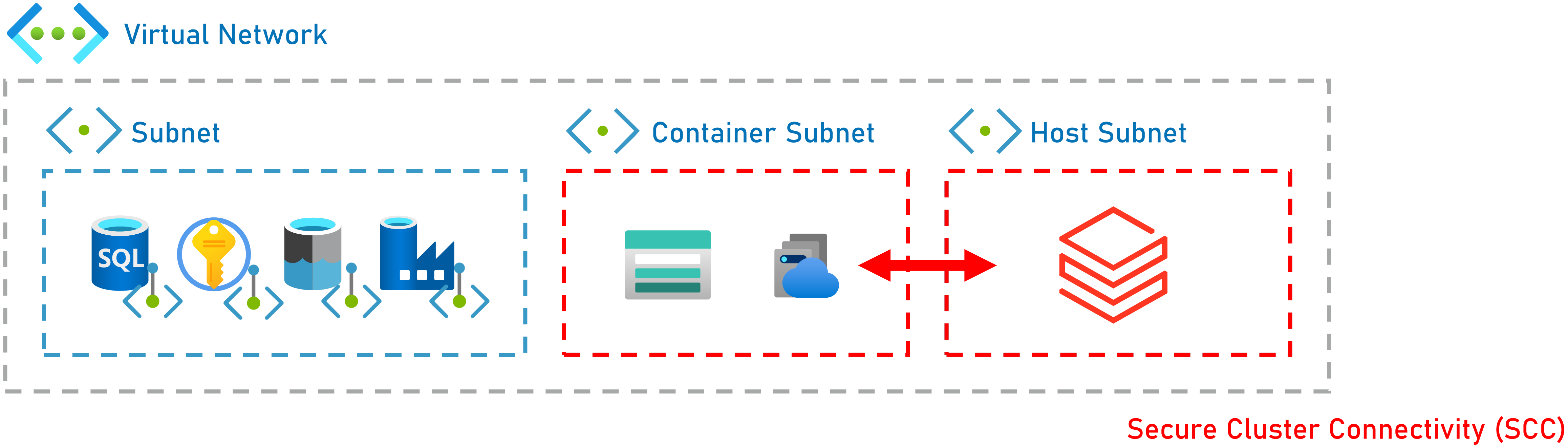
PRIVATE ENDPOINTS



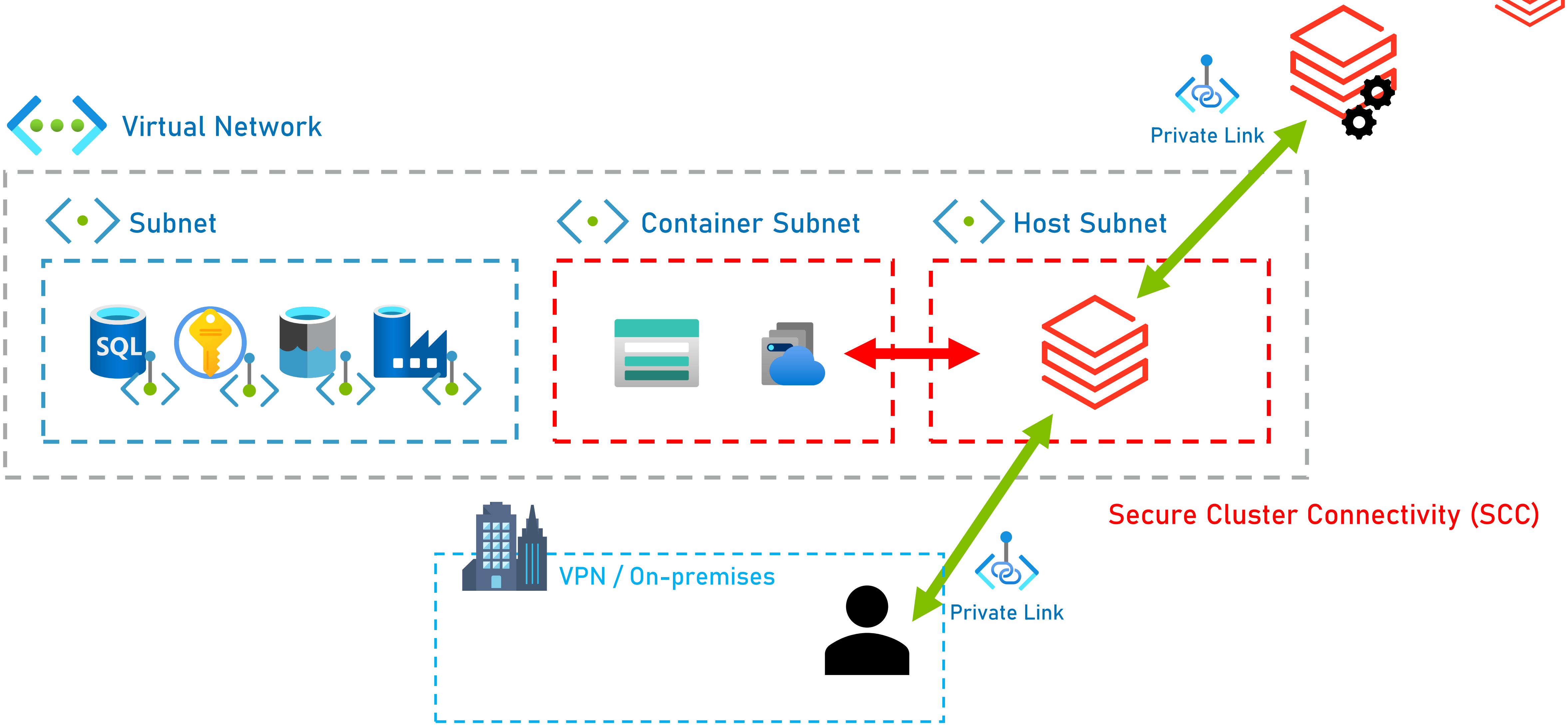
DATABRICKS VNET PEERING



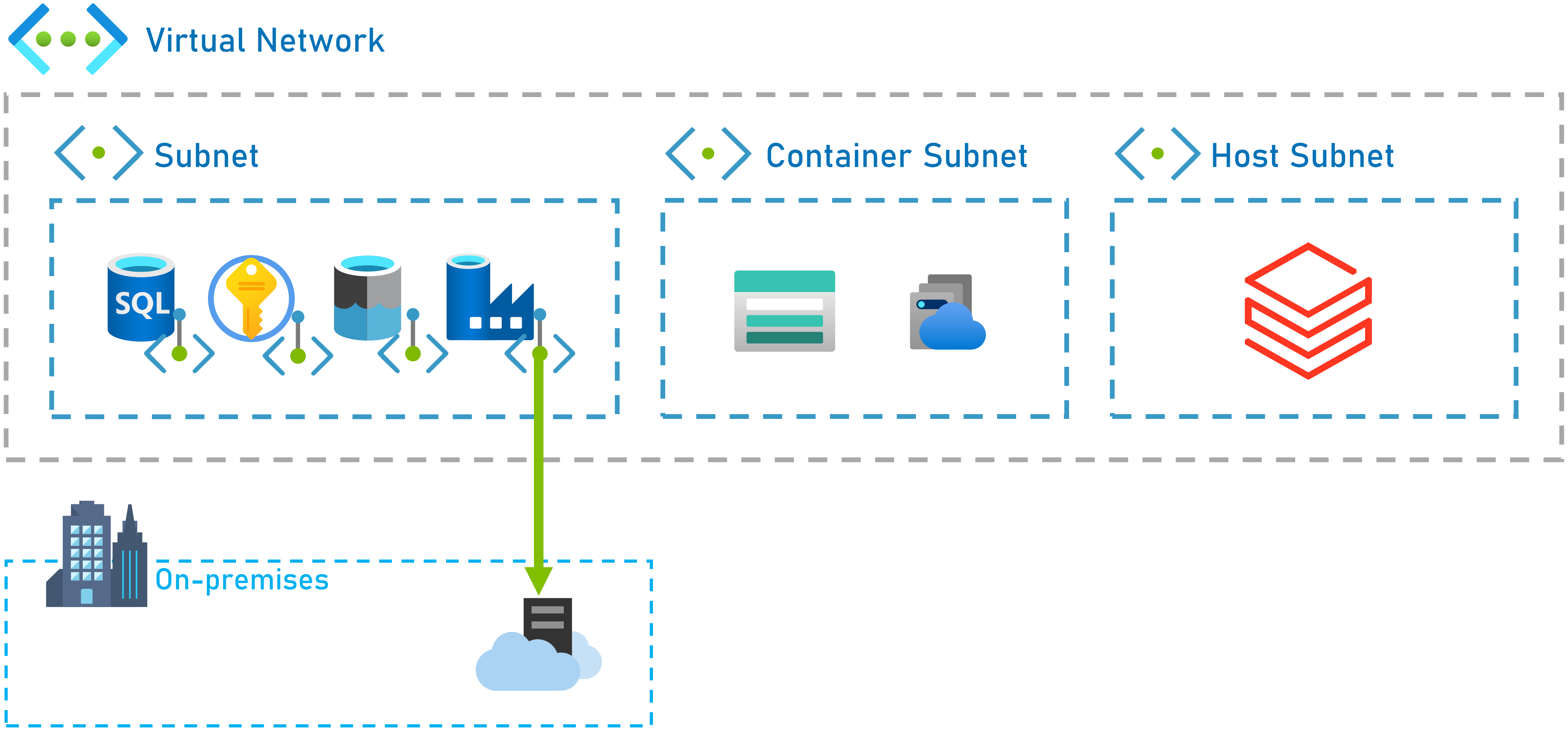
DATABRICKS VNET INJECTION



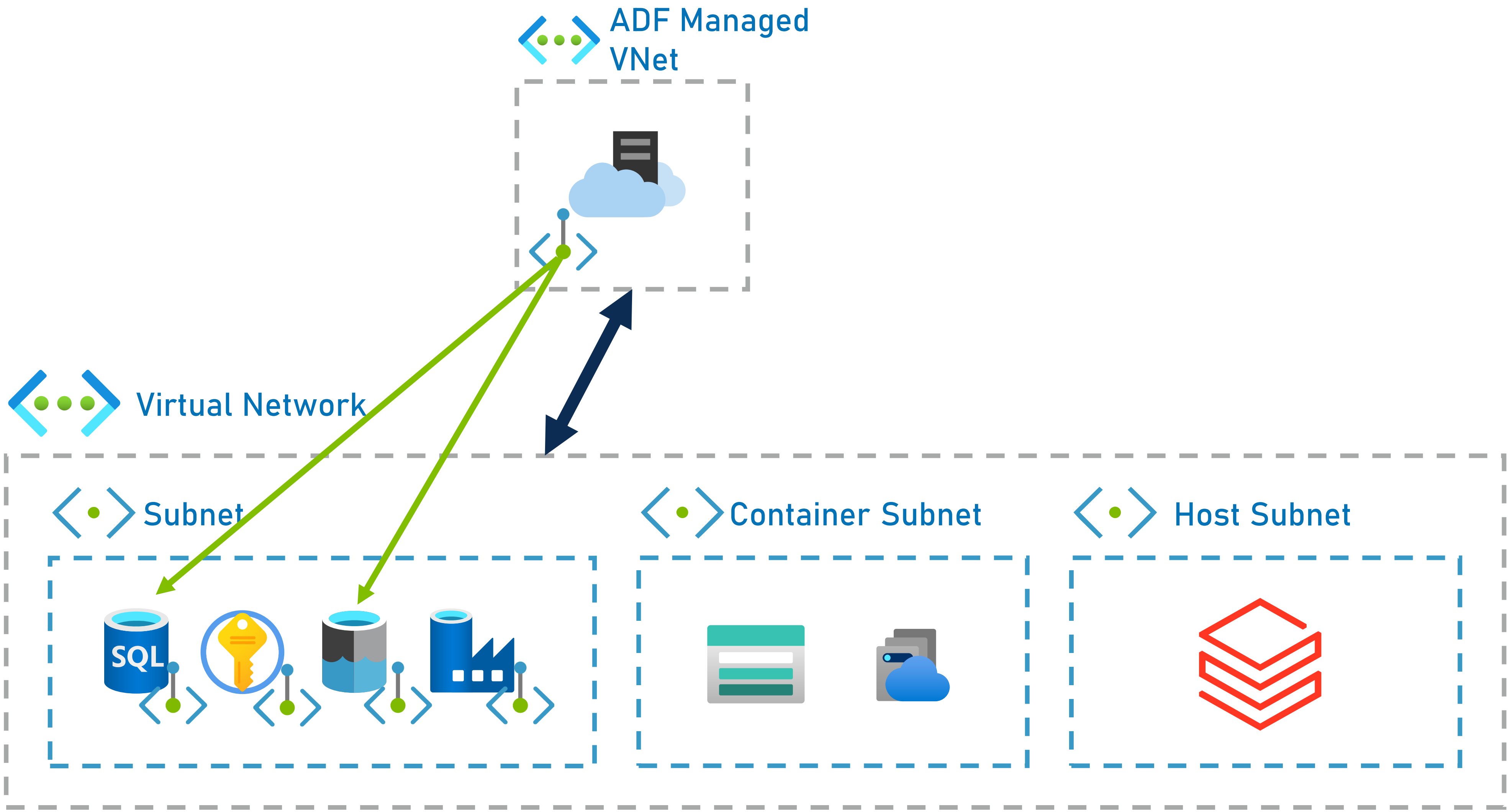
DATABRICKS VNET INJECTION



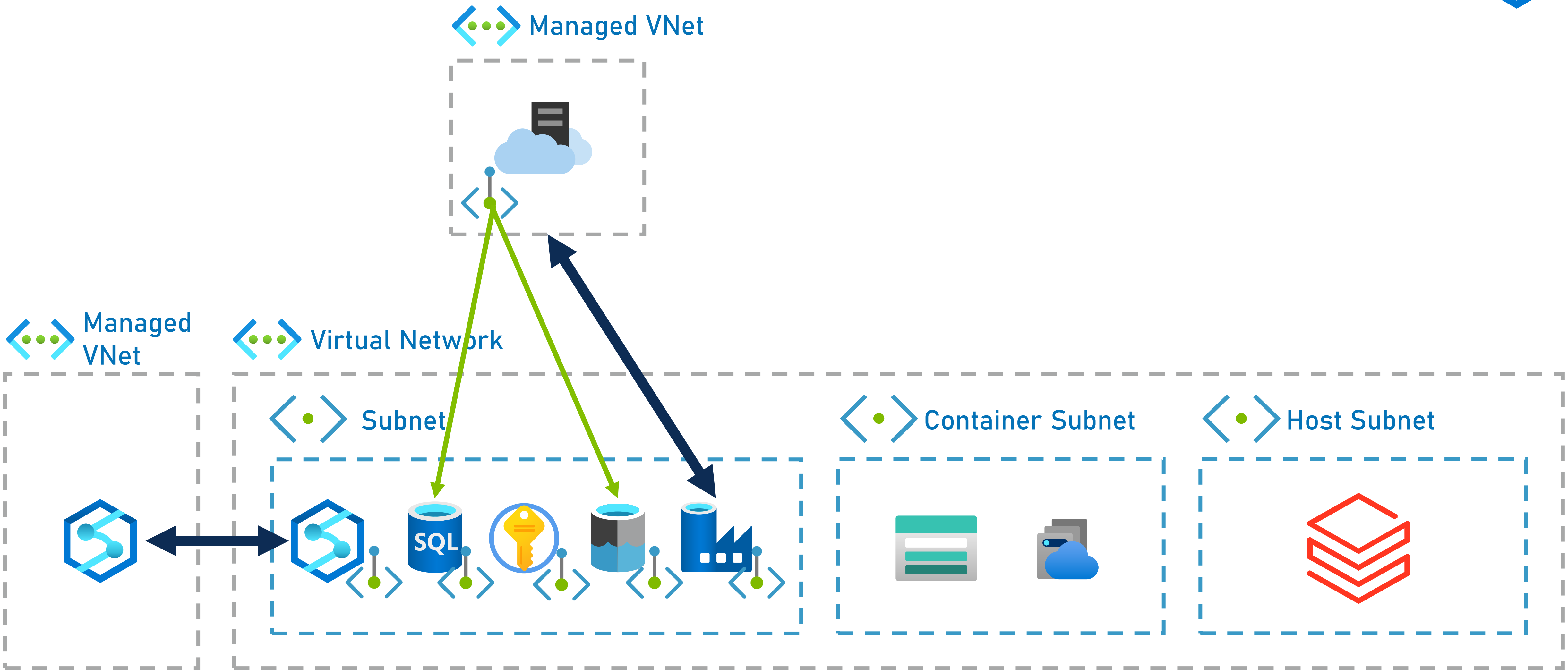
DATA FACTORY ON-PREMISES CONNECTIVITY



DATA FACTORY

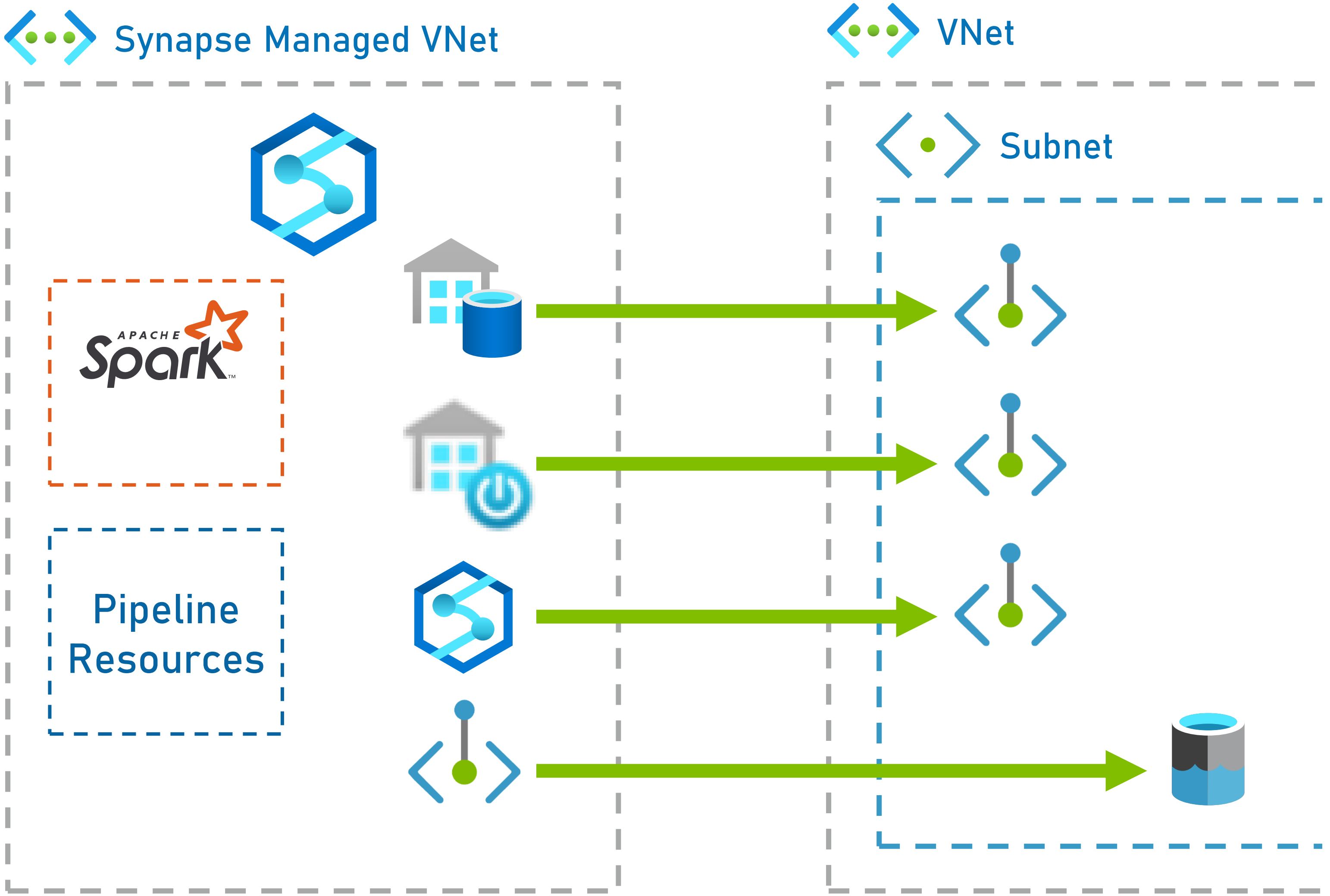


WHAT ABOUT AZURE SYNAPSE?



ADVANCING ANALYTICS

WHAT ABOUT AZURE SYNAPSE?



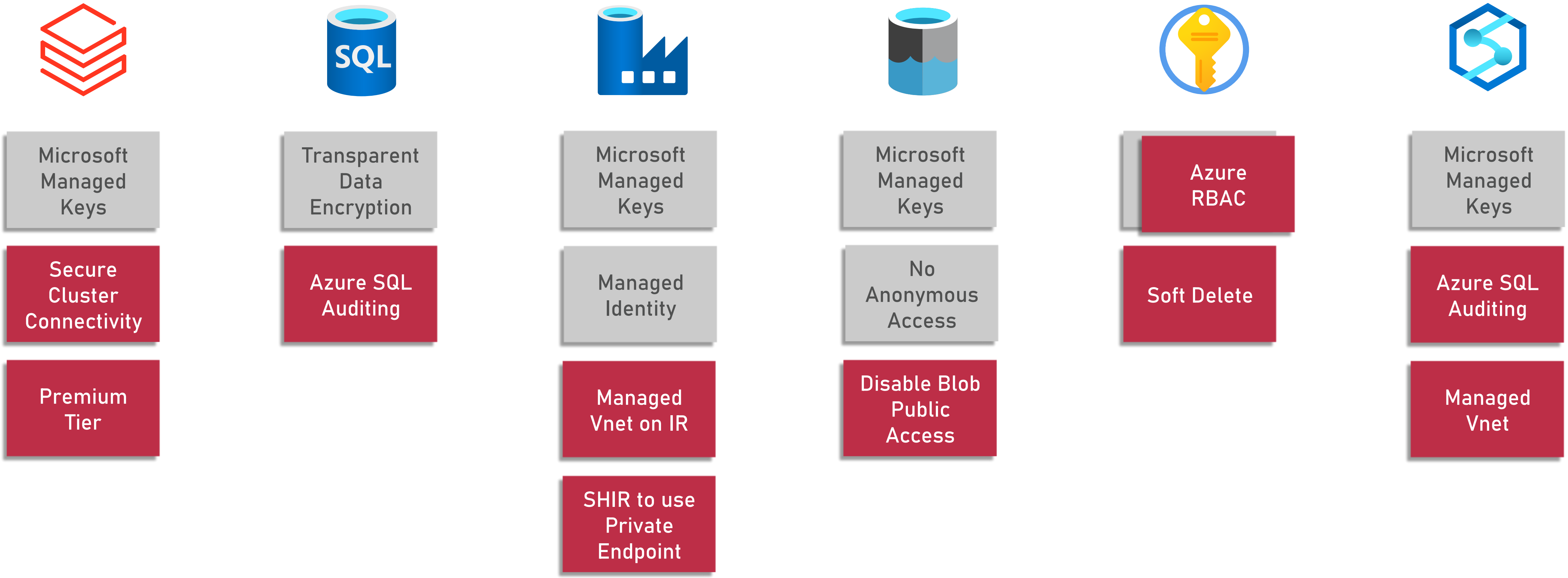
SUMMARY

Virtual Network (VNet)

- ✓ Traffic is privately secured within the organisation
- ✓ Integrate with existing securely networked resources via Hub › Spoke
- ✗ Microsoft-hosted Azure DevOps Agent → Self-hosted (IaaS)
- ✗ Connectivity restrictions → Azure Bastion/Jump box (IaaS)
- ✗ Increased costs
- ✗ Don’t underestimate complexity (NSGs, DNS zones, etc)

DATA & IDENTITY SECURITY

SECURITY FEATURES



Microsoft Managed Keys

Secure Cluster Connectivity

Premium Tier

Transparent Data Encryption

Azure SQL Auditing

Microsoft Managed Keys

Managed Identity

Managed Vnet on IR

SHIR to use Private Endpoint

Microsoft Managed Keys

No Anonymous Access

Disable Blob Public Access

Azure RBAC

Soft Delete

Microsoft Managed Keys

Azure SQL Auditing

Managed Vnet

USE WITH CAUTION

Azure Resource Locks

Infrastructure Encryption (dbfs)

Customer Managed Keys

Encryption between Worker Nodes

Azure Resource Locks

Customer Managed Keys

Infrastructure Encryption

Customer Managed Keys

Soft Delete

Customer Managed Keys

=

Functionality Breaking

Performance Impact

Management overhead

Performance Impact

Cost Impact

SUMMARY

Existing Azure Policies

Some features don’t make sense

Additional support overhead

INFOSEC WISH LIST

Azure Sentinel

CIS Benchmark

SUMMARY

- Design for Security
- RBAC First
- Defence in Depth
- Don't just turn everything on
- Don't underestimate complexity

THANK YOU

Please leave feedback

https://craigporteous.com

@cporteous

https://github.com/cporteou

https://sqlb.it/?9540

REFERENCES

- How to protect Data Exfiltration with Azure Databricks to help ensure Cloud Security
- Deploy Azure Databricks in your Azure virtual network (VNet injection) - Azure Databricks | Microsoft Docs
- Secure cluster connectivity (No Public IP / NPIP) - Azure Databricks | Microsoft Docs
- Azure Synapse Analytics security white paper: Network security - Azure Synapse Analytics | Microsoft Docs
- The Purpose and Pain of Azure Resource Locks - Craig Porteous
- Mapping Data Personas to your Data Platform - Craig Porteous