AWS re:Invent

TLC304

Zero to Cloud: BT's CCoE challenges, solutions, and patterns

Guy Ben-Baruch
Senior Solution Architect
Amazon Web Services

Simon Howe
Senior Manager, Public Cloud Engineering Technology
British Telecommunications

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What to expect from this session



300 level session, you should have a good understanding of AWS services



The session will describe architectural patterns and a variety of AWS products in a broad range of challenges



A great start to the morning!

Agenda

1. Introduction to BT
2. Why AWS and public cloud for BT
3. Establishing a platform team in a cloud center of excellence (CCoE)
4. Adopting a Landing Zone
5. Connectivity design patterns and unique hybrid scenarios
6. Some key takeaways from the journey so far

1846
The Electric Telegraph Company

620
retail stores



180
countries

1.2
million businesses

30
million customers

106,000
employees



To use the power of communications to make a better world

Consumer	Enterprise	Global	Openreach

Technology

We are the internal technology unit responsible for creating and operating BT's networks, platforms and IT Systems

Cloud is supporting BT's strategy

To use the power of communications to make a better world



Differentiated customer experiences

Simplified lean and agile business

The “ask” of public cloud



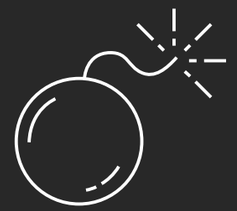
Self-service platform



Many teams



Scale to many applications



Blast radius isolation



Must be secure and safe



Hybrid integration



Clear billing



Flexible change/business processes

Public cloud centre of excellence



Dedicated team

Invest in your own people

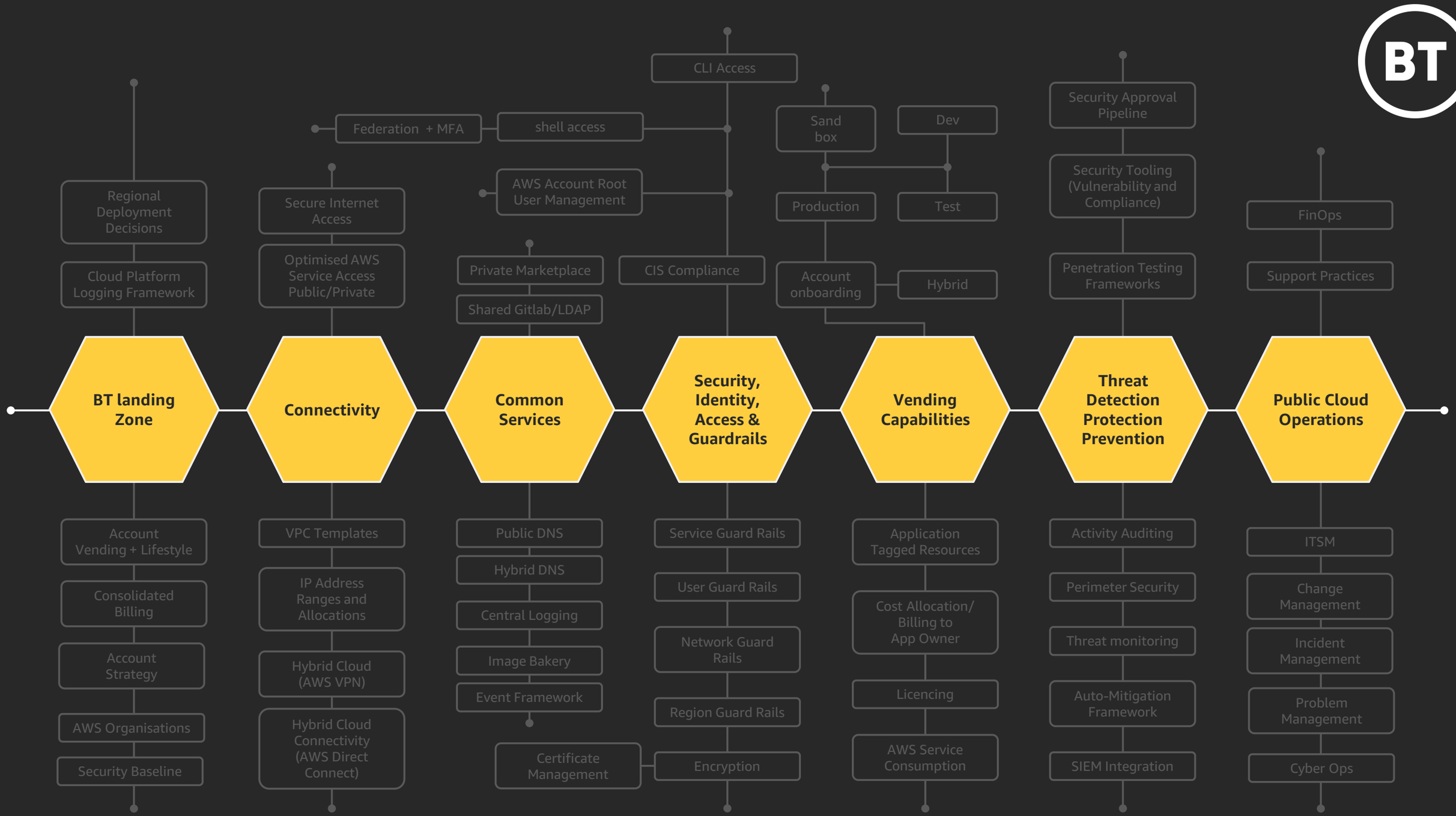
Support training and certification

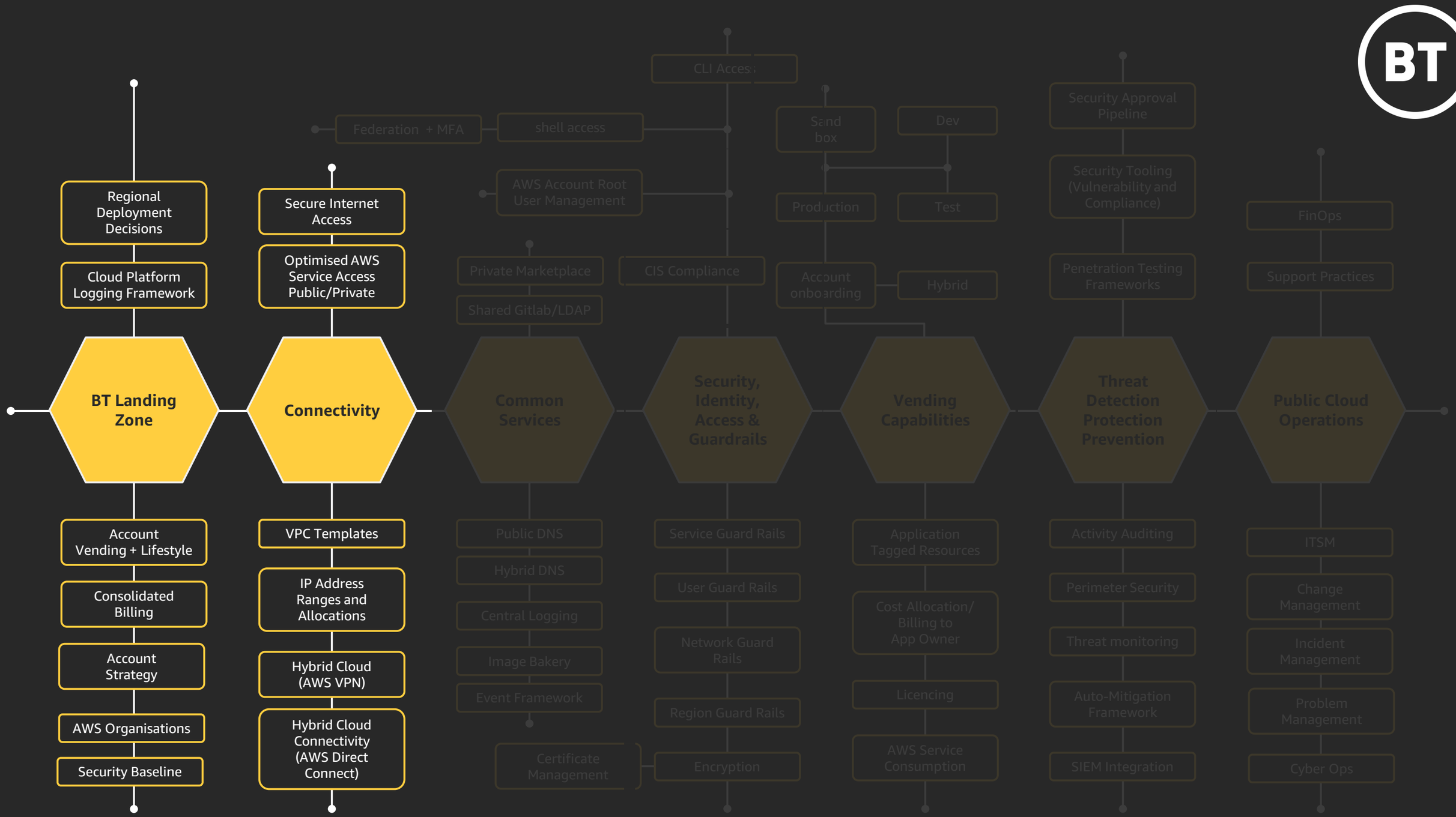
Continuous development and learning

To create a place where the business is enabled to be innovative, agile, and relevant through secure adoption of AWS public cloud services

Building a ~~roadmap~~ tube map

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

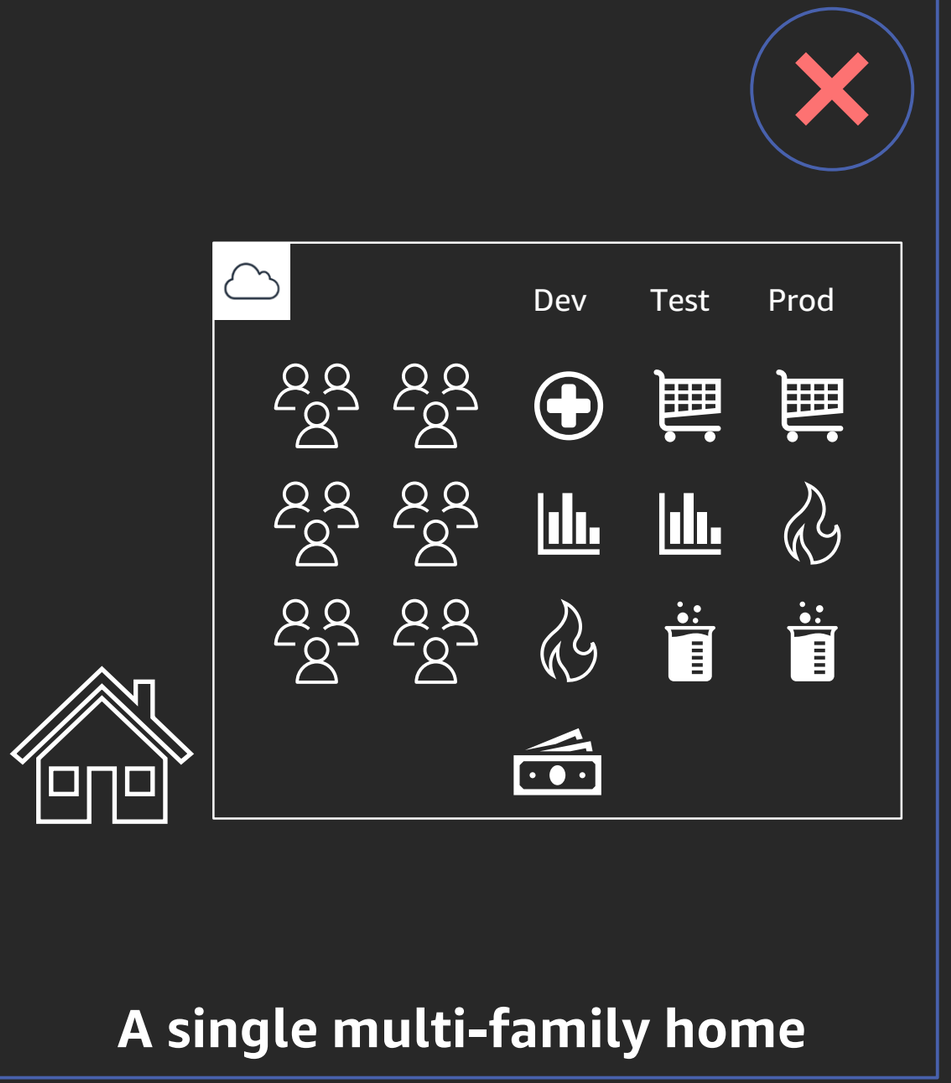

BT
BT landing Zone
Regional Deployment Decisions
Cloud Platform Logging Framework
Account Vending + Lifestyle
Consolidated Billing
Account Strategy
AWS Organisations
Security Baseline
Connectivity
Secure Internet Access
Optimised AWS Service Access Public/Private
VPC Templates
IP Address Ranges and Allocations
Hybrid Cloud (AWS VPN)
Hybrid Cloud Connectivity (AWS Direct Connect)
Common Services
Private Marketplace
Shared Gitlab/LDAP
Public DNS
Hybrid DNS
Central Logging
Image Bakery
Event Framework
Certificate Management
Security, Identity, Access & Guardrails
CLI Access
Federation + MFA
shell access
AWS Account Root User Management
CIS Compliance
Service Guard Rails
User Guard Rails
Network Guard Rails
Region Guard Rails
Encryption
Vending Capabilities
Sand box
Dev
Production
Test
Account onboarding
Hybrid
Application Tagged Resources
Cost Allocation/ Billing to App Owner
Licencing
AWS Service Consumption
Threat Detection Protection Prevention
Security Approval Pipeline
Security Tooling (Vulnerability and Compliance)
Penetration Testing Frameworks
Activity Auditing
Perimeter Security
Threat monitoring
Auto-Mitigation Framework
SIEM Integration
Public Cloud Operations
FinOps
Support Practices
ITSM
Change Management
Incident Management
Problem Management
Cyber Ops


BT Landing Zone
Regional Deployment Decisions
Cloud Platform Logging Framework
Account Vending + Lifestyle
Consolidated Billing
Account Strategy
AWS Organisations
Security Baseline
Connectivity
Secure Internet Access
Optimised AWS Service Access Public/Private
VPC Templates
IP Address Ranges and Allocations
Hybrid Cloud (AWS VPN)
Hybrid Cloud Connectivity (AWS Direct Connect)
Common Services
Private Marketplace
Shared Gitlab/LDAP
Public DNS
Hybrid DNS
Central Logging
Image Bakery
Event Framework
Certificate Management
Security, Identity, Access & Guardrails
CLI Access
Federation + MFA
shell access
AWS Account Root User Management
CIS Compliance
Service Guard Rails
User Guard Rails
Network Guard Rails
Region Guard Rails
Encryption
Vending Capabilities
Sand box
Dev
Production
Test
Account onboarding
Hybrid
Application Tagged Resources
Cost Allocation/ Billing to App Owner
Licencing
AWS Service Consumption
Threat Detection Protection Prevention
Security Approval Pipeline
Security Tooling (Vulnerability and Compliance)
Penetration Testing Frameworks
Activity Auditing
Perimeter Security
Threat monitoring
Auto-Mitigation Framework
SIEM Integration
Public Cloud Operations
FinOps
Support Practices
ITSM
Change Management
Incident Management
Problem Management
Cyber Ops

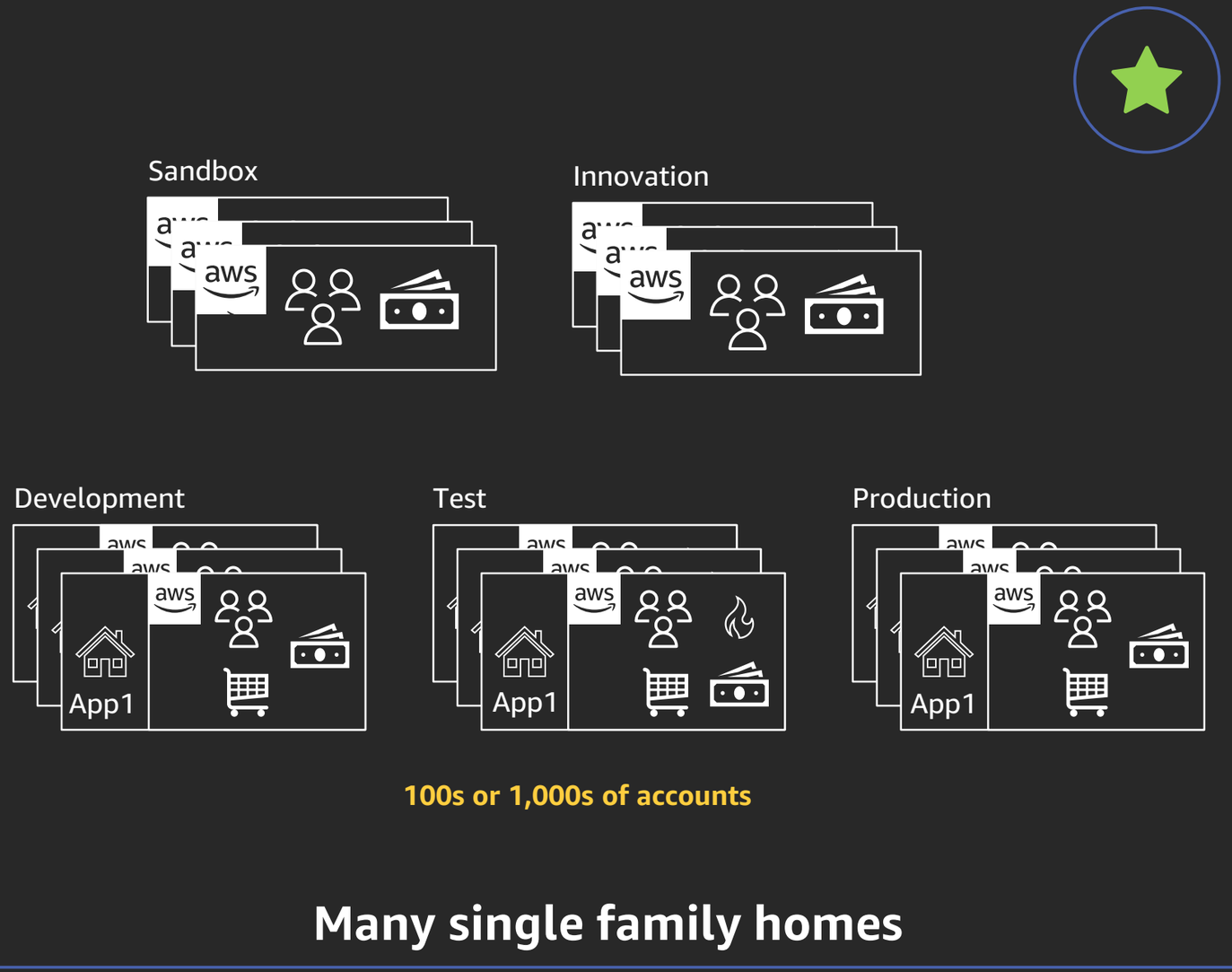
Challenge #1: Landing in the cloud

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Account strategies

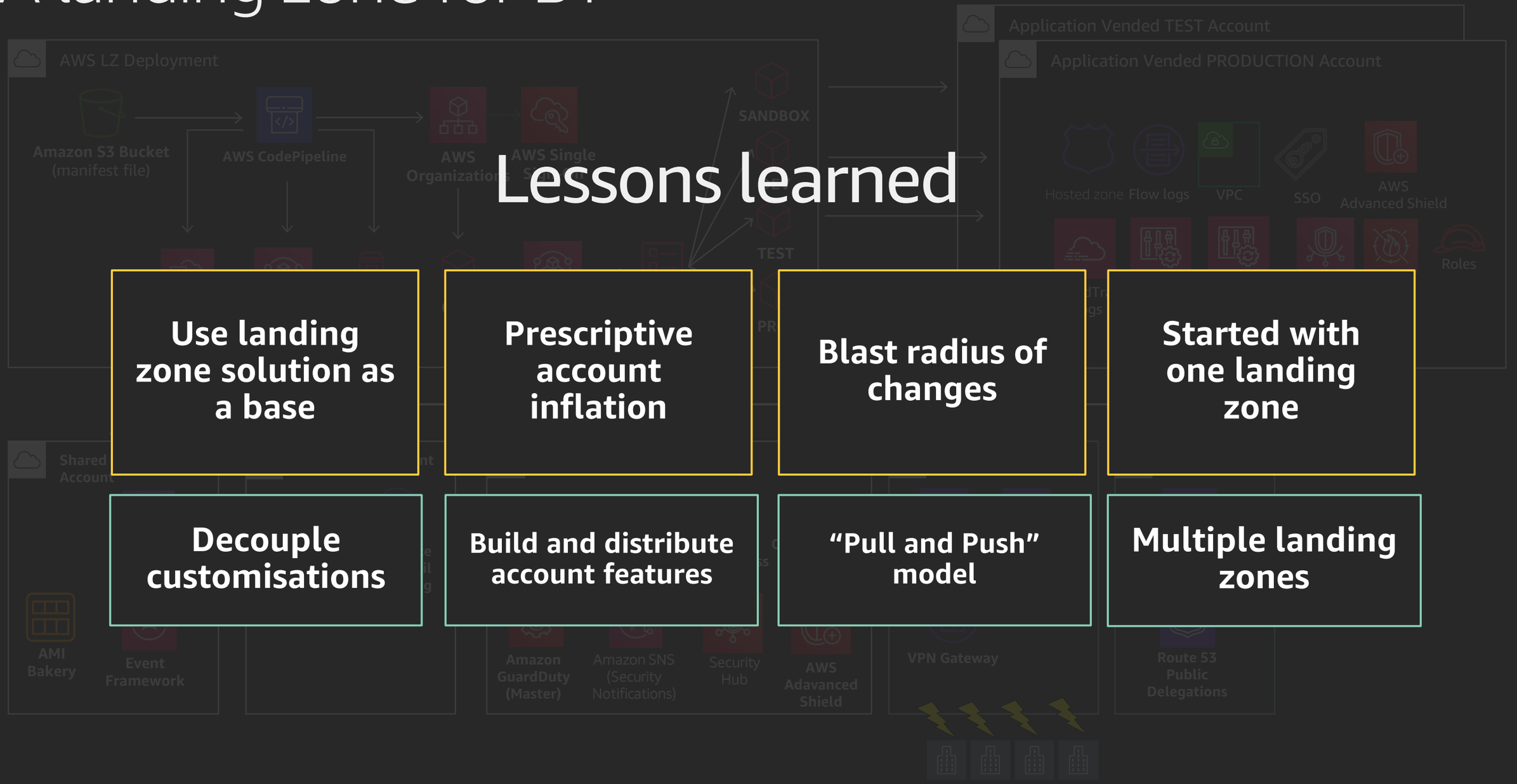


A single multi-family home



Many single family homes

A landing zone for BT



Lessons learned

Use landing zone solution as a base

Prescriptive account inflation

Blast radius of changes

Started with one landing zone

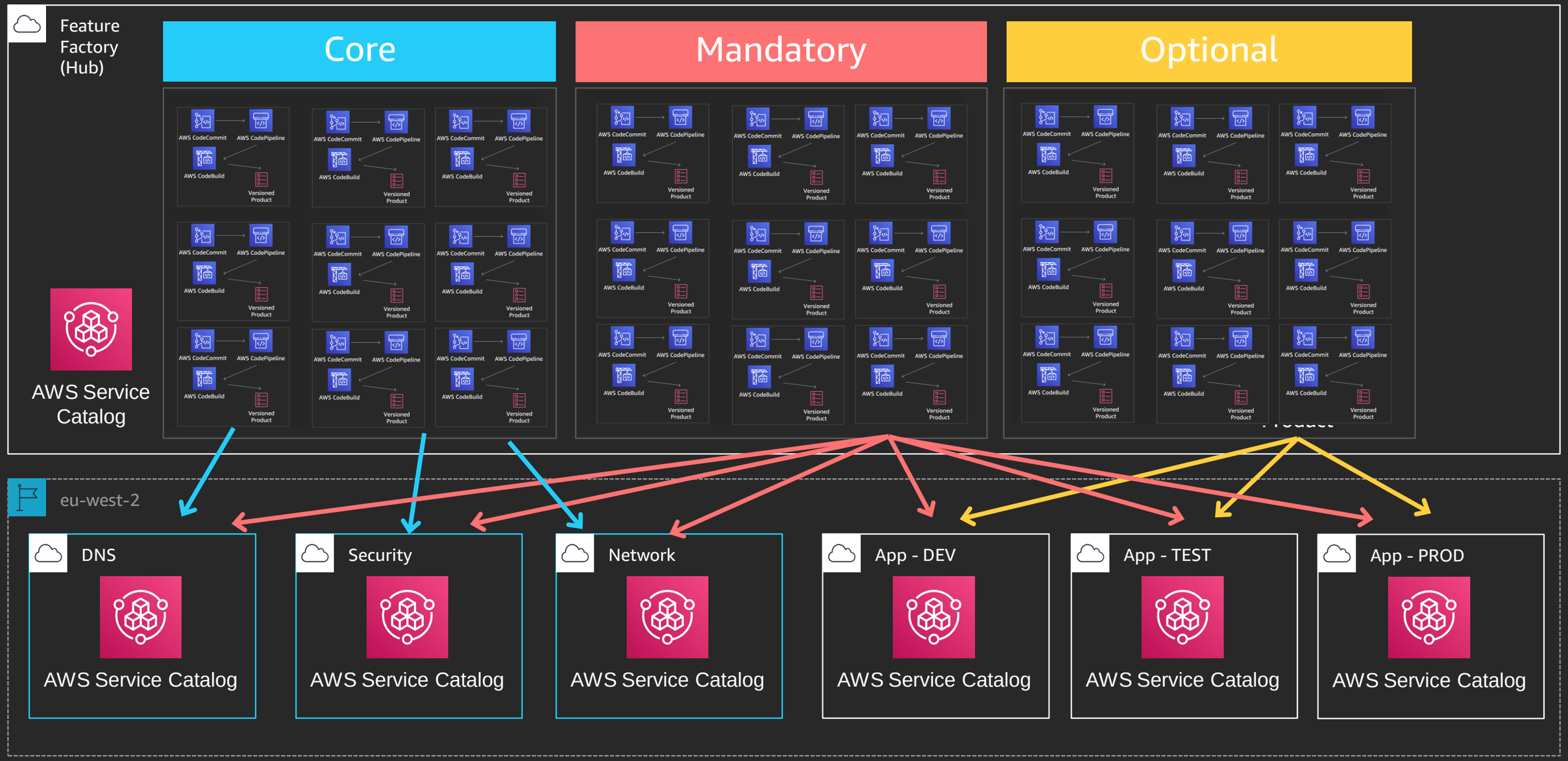
Decouple customisations

Build and distribute account features

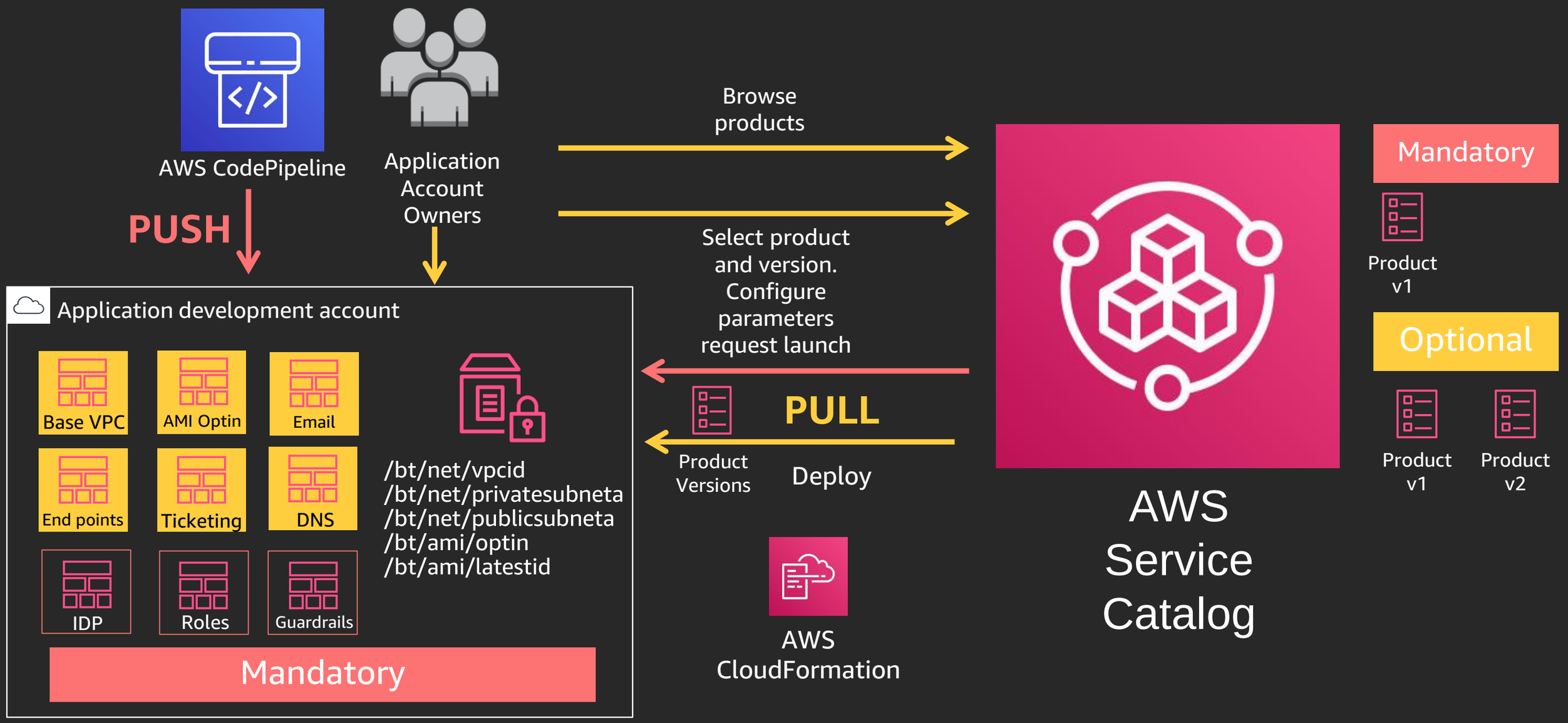
“Pull and Push” model

Multiple landing zones

Build and distribute products as “Account Features"



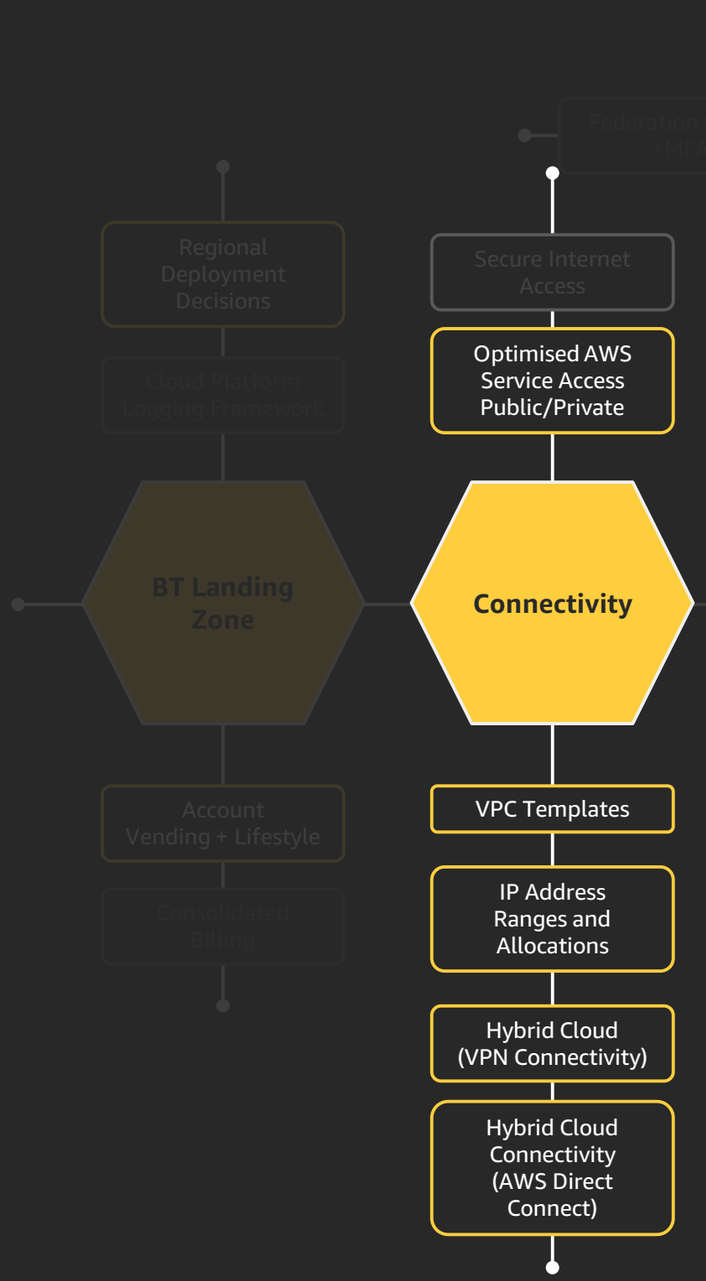
Consuming “Account Features” — a push + pull model



Challenge #2: Hybrid connectivity

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hybrid connectivity challenges



Complex environment

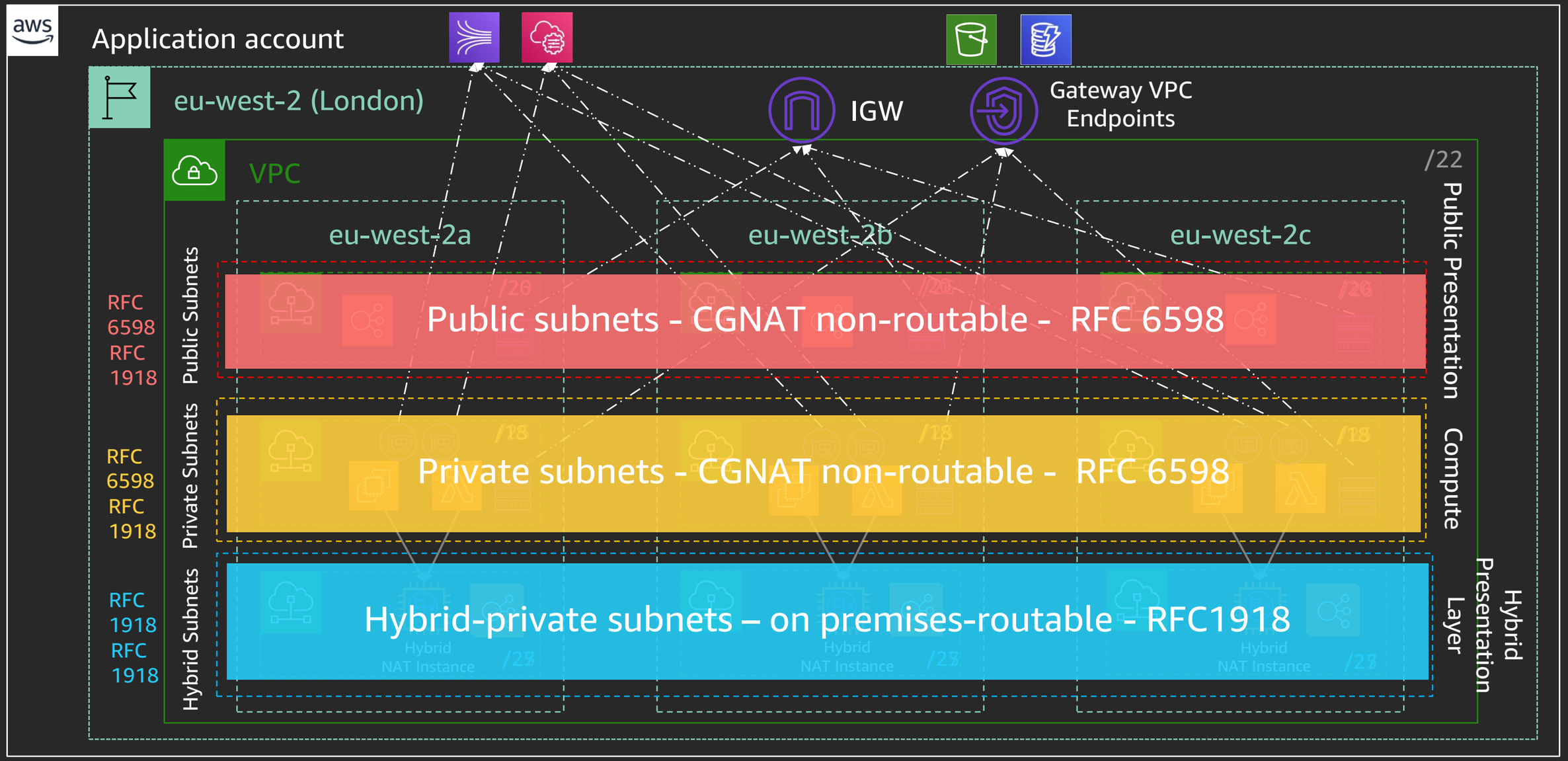
Private RFC1918 IP space at a premium

Multi-account strategy

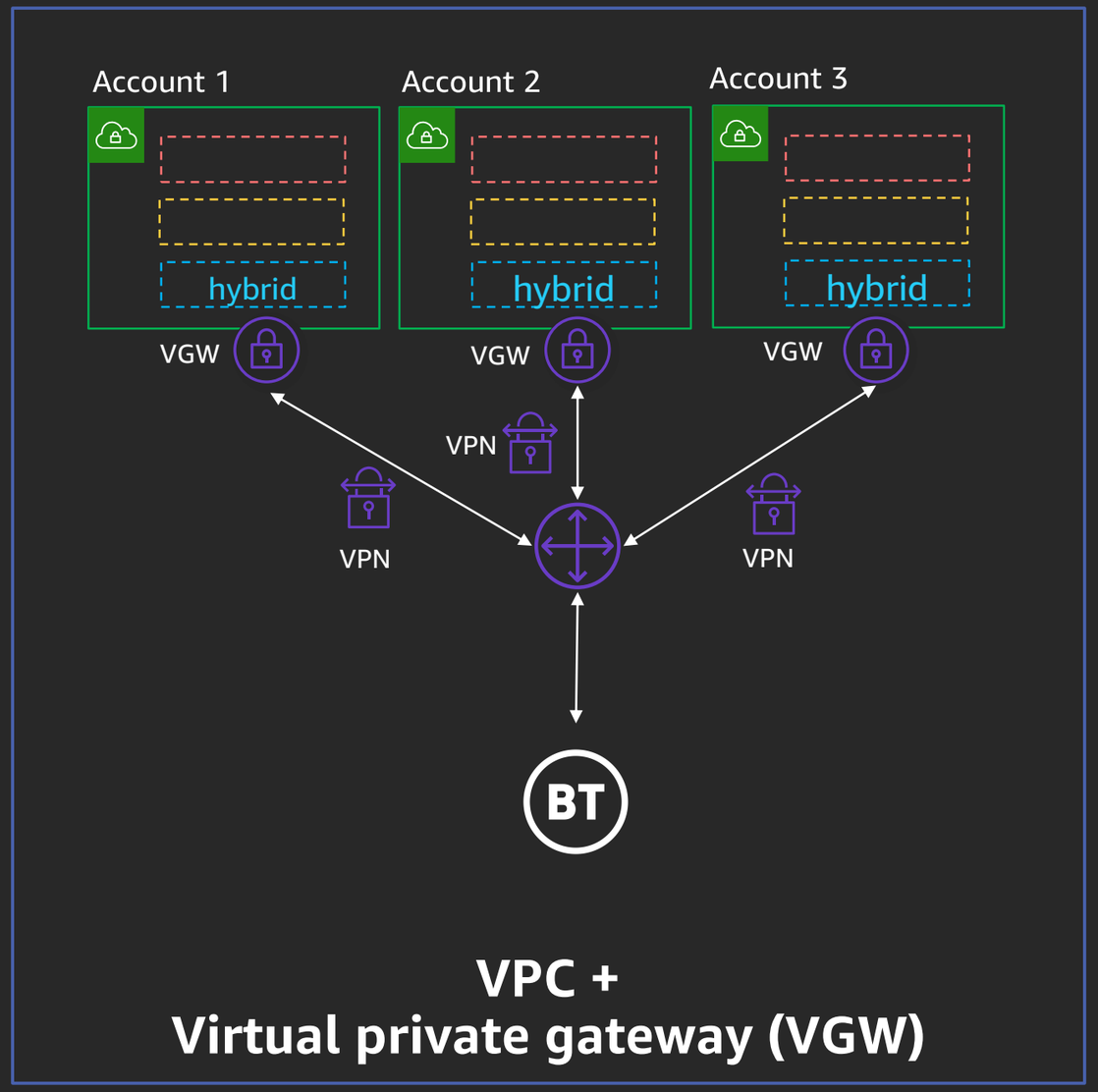
Application elasticity and autonomy

Many reference architectures

VPC for hybrid connected applications

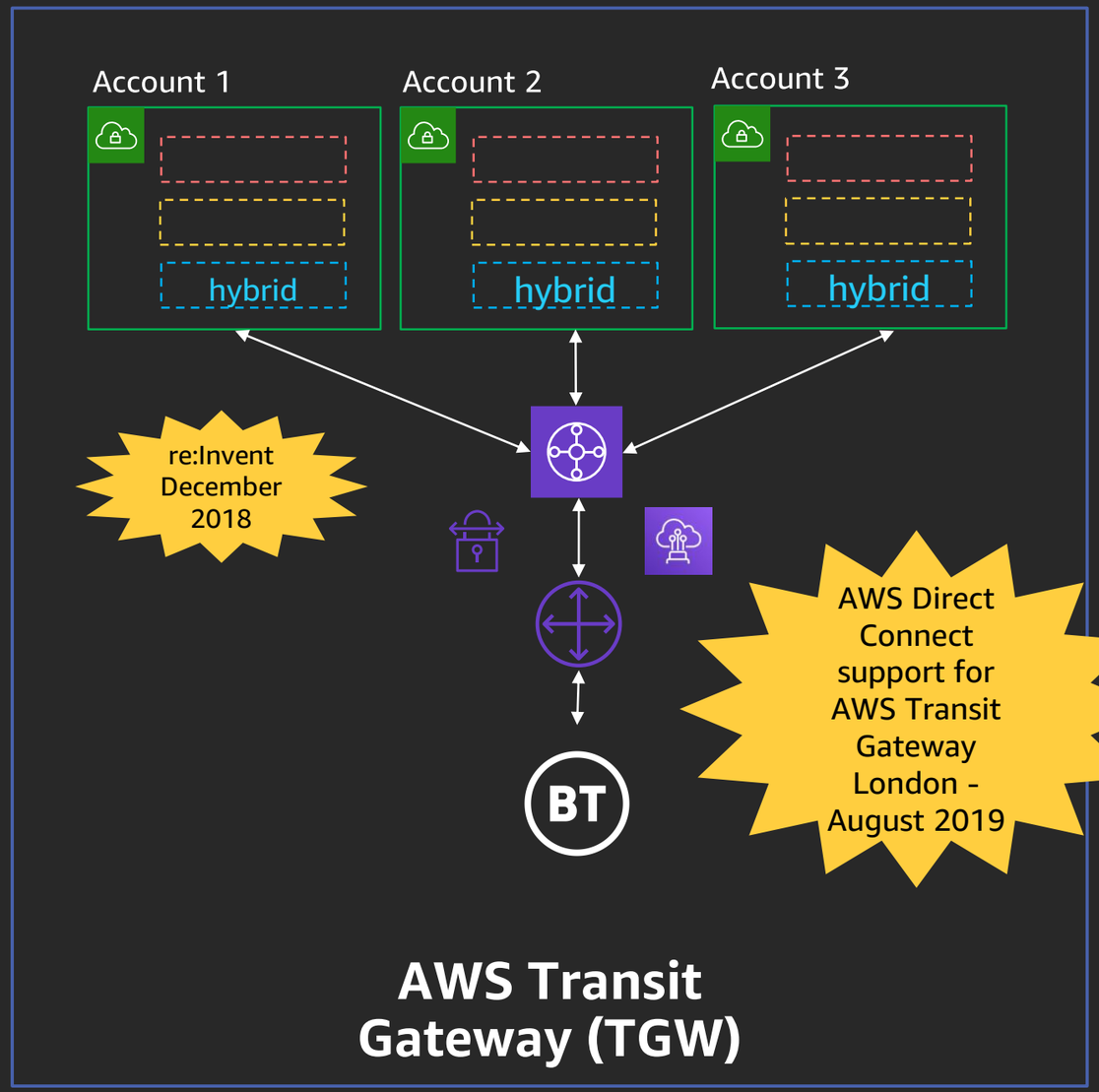


The hybrid journey: connectivity patterns



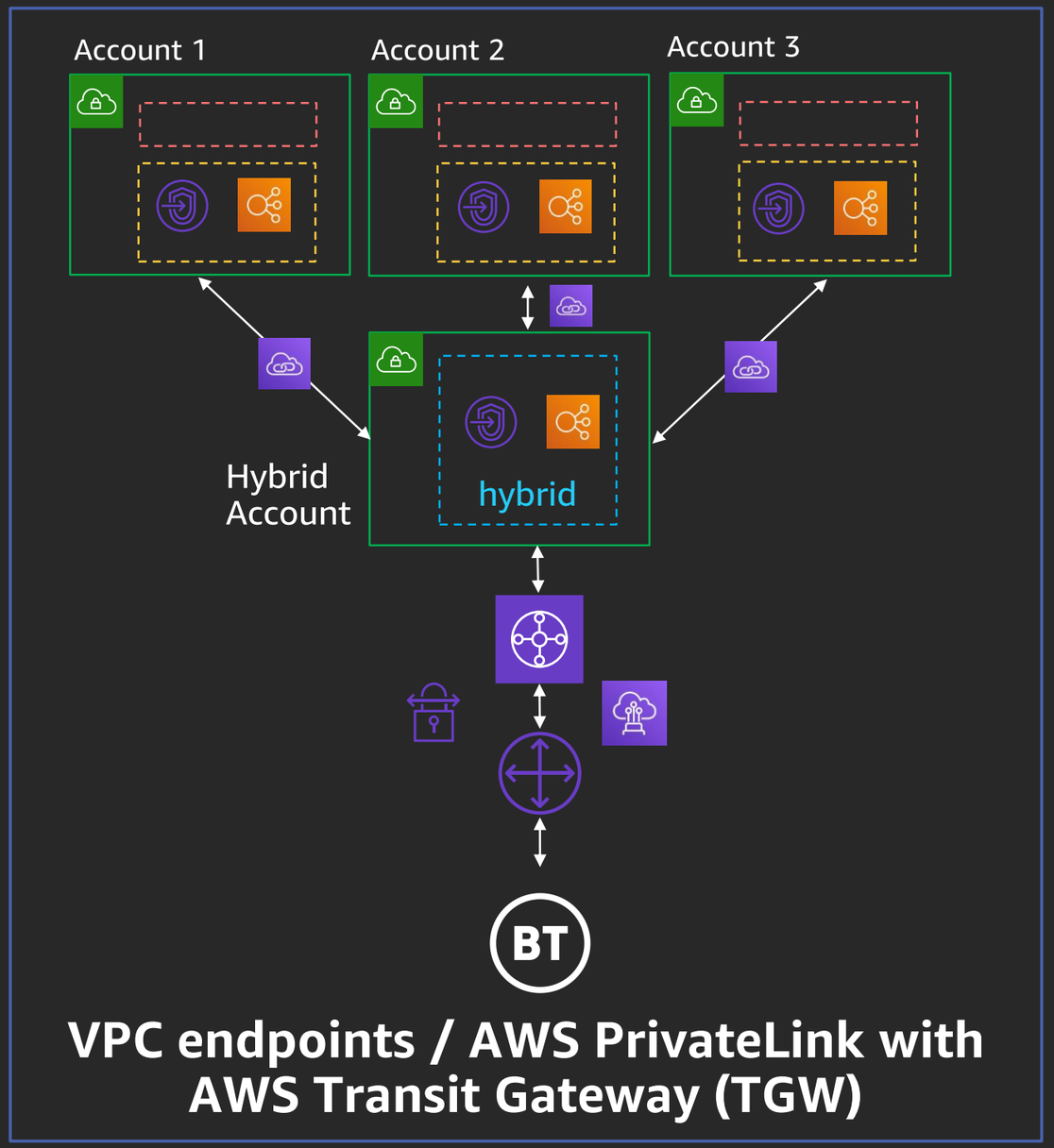
	Pattern/score
Supports multi-account strategy at scale?	
Conserves RFC1918 hybrid IP space	
Reduces on-premises network changes for each VPC deployed?	
Elastic application workloads	

The hybrid journey: Connectivity Patterns



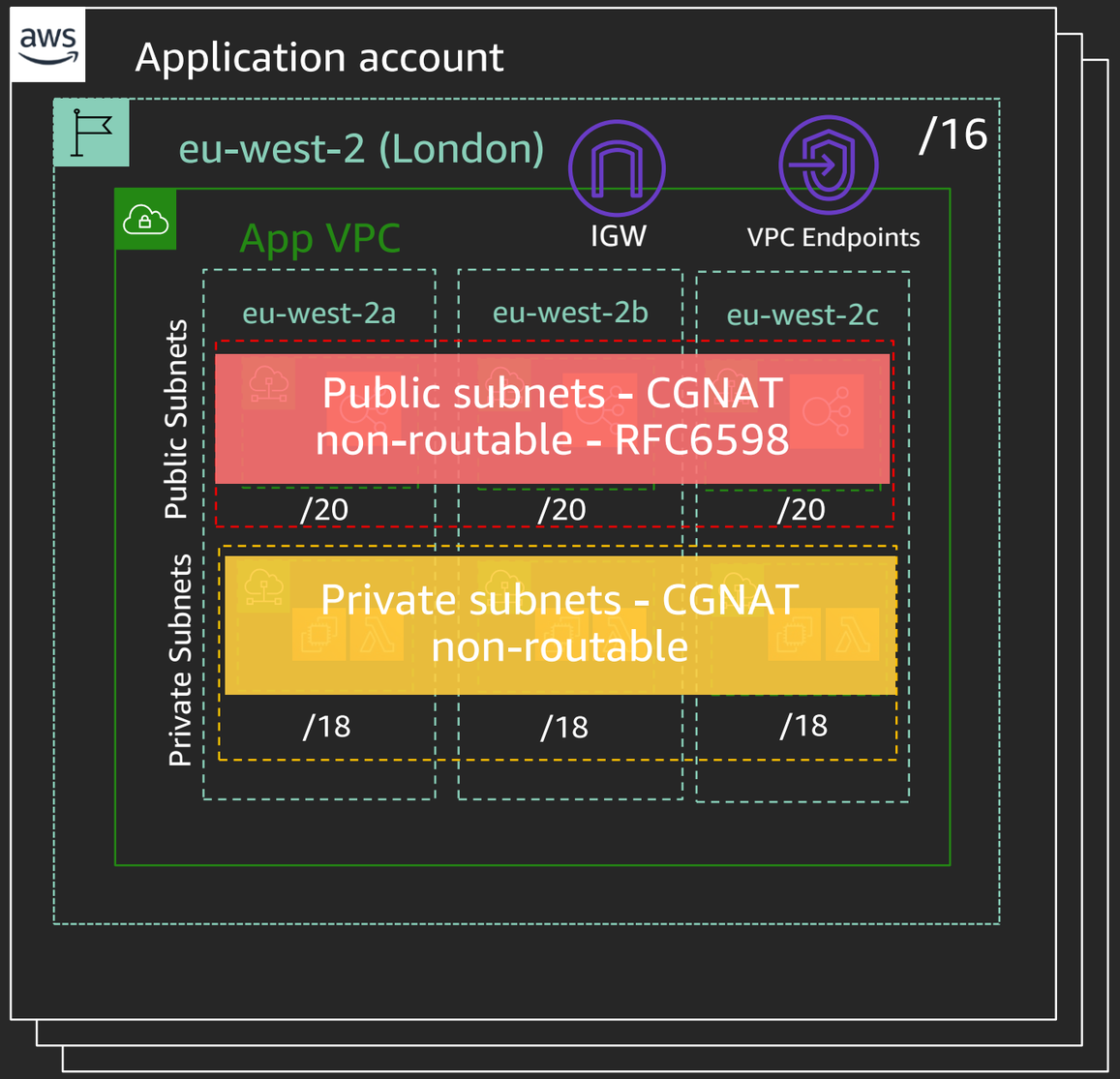
	AWS Transit Gateway
Supports multi-account strategy at scale?	★
Conserves RFC1918 hybrid IP space	✗
Reduces on-premises network changes for each VPC deployed?	★
Elastic application workloads	★

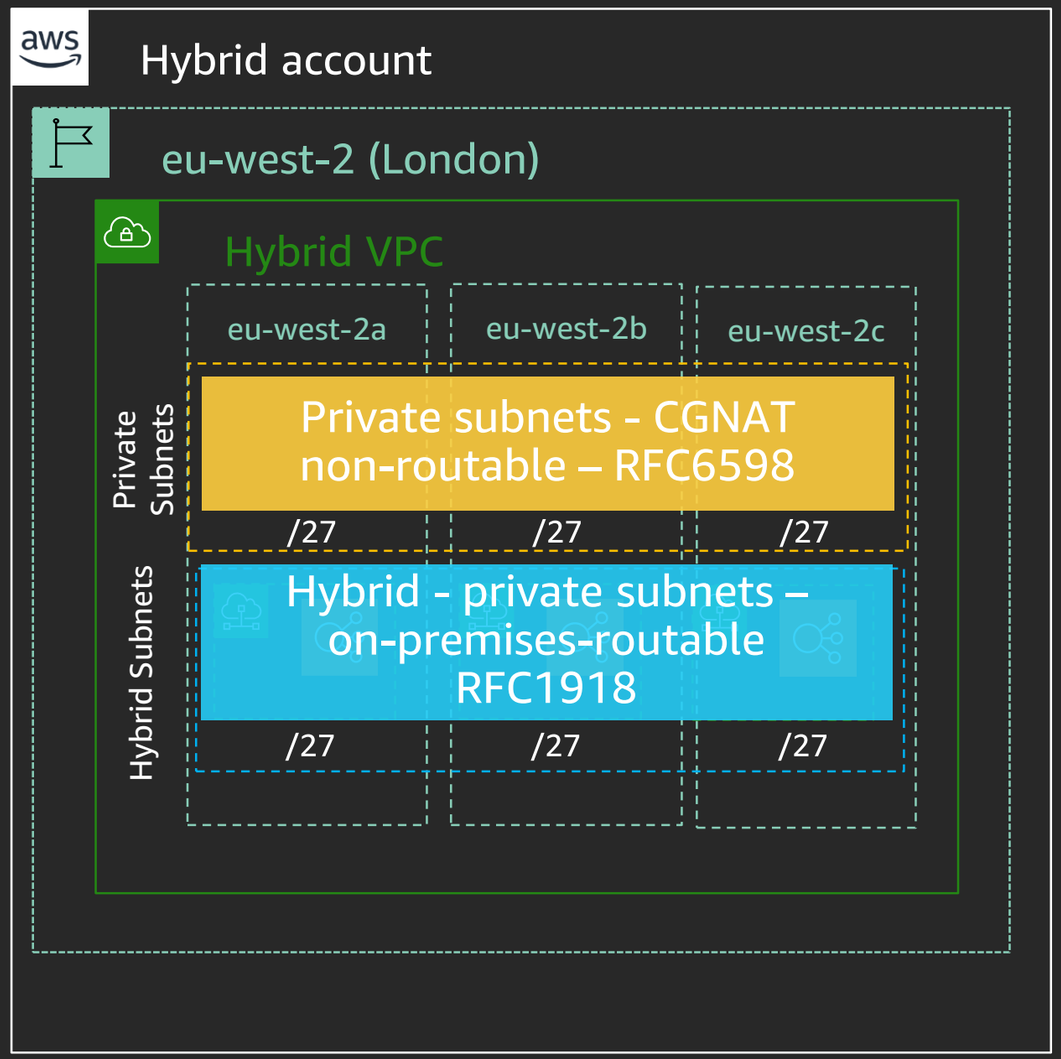
The hybrid journey: Connectivity Patterns



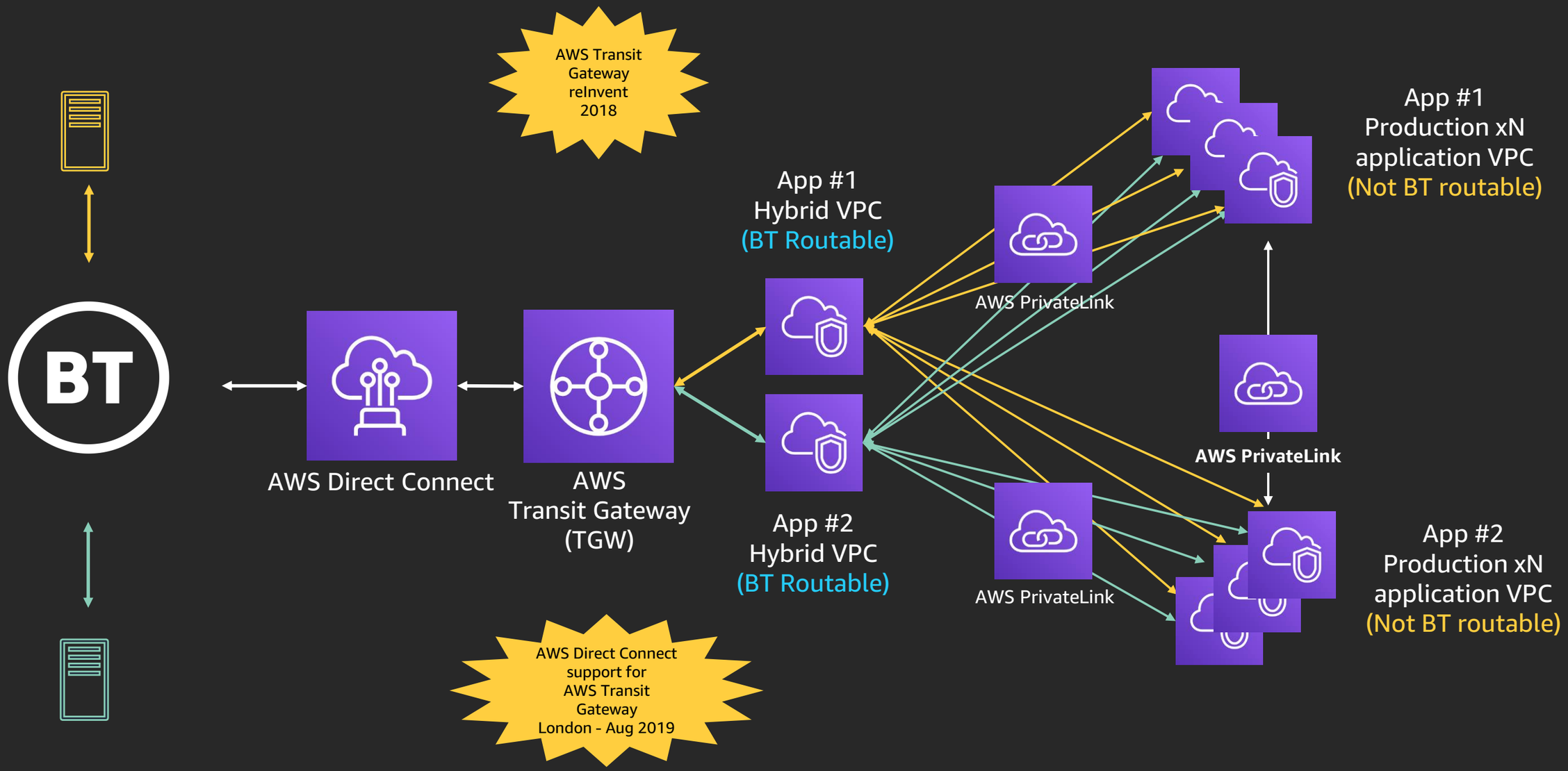
	VPC endpoints + AWS PrivateLink
Supports multi-account strategy at scale?	★
Conserves RFC1918 hybrid IP space	★
Reduces on-premises network changes for each VPC deployed?	★
Elastic application workloads	★

Refining a VPC for Hybrid Connected Applications

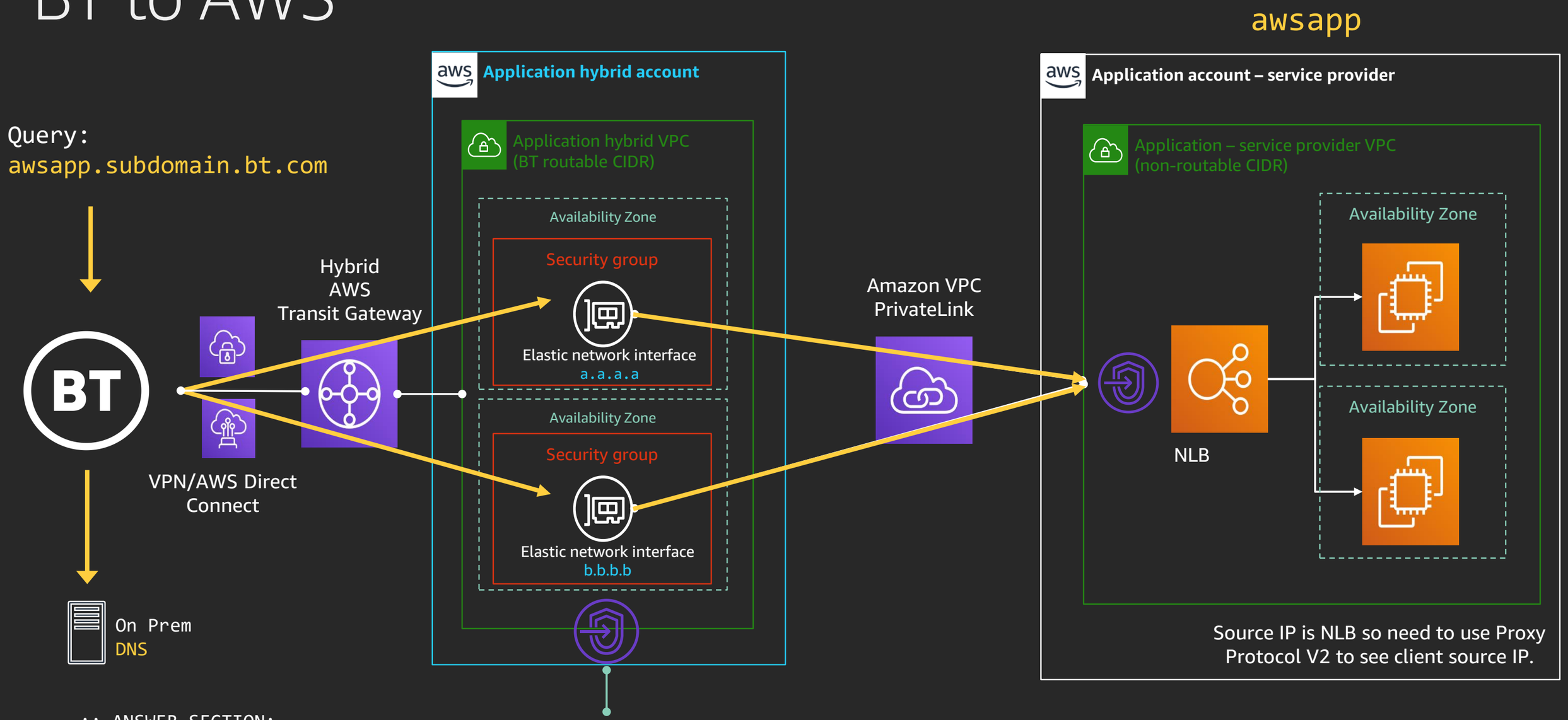




Hybrid connectivity pattern: one-to-many VPC's

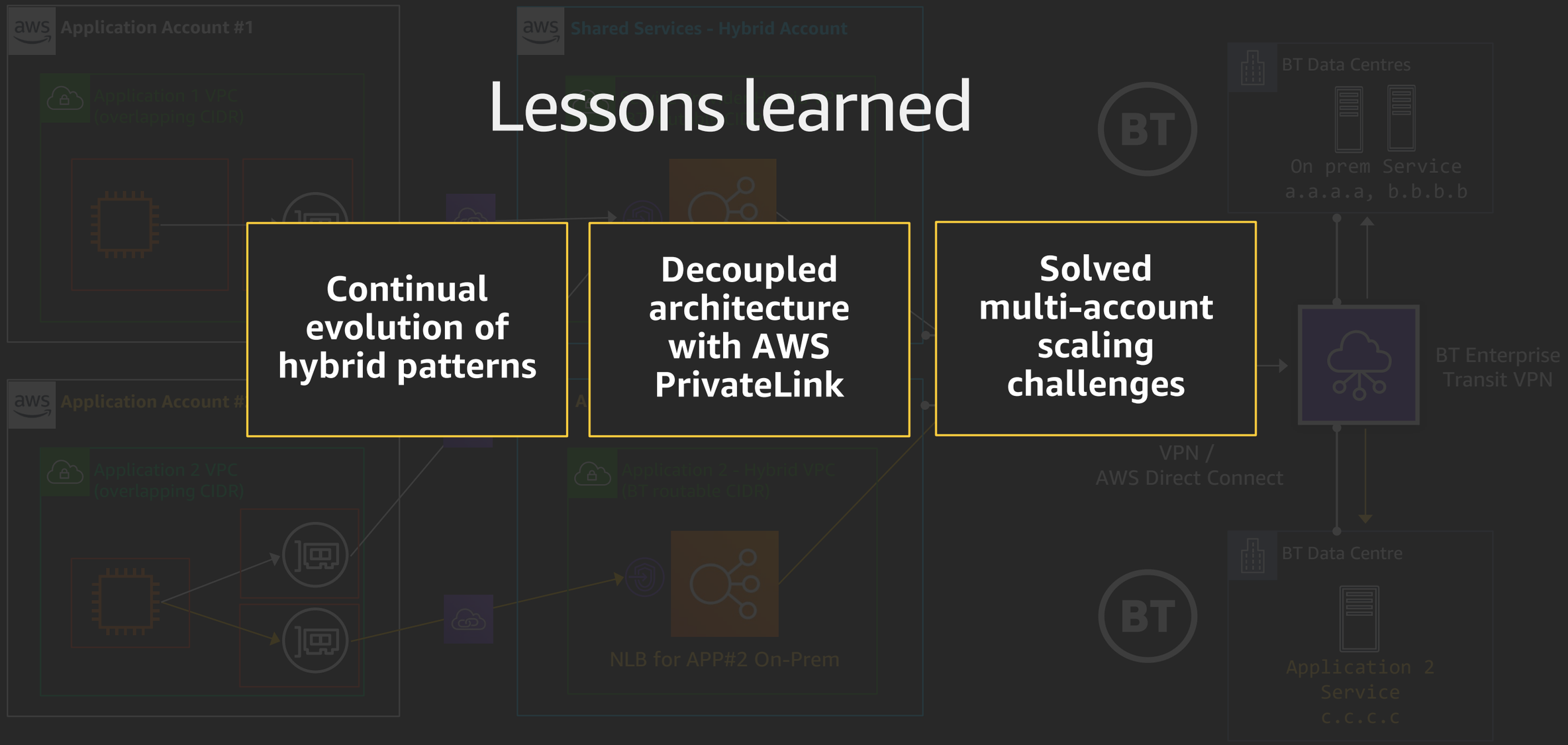


BT to AWS




```
;; ANSWER SECTION:
awsapp.subdomain.bt.com. 3575 IN     CNAME    vpce-000e123456789a123-aa11a1l1a.vpce-svc-01f1111fff01f1fff.eu-west-2.vpce.amazonaws.com.
vpce-000e123456789a123-aa11a1l1a.vpce-svc-01f1111fff01f1fff.eu-west-2.vpce.amazonaws.com. 275 IN A a.a.a.a
vpce-000e123456789a123-aa11a1l1a.vpce-svc-01f1111fff01f1fff.eu-west-2.vpce.amazonaws.com. 275 IN A b.b.b.b
```

AWS to BT—IP targets in hybrid applications



Lessons learned

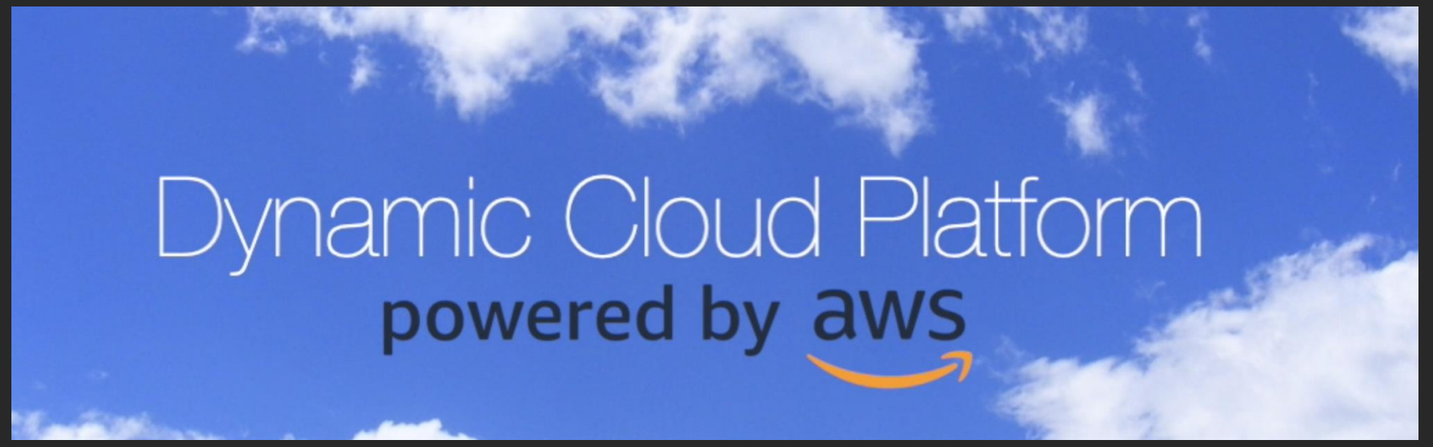
Continual evolution of hybrid patterns

Decoupled architecture with AWS PrivateLink

Solved multi-account scaling challenges

Socialise!

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

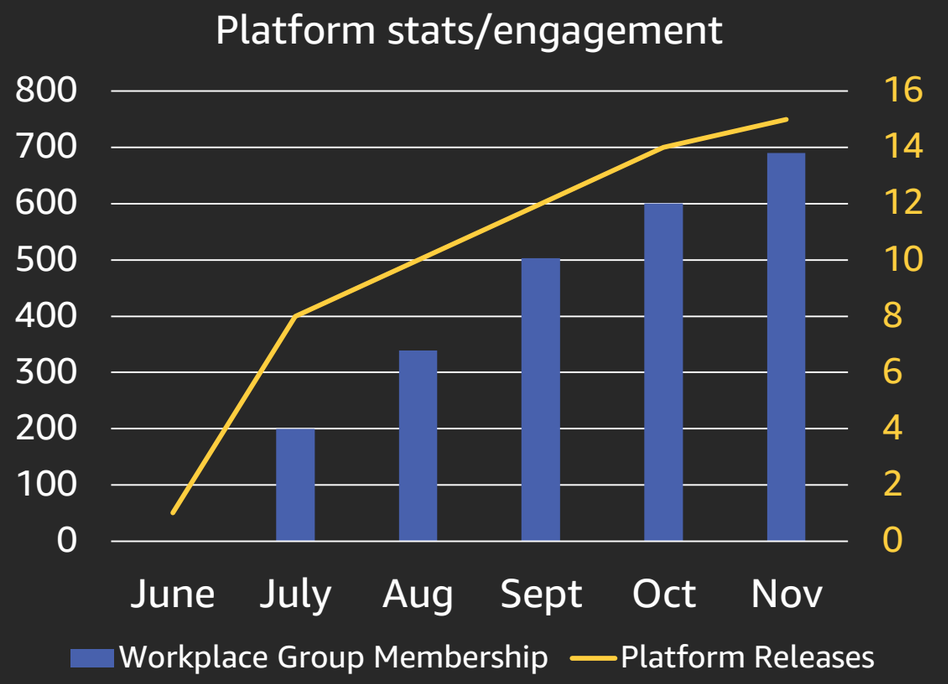


Wiki

Workplace by Face

Microsoft Teams

Brown bags , deep dives, game days



Takeaways

1. Establish your CCoE – the best talent with broad enterprise experience
2. Keep the AWS Landing Zone solution simple and don’t over-customise
3. AWS PrivateLink to create highly scalable decoupled hybrid architectures
4. Grow and stimulate community adoption through your internal social media platforms

Please join me
for a meet and greet!

Telecom Lounge

MGM | Level 3 | Pre-function foyer



Thank you!

Guy Ben-Baruch

gubaruch@amazon.com

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.