FINANCIAL SERVICES CLOUD SYMPOSIUM | 2022

Santander's journey to achieving security-at-scale on AWS

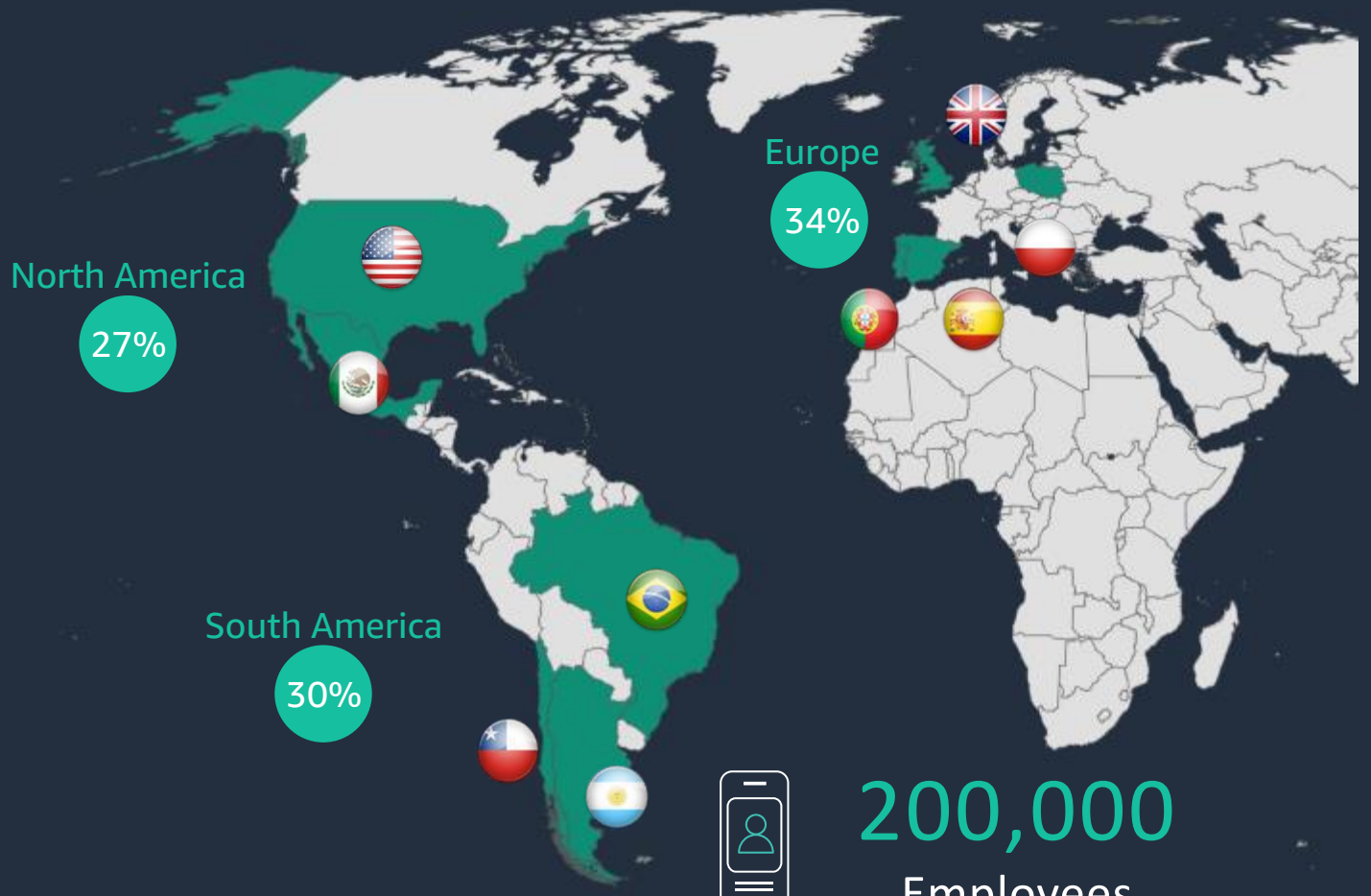
Luis Enríquez Matas

Group VP – CTO for Cloud, Infrastructure & Automation @ Santander Group

Jorge Álvarez Fernández

Global Head of Public Cloud Architecture @ Santander Group

Grupo Santander Scale



200,000
Employees

10,000
Branches

"Local scale and leadership based on three regions.

Worldwide reach through our global businesses and PagoNxt"

PagoNxt

Santander
Corporate & Investment Banking

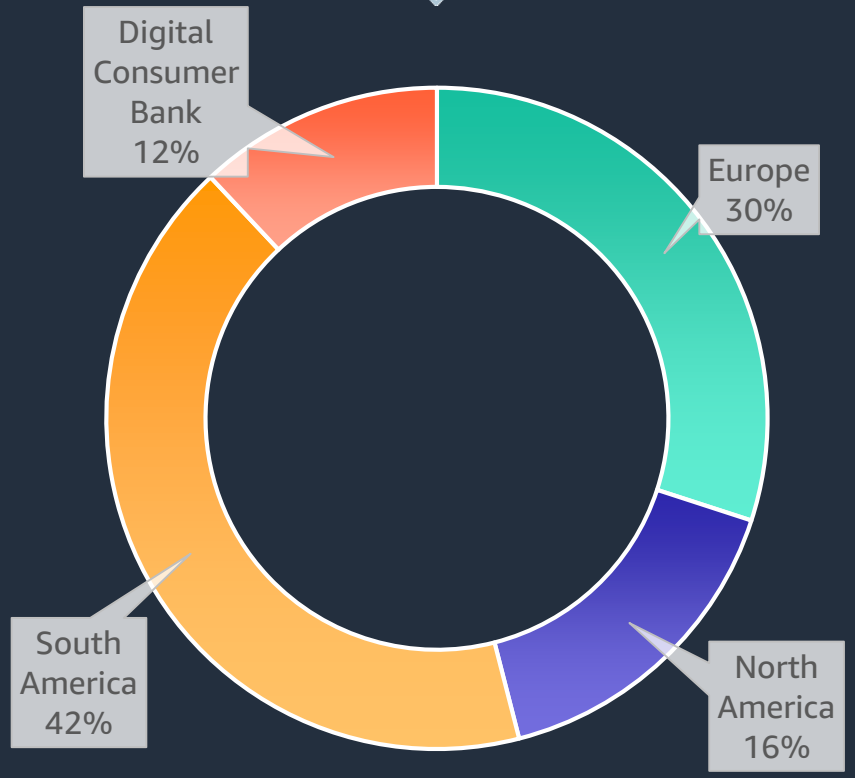
Santander
Wealth Management & Insurance

Santander
Digital Consumer Bank

9%

Customer Focus

155 mn (+11%) customers



26.0 mn Loyal customers

23.8 mn (+12%) Individuals

2.2 mn (+7%) Companies

49.2 mn Digital customers

Tech investments to transform the business ...

€2 bn / year

... help customers transact online

80% Digital TX

56% Digital sales

43.5 mn Mobile customers

Cloud Strategy

In 2019, the Santander Board approved a "Cloud First" strategy that considers a hybrid approach, both evolution of on premises infrastructure with Optimized Hosting Environment (OHE) and Public Cloud for new applications or innovation use cases.

Cloud Strategy

It allows us to enable quick cloud solutions by homogenizing architecture and software development processes, running digital-native applications across physical, virtual, public, private or hybrid cloud infrastructure.

Setting infra foundations to achieve homogenization & simplification

Deploy digital native applications in a faster and simpler way

Enabling an end-to-end automation process

On premises obsolescence reduction and data centers consolidation

Reduction of global power consumption in our data centers

Landing Zone

“A configured, secure, scalable, multi-account, Cloud environment based on common best practices that allows a team to start deploying workloads in a fast, secure and consistent way”

Builders: Stay Agile

Innovate with the speed and agility of AWS

Cloud IT: Establish governance

Govern at scale with central controls

Santander Cloud Landing Zone

Global Products


Public Cloud


Cloud OHE


Network as a Service


DR & Backup


Container as a Service


Application Lifecycle


CMDB


Mandatory Policies, Requirements & Architectural Decisions

Global Teams


Cyber Architecture


Cyber Detect


Cyber Protect


Regulator


Risk & Compliance

Santander Cloud Landing Zone

Core component

1. Centralized infrastructure as a code repository for all entities
2. Security perimeters (firewalls)
3. IAM
4. RBAC for segregation of duties
5. Networking (connectivity to DC and internal networking + Zero-trust segmentation)
6. Log account and compliance monitor
7. ServiceNow integration (assets inventory)
8. Preventive (guardrails) and detective (CSPM) controls

Managed by Global Teams

Non-core components

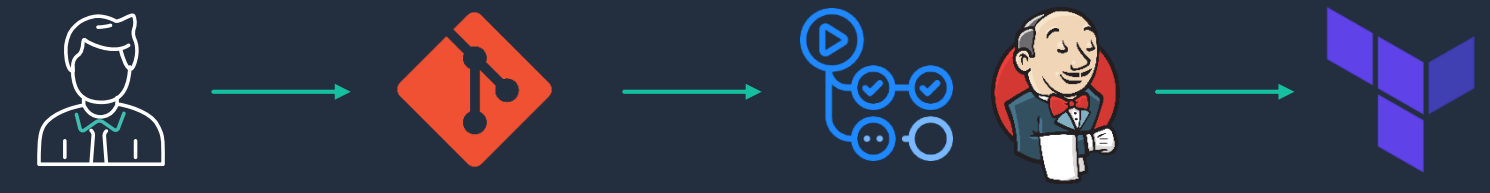
These modules can be evolved/extended by the entities to **provide more agility and flexibility** in the evolution of the Landing Zone.

The evolution of these modules can be done under a federated approach to **boost inner-source model** with entities.

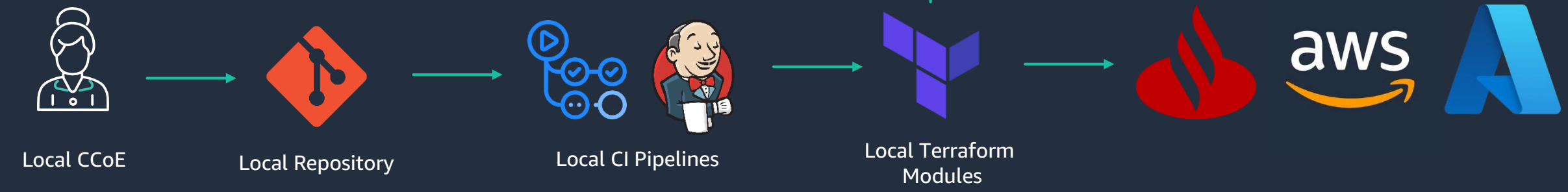
Managed by Entity Cloud Center of Excellence (CCoE)

Santander Cloud Landing Zone

Core modules



- Enforce compliance with the Security Policies and the Cloud Landing zone architecture (modules and providers)
- Roles, secrets and environment segregation
- State is consistently managed during the asset lifecycle



Non-core modules

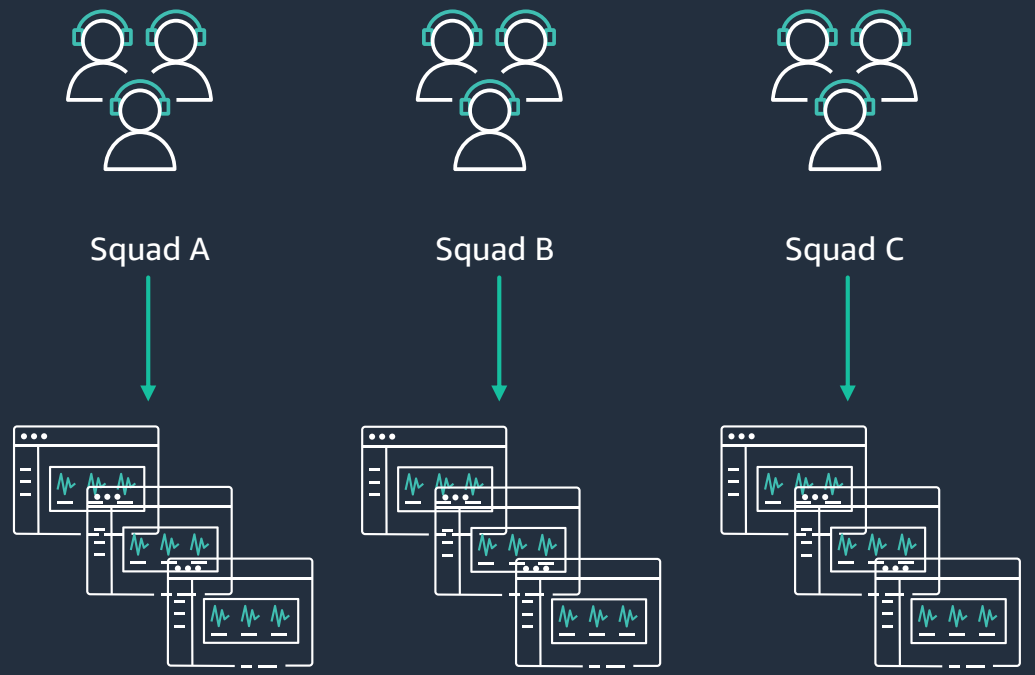
Santander Cloud Landing Zone

Entity

Local CCoE

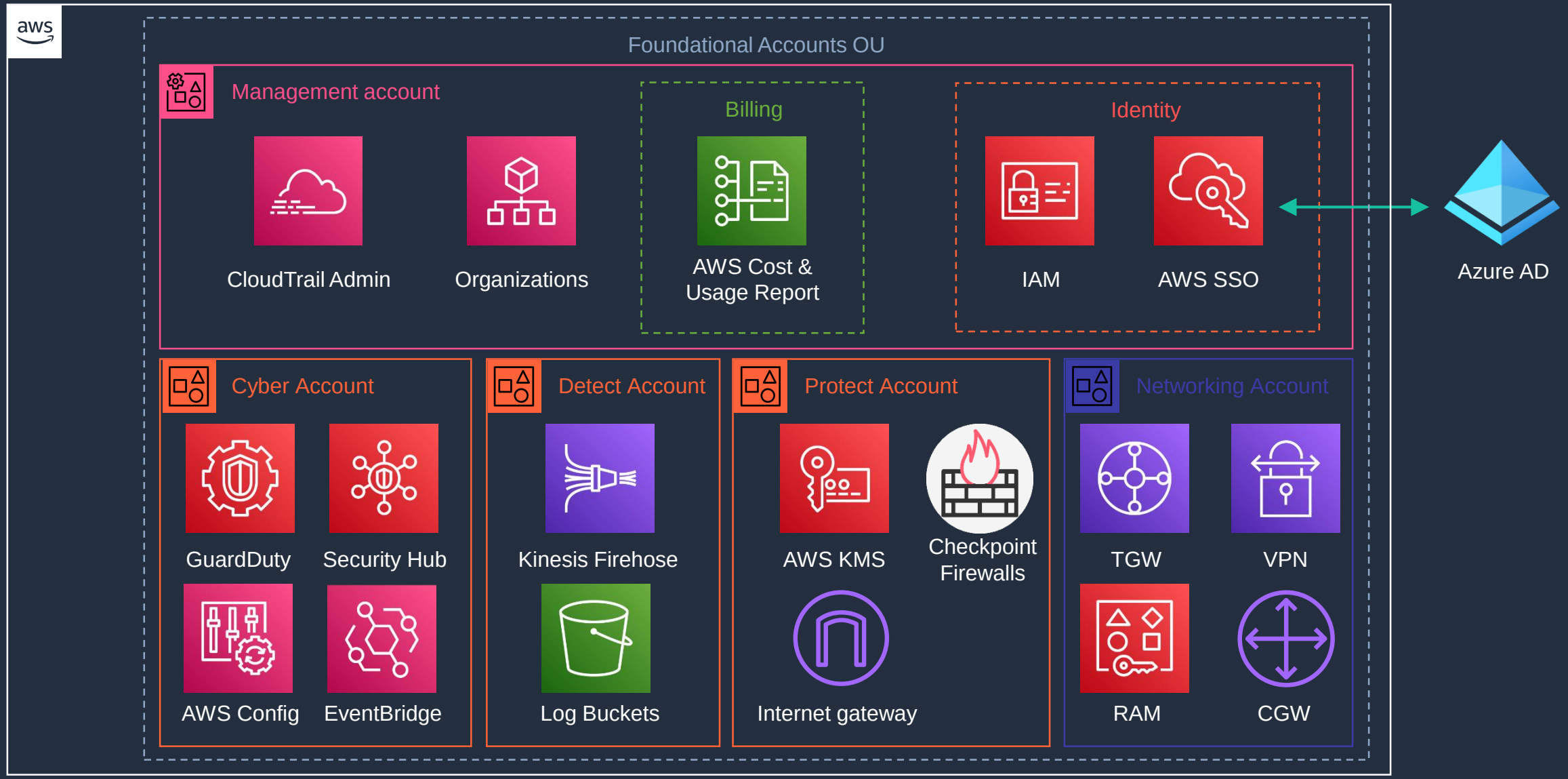
Cloud Data Center

Agile Teams

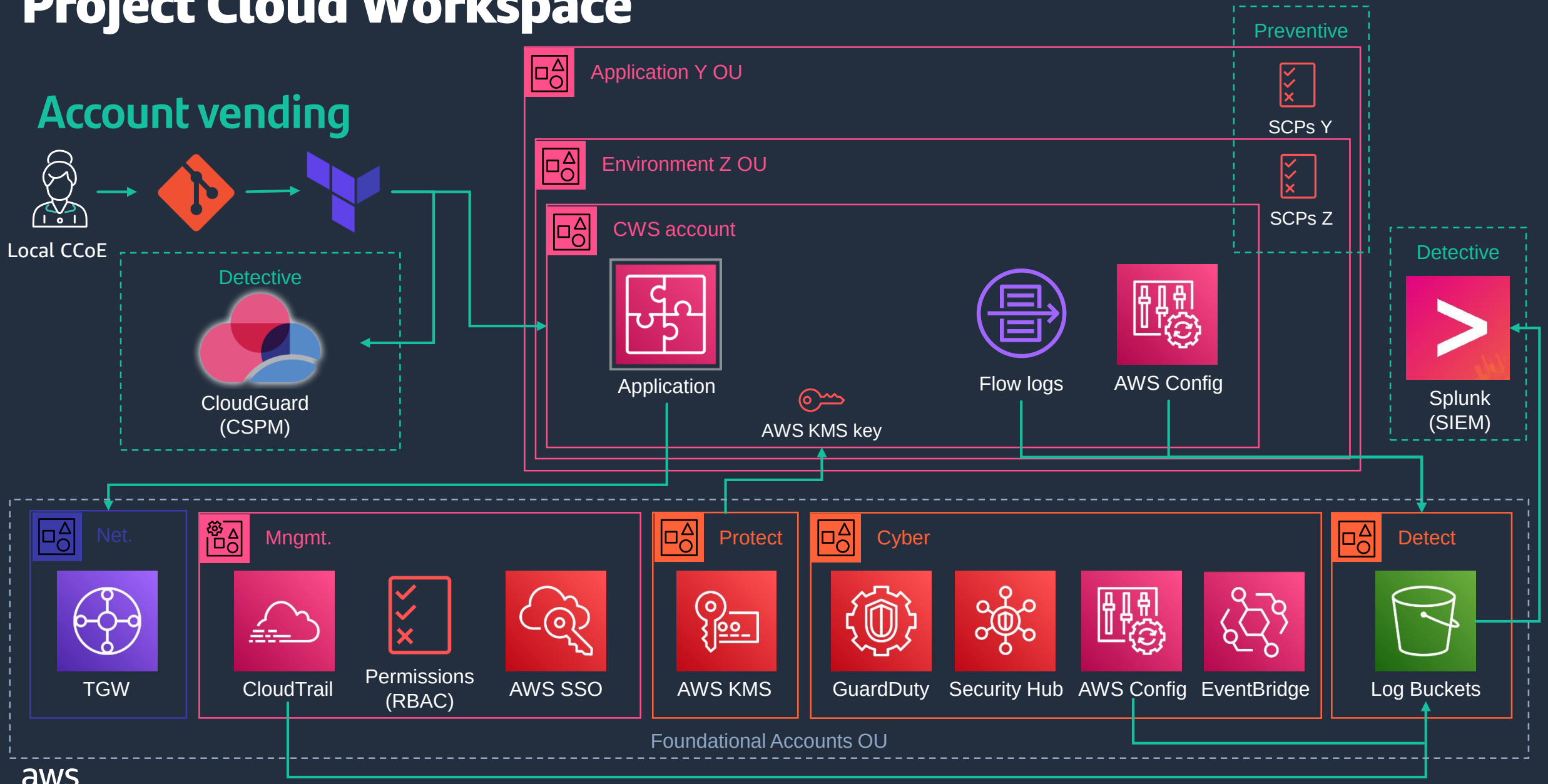


Cloud Workspaces (Vended Accounts)

Cloud Data Center



Project Cloud Workspace



Curated Modules

"A set of centrally managed and **Terraform modules** for commonly used AWS services, which **project teams can deploy** into their application accounts, applying specific service configuration following **security policies and best practices**.

Tech stack validated

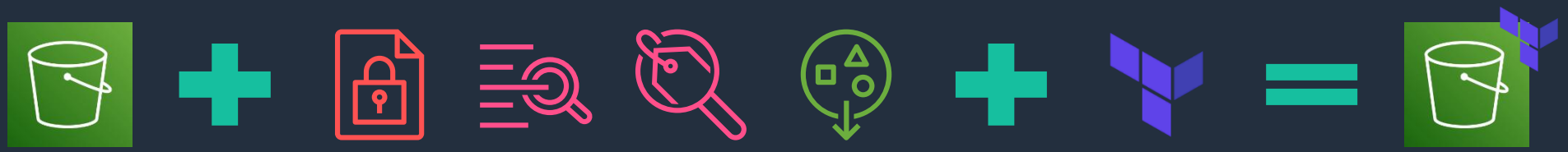
Reviewed by architectural domain to ensure the alignment

Inner source model

Based in a federated model and entities' collaboration

Secure by design

Enforcing tag and Santander standards, with CISO supervision



Public Control Framework

Security controls for cloud

Santander cybersecurity standard and guidelines.

Public Cloud Operating Model

Santander framework mapping the functions/activities with local and global areas.

CSA Framework

It is considered a de-facto standard for cloud security assurance and compliance.

Preventive

Landing Zone Curated Modules

Service Control Policies

Detective

CloudGuard

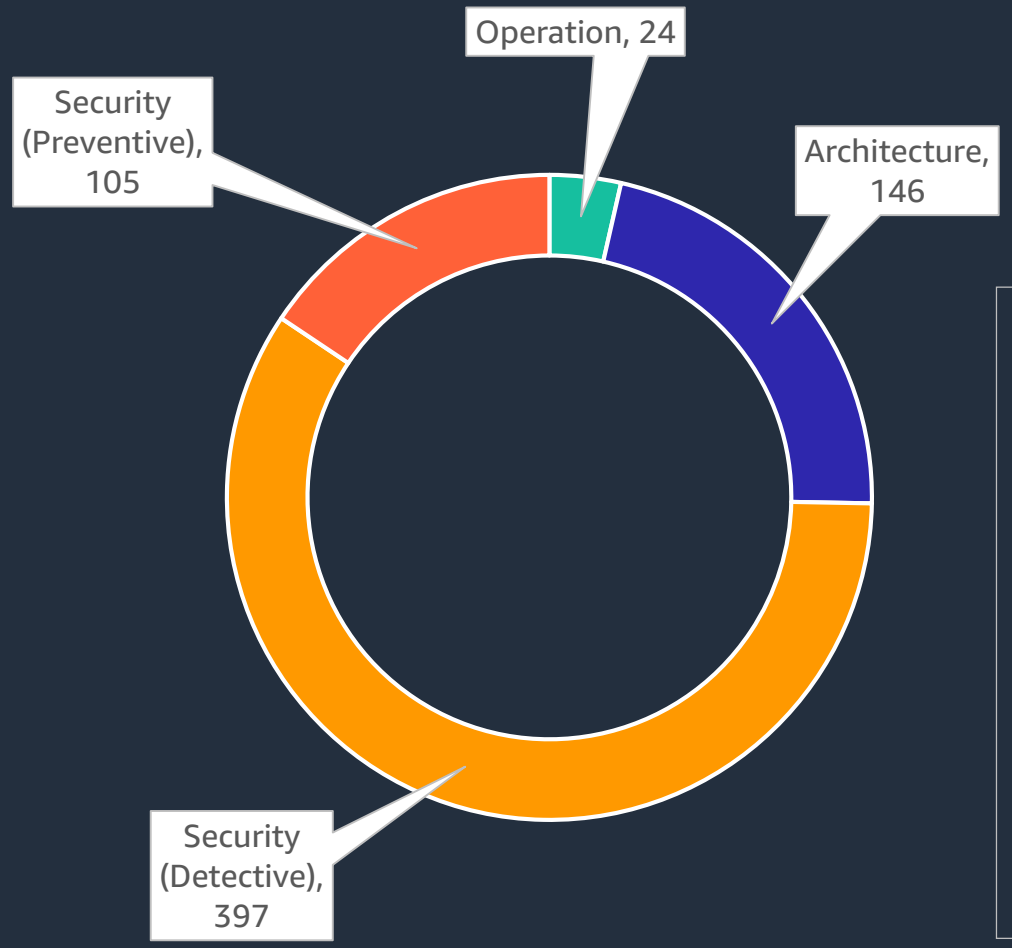
Dashboard

PowerBI

Public Control Framework

Typologies

- Security
- Architecture
- Operation



+500
Accounts

+450,000
Artifacts

12
Entities

Lessons Learned

- Include controls definition, from the beginning, in an architectural evolution (or adoption of new services), is key to ensure the adoption in a secure way.
- Different types of controls (automatization layer, CSPs, detective, etc.) are complimentary, and they are required to ensure a successful model.
- It is not easy to keep the pace, with the continuous evolution of the public cloud, so native services are a key piece (as new functionality appears).
- With the right tools and automatization, a federated model is viable.

Thank you!

Luis Enríquez Matas

luis.enriquez@gruposantander.com

https://www.linkedin.com/in/luisenriquezmatas/

Jorge Álvarez Fernández

jorge.alvarezfernandez@gruposantander.com

https://www.linkedin.com/in/jorgealvarezfernandez/