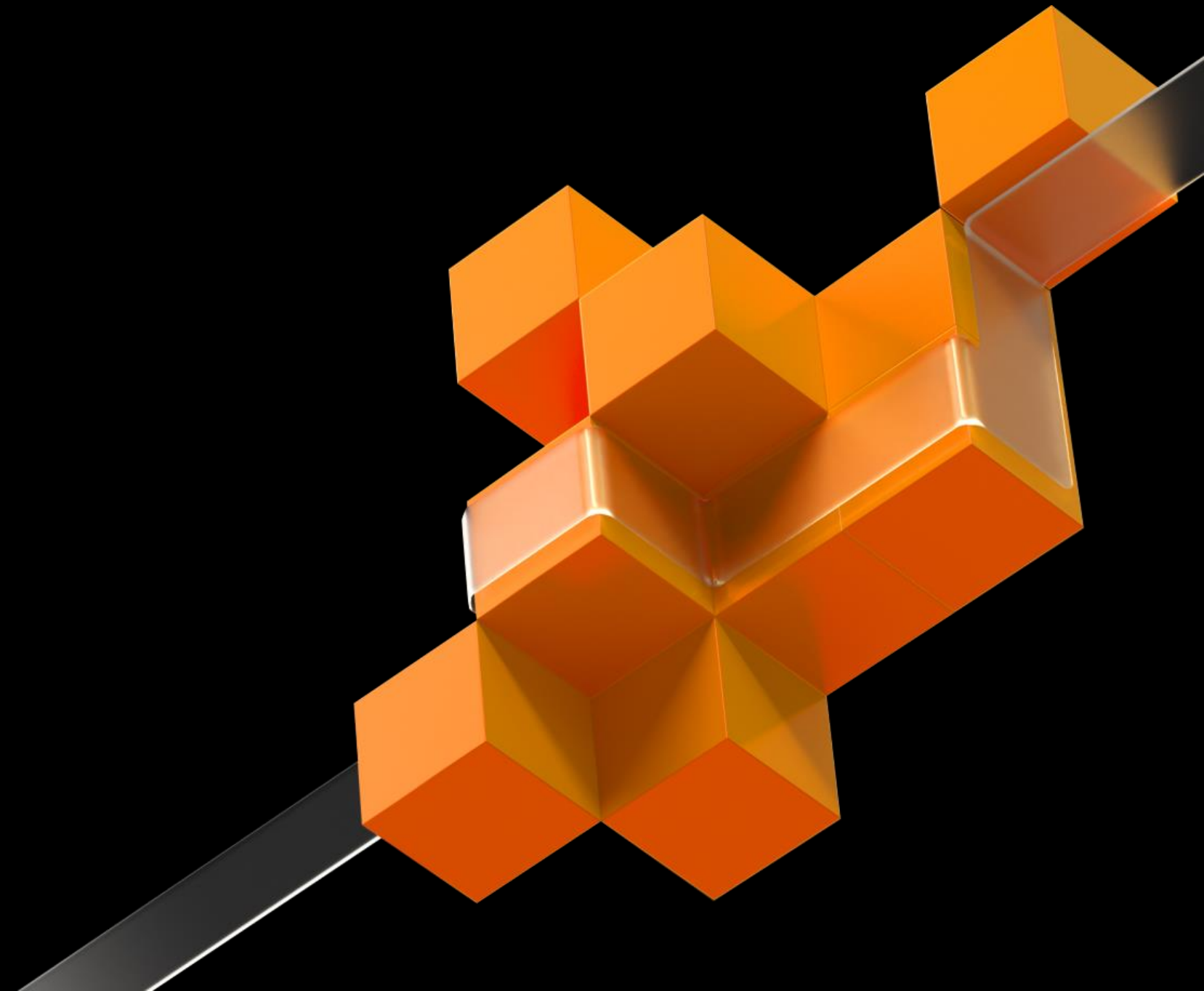
Microsoft

Azure Private Link

Adam Stuart
Technical Specialist, Azure Networking
Microsoft



Azure Networking

Virtual Network

Virtual WAN

ExpressRoute

VPN

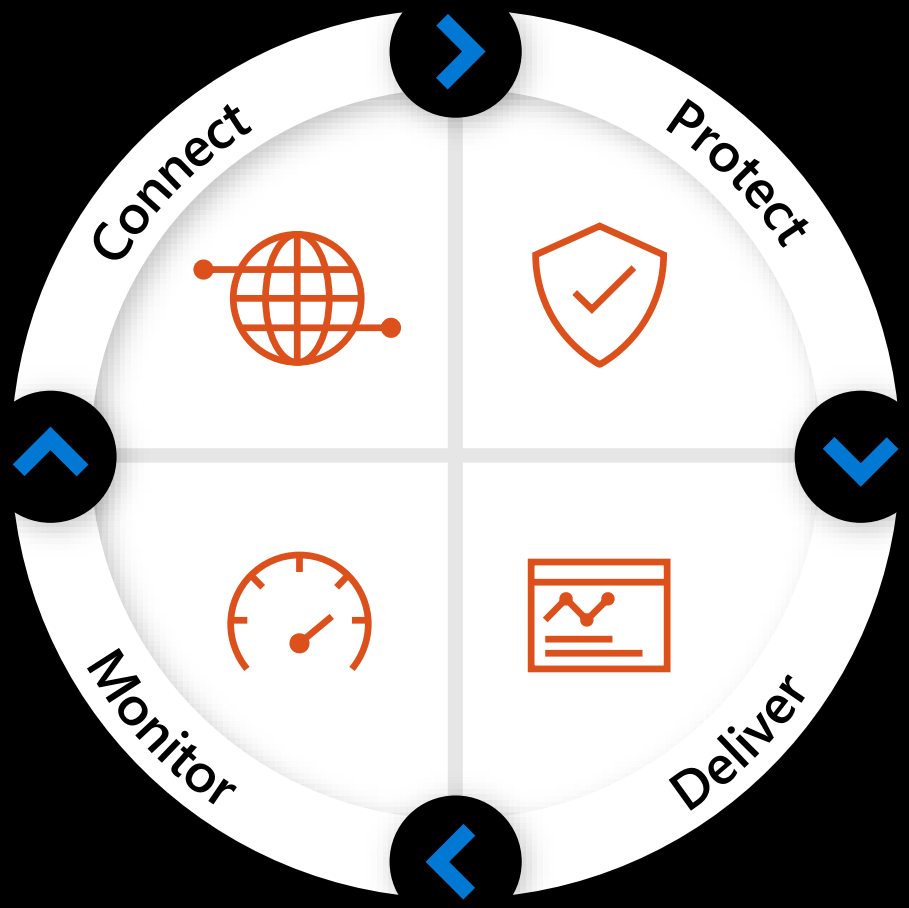
DNS

Network Watcher

ExpressRoute Monitor

Azure Monitor

Virtual Network TAP



DDoS Protection

Firewall

Network Security Groups

Web Application Firewall

Service Endpoints & Private Link

CDN

Front Door

Traffic Manager

Application Gateway

Load Balancer

Agenda

- Azure networking overview
- Private Link
  - Why you should care
  - What is it
  - A demo
  - Even more Private Link

Stuff companies say

How can I access PaaS services privately?

How to configure properly the network dependencies?

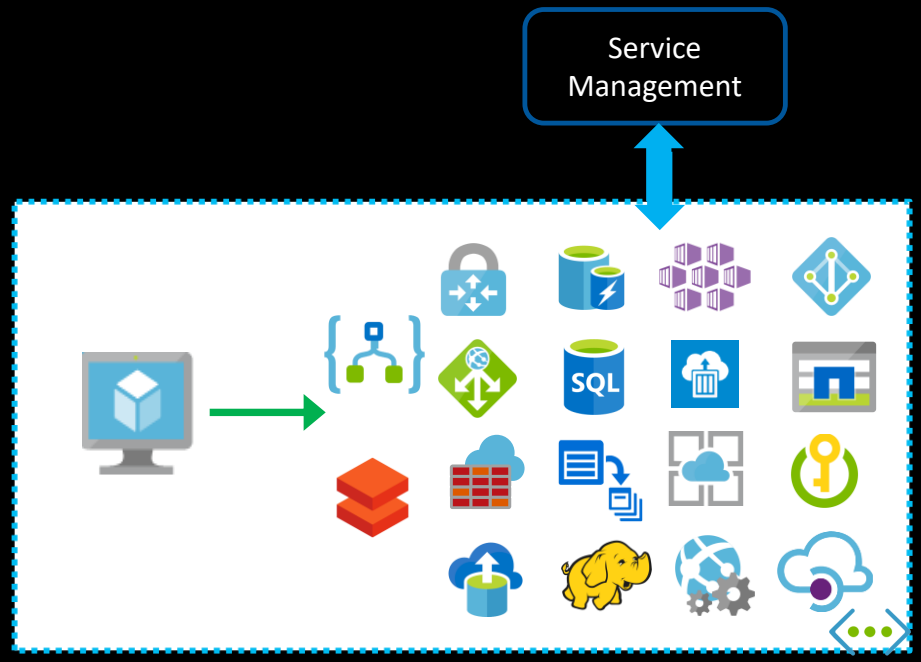
Does it fit with my compliance requirements?
Not exposed to Internet
Inspection using appliance (force tunneling)

How to secure access only from trusted applications or prevent from data exfiltration?

How to scale without all the configuration complexity?

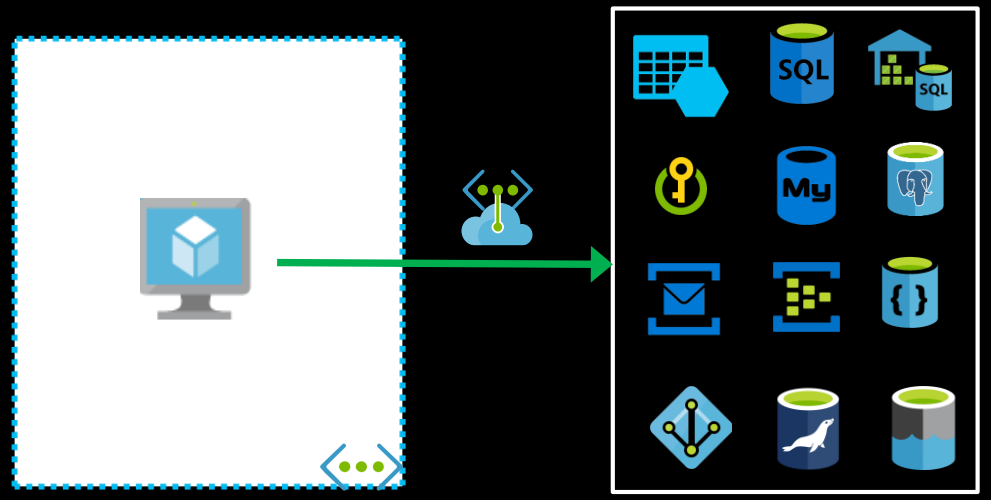
Two types of PaaS service

Service instances running inside customer's VNet



Private access to PaaS resources
Management exposed using public IP addresses
Complex network configuration

Service running outside customer's VNet



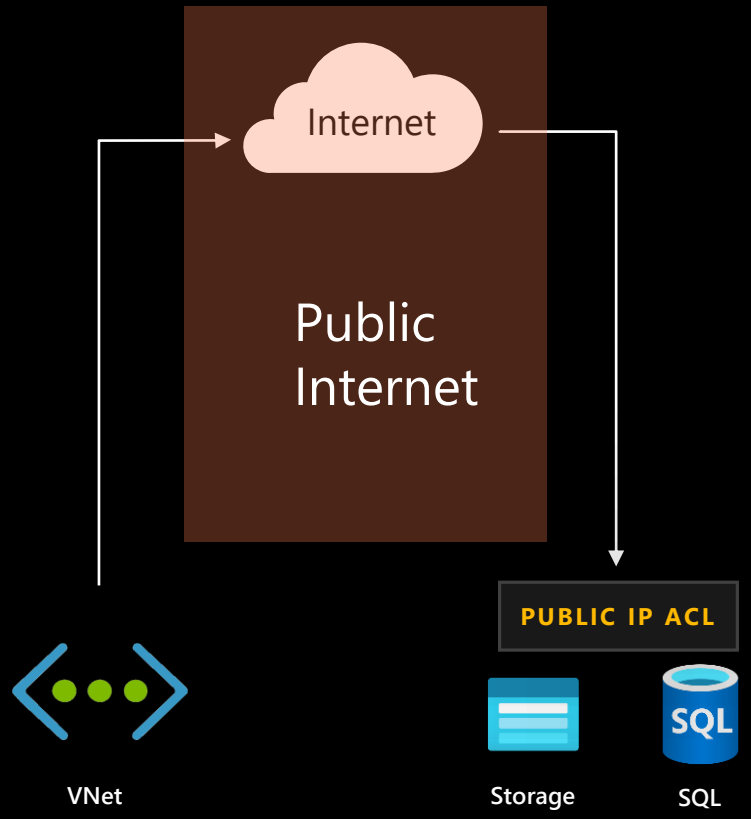
Public access to PaaS resources
Management Isolated
PaaS resource secure to customer VNet's

VNet injection

VNet Service Endpoints + Private Link

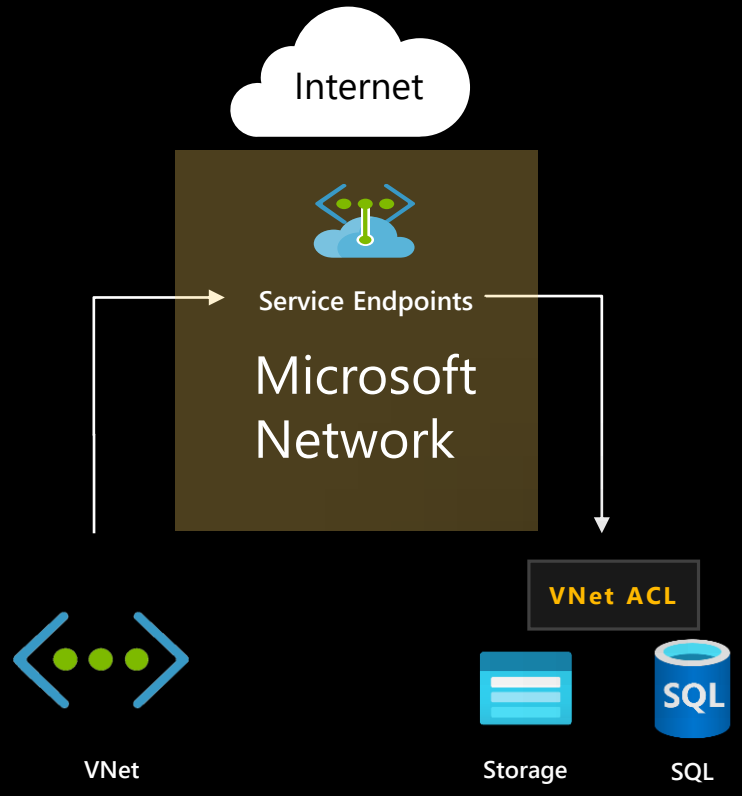
Virtual network to PaaS options

Good



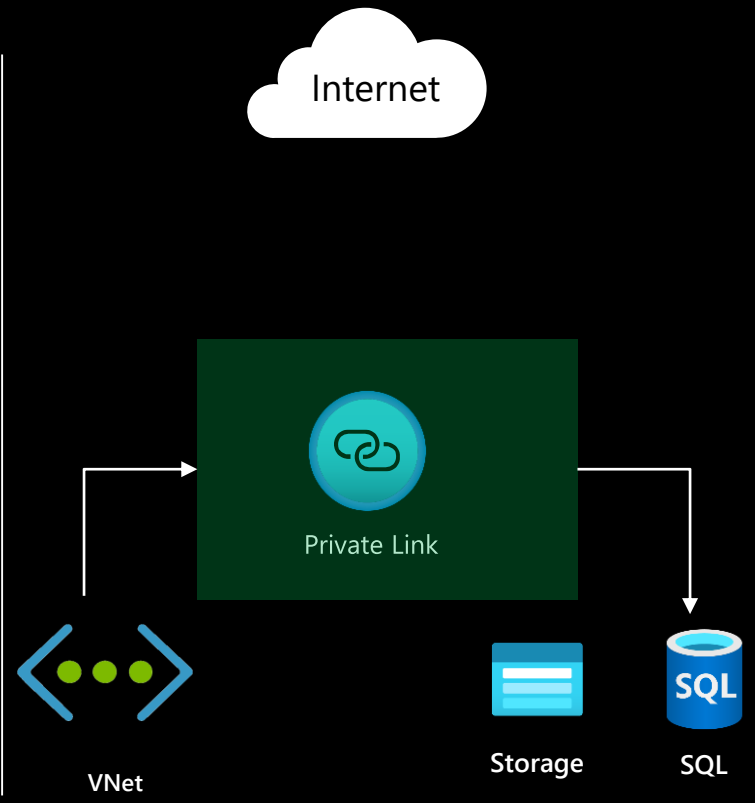
- Traffic traverses the Internet
- Secured using ACLs on Public IPs

Better



- Traffic stays within Microsoft network
- Secured using VNet ACLs
- Service extended to VNet:Subnet

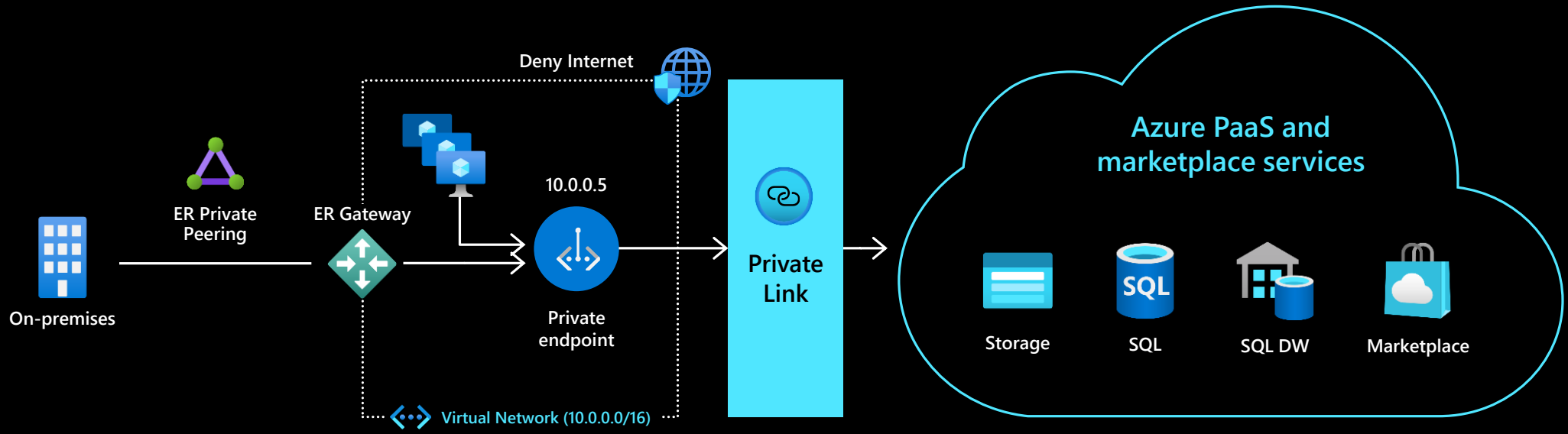
Best



- Traffic is fully private traversing the Microsoft network
- No exposure of public IPs on either side

Azure Private Link

Albert Greenberg (Azure Networking CVP): "*Private Link is as important as the VNet was*"

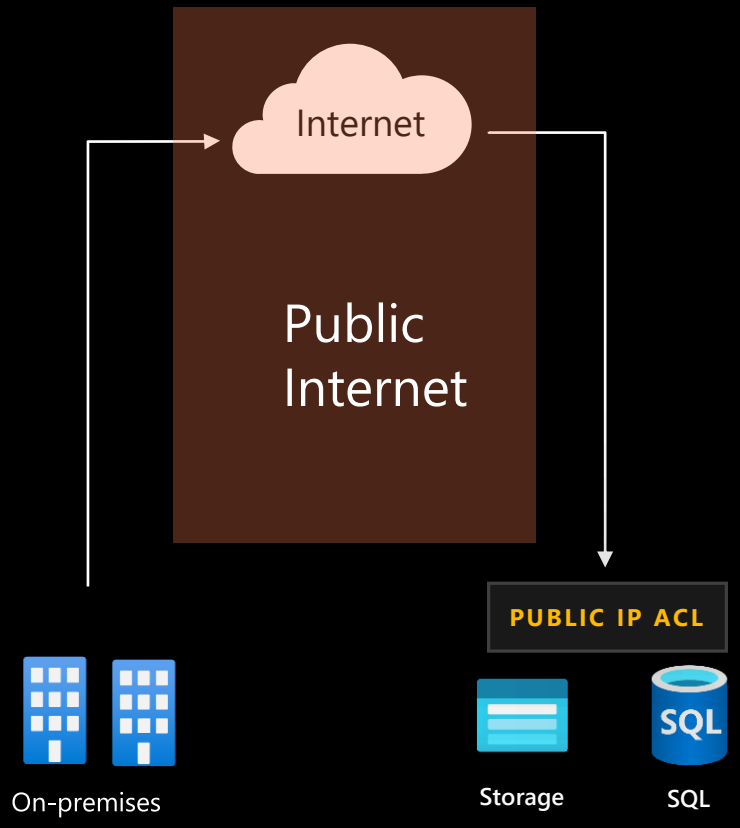


Private Link for Azure Storage, SQL DB and customer own service

Private access from Virtual Network resources, peered networks and on-premise networks	In-built Data Exfiltration Protection	Predictable private IP addresses for PaaS resources	Unified experience across PaaS, Customer Owned and marketplace Services

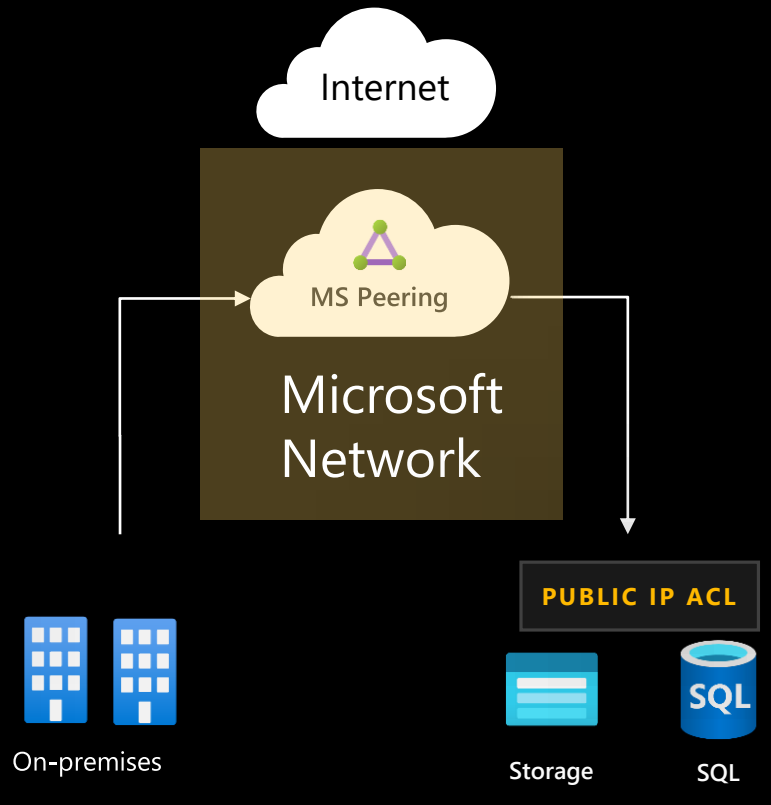
But wait, this also works from on-premises

Good



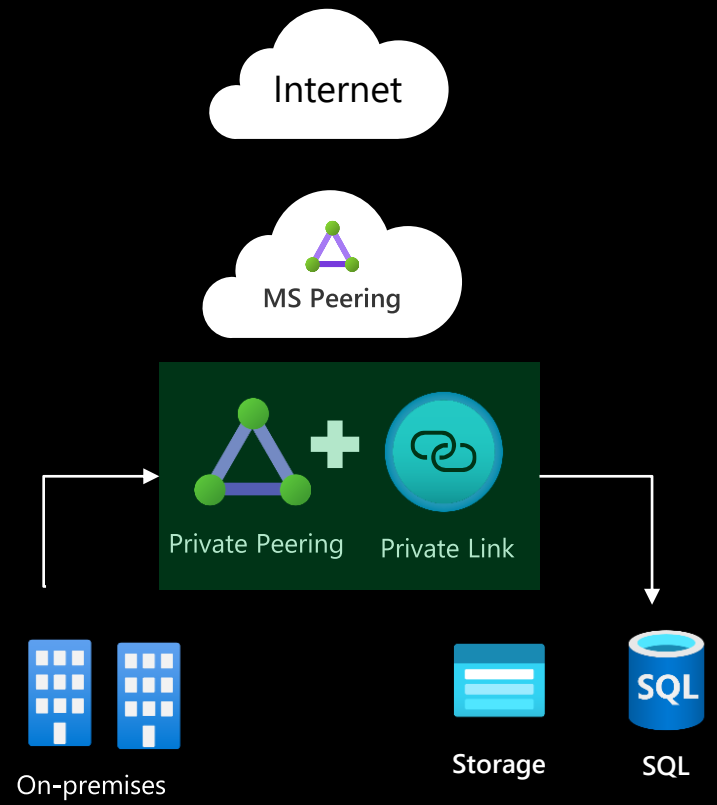
- Traffic traverses the Internet
- Secured using ACLs on Public IPs

Better



- Traffic stays within Microsoft and partner network
- MS Peering draws Microsoft Public IP traffic

Best



- Traffic is fully private traversing the Microsoft network
- No exposure of public IPs on either side

Demo

Private Access for Azure SQL

This is a preview service available in these regions

- Public Preview extended to all Public Cloud Regions
  - Supported Services include: Storage, ADLSv2, SQL DB, SQL DW, Customer Own Service
- Public Preview Private Link available for CosmosDB
  - Supported regions: uswestcentral, usnorth and uswest

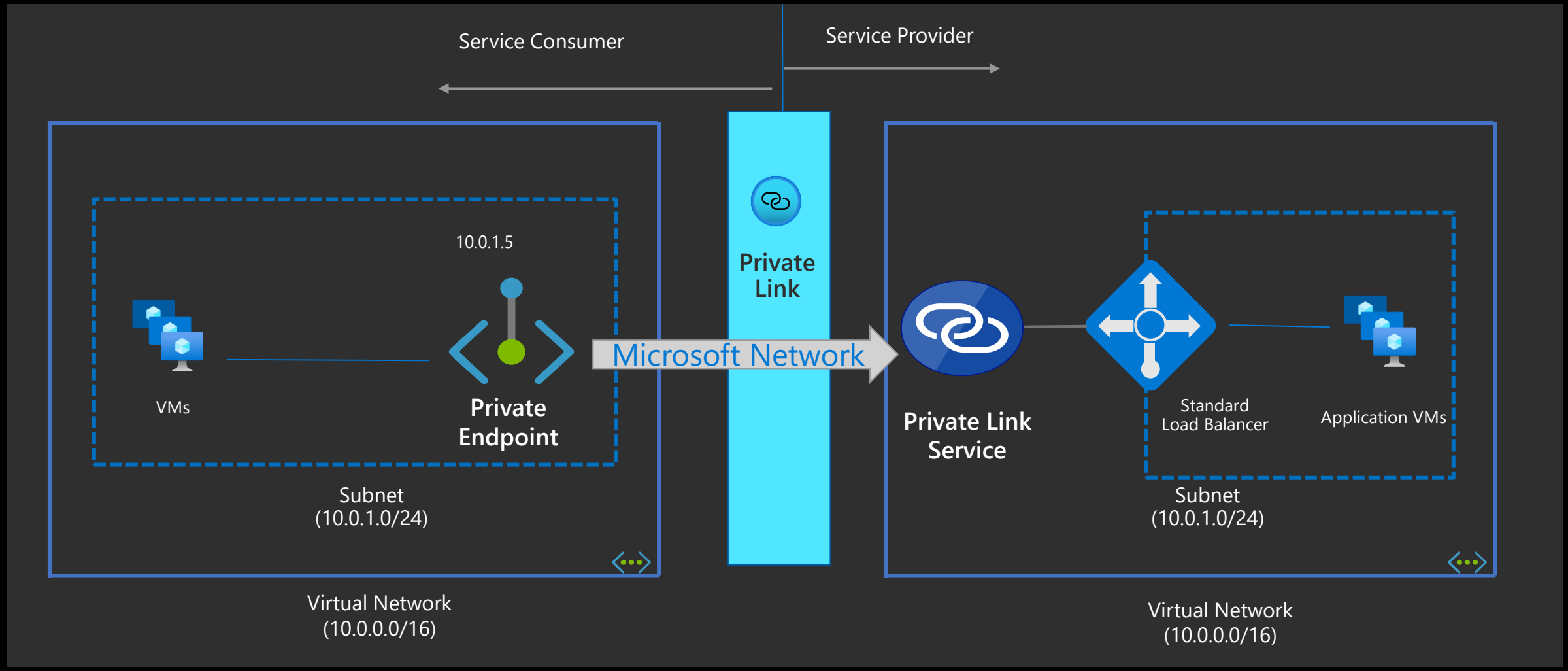
Private Link is not just for Microsoft PaaS services

Render or Consume Services Privately on Azure

Render a Service
Persona: Service Provider
Resource: Private Link Service

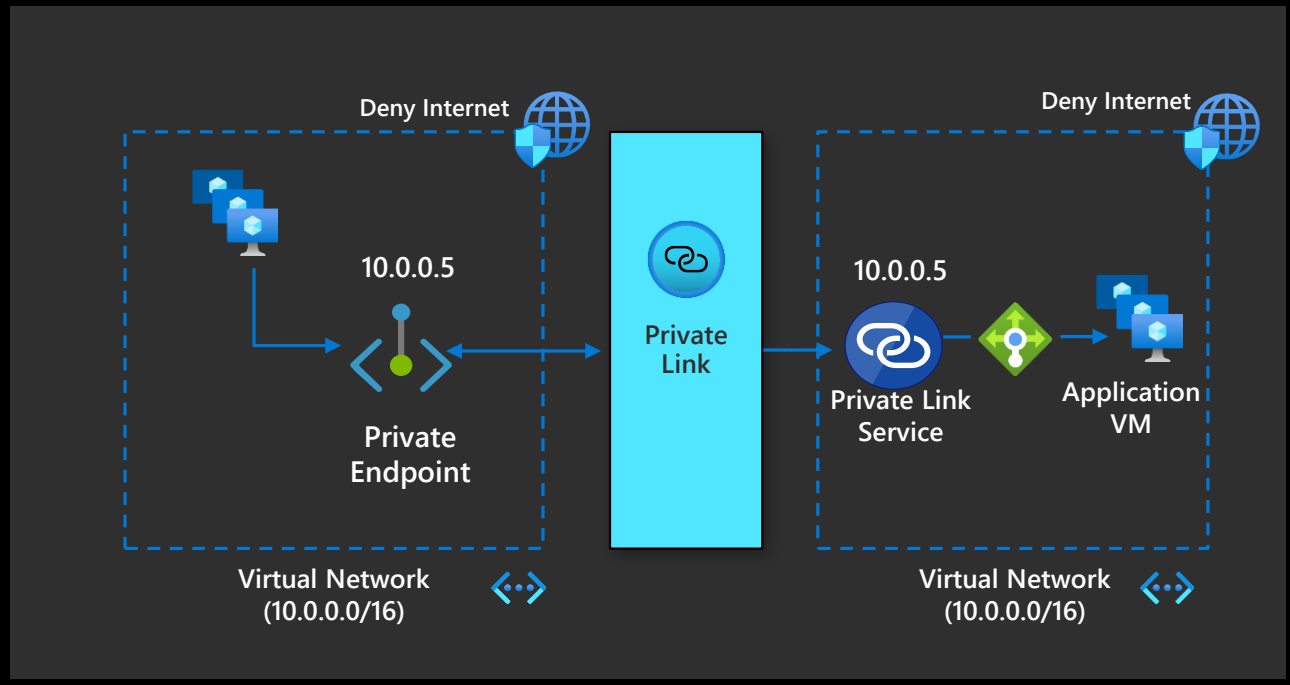
Consume a Service
Persona: Service Consumer
Resource: Private Endpoint

Private Link Service



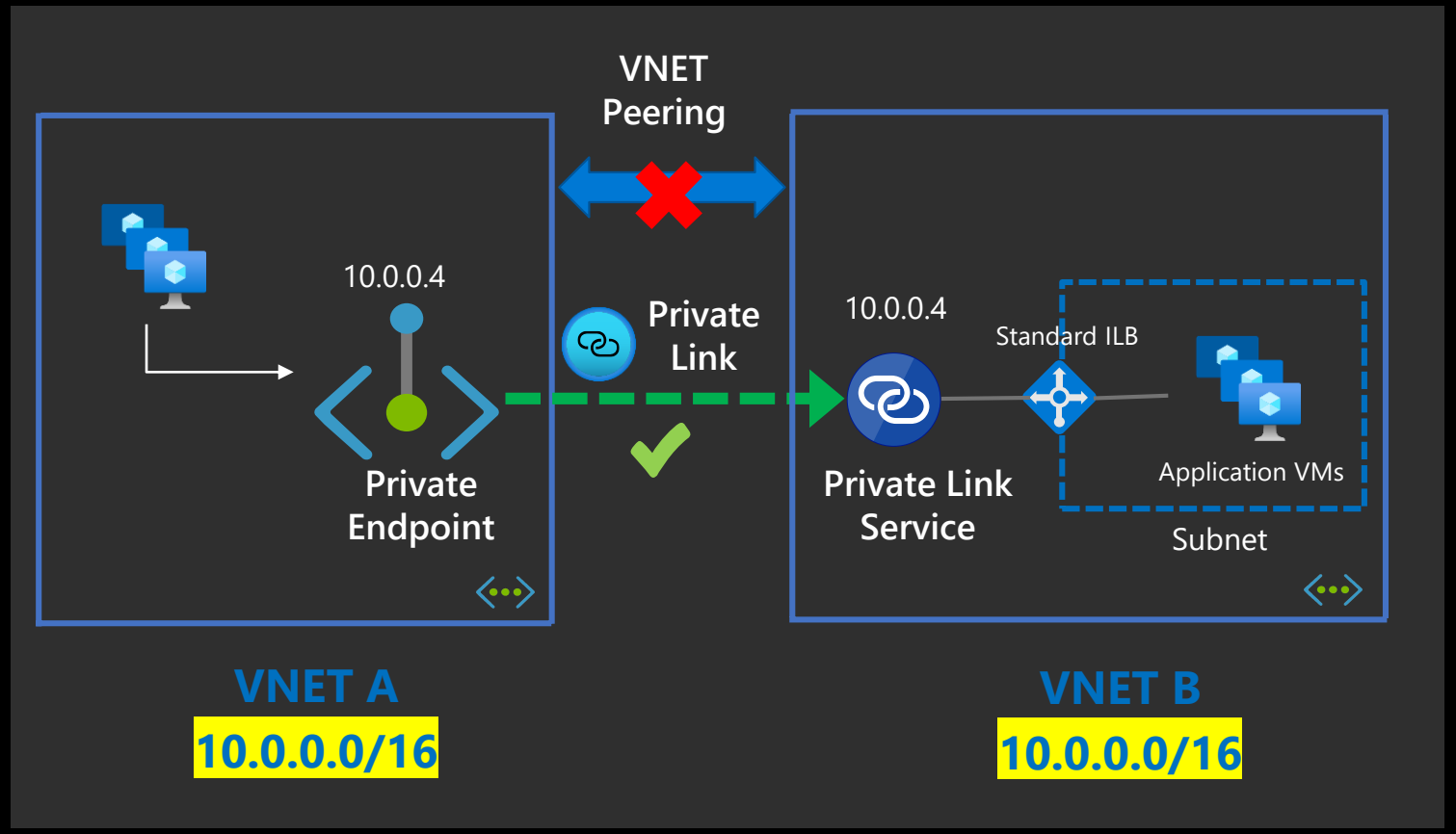
Overlapping IP? No problem.

- Create or Convert your existing services into Private Link Service
- Control the exposure to you service
- Consumption experience like Azure PaaS
- Easily Scale and manage the Private Endpoint Connections
- No regional or tenant restrictions
- No overlapping IP space restrictions



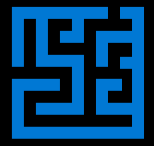
Peering Vs Private Link

- VNet Peering
  - Bi-directional
  - All resources can talk to each other
- Private Link
  - Overlapping IP Space allowed
  - Source info shared through Proxy Protocol
  - Uni-directional
  - Connection through Private Endpoint (1 IP address)

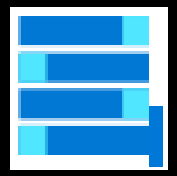


Recap?

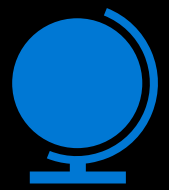
Private Access



Inline with Compliance Requirements



Works with On-Prem and Peered networks



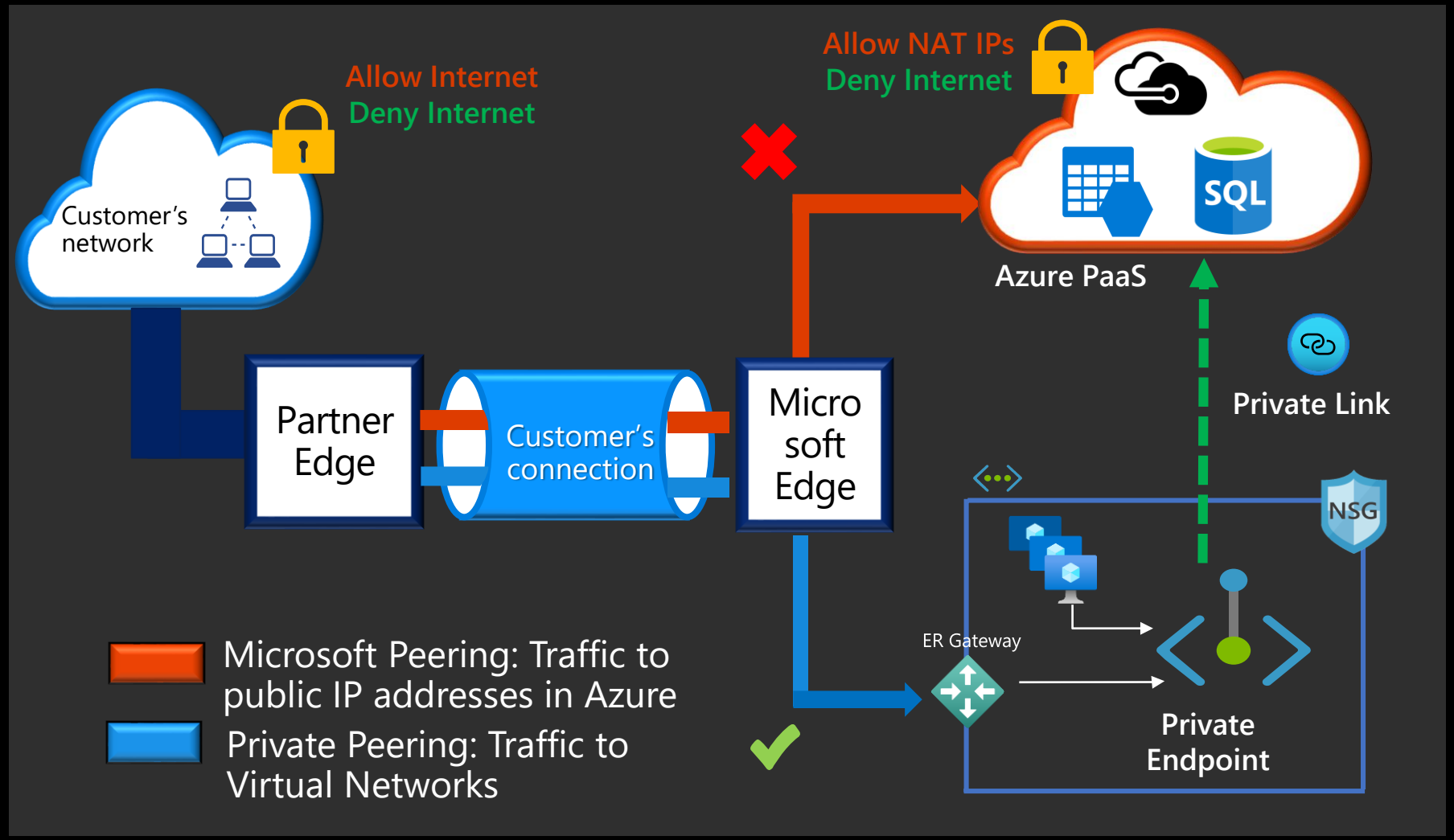
Global Private Connectivity

Data Exfil Protection

Simplified Network Management

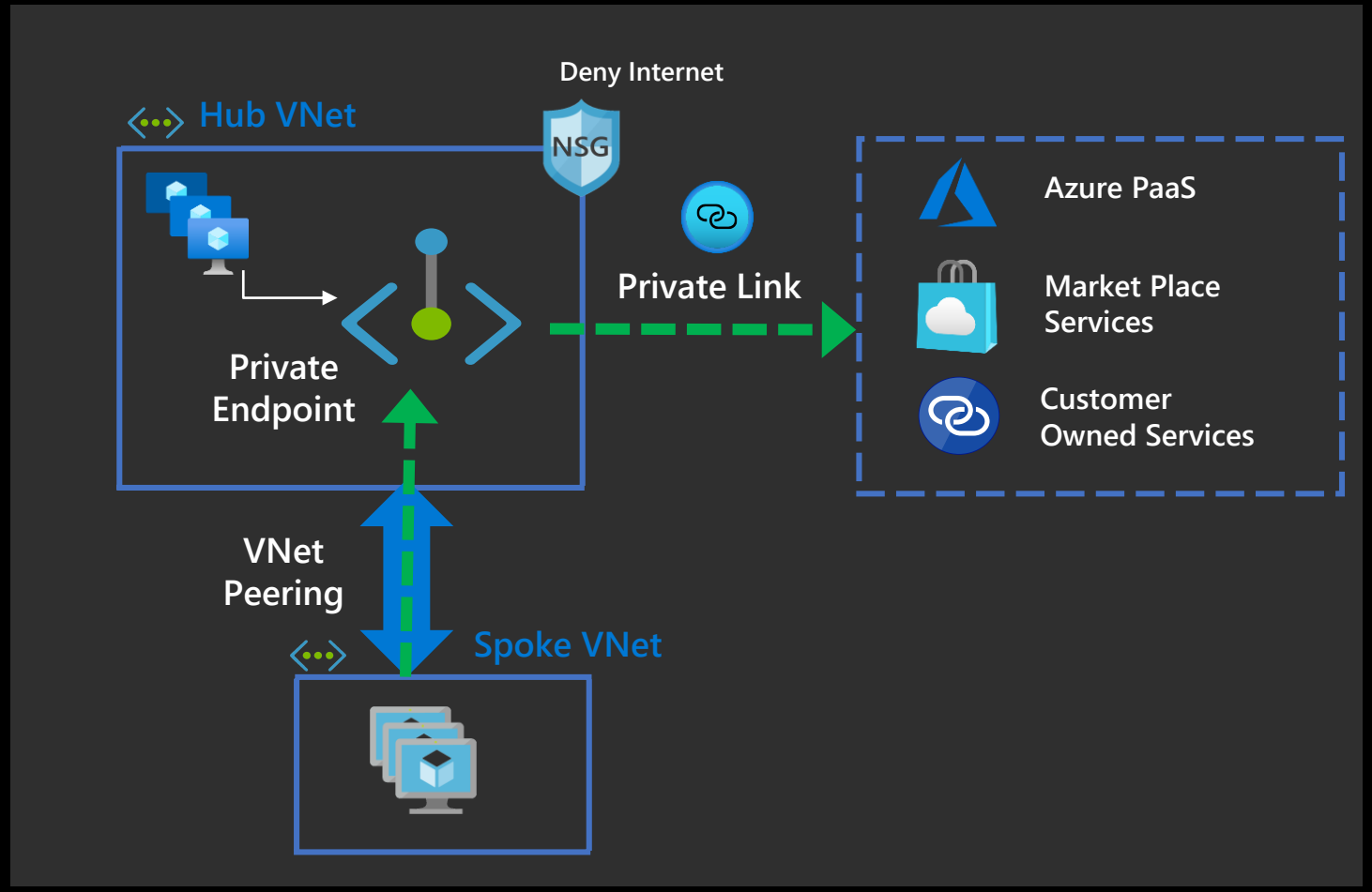
On-Prem Access

- Works with VPN and ExpressRoute
- Clean On-prem and Resource ACLs
- Flexibility with Migration scenarios



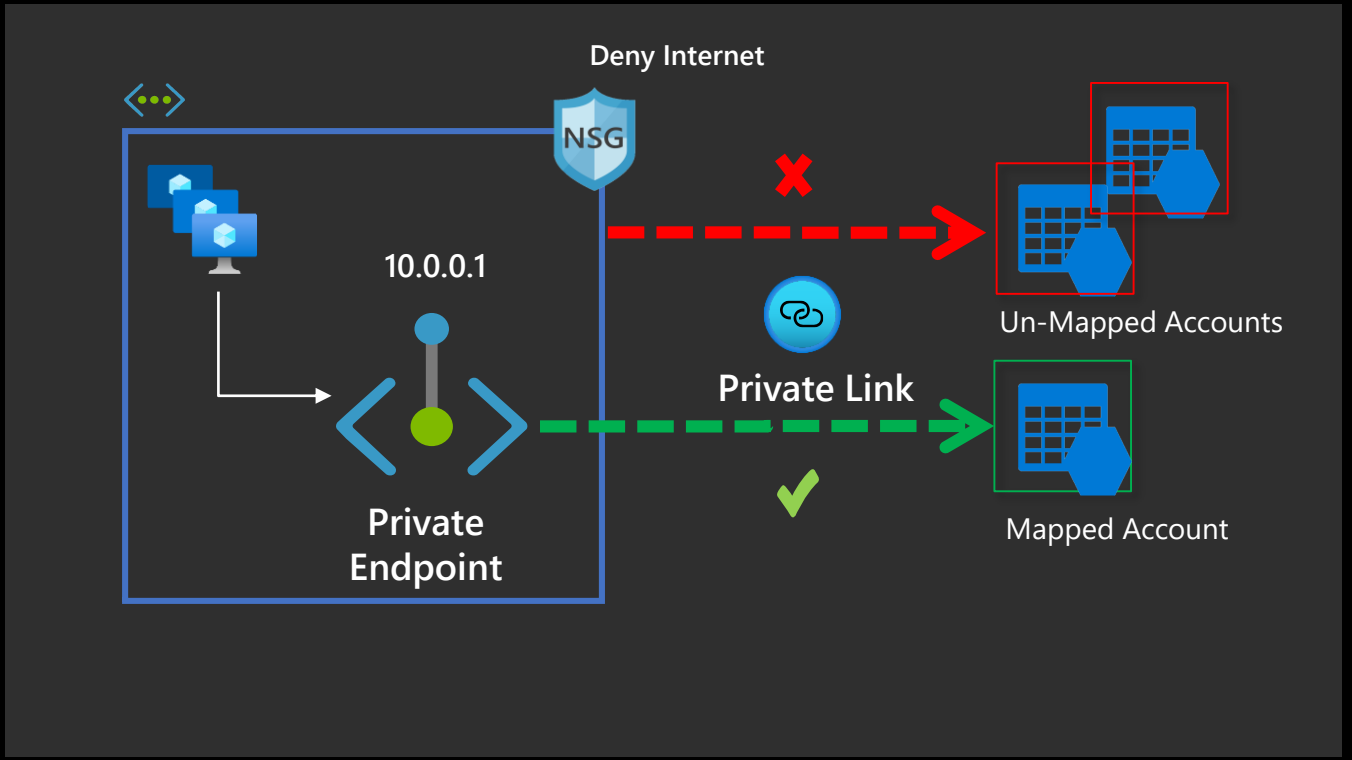
Peered Networks

- Reachable from peered Networks
- Both Local and Global Peering supported
- Hub and Spoke Topology



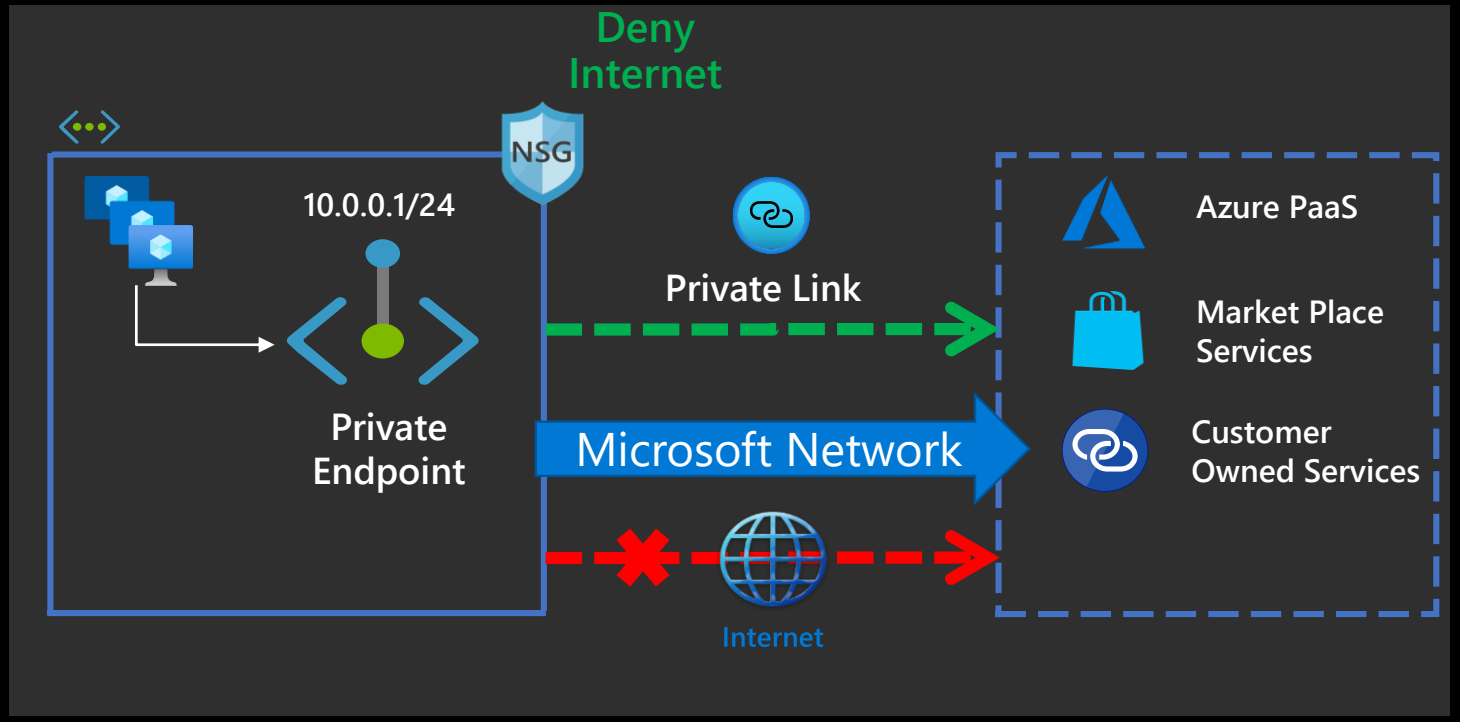
Data Exfiltration Protection

- Data Exfil protection by design
- Map Resources instead of Service
- Access only to mapped resource



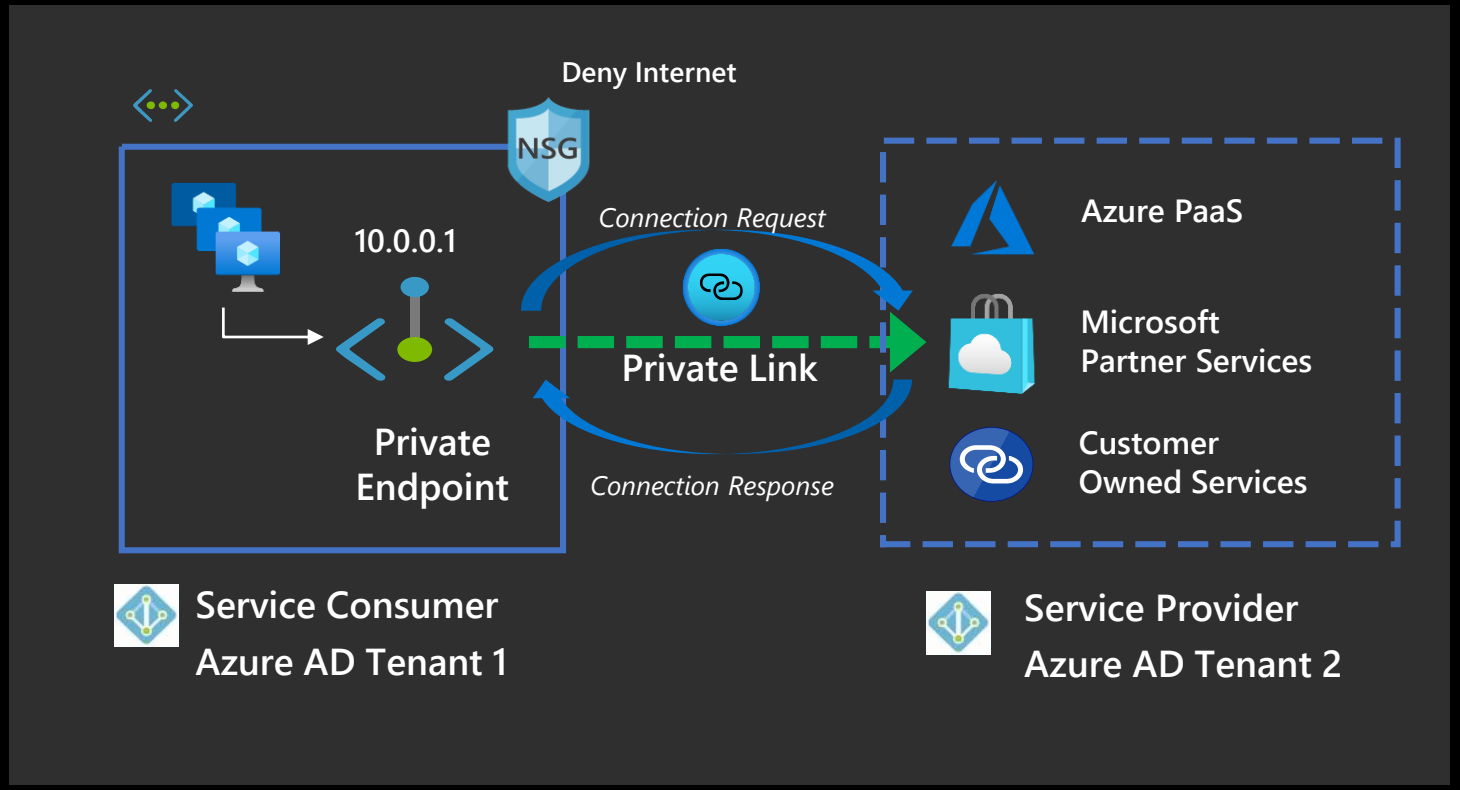
Inline with Compliance Requirements

- Securely use Services
- Data never traverses Internet
- Clean Security Rules



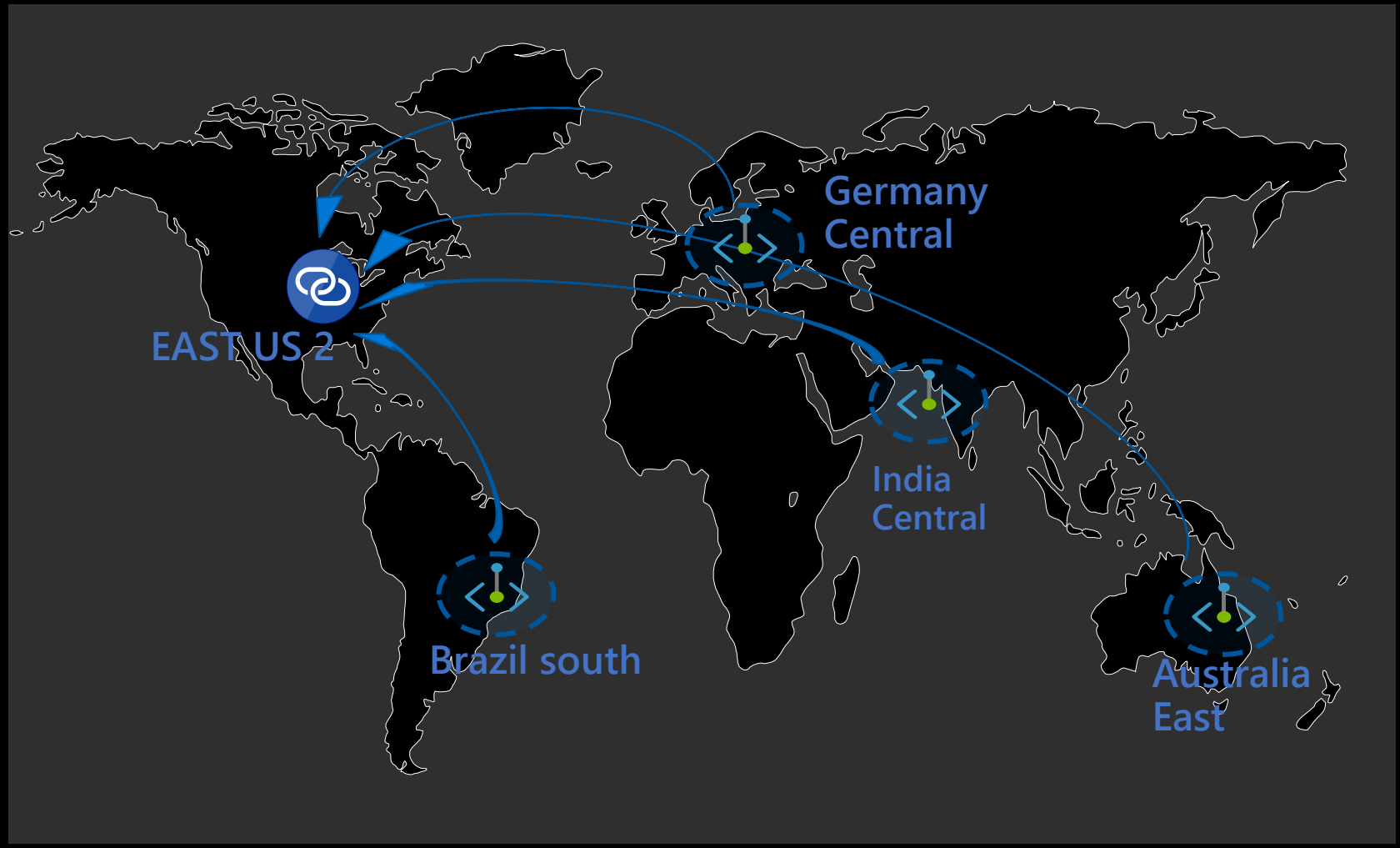
Simplified Network Management

- Predictable IP address for configuring your policies
- Cleaner ACLs both on Azure and On-Prem
- Route the traffic the way you want
- Approval Workflow based modelling. No RBAC dependency
- Works across AD tenants and Subscriptions



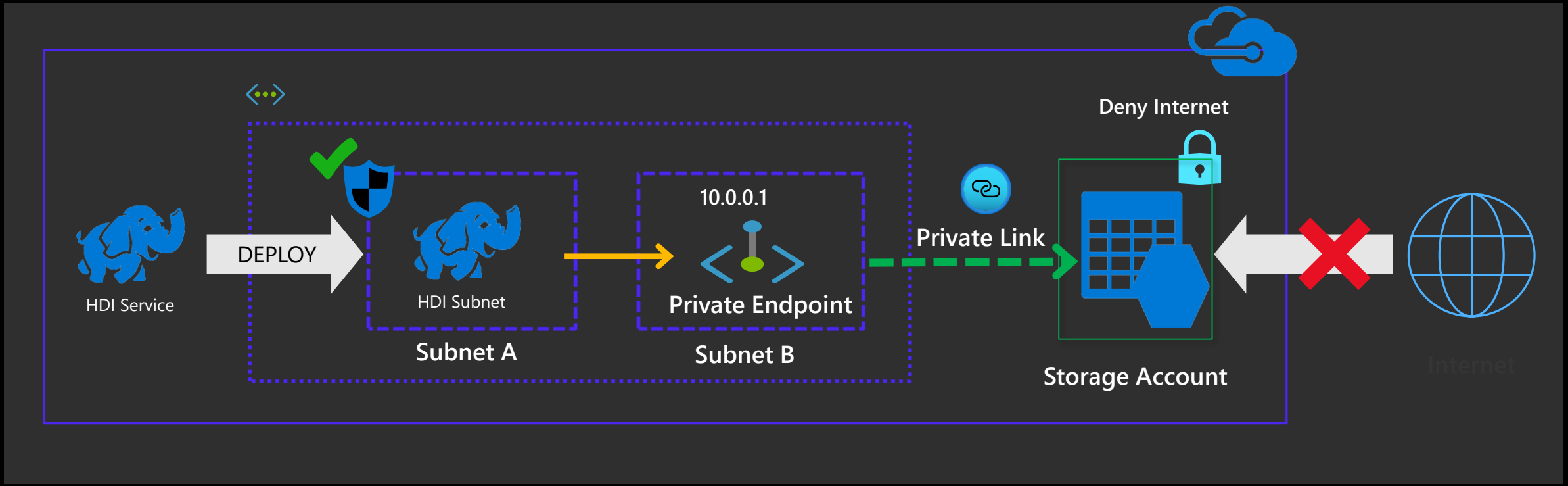
Global Private Connectivity

- No regional restrictions
- Reach your customers or service providers in any region
- Optimal Routing over Microsoft Network for better latency and performance



54+ Azure Regions

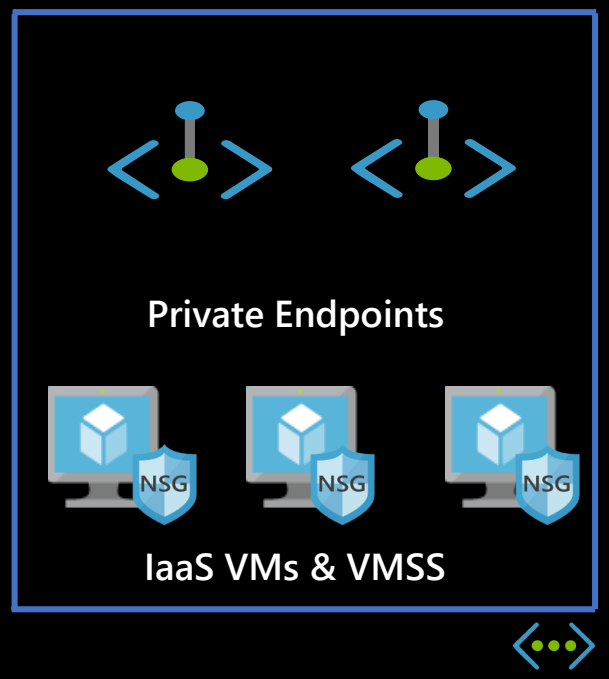
Stitching Services Together



- Secure Azure resources to managed service subnets with endpoints
- Applies to all services directly deployed into VNet

Private Endpoints: Choosing a Subnet

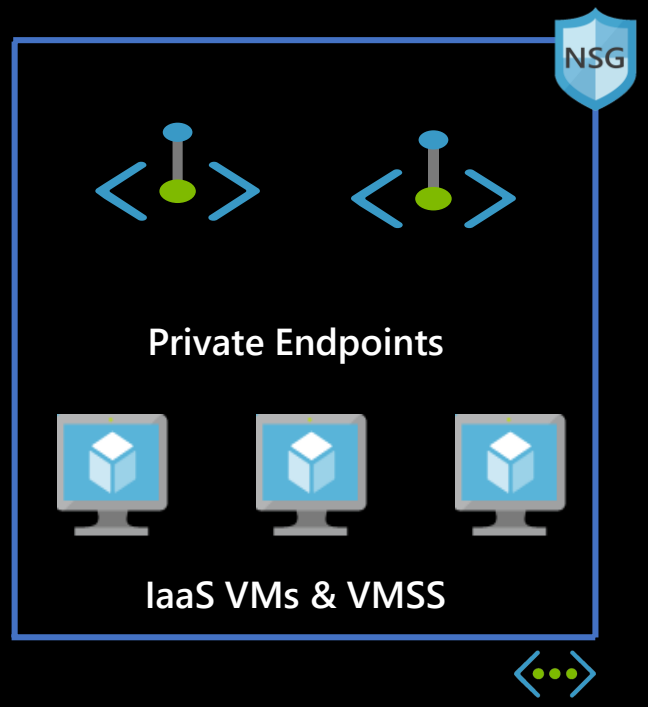
Subnets with no NSG



Subnets with NSG

* With explicit setting on subnet to disable NSG on Private Endpoints

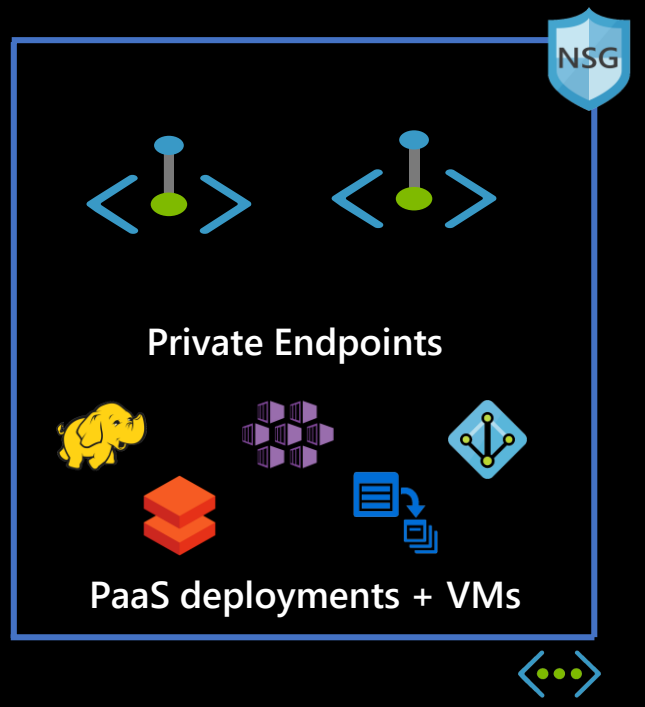
Portal UI will enable the setting during creation of Private Endpoints



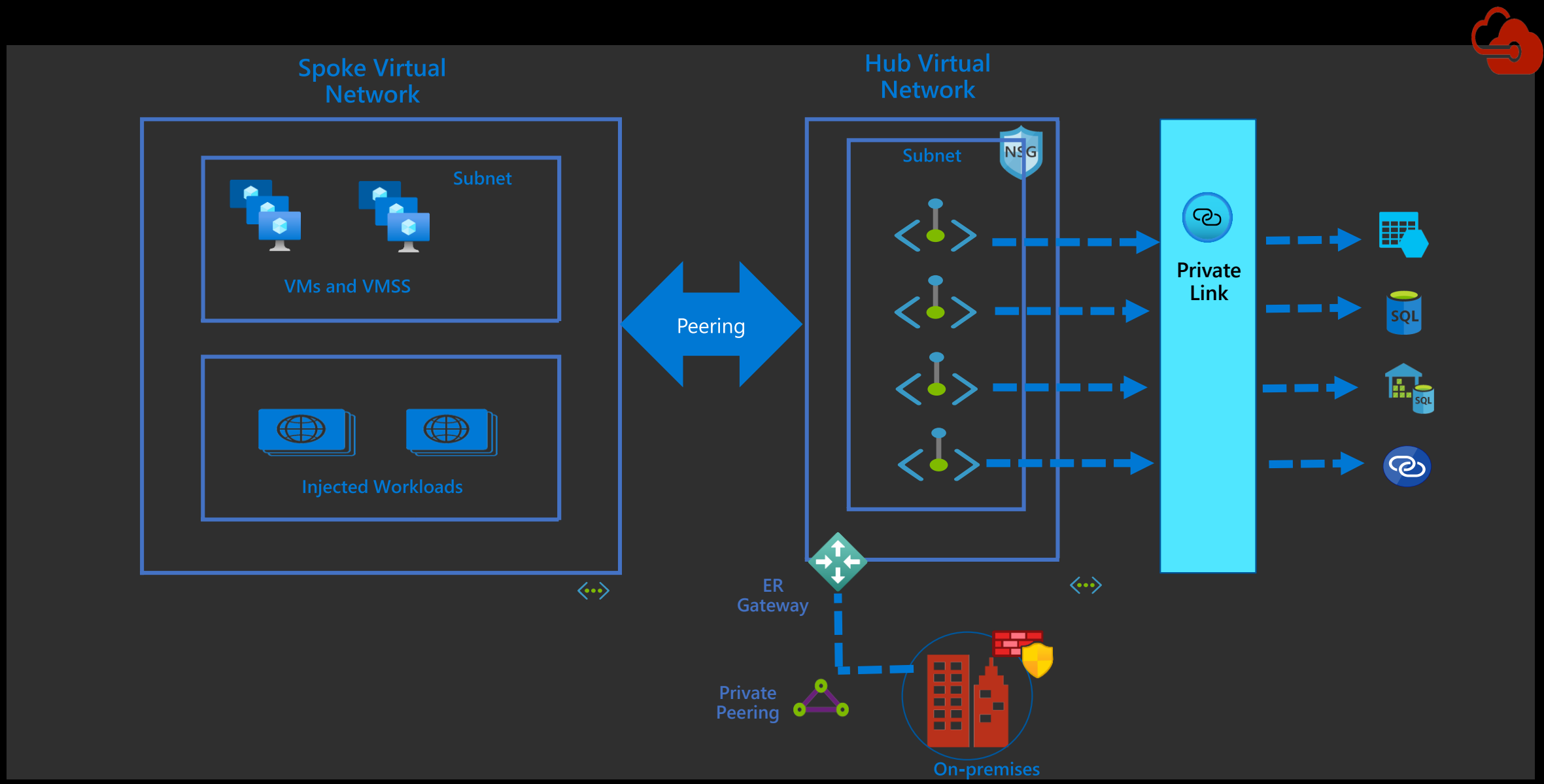
Subnets with Injected Services

* With explicit setting on subnet to disable NSG on Private Endpoints

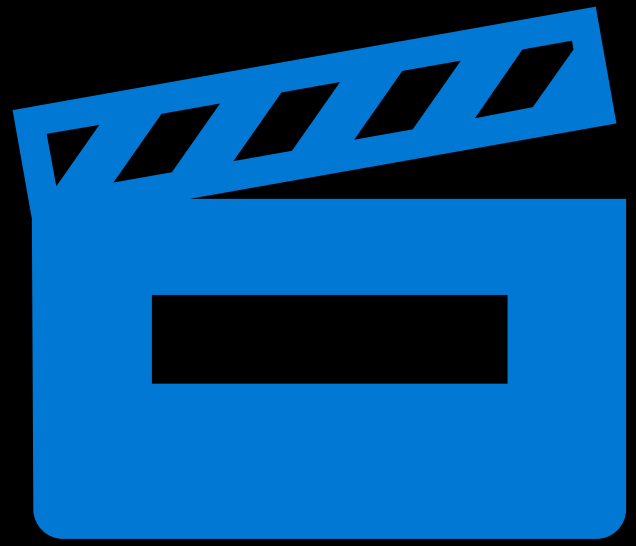
** Based on service support for mixed deployments



Sample Architecture



Click to learn more



- ❑ Start using Private Link today
  - Explore Documentation
  - Try through Portal/CLI/PS/REST
- ❑ Migrate from Service Endpoints to Private Endpoints
  - Setup private endpoint for your resource
  - Configure DNS to direct your traffic to private endpoint. Confirm its working
  - Remove Service endpoints – VNet Setting and Resource ACLs
- ❑ Watch Ignite presentation
  - BRK3168 - Delivering services privately in your VNet with Azure Private Link

Microsoft

Thank You