Azure Landing Zones

Modern Architecture for a Modern "Datacenter"

Scott Corio

Sr. Enterprise Cloud Architect

Microsoft MVP
Azure

MVP

ScottCorio

DumpsterDave

blog.shitstormbrewing.beer

Azure Landing Zones

- What exactly are Azure Landing Zones?
  - Application vs Platform Landing Zones
- Hub and Spoke vs Florida Network Topology
- When do Landing Zones not make sense?
- How to manage costs with Landing Zones?
- How are Private Endpoint and Private Links Important in this model?
- Can I still blame DNS for all my problems?
- How to properly secure Landing Zones
- How do I design workloads to fit into or migrate to the landing zone model?

What is an Azure Landing Zone?

- A Landing Zone is a location that workloads can “Land” in the cloud.
  - Broken up into Platform and Application Landing Zones
- Applications can be a single line of business app such as SAP or a single priority workload
- Applications could also be a collection of workloads maintained by a single group or business unit (ex: finance apps, marketing apps, sales apps, etc)
- Each Landing Zone consists of one or more subscriptions that all resources reside in (Typically a Prod and Non-Prod)
- A Landing zone is the top level that access or policy should be applied for a given application/collection.

What is an Azure Landing Zone? Contd.

- A scalable, modular architecture to meet various deployment needs
- Repeatable
- Conceptual architecture (There is no set layout/one way to do it)

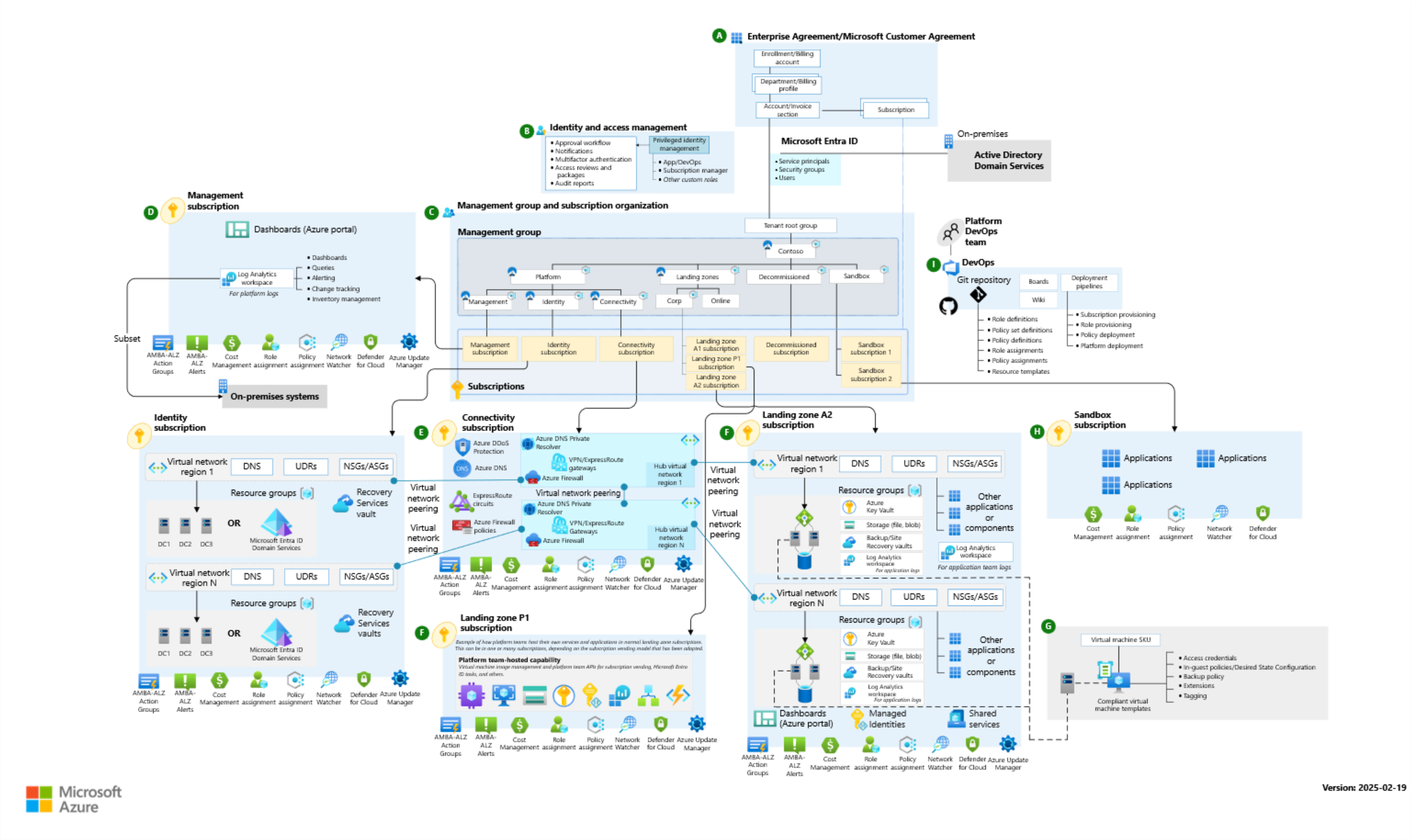
Platform Landing Zones

- Platform Landing Zones are generally Shared Services that deliver a global/environment wide function
    - Firewalls/Network/Front Door/APIM (**Connectivity**)
    - Shared Services, Logs, Automation Accounts, etc (**Management**)
    - Domain Controllers/Authentication Services (**Identity**)
- Platform Landing Zones should be owned by core infrastructure teams and access should be tightly controlled
- Platform Landing Zone networks may or may not be peered to each other

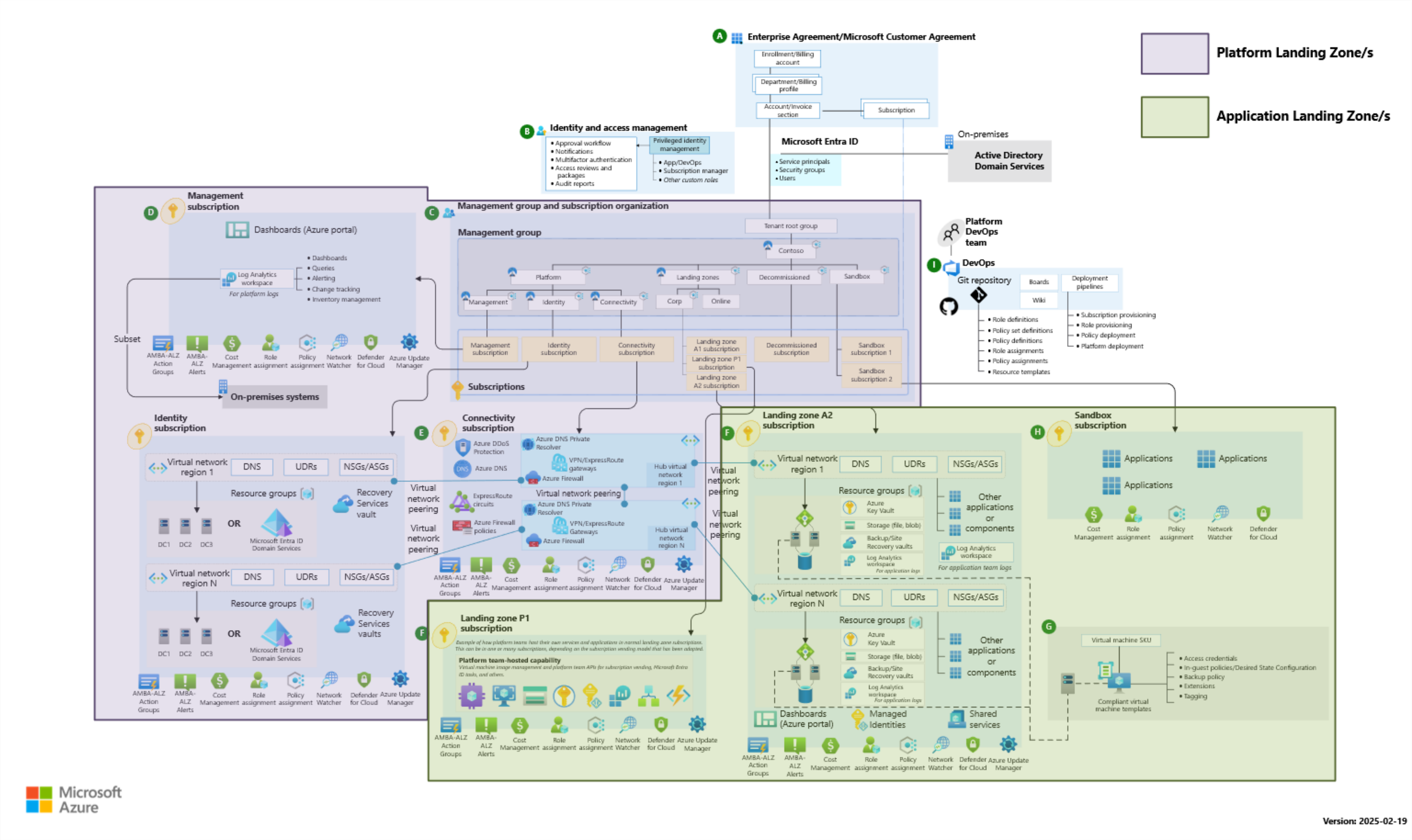
Application Landing Zones

- Each application landing zone should host a single LoB Application or a singe departments/business units applications
- Application Landing Zone networks should not be peered (though some exceptions may exist)
- Pick an IP range that can be re-used for all landing zones (a /20 or /19 is a good starting point)

Cloud Adoption Framework



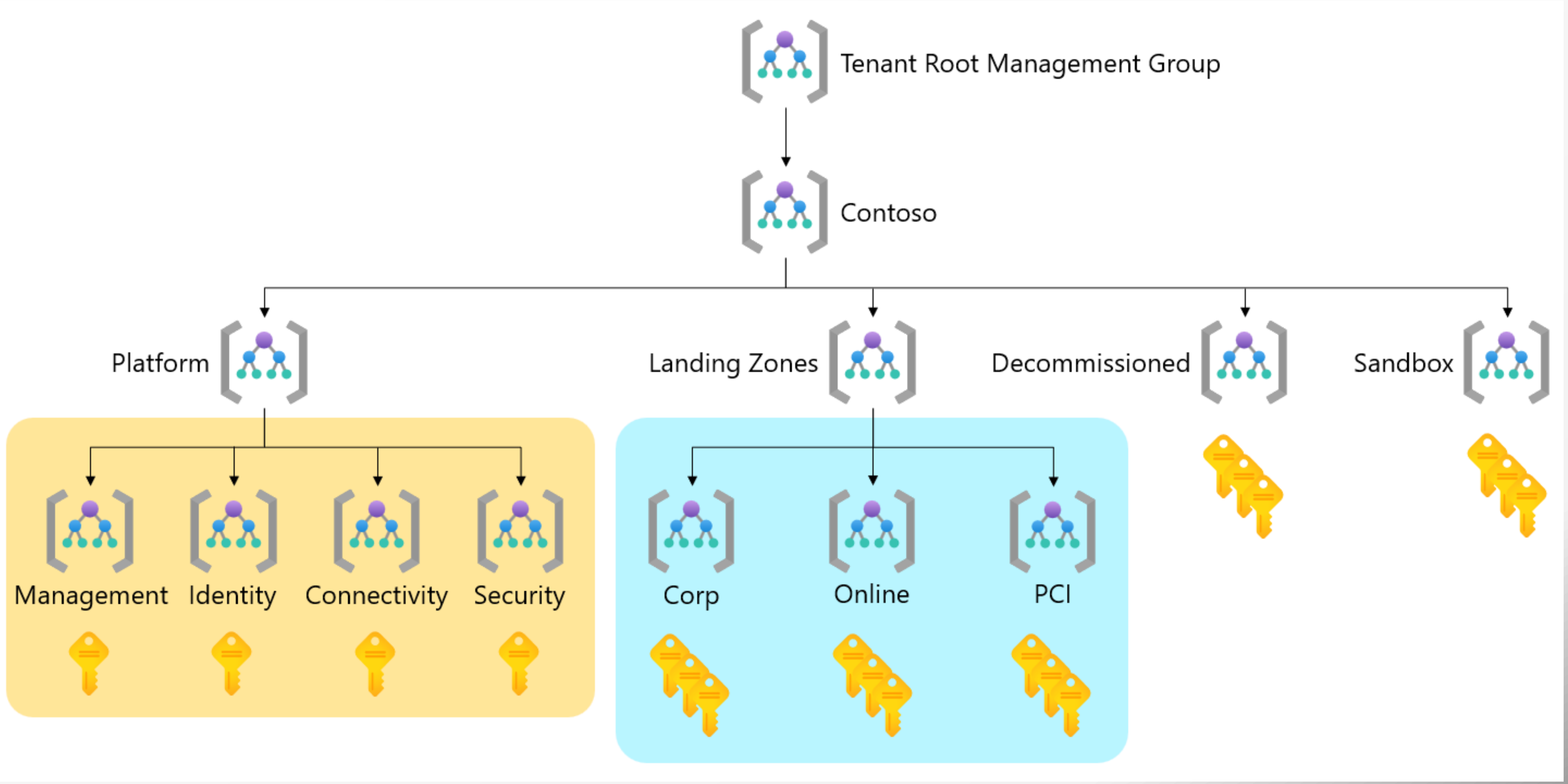
Cloud Adoption Framework - Demarked



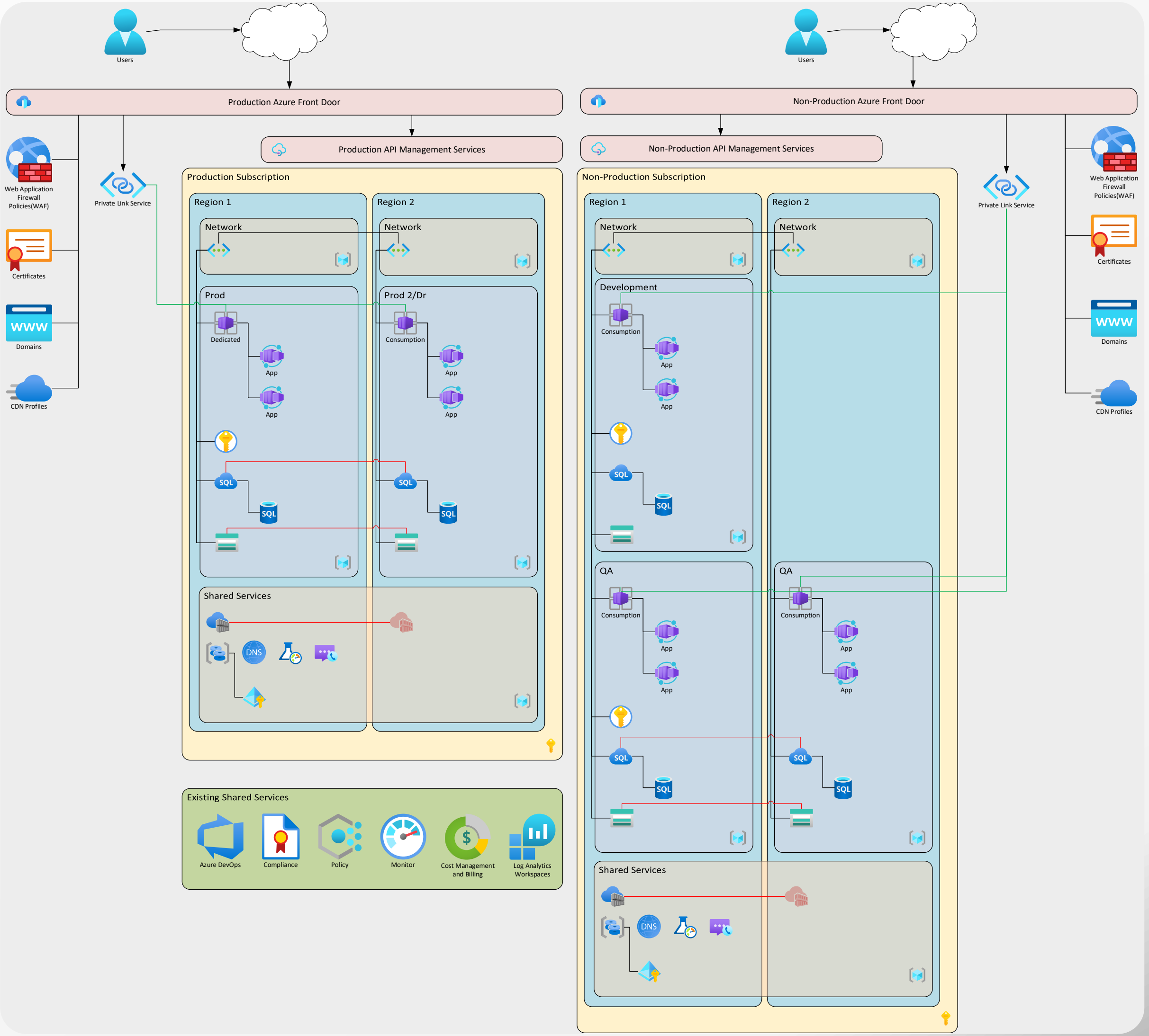
Organization

- Management Groups
  - Do not put any resources/subscriptions under the root management group or assign policies to the root
  - Create a new "Cotoso Root" that contains all child management groups
  - Create a "Default" container to catch rogue subscriptions
  - Create Custom Roles on the Tenant Root
- Subscriptions
  - Each Application Landing Zone should have a Non-Production and Production Subscription. Use Dev/Test pricing on the Non-Production Subscription

Management Group Primer



Subscription and Resource Structure



Workload Design

- Application Landing zones are not [really] designed for legacy (IaaS) focused workloads
  - IaaS resources can still play a supporting role in a landing zone
- Resources that utilize Private Endpoints/Private Links are best suited for Landing Zones
- Utilize Private Endpoints to access LZ resources from within your network
- Containers instead of VMs, Azure SQL instead of Microsoft SQL
- DevBox for local resource access. DevOps Managed Pools for secure DevOps Pipeline access and build activities.
- Workloads should leverage Azure RBAC for secure access (not ACLs or AD Permissions)

When to Landing Zone

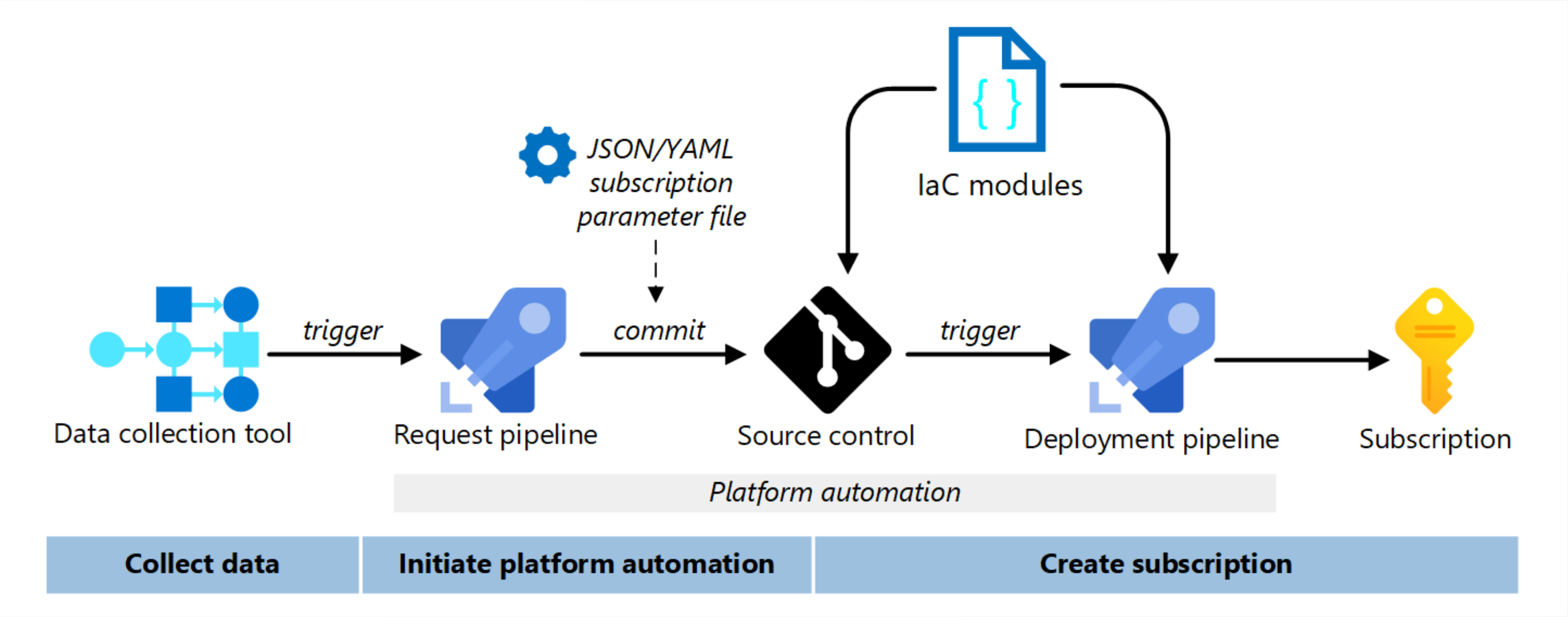
Landing Zone

No Landing Zone

- Modern Workload
- One or Two Services
- External Accessibility
- Regulatory Restrictions
- Isolation Requirements
- 3rd Party Firewall Requirements
- Local Connectivity Only
- Chargeback/Shameback Billing

Landing Zone Vending

- Give the power back to the people – self-service landing zones!



JSON/YAML subscription parameter file

IaC modules

Data collection tool

trigger

Request pipeline

commit

Source control

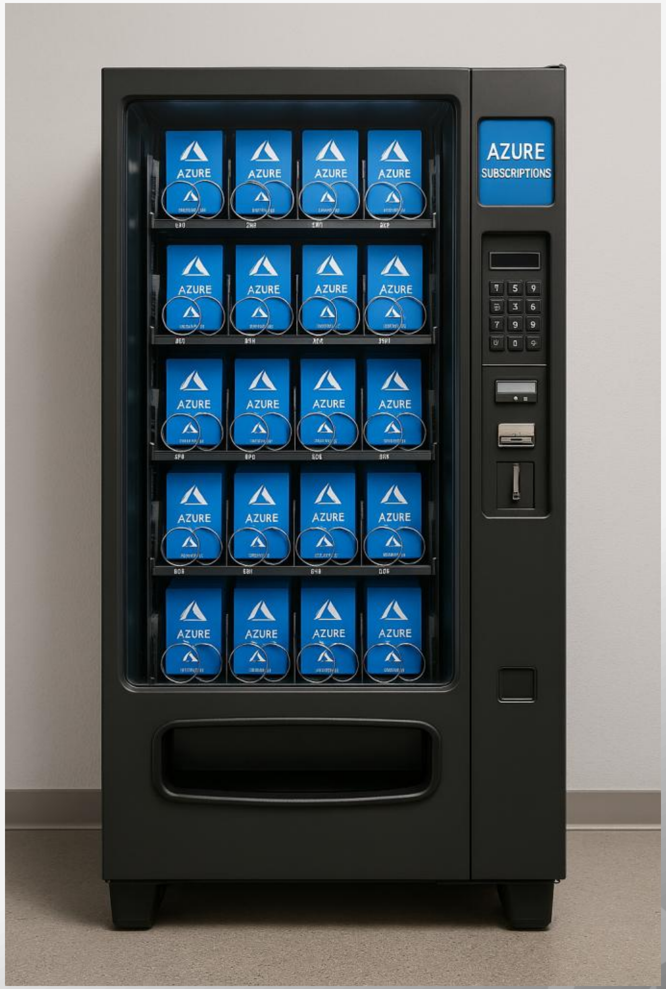
trigger

Deployment pipeline

Subscription

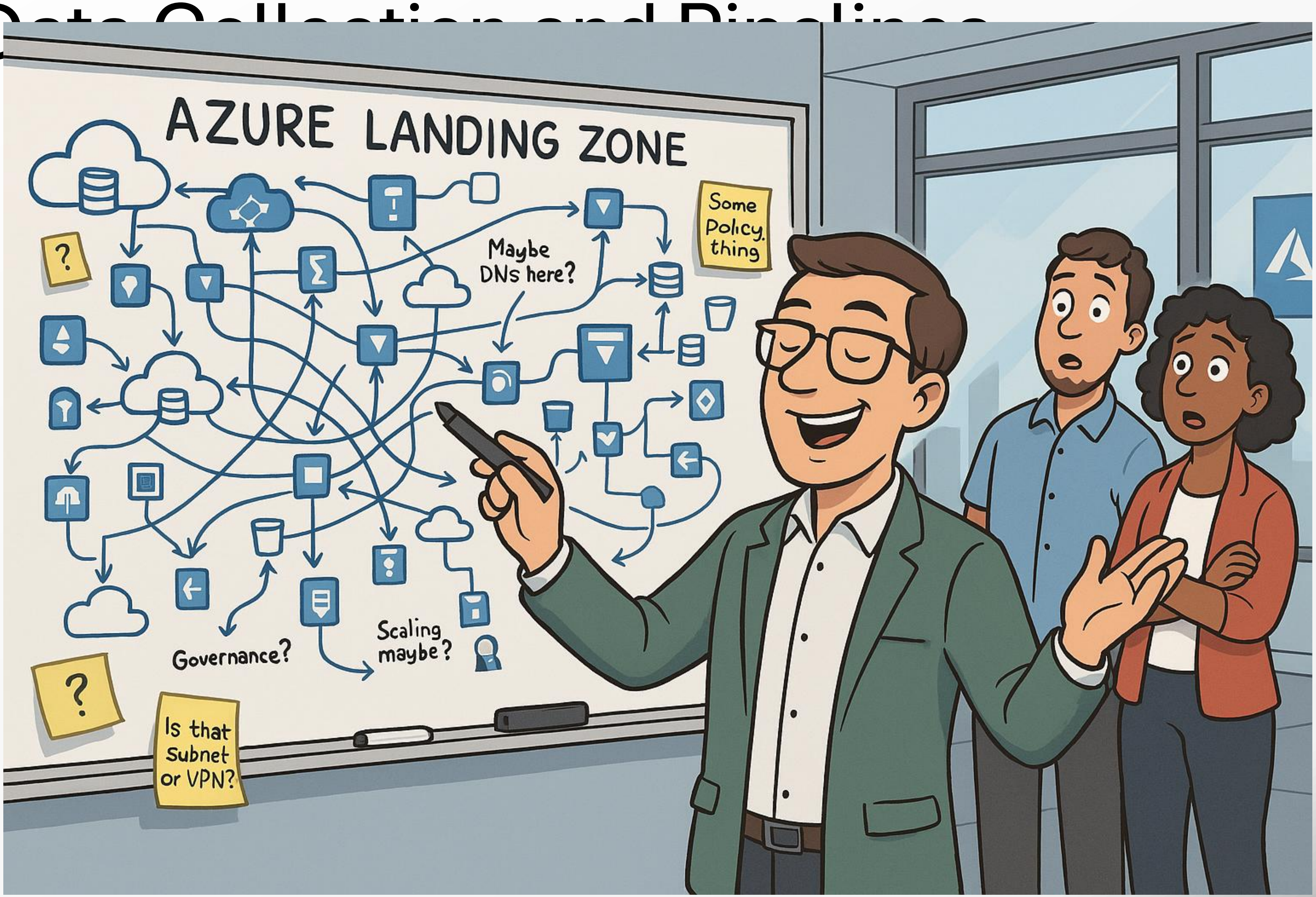
Platform automation

Collect data | **Initiate platform automation** | **Create subscription**



Data Collection and Pipelines

D



LZ and Vending Considerations

- Can be complex to setup – use the Accelerator!
- Learning curve – that's why you are here
- You gotta control those costs – make sure you got those approval processes in place
- App teams need to adapt to the LZ and vending process

Network Considerations

- Decide on isolation and subnet layout
  - Isolated Landing Zones can re-use the same IP block
- Determine VNet IP Space size
  - /19 or /20 is a good starting point
- Determine your ingress traffic control requirements
  - App Gateway/Azure Front Door/API Management/3rd Party Firewall
- Determine Management/Local Access Infrastructure
  - Virtual Desktop/DevBox/Bastion
- Determine outbound connectivity
  - NAT Gateway/Firewall/etc
- Determine Inter-Zone connectivity
  - Private Endpoints

So About those Private Endpoints…………………

- **ALL** Azure Networking is Software Defined Networking
- There is no magical Cat6 cable that connects **your** services, servers, and platforms to each other
- All Connectivity traverses the "shared" Azure Network… Your VNets, Routes, and Peerings determines where it can go on that network
- A Private endpoint is just a fancy DNS trick that isolates your resources so that traffic can only originate from your "network".
- There is no way to 100% isolate (Air-Gap) Azure traffic to your network in a physical capacity (remember, there is no "Cable").
- Private Endpoints can be used to "link" resources to networks without linking networks.

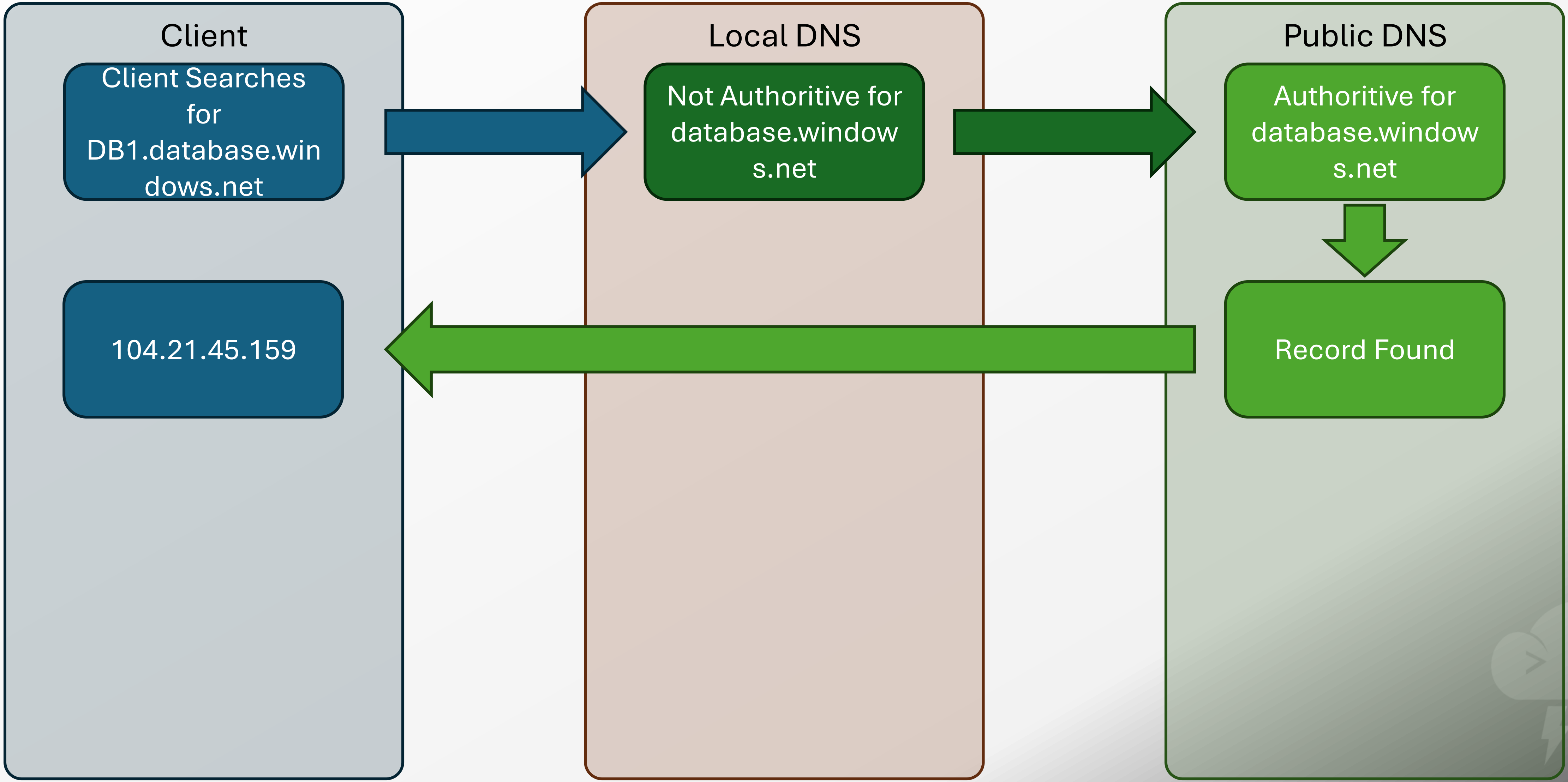
Private Endpoint Cost Considerations

- $0.01 / hour per private endpoint
- Data Charges
  - $0.01/GB for the first PB
  - $0.006/GB for 1-5 PB
  - $0.004/GB for 5+ PB
- Inbound and Outbound Data cost the same, but are separate thresholds
- Reading from a storage account counts as outbound data (Data is going **OUT OF** the storage account)
- Writing to a storage account counts as inbound data (Data is going from the resource **INTO** the private endpoint)
- Resources cannot initiate traffic over their own private endpoint
  - An App Service with a private endpoint cannot use it to connect to a database or storage account, however it can use the database or storage accounts private endpoint. VNet Integration is required to fully isolate traffic.

Private Endpoint Cost Examples

- Example A: Storage account that used as an archive to store 100GB of logs /month
  - $0.01/hr * 730 hours = $7.30
  - 100GB of outbound data = $0.01/GB * 100GB = $1.00
  - $8.30/mo
- Example B: Storage account used as a (massive) application cache
  - $0.01/hr * 730 hours = $7.30
  - 0.5 PB of outbound data = $0.01/GB * 500,000GB = $5,000.00
  - 2 PB of inbound data = $0.01/GB * 1,000,000GB + $0.006/GB * 1,000,000GB = $16,000
  - $21,007.30/mo

How does a Public Endpoint Work?



Client

Client Searches for DB1.database.windows.net

104.21.45.159

Local DNS

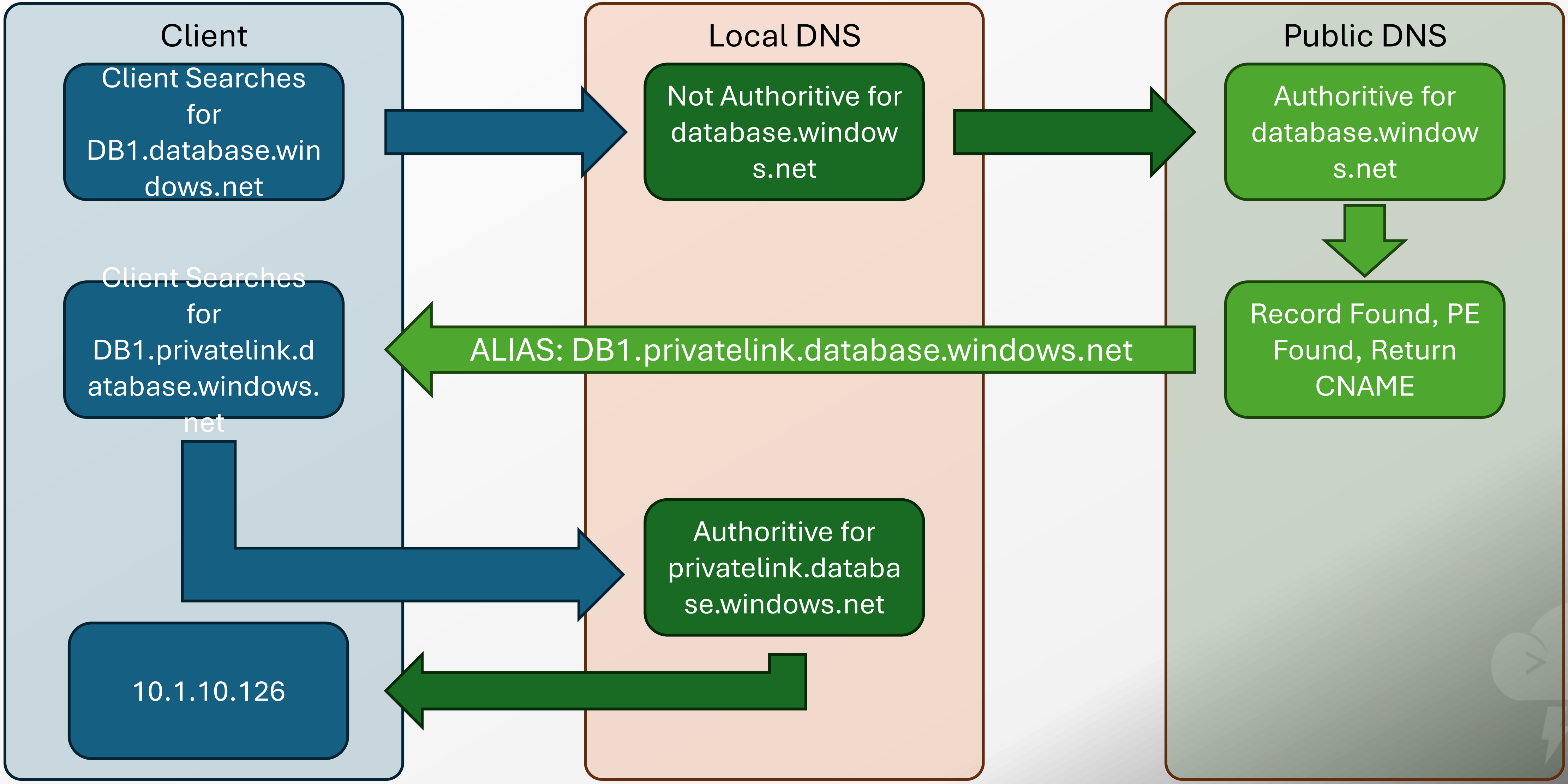
Not Authoritive for database.windows.net

Public DNS

Authoritive for database.windows.net

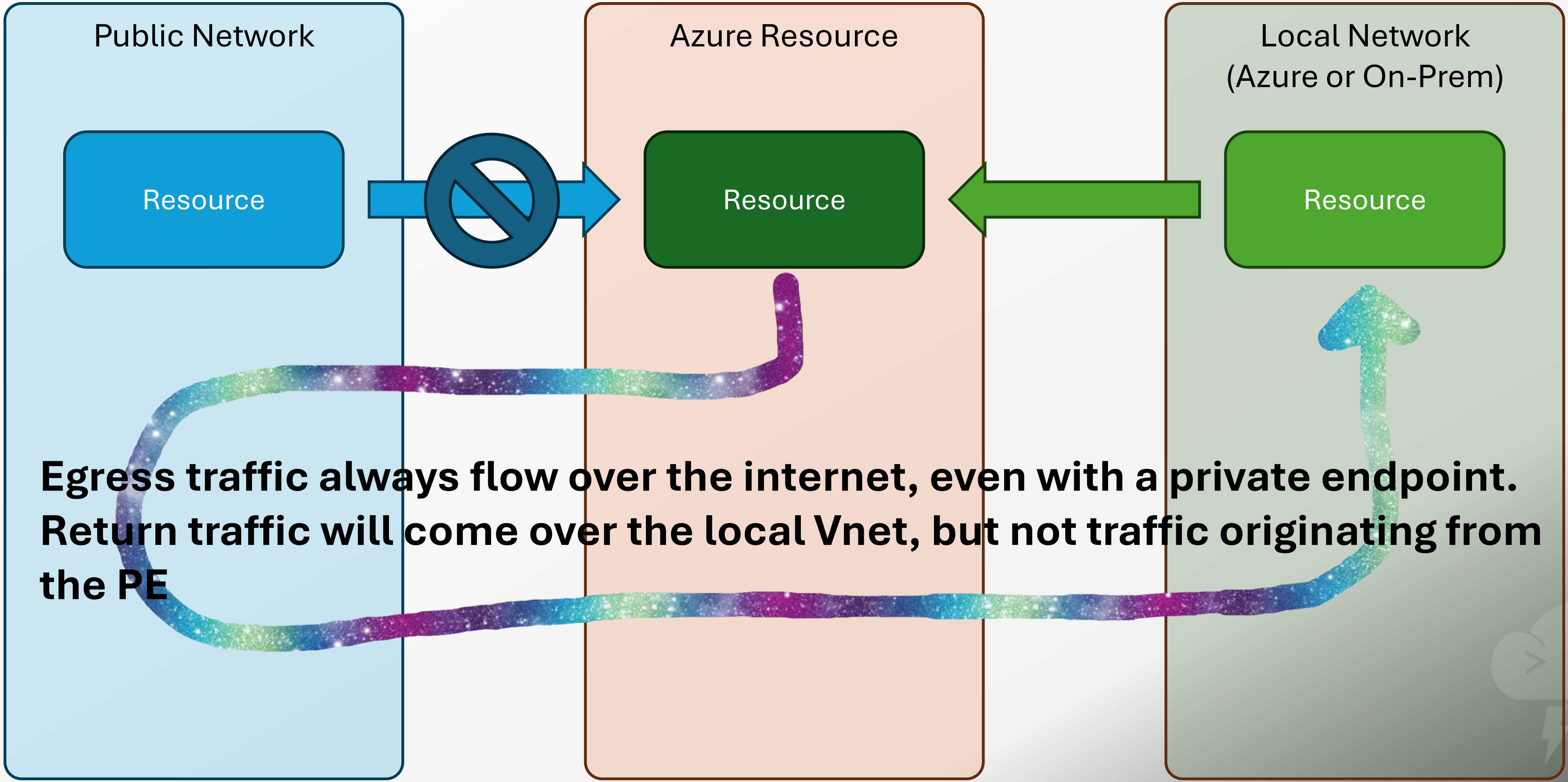
Record Found

How does a Private Endpoint Work?



Client
Client Searches for DB1.database.windows.net
Client Searches for DB1.privatelink.database.windows.net
10.1.10.126
Local DNS
Not Authoritive for database.windows.net
Authoritive for privatelink.database.windows.net
Public DNS
Authoritive for database.windows.net
Record Found, PE Found, Return CNAME
ALIAS: DB1.privatelink.database.windows.net

What About Egress Traffic?



Egress traffic always flow over the internet, even with a private endpoint. Return traffic will come over the local Vnet, but not traffic originating from the PE

Q&A

References

- CAD – Landing Zones