AWS PrivateLink

Establish private connectivity without exposing data to the Internet

May 2021

Agenda

Customer Business Challenges

AWS PrivateLink Introduction and Benefits

PrivateLink Compared to Other Connectivity Choices

Common Use Cases

New: AWS PrivateLink for Amazon S3

Pricing

Partners

Case Study

Next Steps

AWS PrivateLink

Business Challenges, Benefits, Supported AWS Services

Customer Business Challenges

- CIOs and CISOs are driving Zero Trust Initiatives to reduce business risk
- Need to meet regulatory compliance
- Avoid cloud workload traffic for sensitive data from traversing public Internet
- Reduce costs when workloads connect to AWS regional services

Zero Trust Initiatives

Regulatory Compliance

No exposure to Internet for sensitive data

Cost Effective

What is AWS PrivateLink?

Combines two important cloud concepts:

- Virtual Private Cloud (VPC) – A private network that can be isolated from the Internet and other VPCs
- Software delivered as a service – Owned and operated by the provider and consumed by consumer

Access a service in another VPC using private IP

Traffic remains on Amazon's private network

Consumer-initiated communication

Mutual handshake between provider and consumer

AWS PrivateLink Benefits

Secure Your Traffic

Sensitive data doesn’t traverse public Internet

Simplify Network Management

No changes to route table or concerns of overlapping IP address space

Accelerate Your Cloud Migration

Simplify hybrid cloud connectivity while data remains private

Reduce Costs

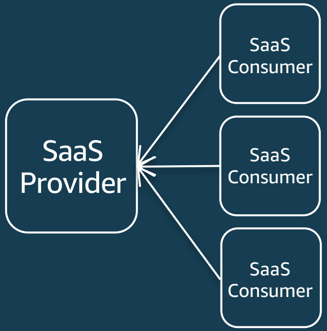
Eliminate NAT gateway costs or unnecessary Egress data transfer costs

AWS PrivateLink Use Cases

Secure Access to AWS Services

Secure and Simple Inter-VPC access

Secure Access to 3rd Party SaaS Applications



Hybrid Cloud

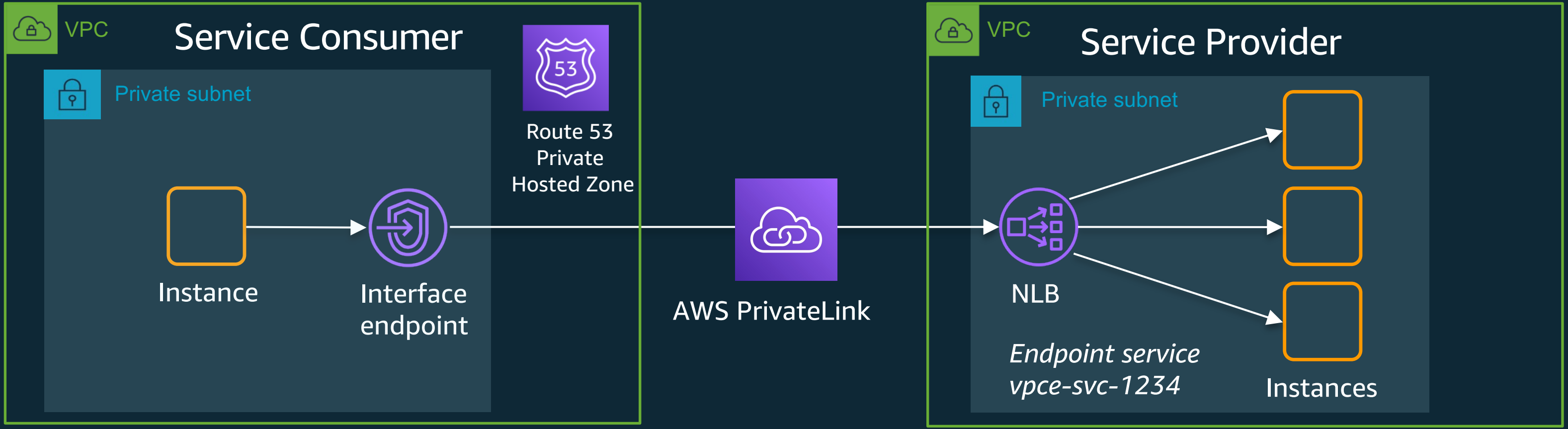
PrivateLink Building Blocks

Interface endpoint (in consumer VPC)

- Entry point for traffic to a PrivateLink-powered service. One or more ENIs[1] created by AWS that uses private IP
- Associate a security group with the ENI to control access
- Apps use the endpoint-specific DNS host name or default DNS name[2] (for AWS and AWS Marketplace Partner services)

Endpoint service (in provider VPC)

- Only needed if you are offering a PrivateLink-powered service to other consumers
- Network Load Balancer used as service front-end
- Create a VPC Endpoint Service configuration and specify your NLB



[1] ENI: Elastic Network Interface

[2] Requires Private DNS to be enabled

Private DNS for Interface Endpoints

- Endpoint-specific DNS name is generated at interface endpoint creation
  - E.g. vpce-1234.kinesis.us-east-2.vpce.amazonaws.com
  - Using this endpoint-specific DNS name requires changes to the application
- For AWS services and AWS Marketplace services, private DNS is supported
  - Associates a private hosted zone with your VPC
  - Enables the default DNS name for the service to be used (kinesis-streams.us-east-2.amazonaws.com in above example)
- Note for S3 over PrivateLink
  - Private DNS names are currently not supported for S3 over PrivateLink
  - Alternative: Create a Route 53 Private Hosted Zone with an alias record & attach to your VPC

Private DNS Names for Endpoint Services

- Problem statement
  - Endpoint-specific DNS name (e.g. vpce-1234.ec2.us-east-1a.vpce.amazonaws.com) must be used by the consumer's application → requires changes to the application
- Solution
  - To avoid making application changes, use Private DNS Names for endpoint services
  - A private DNS name is specified by service provider during endpoint service configuration
  - Provider must verify control of domain before consumers can use the private DNS name

PrivateLink Compared to Other Connectivity Choices

Criteria	VPC Peering	NAT GW + Internet GW	Transit Gateway	PrivateLink
Architecture	Full Mesh	Uses Internet Gateway + NAT Gateway to exchange data	Various Attachments based Hub and Spoke	Point-to-point private connection over AWS backbone
Best fit use cases	Simple connectivity between a few VPCs	Connectivity over Internet with non-AWS resources	Easily connect Amazon VPCs, accounts, and on-premises networks to a single gateway	Secure private connection to AWS or internal services, SaaS provider-consumer or private cross-VPC communication
Complexity	Increases with VPC count	Customer needs to use full-fledged security stack	AWS Managed Service	Low
Overlapping CIDR blocks	Not allowed	Allowed	Not allowed	Allowed
Scale	125 Peers/VPC	Generally limited by other services behind the Internet gateway	5000 Attachments	200 interface endpoints / VPC
Supported flows	TCP, UDP	TCP, UDP	TCP, UDP	TCP
Segmentation and security	Customer Managed	Customer Managed	Multiple Route Tables and ability to insert inline appliances	Built-in: Unidirectional initiation only by consumer. Service provider needs to allow-list and approve consumers
Latency	Lowest	Highest due to #hops on Internet and overall Internet latency	Hyperplane latency	Hyperplane latency
Bandwidth Limit	No Limit	5 Gbps per NAT GW, automatically scales up to 45 Gbps	Bursts of up to 50 Gbps per VPC Attachment	Sustained 10 Gbps per AZ Bursts of up to 40 Gbps
Visibility	VPC Flow Logs or VPC Traffic Mirroring	VPC Flow Logs, VPC Traffic Mirroring	Transit Gateway Network Manager	VPC Flow Logs
Cross VPC Security Group references	Supported	Not Supported	Not Supported	Not applicable
TCO	Lowest	Highest	Medium	Medium

AWS Services Available via AWS PrivateLink

- Amazon API Gateway
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Cloud Directory
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- Amazon CodeGuru Profiler
- Amazon CodeGuru Reviewer
- Amazon Comprehend
- Amazon EBS direct APIs
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon EMR
- Amazon EventBridge
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Keyspaces (for Apache Cassandra)
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- Amazon Managed Blockchain
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon RDS
- Amazon RDS Data API
- Amazon Redshift
- Amazon Rekognition
- Amazon S3
- Amazon SageMaker and Amazon SageMaker Runtime
- Amazon SageMaker Notebook
- Amazon Simple Email Service (Amazon SES)
- Amazon SNS
- Amazon SQS
- Amazon Transcribe
- Amazon Transcribe Medical
- Amazon WorkSpaces
- Application Auto Scaling
- AWS App Mesh
- AWS Auto Scaling
- AWS Certificate Manager Private Certificate Authority
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Config
- AWS Data Exchange
- AWS DataSync
- AWS Device Farm
- AWS Elastic Beanstalk
- AWS Glue
- AWS IoT SiteWise
- AWS Key Management Service
- AWS Lambda
- AWS License Manager
- AWS Secrets Manager
- AWS Security Token Service
- AWS Server Migration Service
- AWS Service Catalog
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- EC2 Image Builder
- Elastic Load Balancing
- Endpoint services hosted by other AWS accounts
- Supported AWS Marketplace Partner services

With many more…. and more to come!

New!

Top Customers

Significant adoption in Technology and regulated verticals (FSI, Healthcare, Life Sciences, Government)

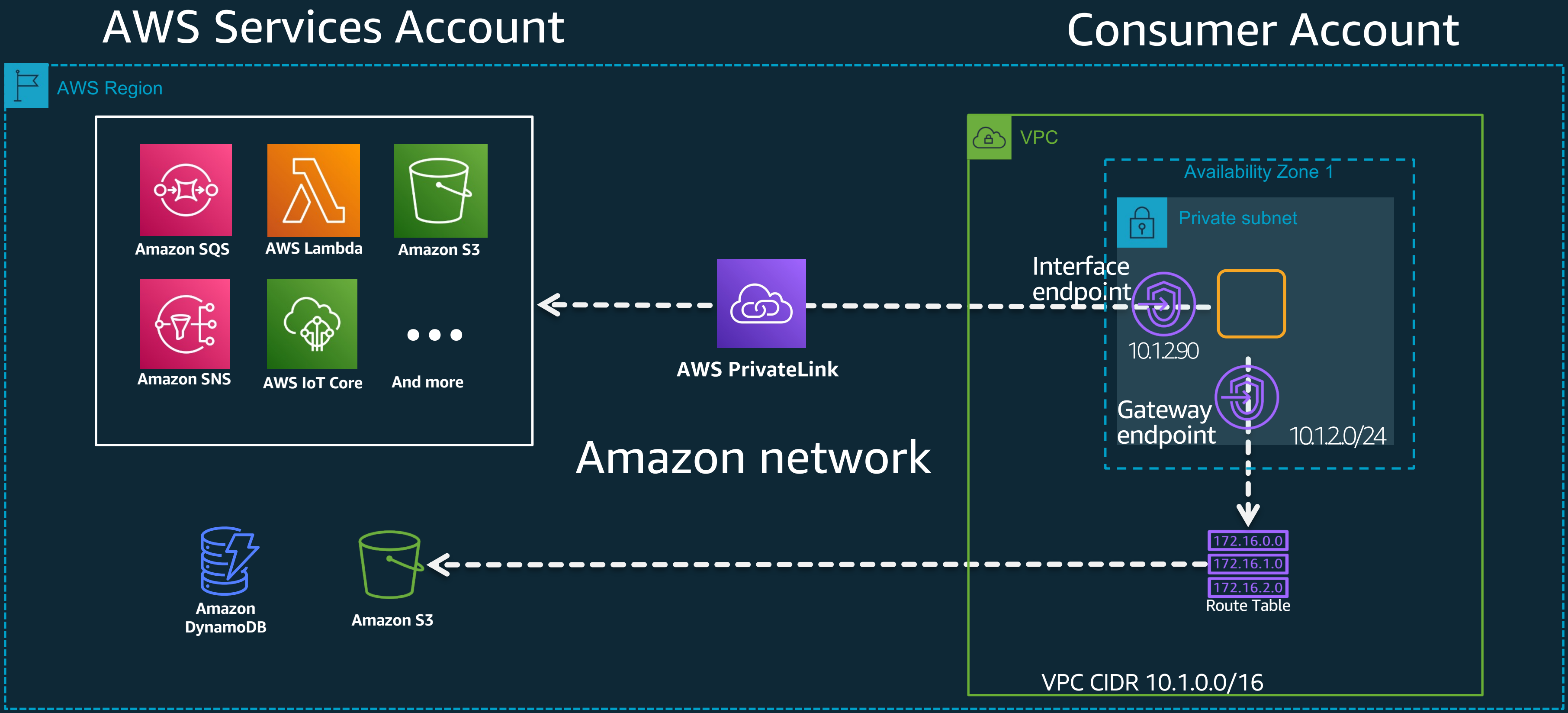
Expedia
HSBC
Goldman Sachs
JPMorgan Chase & Co.

"AWS PrivateLink provides fine-grained network access control to specific resources in a VPC instead of all resources by default, and is therefore more suited for environments that want to follow a lower trust model approach, thus reducing their risk surface." – Goldman Sachs

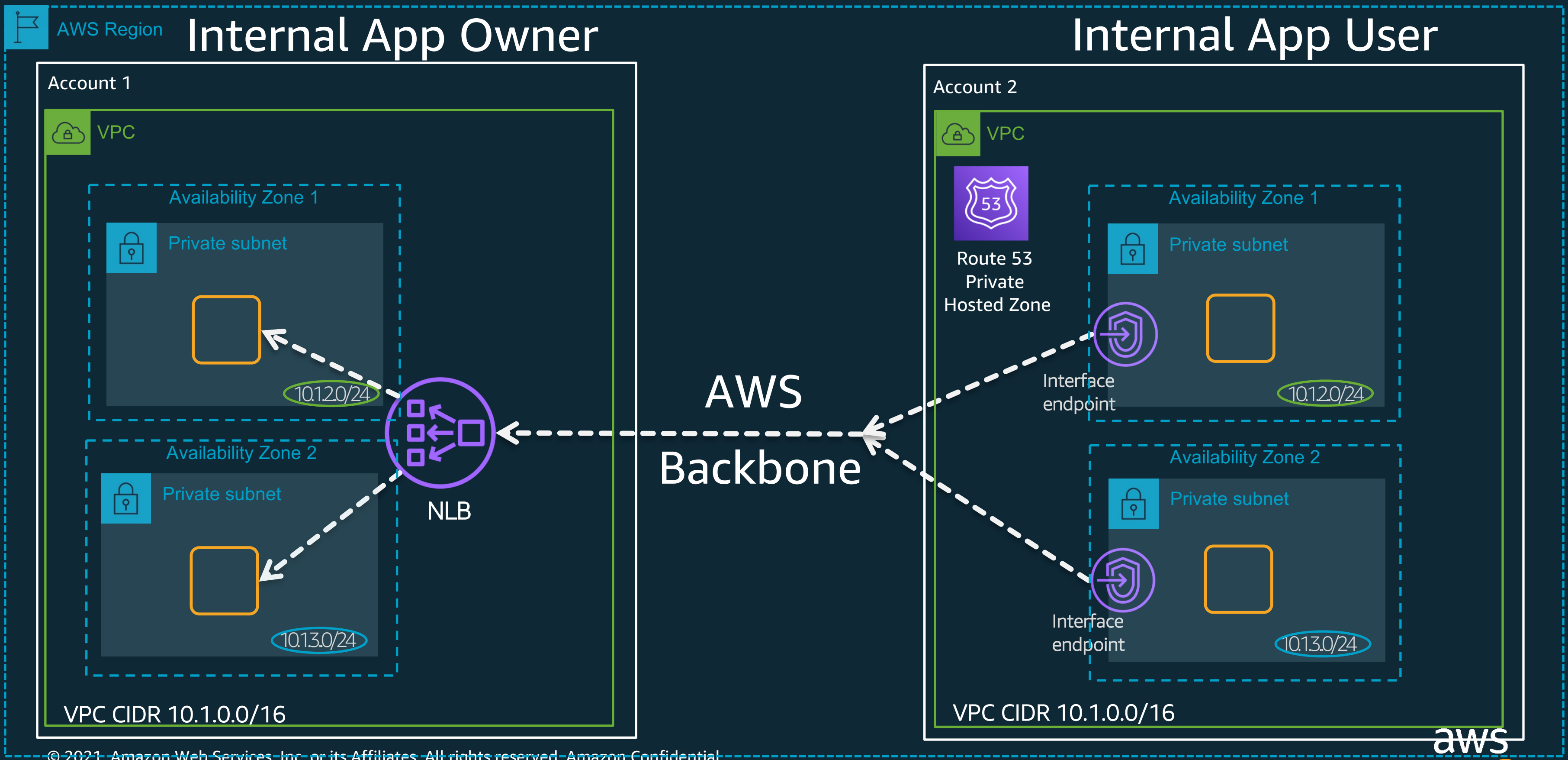
AWS PrivateLink

Common Use Cases Explained

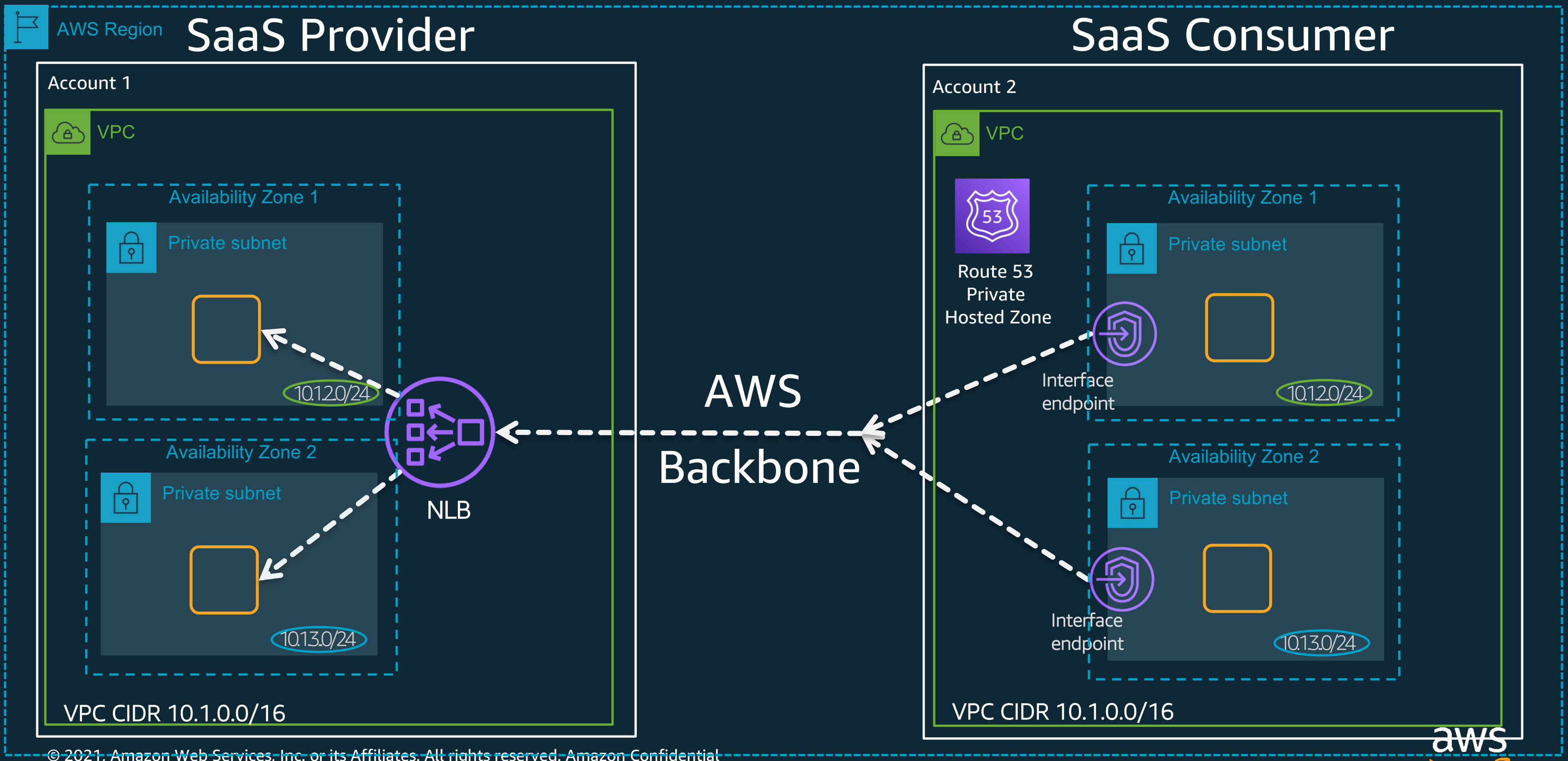
Secure Access to AWS Services



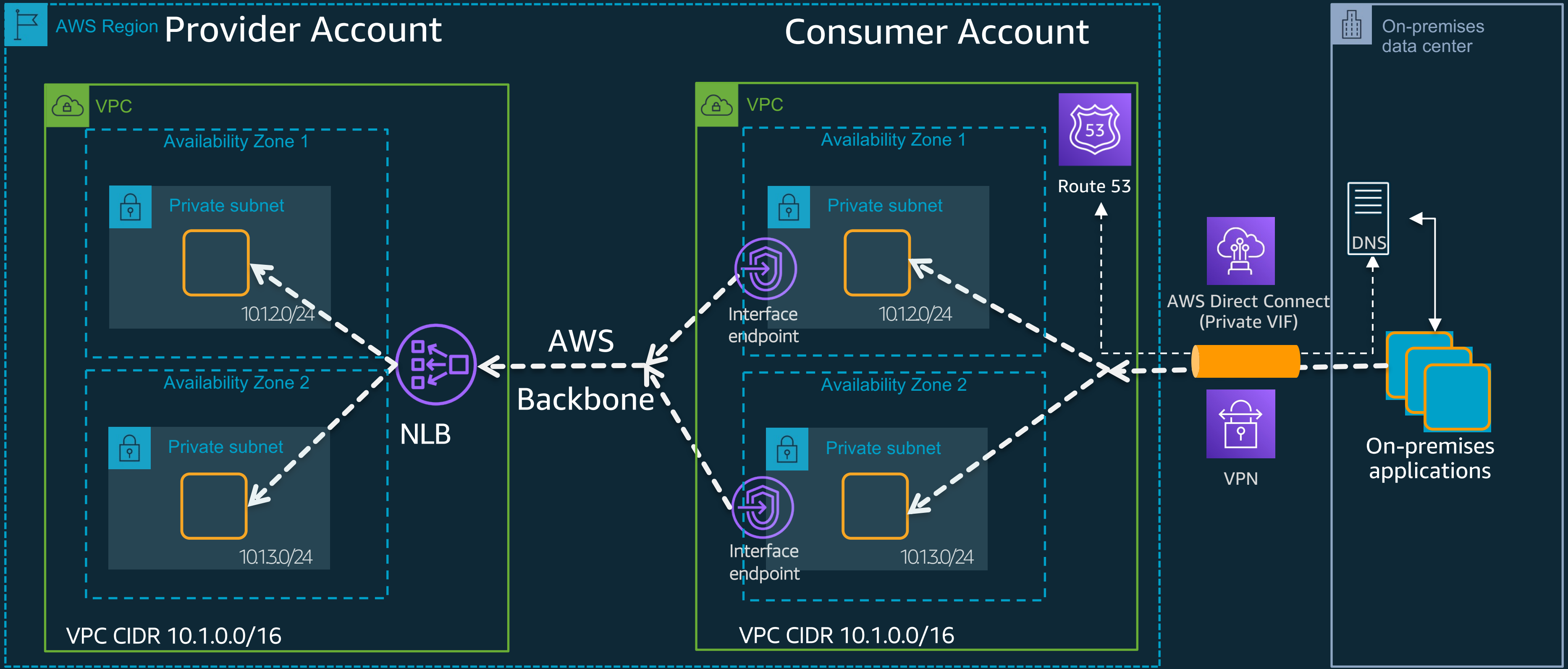
Secure Access to Internal Apps Across VPCs/Accounts



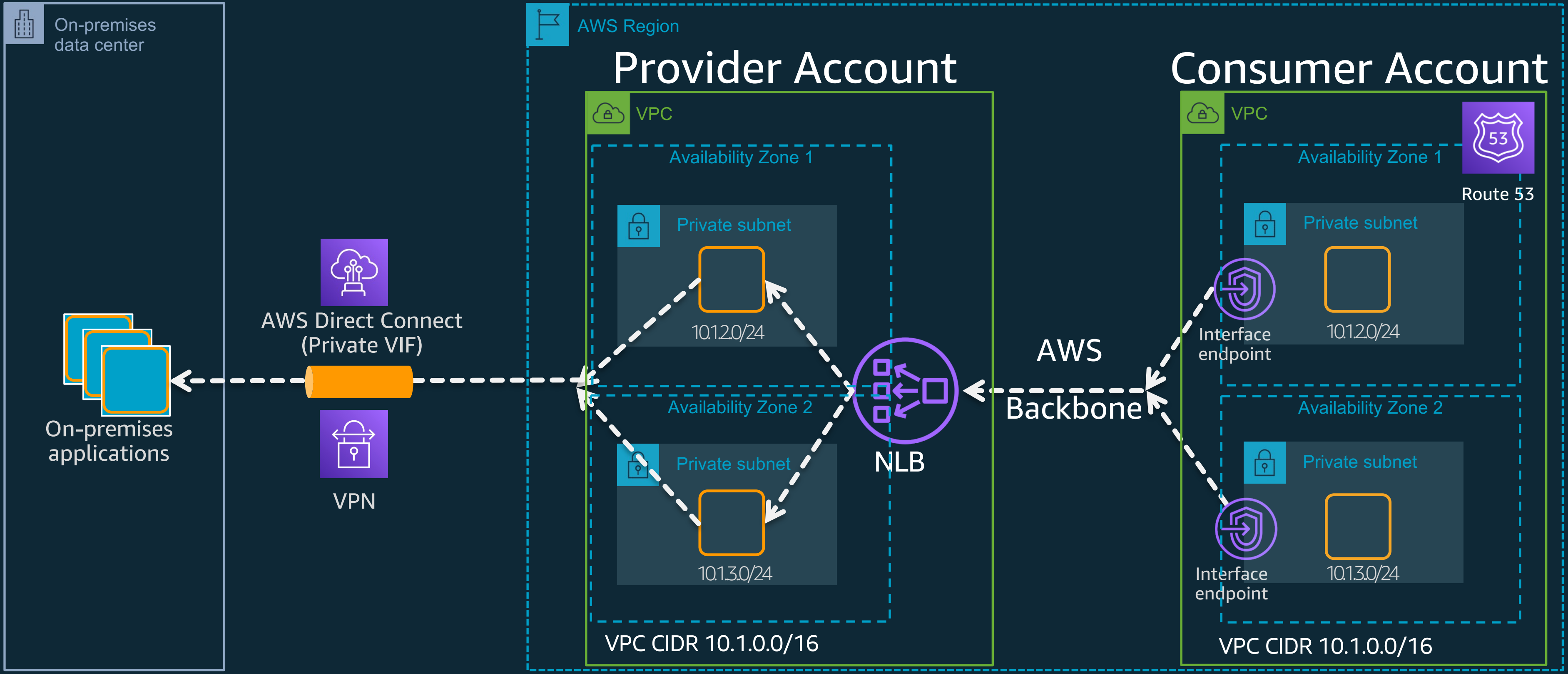
Secure Access to 3rd Party SaaS Apps



Hybrid Architecture – Access from On-premises



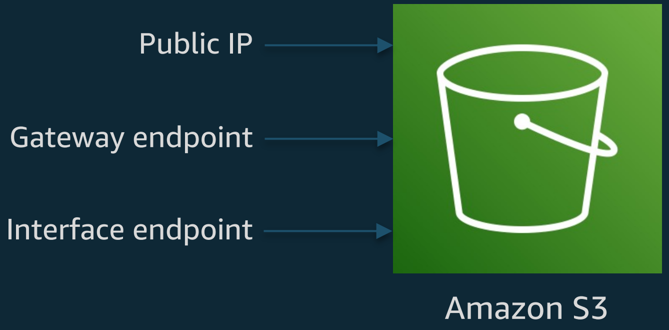
Hybrid Architecture – Access to On-premises



New: AWS PrivateLink for Amazon S3

AWS PrivateLink for Amazon S3: Interface Endpoints

Three ways to access Amazon S3 buckets



Public IP

Gateway endpoint

Interface endpoint

Amazon S3

New: Interface endpoints for Amazon S3

- Launched in Feb 2021
- Data stays on the Amazon private network
- Benefit: Eliminates need for proxies when accessing S3 from on-premises

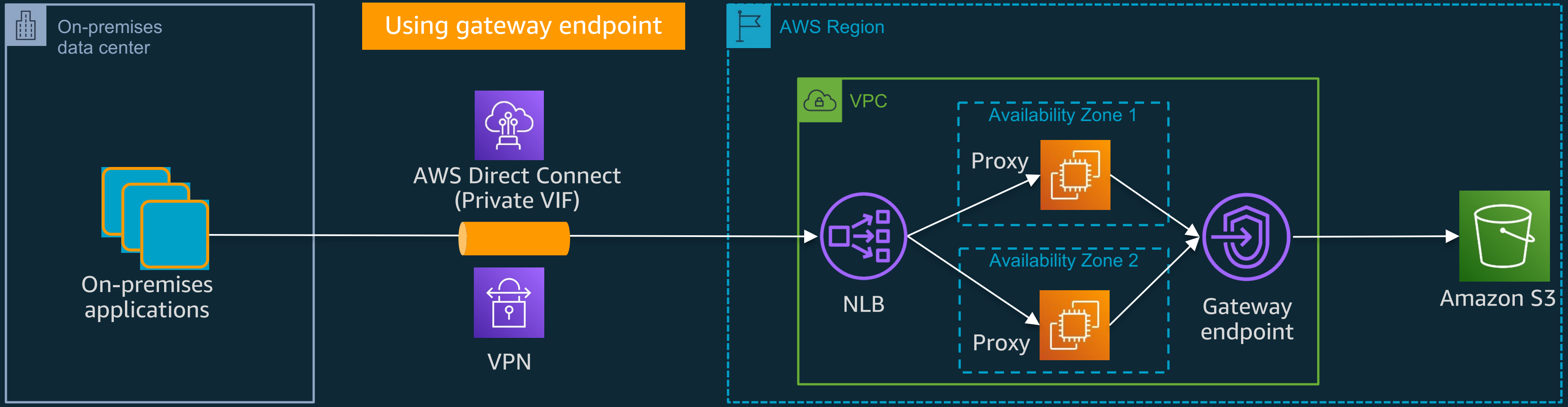
AWS PrivateLink for Amazon S3 Access

- S3 access can now be done over PrivateLink in addition to public VIF and gateway endpoints
- No changes to route table required (unlike gateway endpoints)
- S3 access via private VIF now supported in hybrid deployments

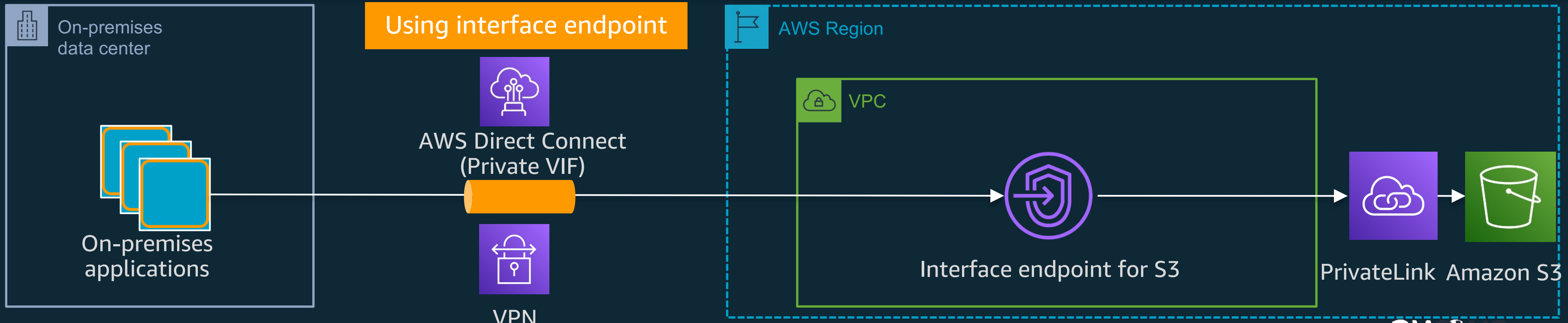
	Public VIF	**Gateway Endpoint**	**PrivateLink (Interface Endpoint)**
Data transfer	Public Internet	Amazon network	Amazon network
How it works	Uses S3 public IP address	S3 endpoint added to route table using prefix list id	ENI with a private IP address created for endpoint
Hybrid connectivity: On-premises access	Supported via public VIF	No (requires proxy servers)	Yes (with Direct Connect and using private VIF)
Inter-region access	Supported	Not supported	Yes (with VPC peering)
Access across accounts	Supported	Not supported	Supported
Shared services VPC	Supported	No: one gateway endpoint / route table	Supported (single endpoint in shared services VPC)
VPC Flow Logs	No	No	Yes
Other considerations		Not supported with AWS Direct Connect, VPN endpoints and VPC peering	Compatible with AWS Direct Connect, VPN endpoints and VPC peering
Price	Free within region	No additional charge for gateway endpoints but factor cost of proxy server, EC2 instance, maintenance costs and impact of outages due to failed proxies in a hybrid scenario	$.01 hourly cost/Interface Endpoint (us-east-1) $.01 cost/GB processed via Interface Endpoint (us-east-1)

Use Case 1: Amazon S3 Access from on-premises

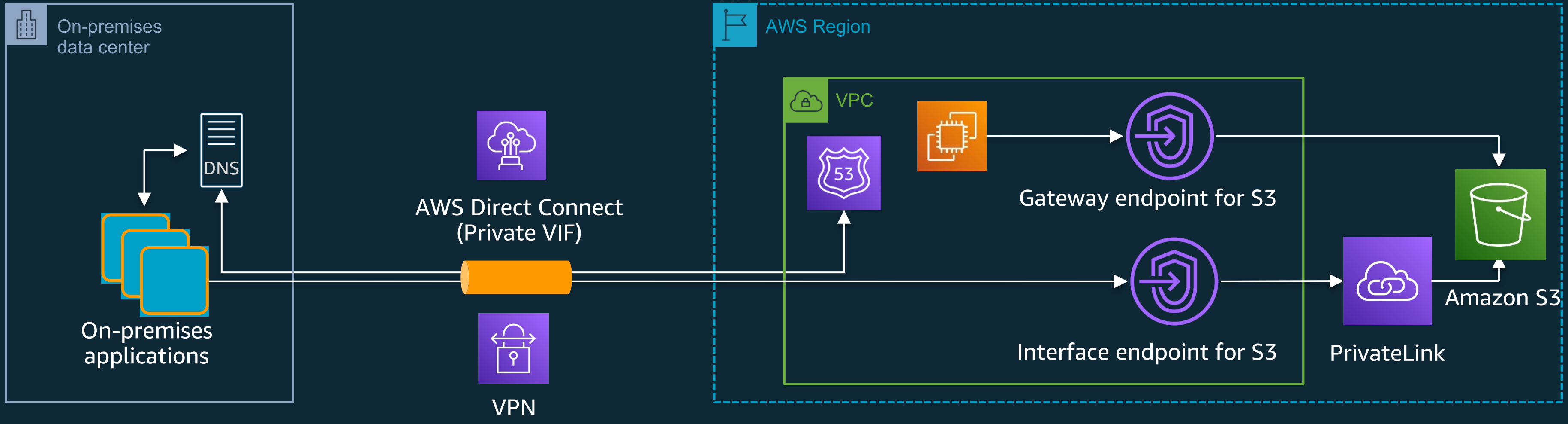
Using gateway endpoint



Using interface endpoint

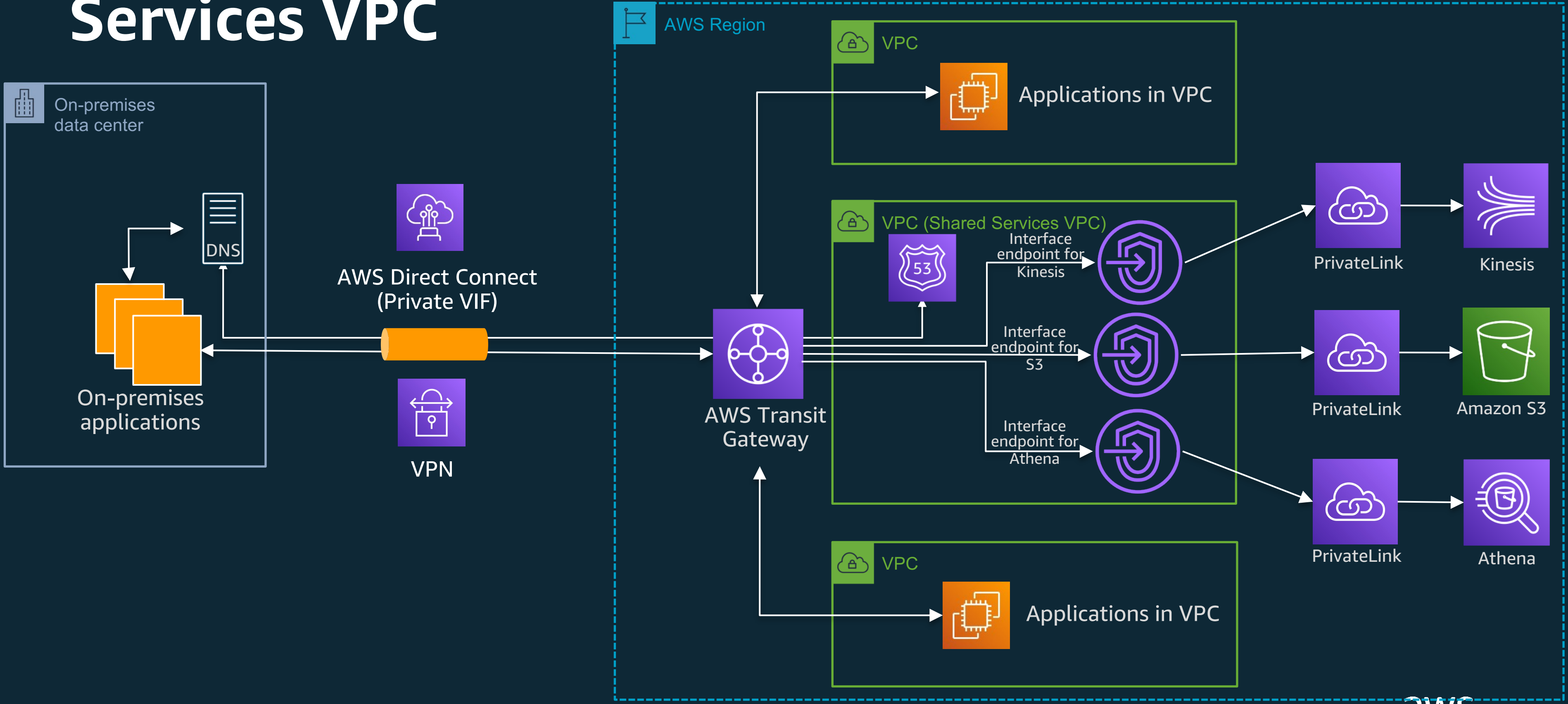


Use Case 2: S3 Access in a Hybrid Environment

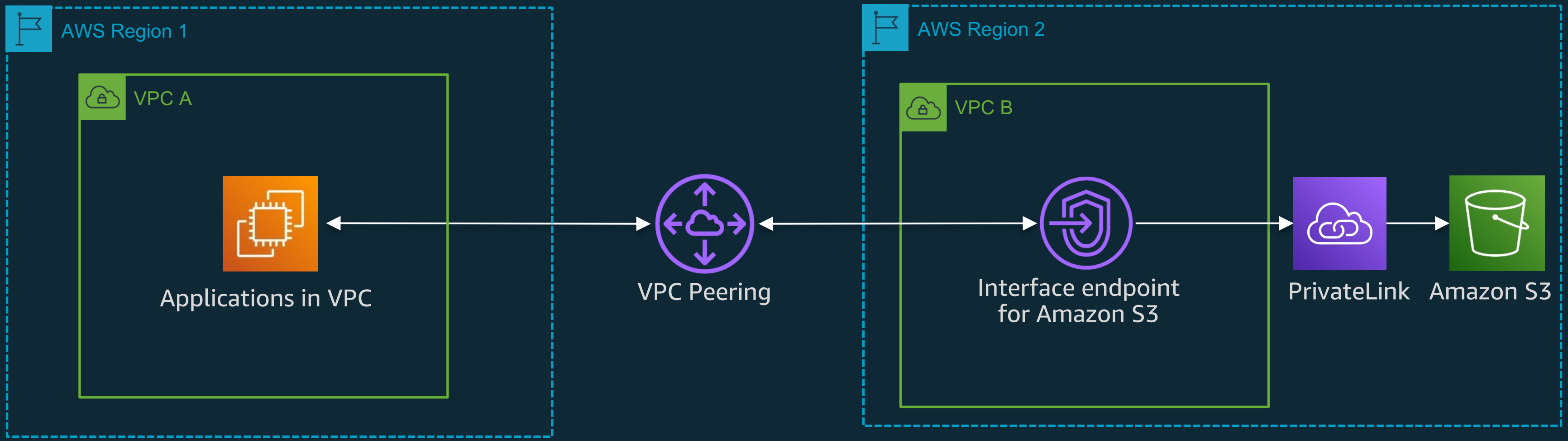


On-premises applications access S3 through the interface endpoint, apps in the VPC access S3 through the gateway endpoint

Use Case 3: Centralized Access with a Shared Services VPC



Use Case 4: S3 Access from Apps in a Different Region



Access S3 from apps in a different AWS region using interface endpoints for S3

AWS PrivateLink

Pricing

AWS PrivateLink Pricing

Consumer of a Service

1. Low Hourly Charges per Interface Endpoint in an AZ
   - $.01/hr in us-east-1

   (78% lower than NAT GW)
2. Data Processing Charges on per GB basis
   - $.01/GB in all regions

Service Provider

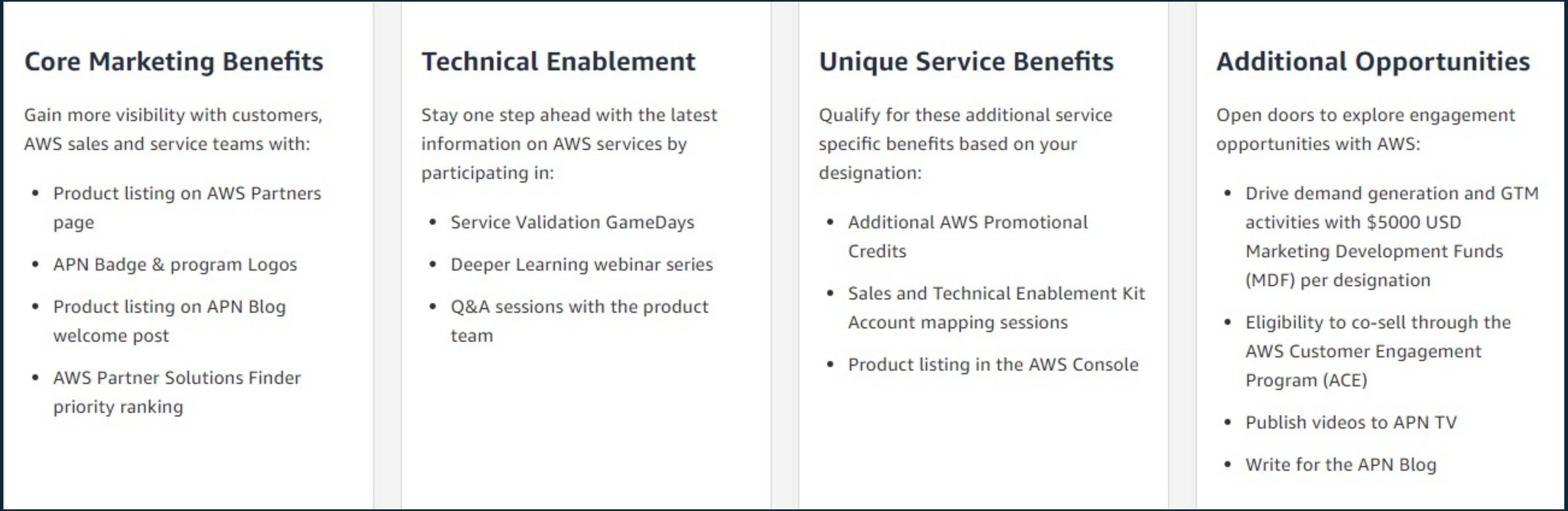
(For internal services and 3rd party providers)

1. Standard Charges for Network Load Balancer (NLB)
2. No additional charges for creating a PrivateLink based service

There are NO Data Transfer Charges between a consumer endpoint and a Service Provider NLB

Partners

AWS PrivateLink Ready Program



Core Marketing Benefits

Gain more visibility with customers, AWS sales and service teams with:

- Product listing on AWS Partners page
- APN Badge & program Logos
- Product listing on APN Blog welcome post
- AWS Partner Solutions Finder priority ranking

Technical Enablement

Stay one step ahead with the latest information on AWS services by participating in:

- Service Validation GameDays
- Deeper Learning webinar series
- Q&A sessions with the product team

Unique Service Benefits

Qualify for these additional service specific benefits based on your designation:

- Additional AWS Promotional Credits
- Sales and Technical Enablement Kit Account mapping sessions
- Product listing in the AWS Console

Additional Opportunities

Open doors to explore engagement opportunities with AWS:

- Drive demand generation and GTM activities with $5000 USD Marketing Development Funds (MDF) per designation
- Eligibility to co-sell through the AWS Customer Engagement Program (ACE)
- Publish videos to APN TV
- Write for the APN Blog

https://aws.amazon.com/partners/service-ready/

AWS PrivateLink Ready Partners

- ALGOMI
- Bloomberg
- DATADOG
- epsagon
- NuData Security mastercard
- snowflake
- APPDYNAMICS part of Cisco
- CDL
- druva
- mongoDB. Atlas
- Qubole
- teradata.
- axway
- CONFLUENT
- dynatrace
- NetApp
- salesforce heroku
- TREND MICRO

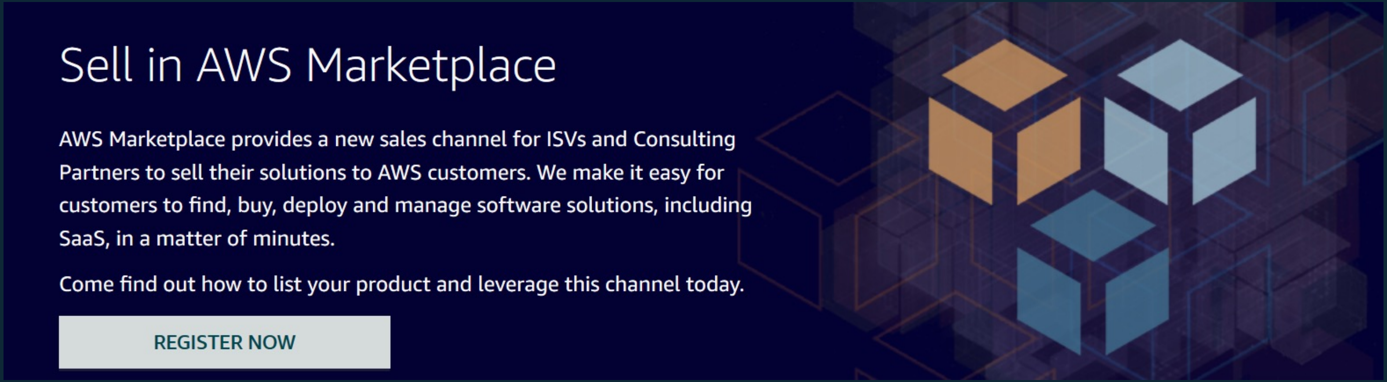
"[AWS] PrivateLink really is in effect the missing link in being able to deliver between on-prem, to the cloud, to SaaS services, all without going over the Internet."

- Matthew Glickman, Vice President Product Management, Snowflake

Link to PrivateLink partners: https://aws.amazon.com/privatelink/partners/

AWS Marketplace Integration

Services discoverable when customers purchase SaaS on AWS Marketplace



Sell in AWS Marketplace

AWS Marketplace provides a new sales channel for ISVs and Consulting Partners to sell their solutions to AWS customers. We make it easy for customers to find, buy, deploy and manage software solutions, including SaaS, in a matter of minutes.

Come find out how to list your product and leverage this channel today.

Easily create secure endpoints

AWS Market Place confirms each sellers endpoint DNS name, making it easier to find and set up the endpoints your customers need.

No public IP addresses

Connect services directly from VPC without requiring any internet gateways, and not traversing the internet.

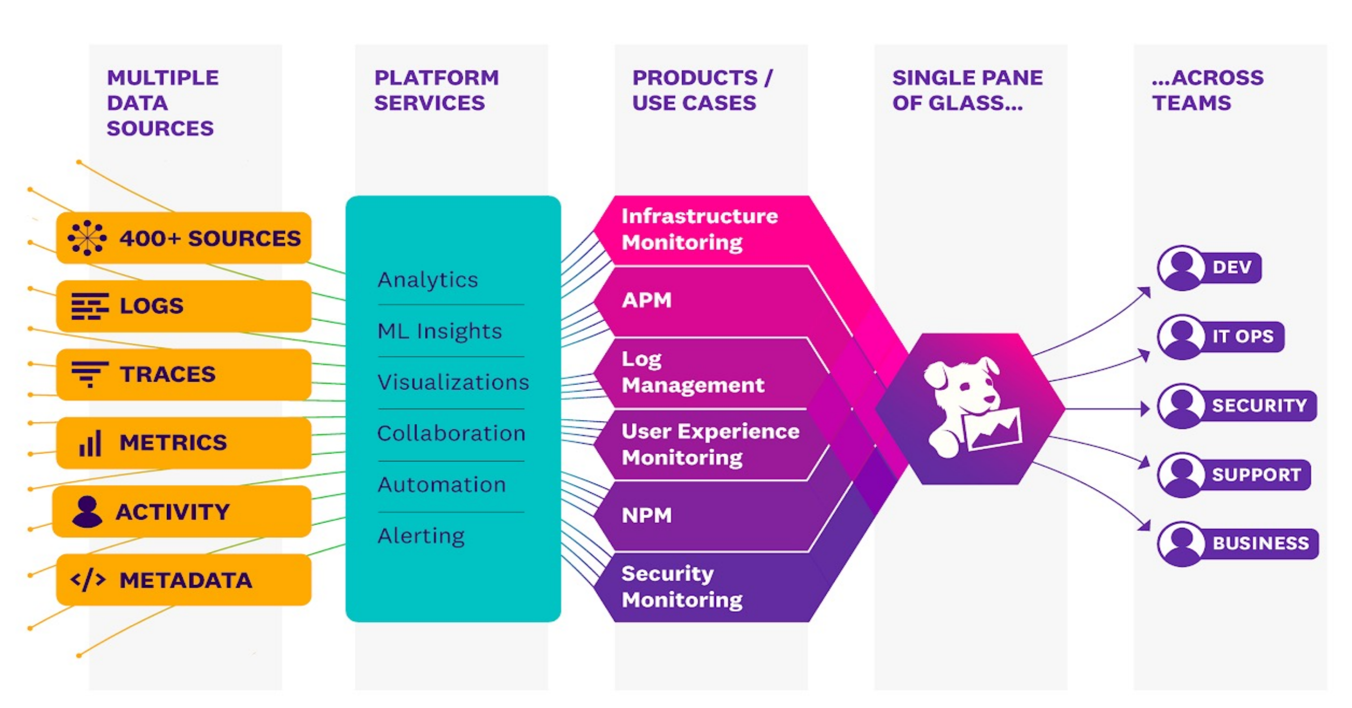
Curated SaaS Products

Products architected to run on AWS by popular software vendors are found easily on the marketplace

Case Study

Datadog

Unified observability SaaS platform



Datadog and AWS PrivateLink

Key Use Cases

Managing Hybrid Cloud

- Combined Public and Private observability environments

Optimizing Cloud Spend

- Reduced Data Egress Costs

Securing Data In-transit

- Compliance with government regulations
- Handling sensitive data

Proof Points

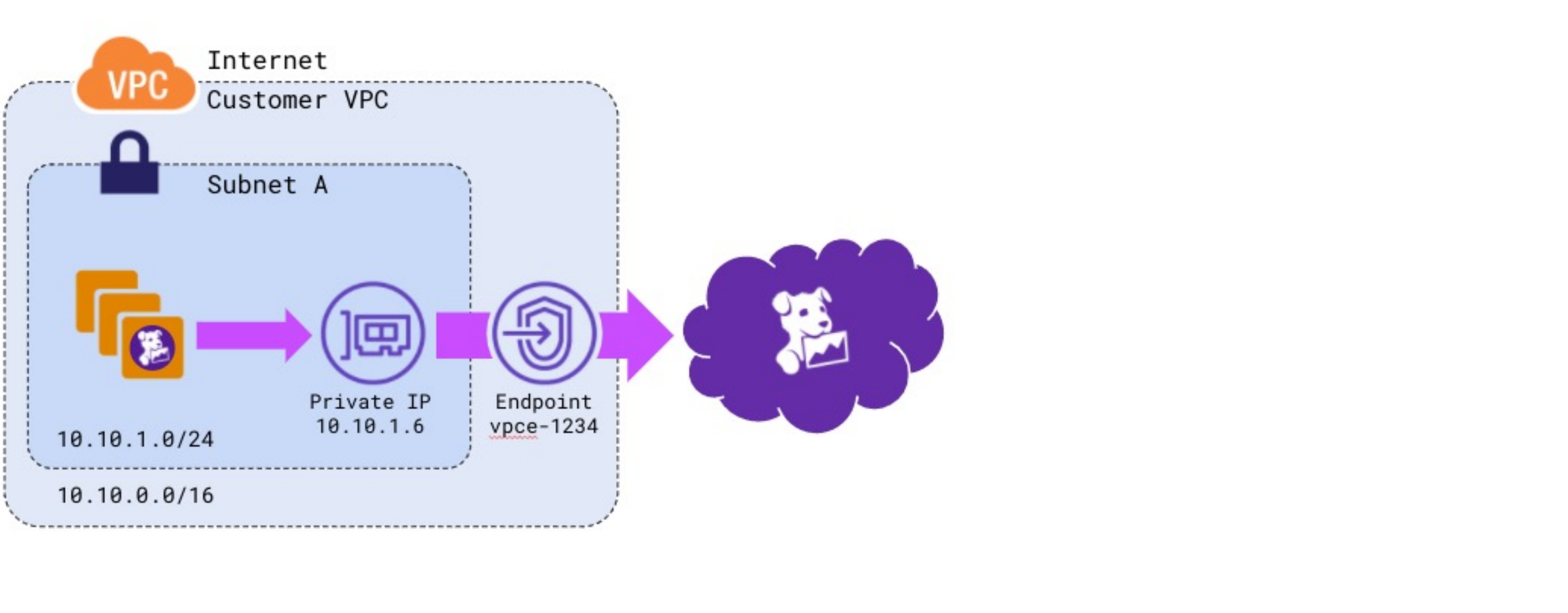
Large Financial Institution

- 3 Pillar solution – Metrics, Traces, & Logs
- *"Support for AWS PrivateLink was instrumental in securing the deal"* (security, hybrid cloud)

Large consumer apparel company & large consumer streaming service

- Log management solution – several TB/day
- *"Support for PrivateLink was key requirement "* (cost optimization)

Example Partner Use Case: Datadog



Next Steps

AWS PrivateLink Web Page (Learn more & access the AWS console)

Blog: “How Goldman Sachs builds cross-account connectivity to their Amazon MSK clusters with AWS PrivateLink”

Free Course: Configure and Deploy AWS PrivateLink

Thank you!

Contact: