SaaS-based Operations

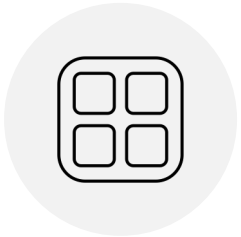
Distributed Infrastructure and POP Management

Shain Singh, Principal Security Architect, F5

ss@f5.com | @shainsingh

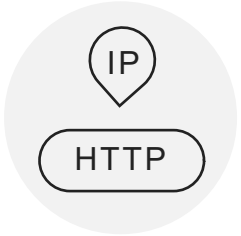
Fundamental shift in how apps are designed & deployed

Monolithic Apps



One Cloud Provider

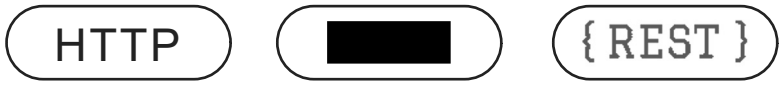
Network-based Communication



Microservices-based Apps

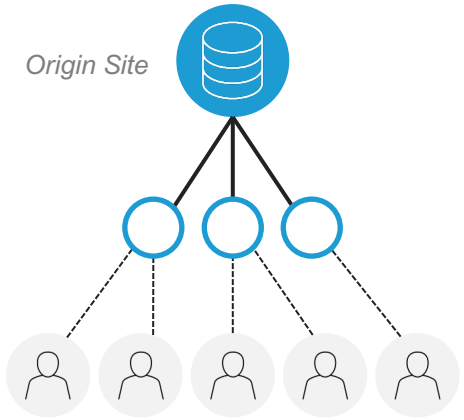
Multi-cloud and Edge Computing

API-based Communication

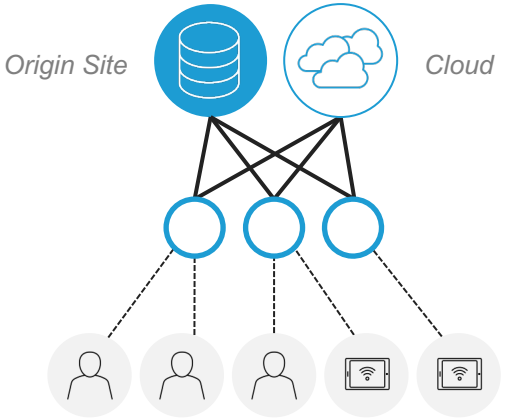


Application delivery is changing

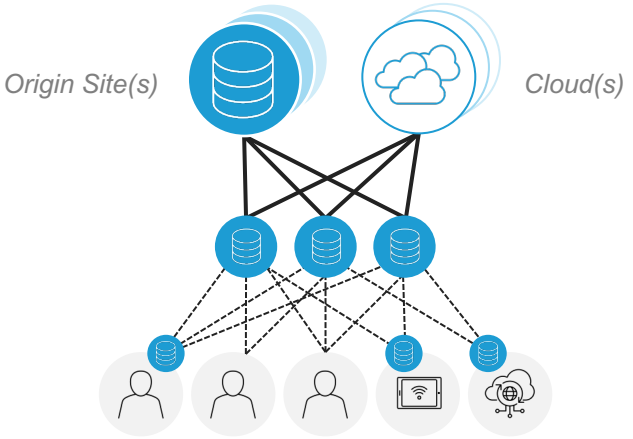
CDNs
Scale out static object serving

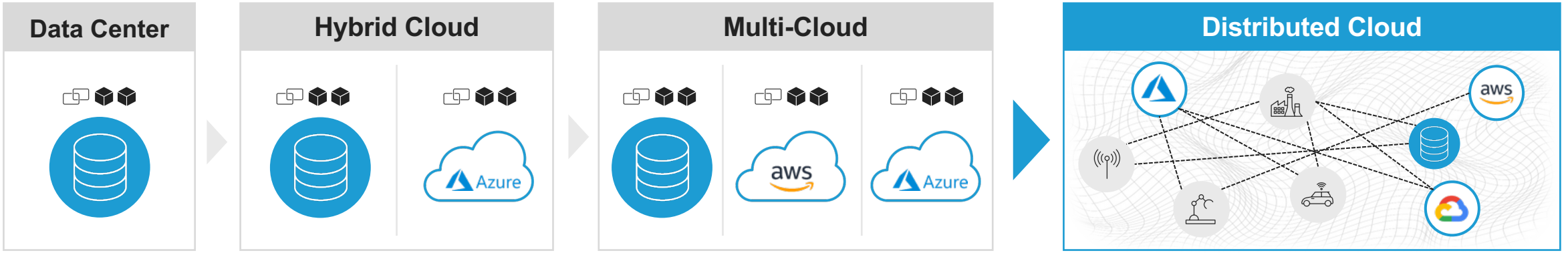


Cloud
Scale out app servers



Distributed Cloud
Scale and connect everything





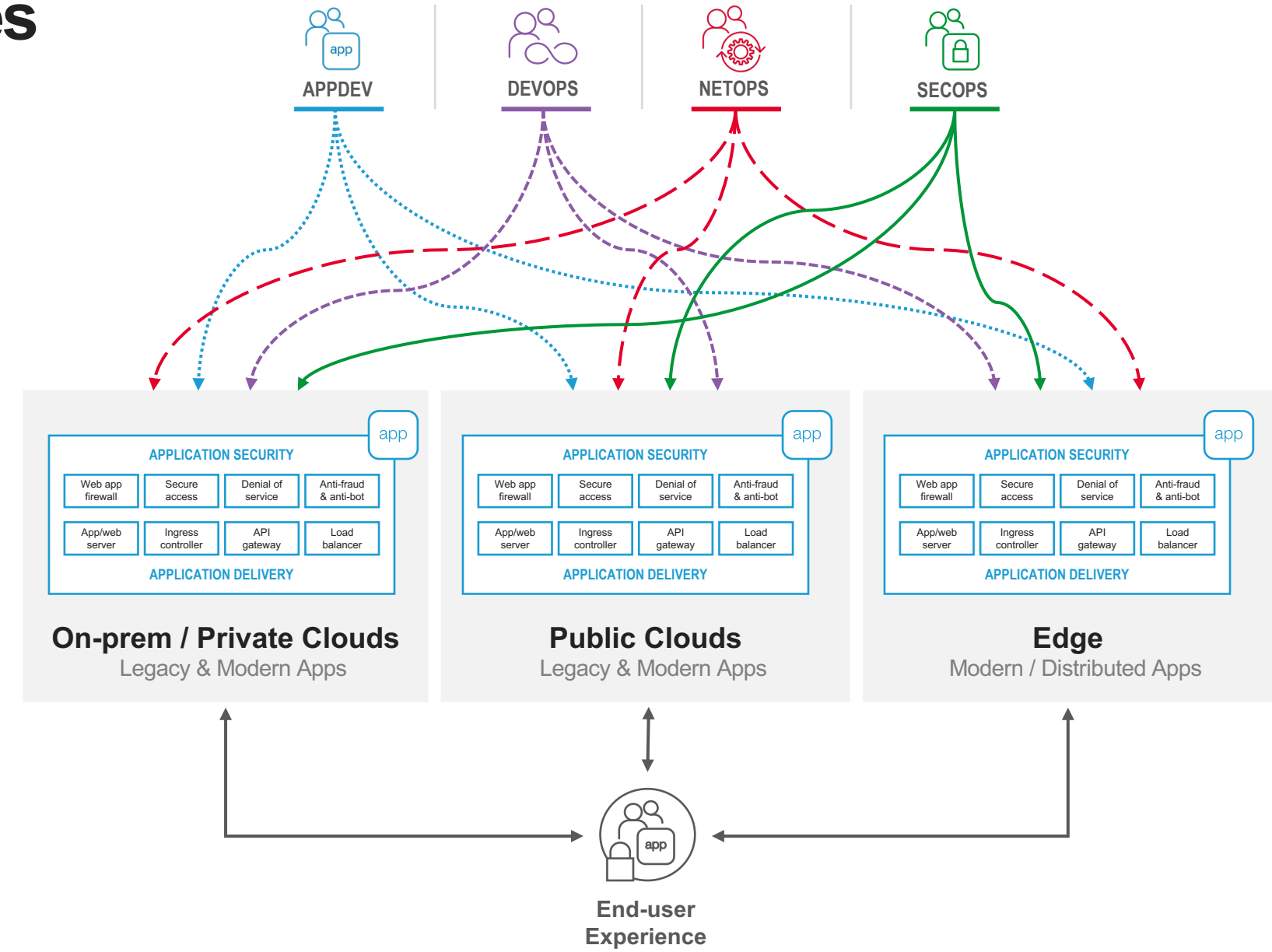
Technical challenges of delivering apps

#1 Complex coordination because of technology inconsistencies between teams and across environments

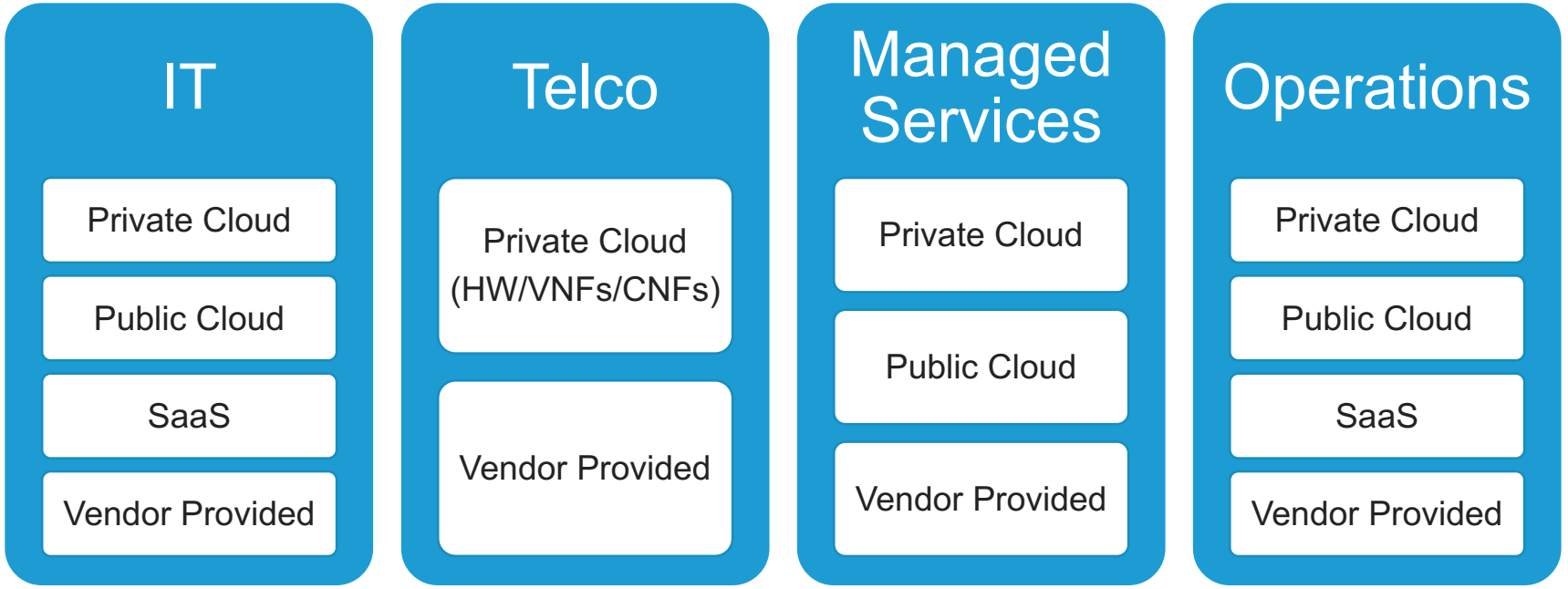
#2 Automation challenge ”stitching” multiple environments, layering net, security, and apps, at scale

#3 Security difficulties due to multiple different attack surfaces and sophistication of bad actors

#4 Limited observability of silo-ed telemetry trapped in disjointed systems & environments



Siloed operations in SPs is a roadblock

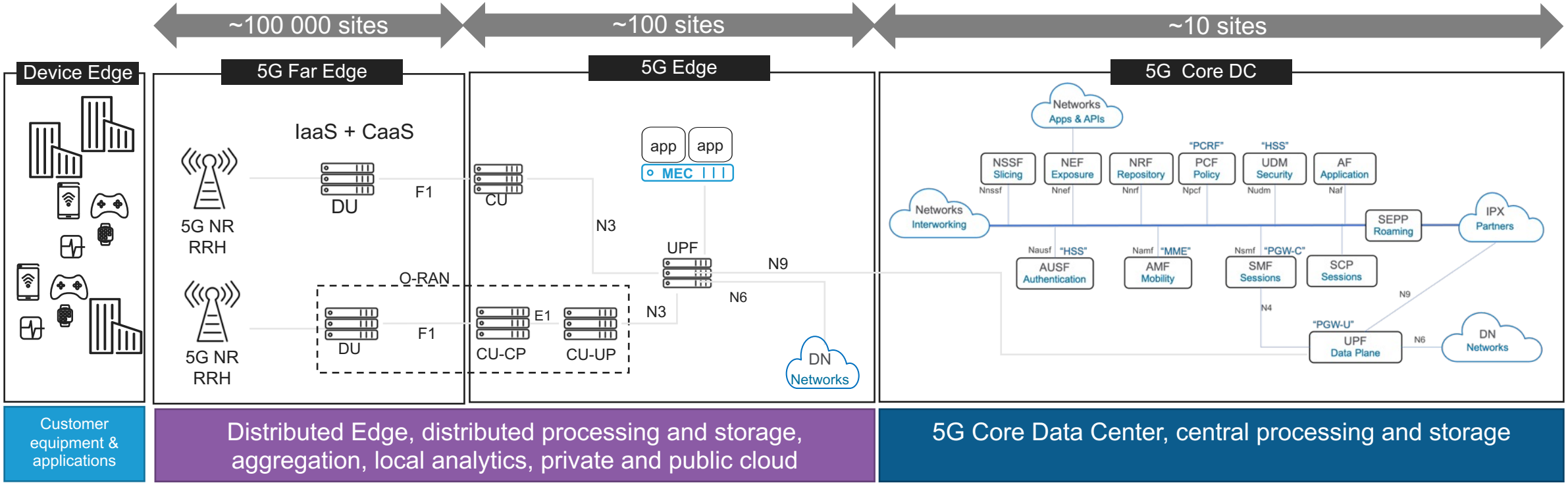


- **High Cost**
- **Slow to Deploy**
- **Limited Scalability**
- **Decreased Visibility**
- **Reduced Security**
- **Interoperability Issues**

Distributed 5G Architecture – Target State for SPs

Merging Multi-Cloud, Hybrid Cloud and Enterprise IT with a Common Platform

- Explosion in the number of sites that need to be deployed and managed from ~10s of MTSOs to ~250 MTSOs
- RAN and Small Cell densification leads to 10s of thousands of site deployments at the far edge
- Managing a hybrid network with CNFs and VNFs where initial deployments will have both VNFs with a Kubernetes wrapper (Kubevirt) (IaaS) along with pure Kubernetes Pods (CaaS)



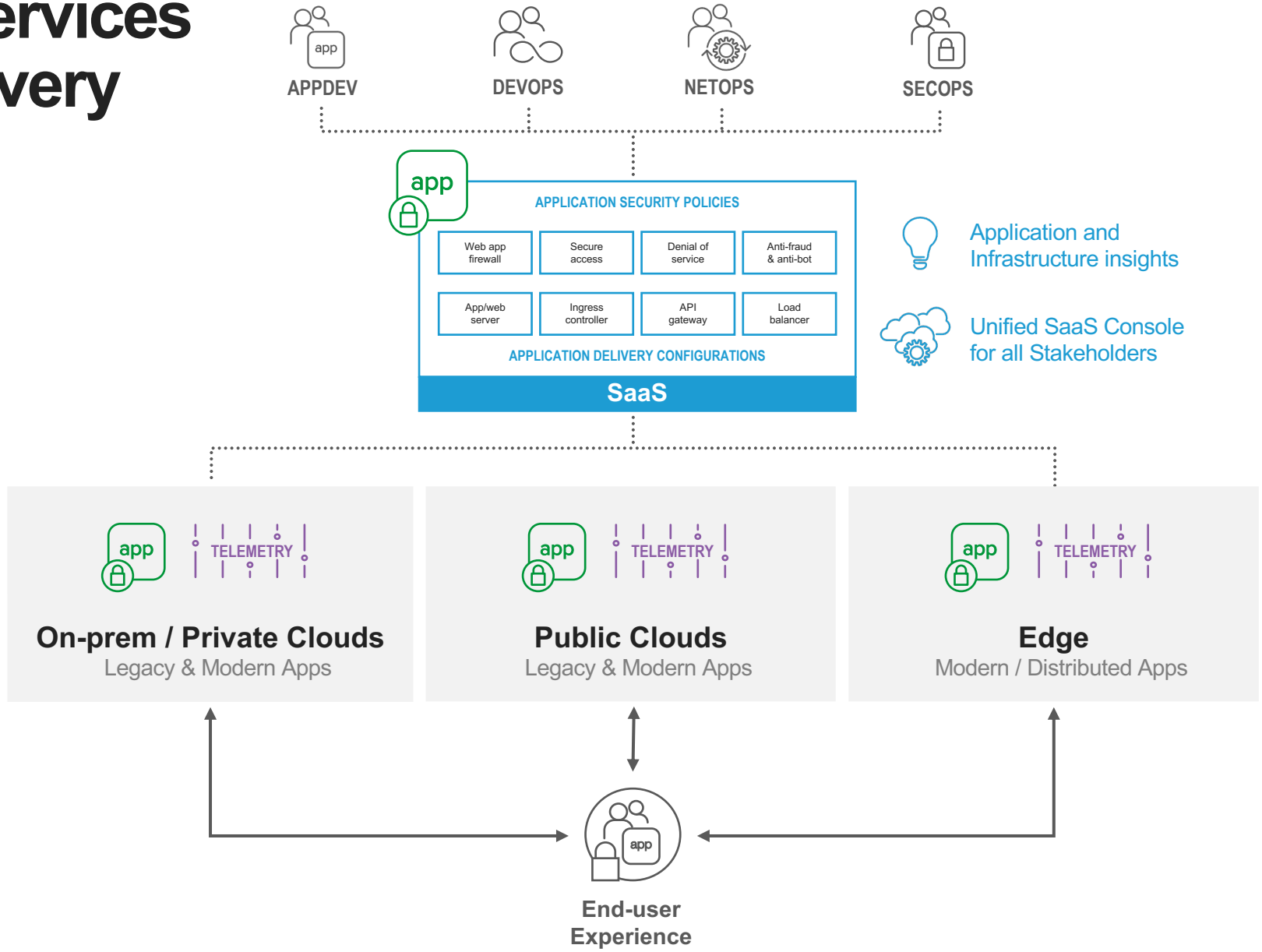
Distributed Cloud Services for Modern App Delivery

#1 Collaborate across teams with a centralized SaaS console to simplify planning and streamline execution

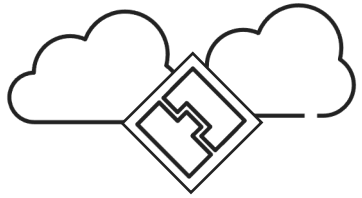
#2 Automate network configs and security deployment to reduce effort, errors, and gaps in coverage

#3 Advanced security filters out bad traffic before it hits customer networks, stays up to date

#4 Full stack observability of network, security, and application performance, cloud-agnostic and exportable



Distributed Cloud Services - Use Cases



Networking:
Hybrid and Multi-cloud

Uniform multi- and hybrid- cloud connectivity for workloads deployed across clouds

- Multi-cloud transit
- Multi-cloud load balancing
- Multi-cluster app mesh
- Global high-speed high-capacity backbone network

Security:
Web App and API Protection

API security, WAF, DDoS protection, firewall, bot defense, anomaly detection

- Streamline multi-cloud security orchestration
- Manage and secure APIs
- Reduce fraud and abuse
- Simplify security to aid app development

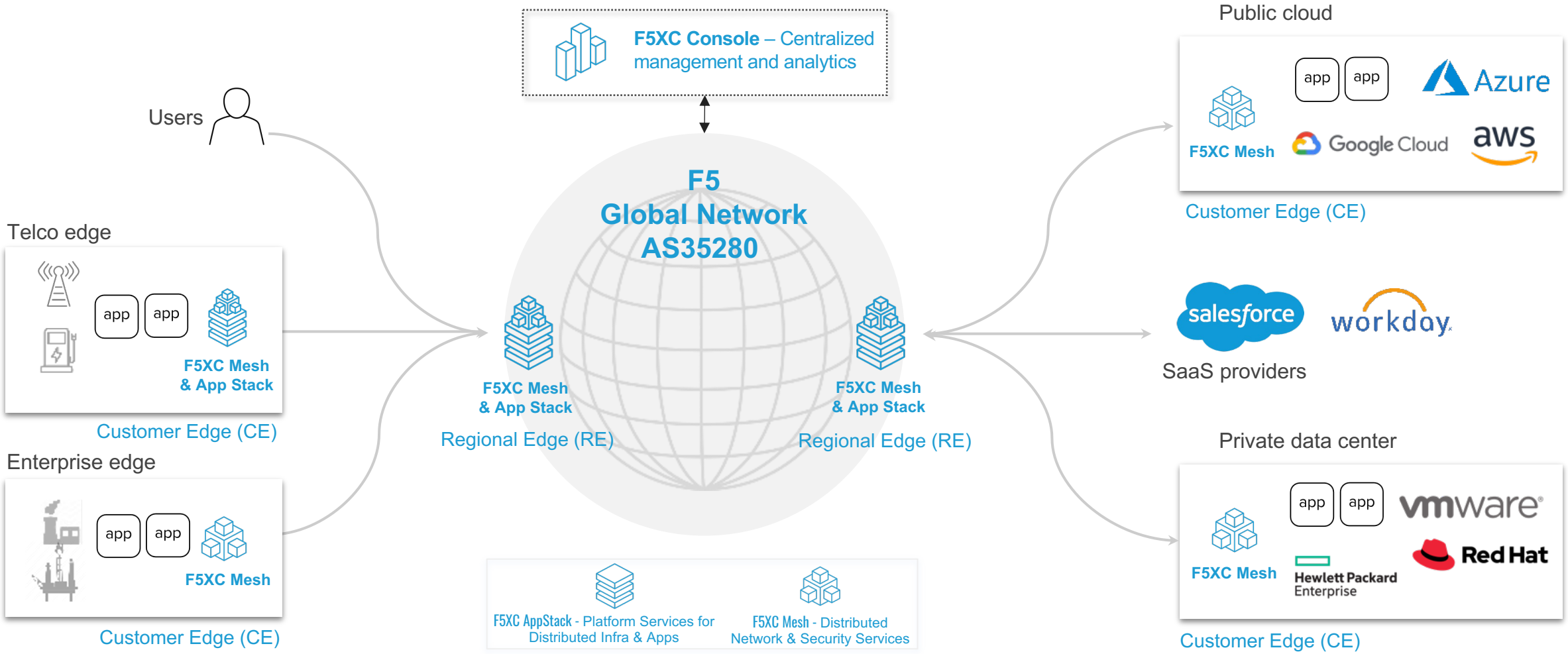
Application Delivery:
Cloud and Edge

Run microservice-based apps wherever you require, globally, in the cloud, data center, or the edge

- Secure Kubernetes gateway
- Managed Kubernetes
- Edge infrastructure & application management
- Distributed apps

Distributed Cloud Services - Platform Overview

Scaling infrastructure and POPs with a Customer Edge



Use cases

Scenarios taken from Carrier Service Providers we are working with

https://youtube.com/playlist?list=PL5jC9WagzrjH-mlBSmHdVa5G_S52jKbKa

- **5G Core Service Based Architecture** using a distributed cloud platform ~3mins
- **CGNAT as CNF** for a de-centralised N6 interface ~3mins
- **Kubevirt and SmartNICs** using COTS and managed Kubernetes platform for CGNAT ~9mins