Modernising On-Prem Infrastructure

Shain Singh, Principal Security Architect @ F5, ss@f5.com

Our Speaker

Shain Singh

Principal Security Architect @F5

25+ years in security, network and IT

Worked in Telco/ISPs, Education, Government sectors

- DevSecOps (Continuous security in operations)
- MLSec, MLOps
- 5G Security (IIoT, Smart Cities, Edge Networks)
- API/Application Security
- Government/Industry Standards and Compliance

Social

in   https://linkedin.com/in/shsingh

✉   shain.singh@owasp.org

🐦   https://twitter.com/shainsingh

○   https://github.com/shsingh

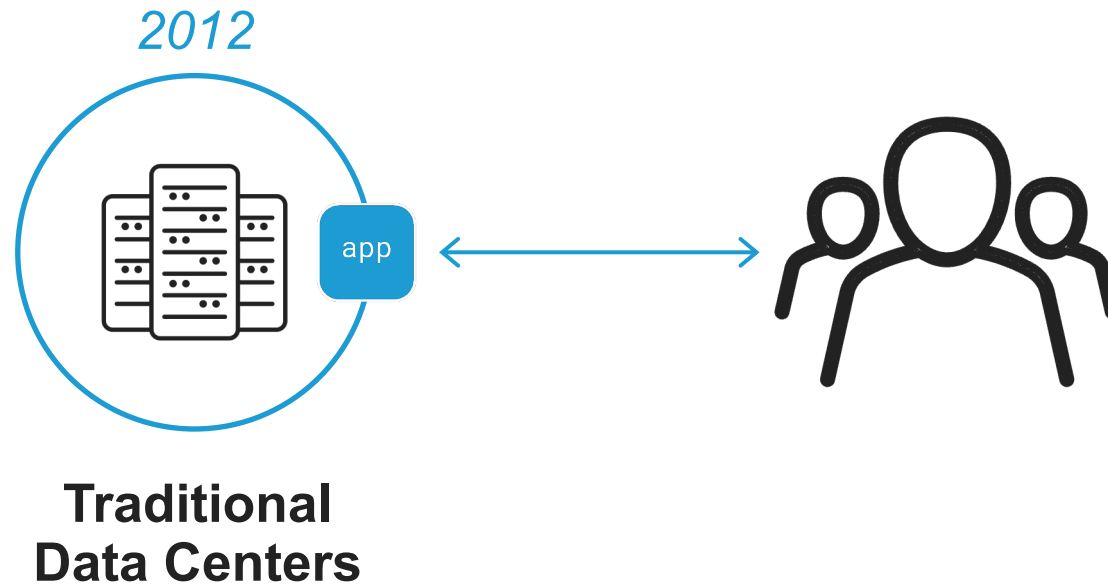## Professional Memberships

A brief look at the past – the world in 2012

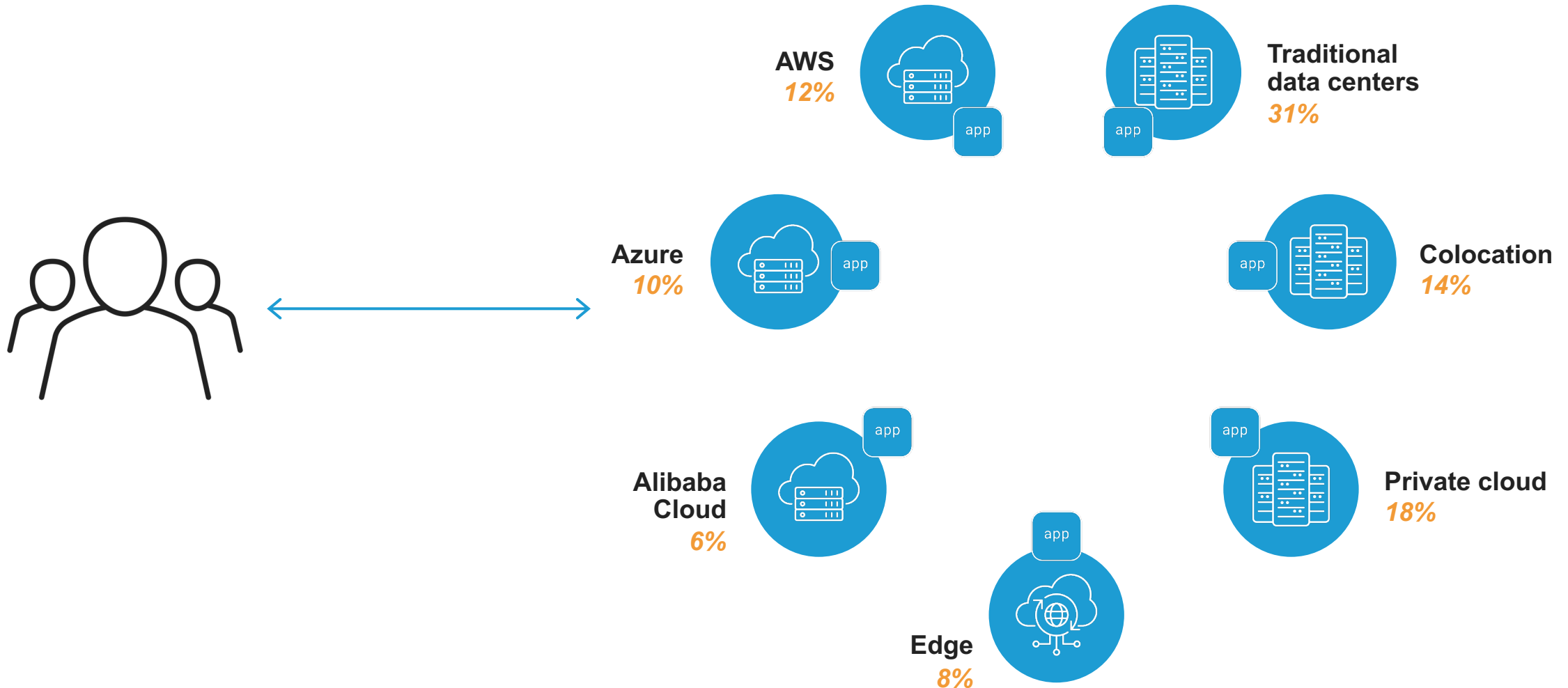# The way organizations deployed apps used to be very simple

2012

app

Traditional Data Centers

©2023 F5

In 2017, it was commonly assumed that in the 'end state', all apps would be in the public cloud

2012

app

Traditional Data Centers

2017

app
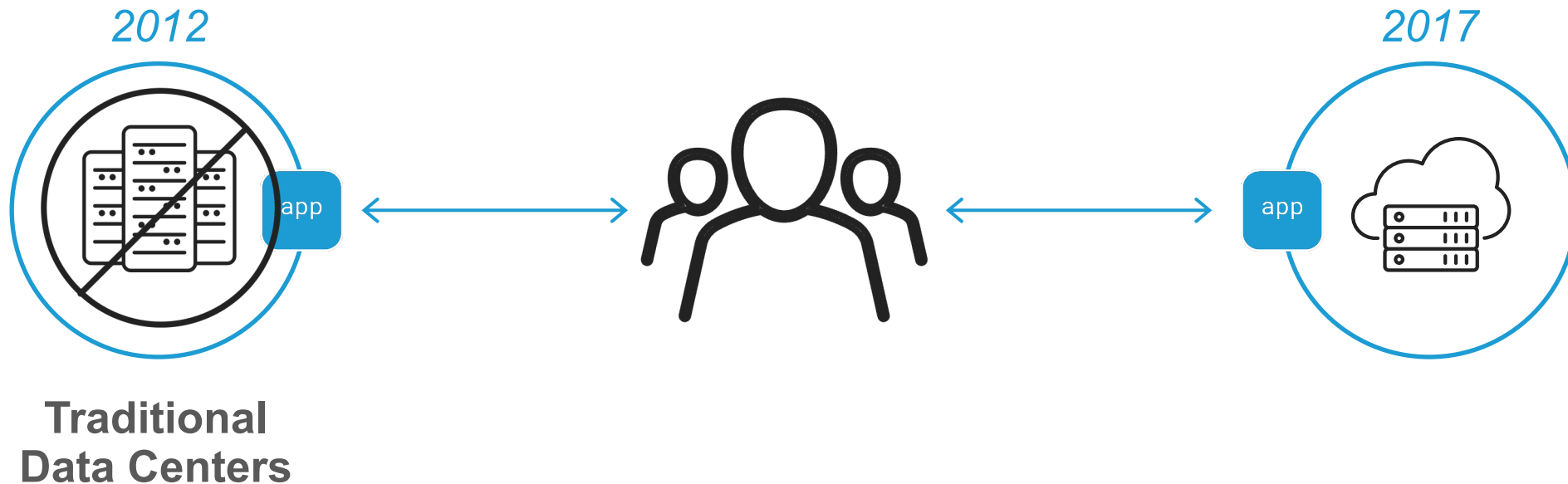
That prediction was wrong on multiple levels

Firstly, apps went where the business needed them

AWS
12%

Traditional
data centers
31%

Azure
10%

Colocation
14%

Alibaba
Cloud
6%

Private cloud
18%

Edge
8%

©2023 F5
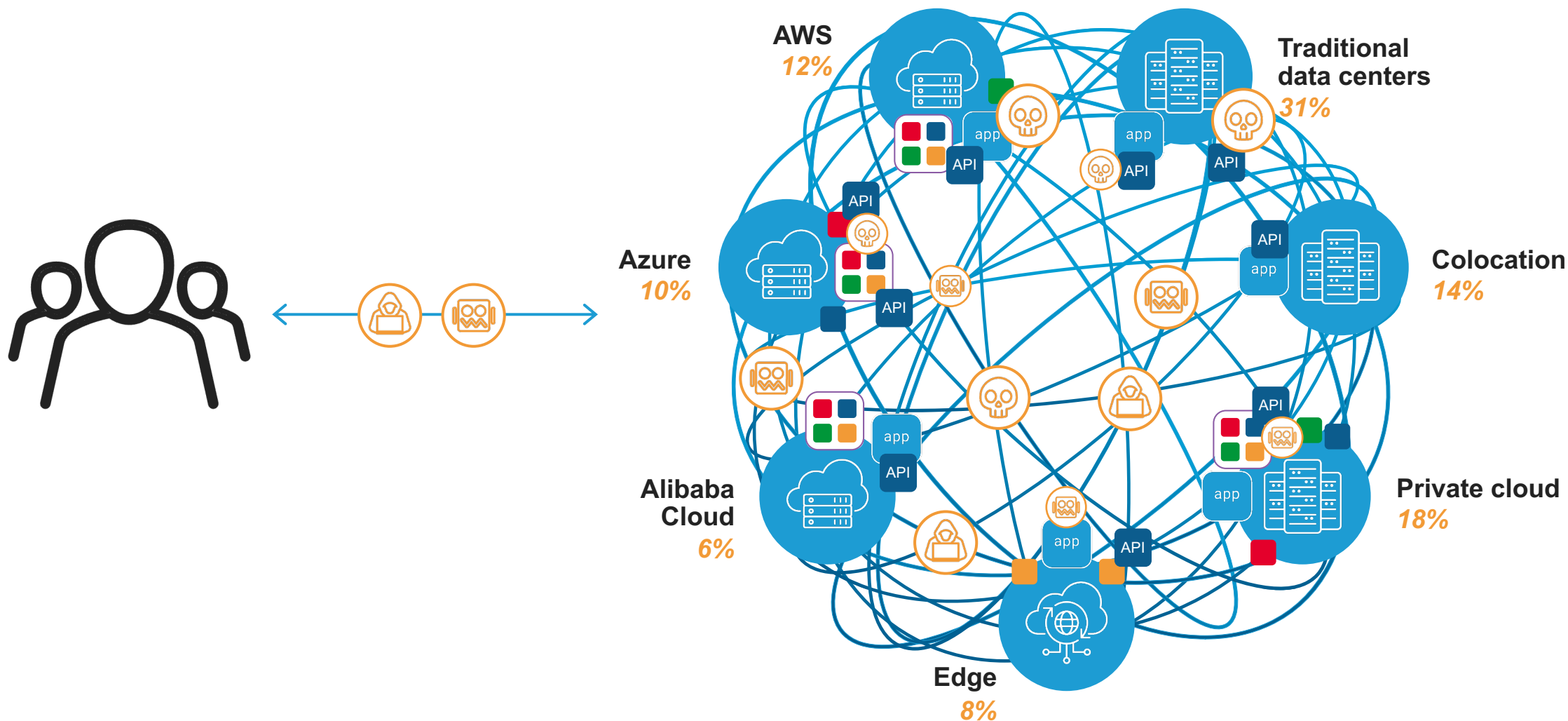
… but modern apps exploded and are now distributed dynamically across locations

AWS
12%

Traditional
data centers
31%

Azure
10%

14%

Alibaba
Cloud
6%

Private cloud
18%

Edge
8%
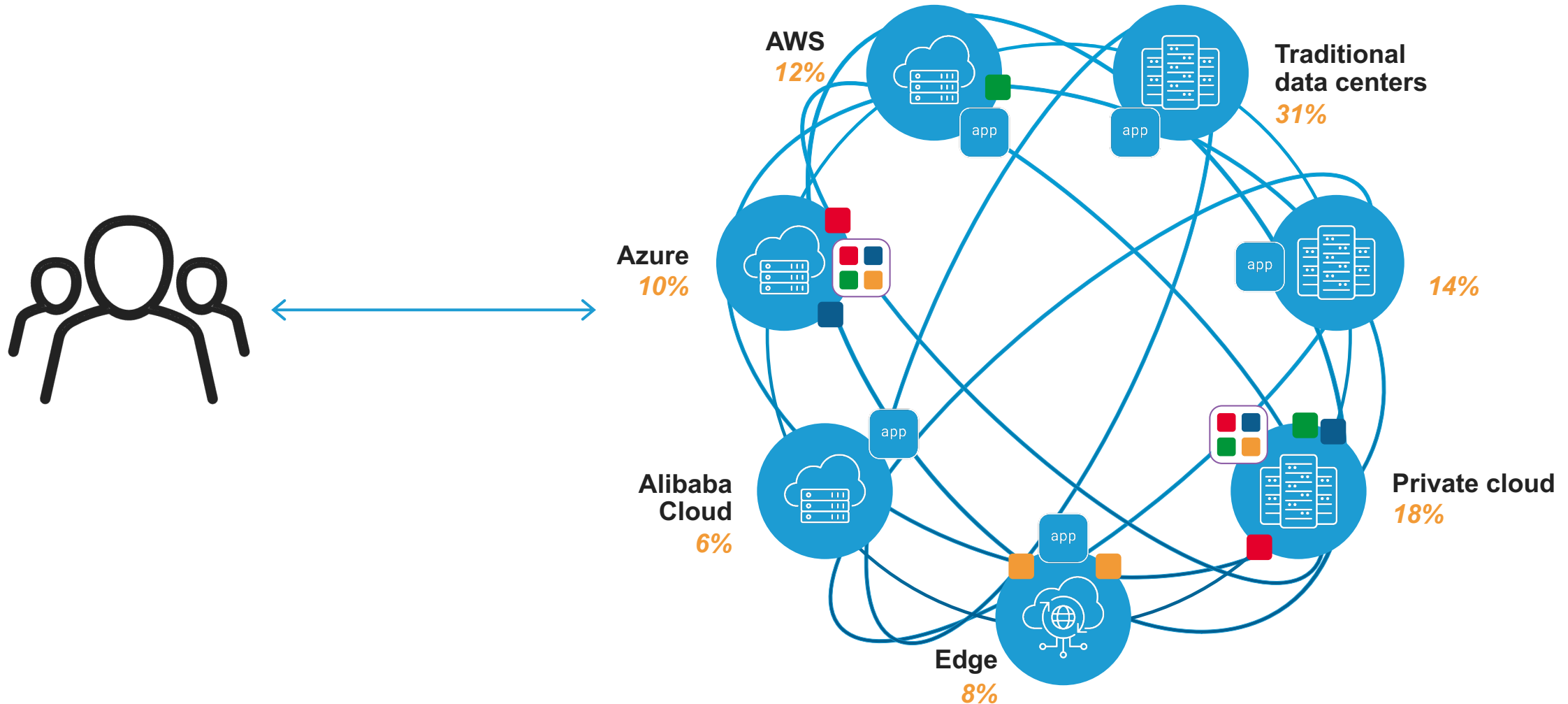
APIs and app-to-app connections have increased complexity

- AWS 12%
- Traditional data centers 31%
- Azure 10%
- Colocation 14%
- Alibaba Cloud 6%
- 18%
- Edge 8%
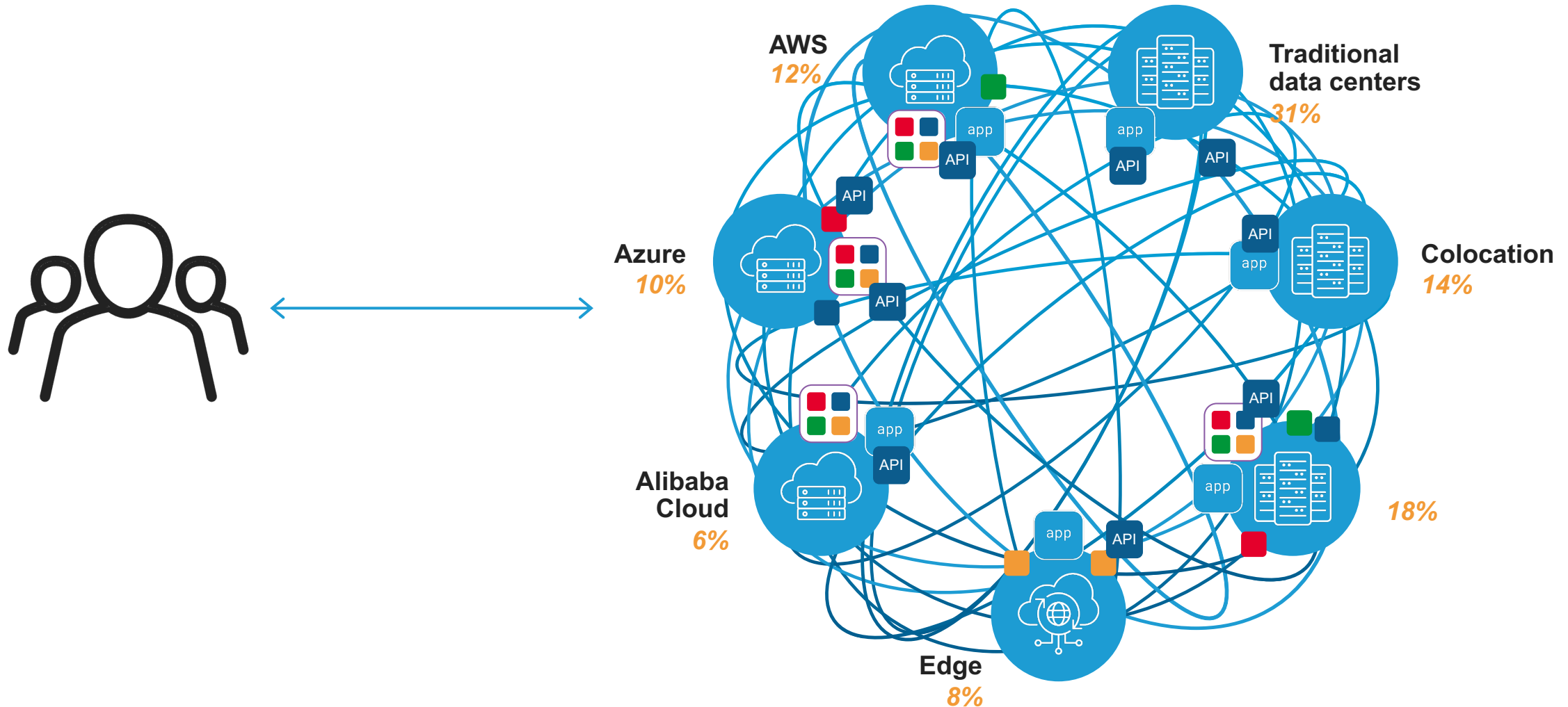
Lastly, expanded attack surfaces and increased attacker sophistication have made security more difficult

AWS
12%

Traditional data centers
31%

Azure
10%

Colocation
14%

Alibaba Cloud
6%

Private cloud
18%

Edge
8%

This is where we thought we would be...
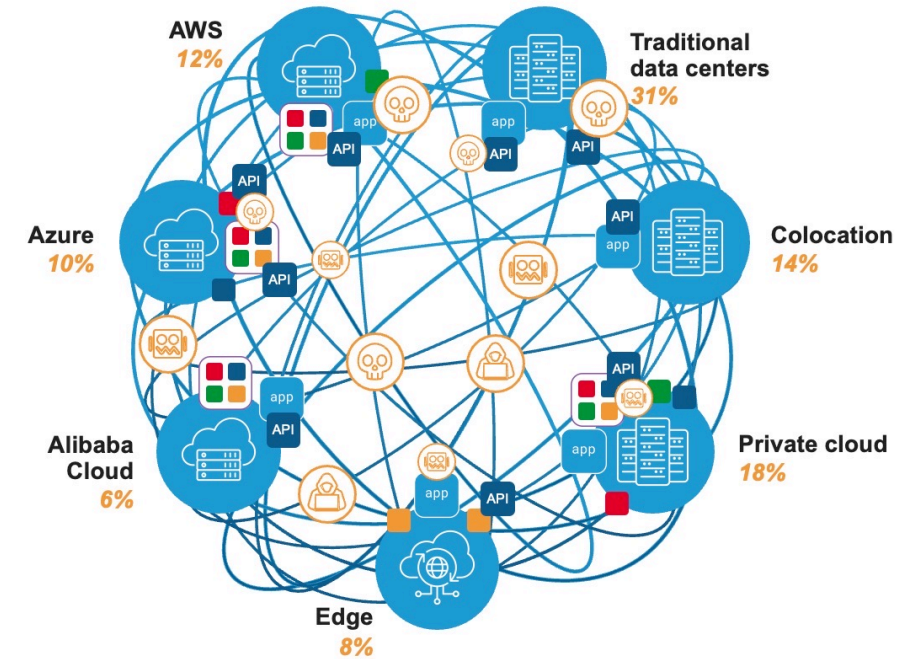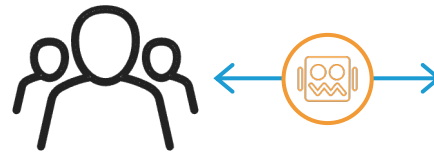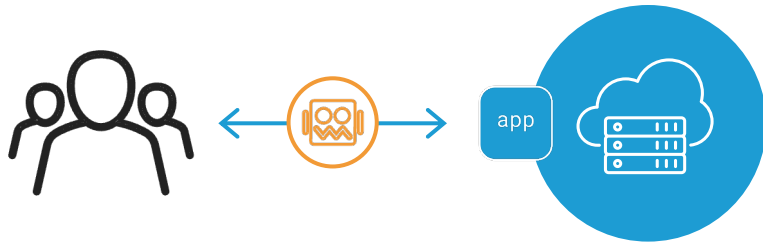
and this is where we have ended up

AWS 12%

Azure 10%

Alibaba Cloud 6%

Edge 8%

Traditional data centers 31%

Colocation 14%

Private cloud 18%

I thought F5 made load balancers – how can you help with this challenge?

We refactored BIG-IP for pure software and cloud environments

BIG-IP

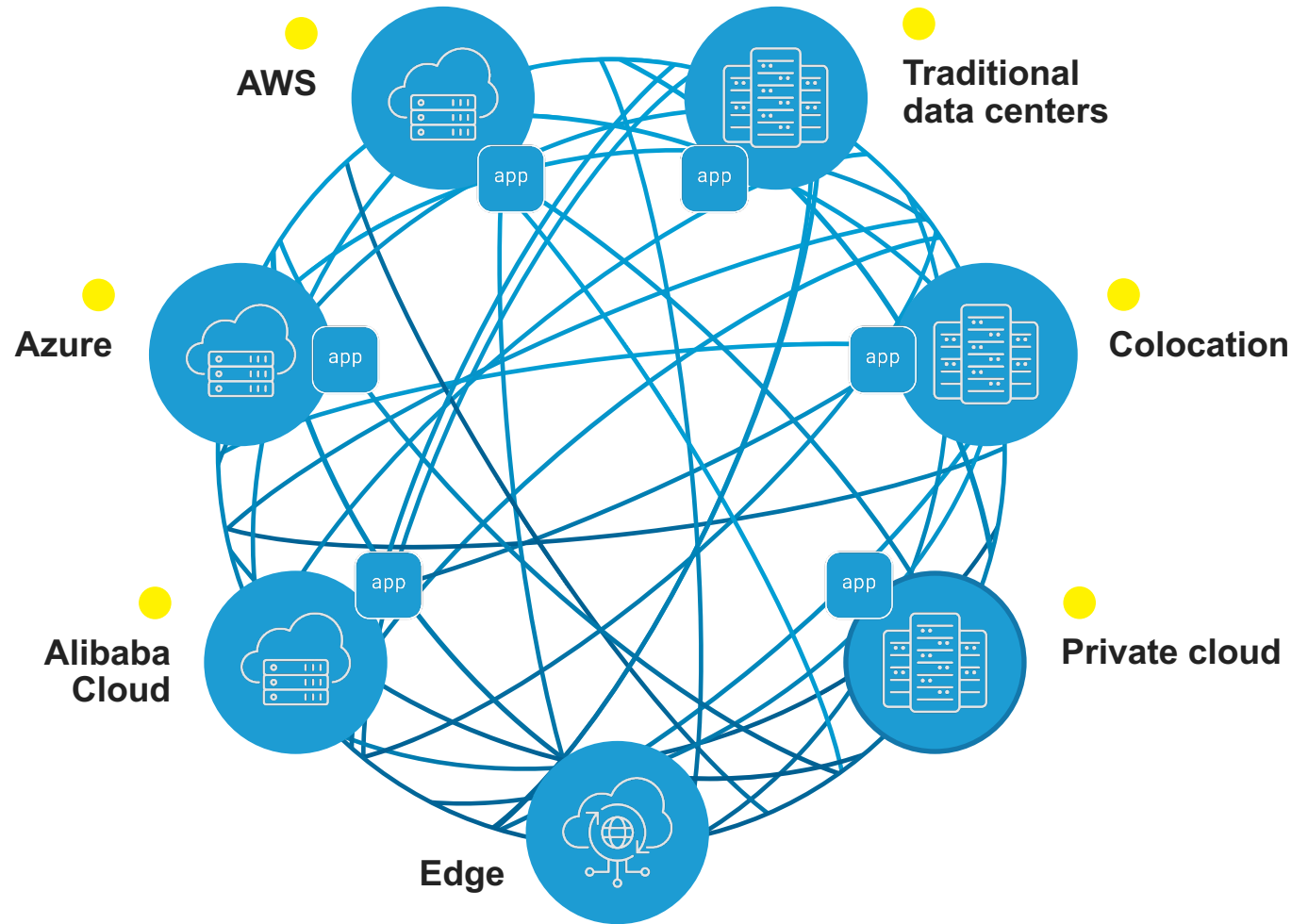An enterprise-class application delivery controller that secures and delivers traditional applications in on-premises, hybrid, and multi-cloud environments.

AWS

Traditional data centers

Azure

Colocation

Alibaba Cloud

Private cloud

Edge

We acquired NGINX to power apps and APIs in containerized environments
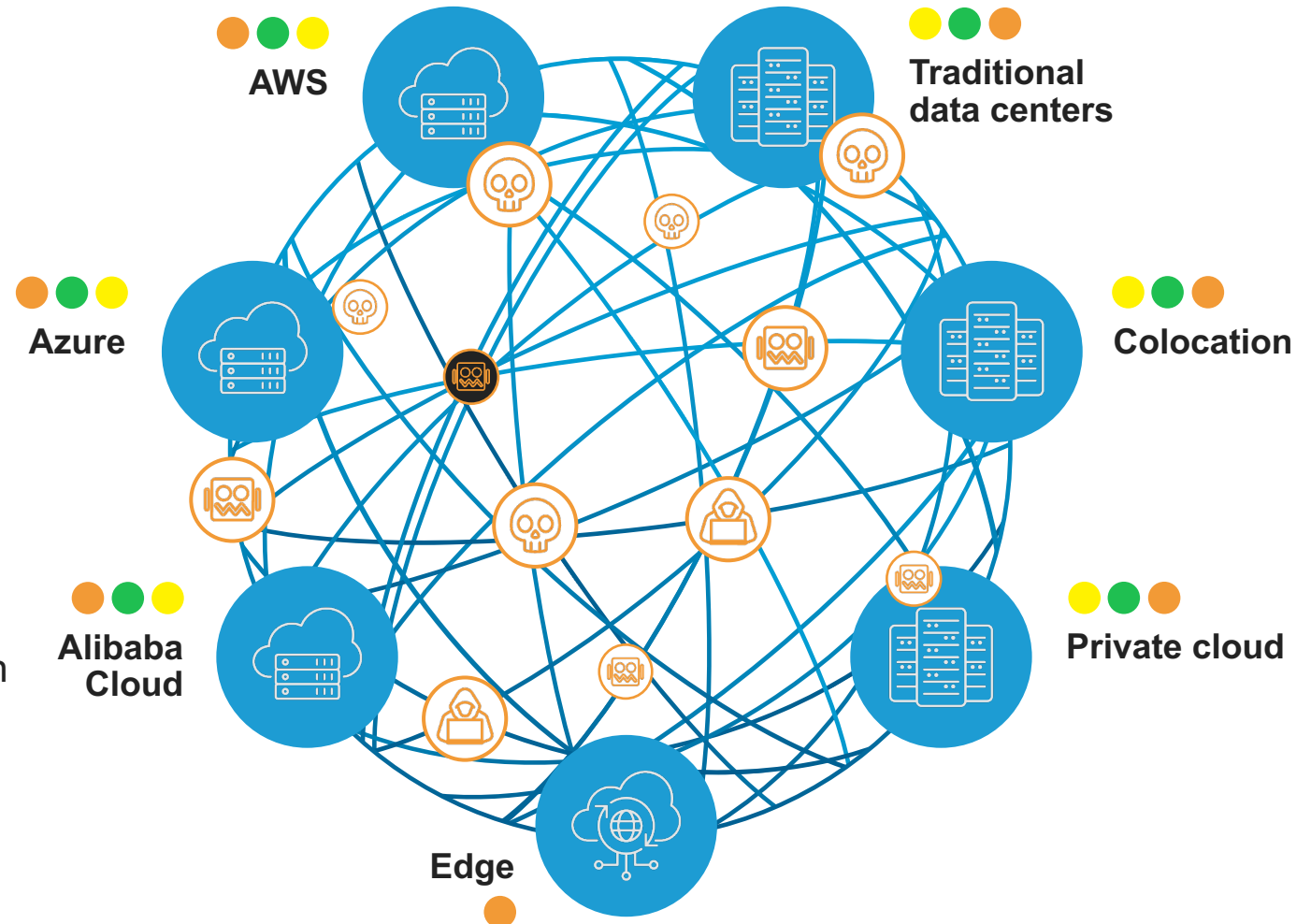
- BIG-IP

- **NGINX**

  Cloud-native, Kubernetes-friendly open source and enterprise solutions that drive mission-critical apps and APIs with scalability, visibility, security, and governance.

AWS

Azure

Alibaba Cloud

Edge

Traditional data centers

Colocation

Private cloud

©2023 F5
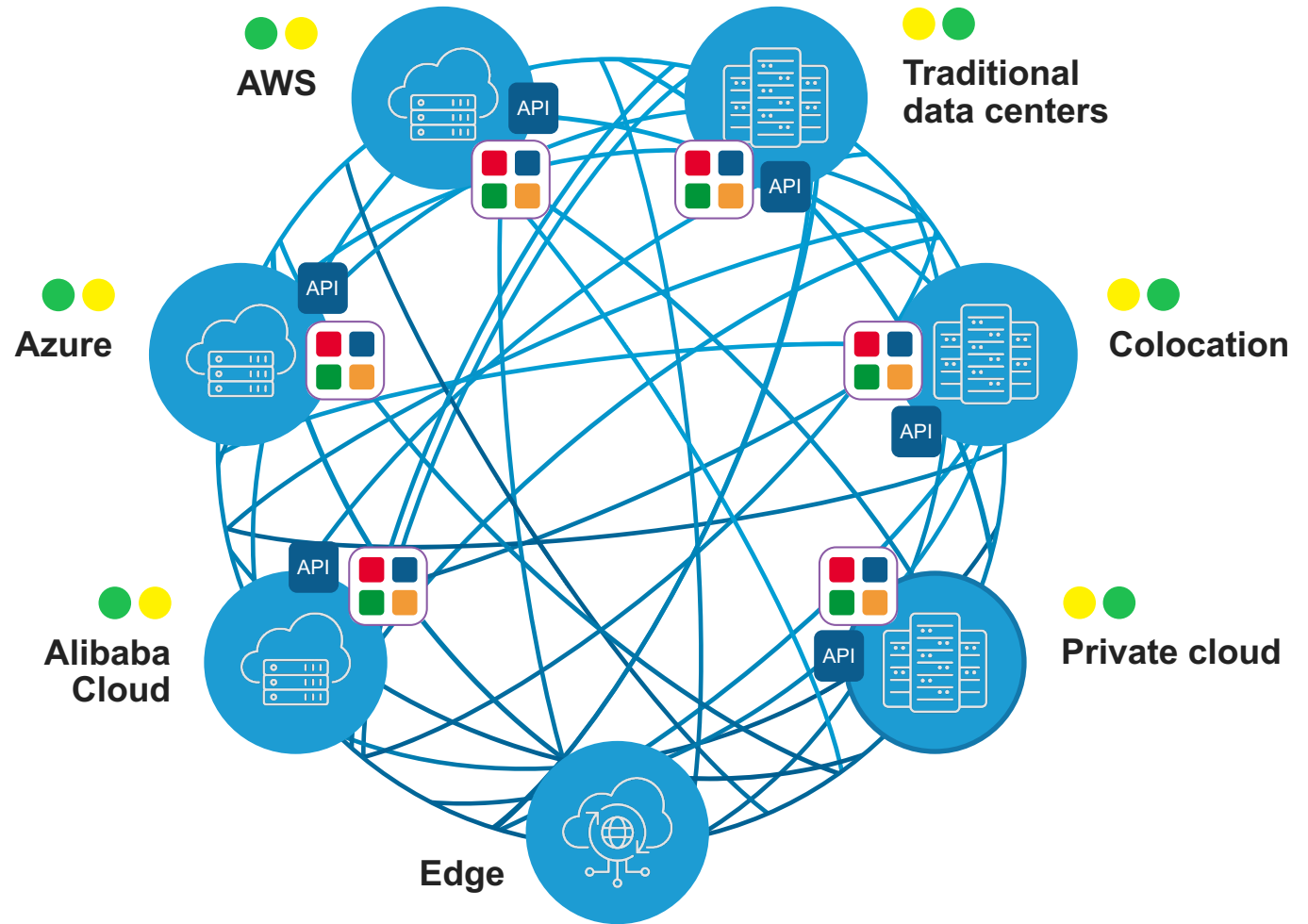
We enhanced our app security portfolio by acquiring Shape

- ● BIG-IP
- ● NGINX
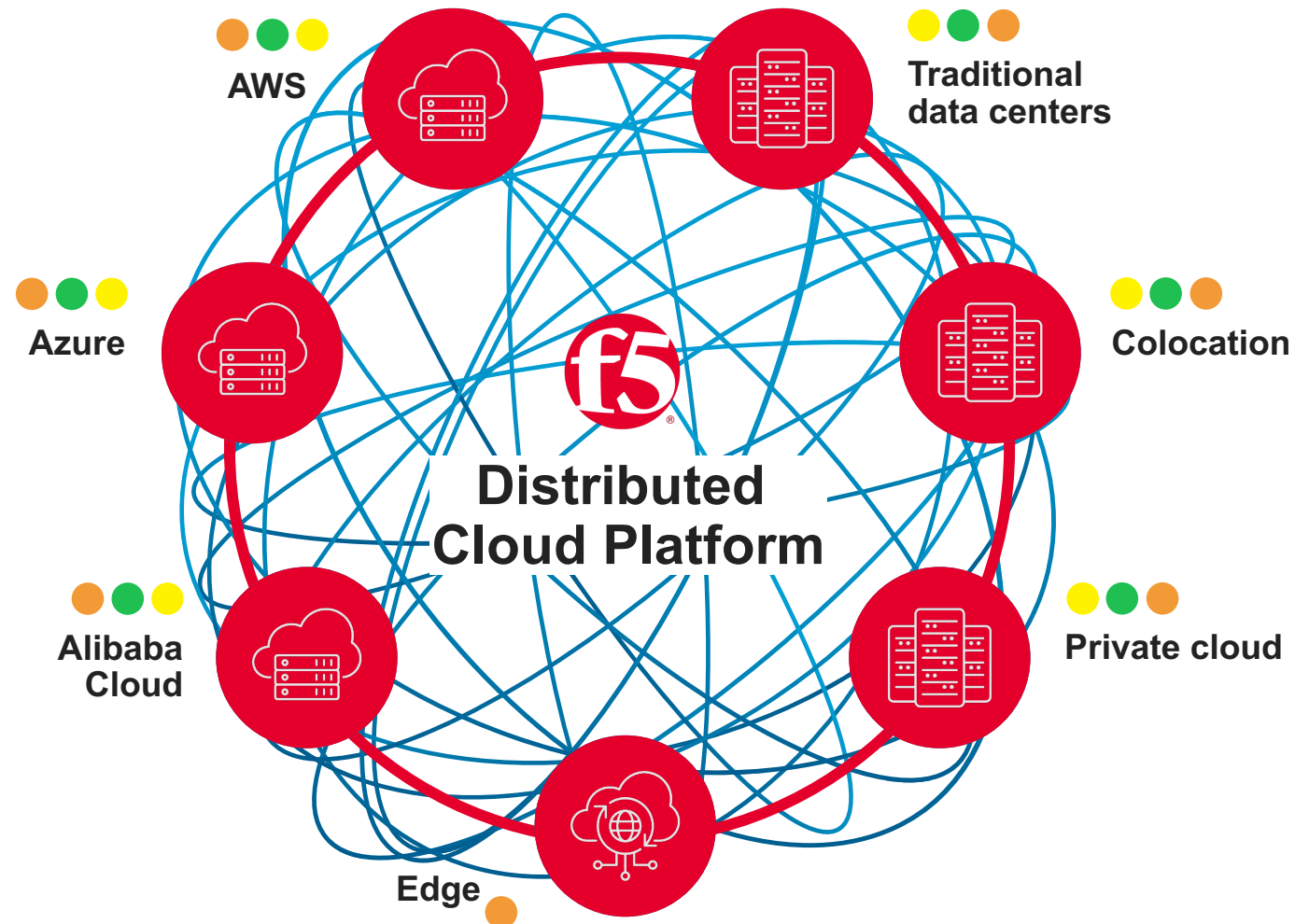- ● **Enhanced App Security**

Multiple layers of security controls for modern and legacy apps. Industry-leading WAF and DDoS protection augmented with highly efficacious mitigation of bot attacks and digital fraud, as well as protection of app infrastructure through advanced telemetry and behavioral analysis.

AWS

Traditional data centers

Azure

Colocation

Alibaba Cloud

Private cloud

Edge

©2023 F5

Presenting:
Distributed Cloud

- BIG-IP

- NGINX

- Enhanced App Security
(WAF, anti-bot, DDoS)

- **Distributed Cloud Platform**

A SaaS-based service delivery platform that **automates** the deployment of app security services, app delivery across locations, app-to-app networking, and deployment in containers-as-a-service for distributed workloads.

AWS

Traditional data centers

Azure

Colocation

Distributed Cloud Platform

Alibaba Cloud

Private cloud

Edge

©2023 F5

Introducing F5 Distributed Cloud Services

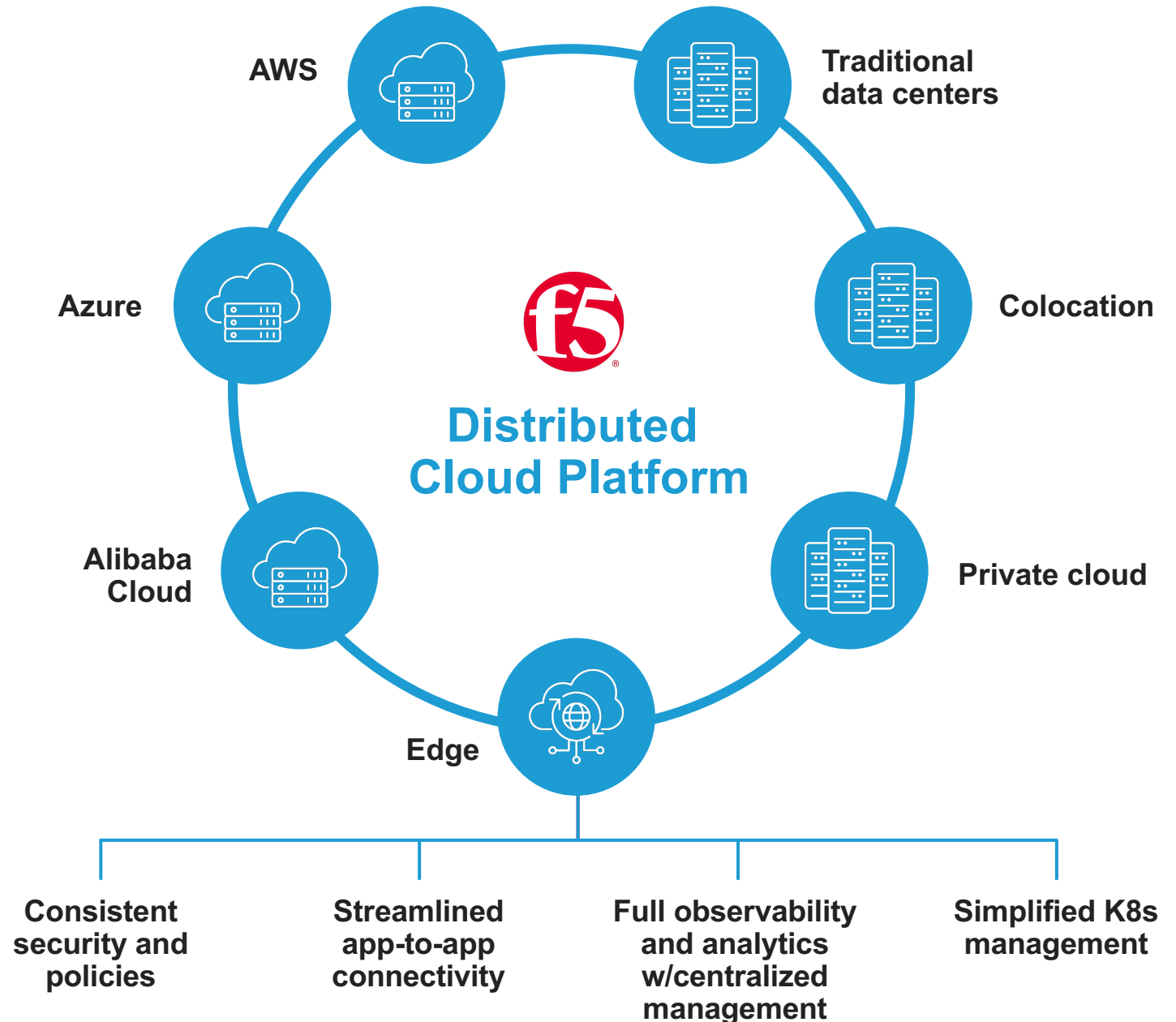©2022 F5

Introducing F5 Distributed Cloud

A SaaS-based service delivery platform that ***automates*** the deployment of app security services, app delivery across locations, app-to-app networking, and deployment in containers-as-a-service for distributed workloads.

AWS

Traditional data centers

Azure
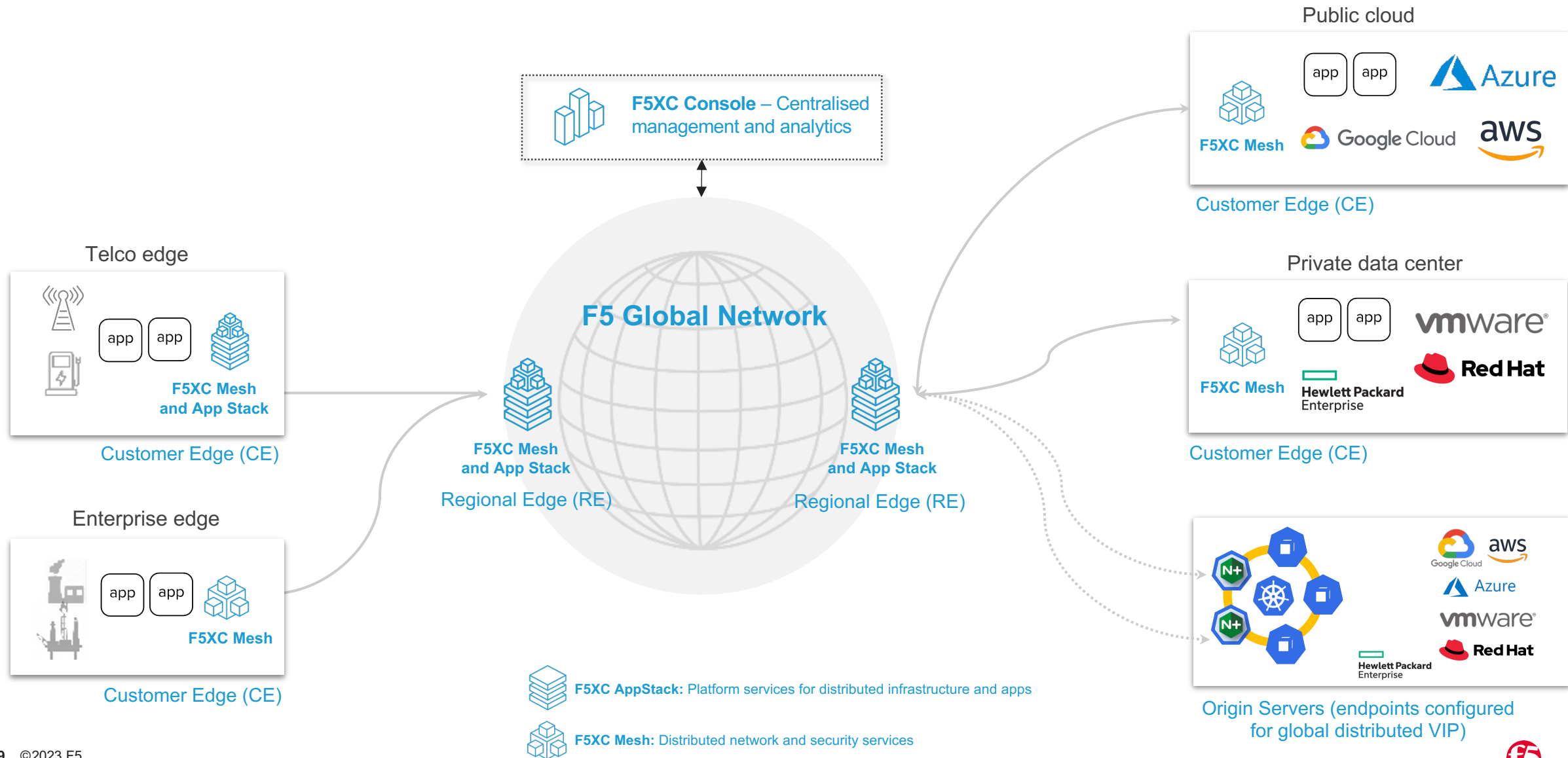
Distributed Cloud Platform

Colocation

Alibaba Cloud

Private cloud

Edge

Consistent security and policies

Streamlined app-to-app connectivity

Full observability and analytics w/centralized management

Simplified K8s management

©2023 F5

App Services with a global footprint

Public cloud

F5XC Mesh
Azure | Google Cloud | aws
app | app

Customer Edge (CE)

F5XC Console – Centralised management and analytics

F5 Global Network

F5XC Mesh and App Stack
Regional Edge (RE)

F5XC Mesh and App Stack
Regional Edge (RE)

Telco edge

app | app
F5XC Mesh and App Stack

Customer Edge (CE)

Enterprise edge

app | app
F5XC Mesh

Customer Edge (CE)

Private data center

F5XC Mesh
vmware | Red Hat | Hewlett Packard Enterprise
app | app

Customer Edge (CE)

Origin Servers (endpoints configured for global distributed VIP)
Google Cloud | aws | Azure | vmware | Red Hat | Hewlett Packard Enterprise

F5XC AppStack: Platform services for distributed infrastructure and apps

F5XC Mesh: Distributed network and security services

Use Case – DC to Public Cloud Migration

©2022 F5

Current state of cloud migrations

- Deploy workload in cloud

- Enable connectivity between client and cloud workloads

- Migrate client traffic to cloud, rollback if necessary

Pain points

- NAT/firewall configuration is time consuming, error prone, and costly

- Difficult to correlate firewall rules with applications

- Rollback can take time

Repeat if another migration is required
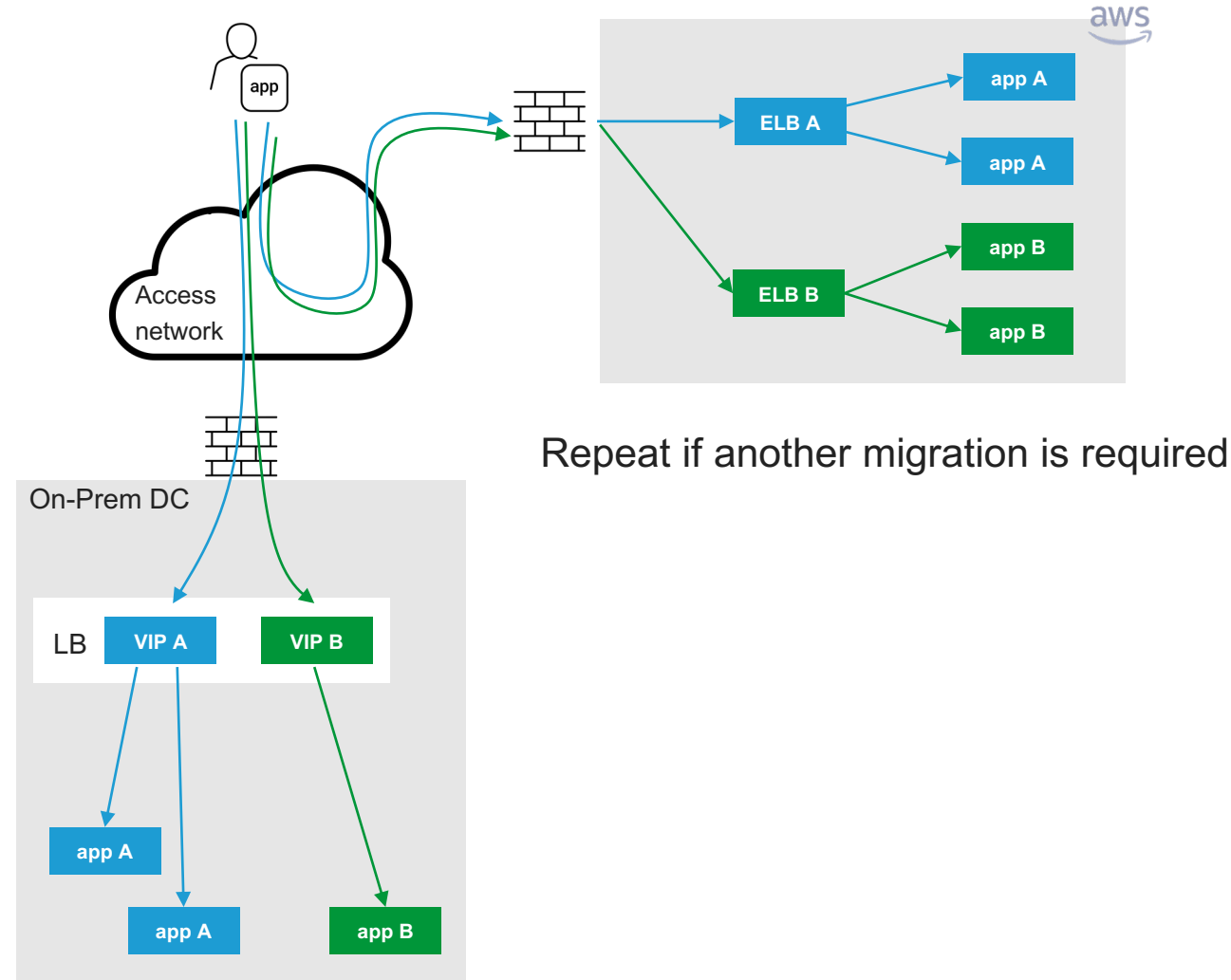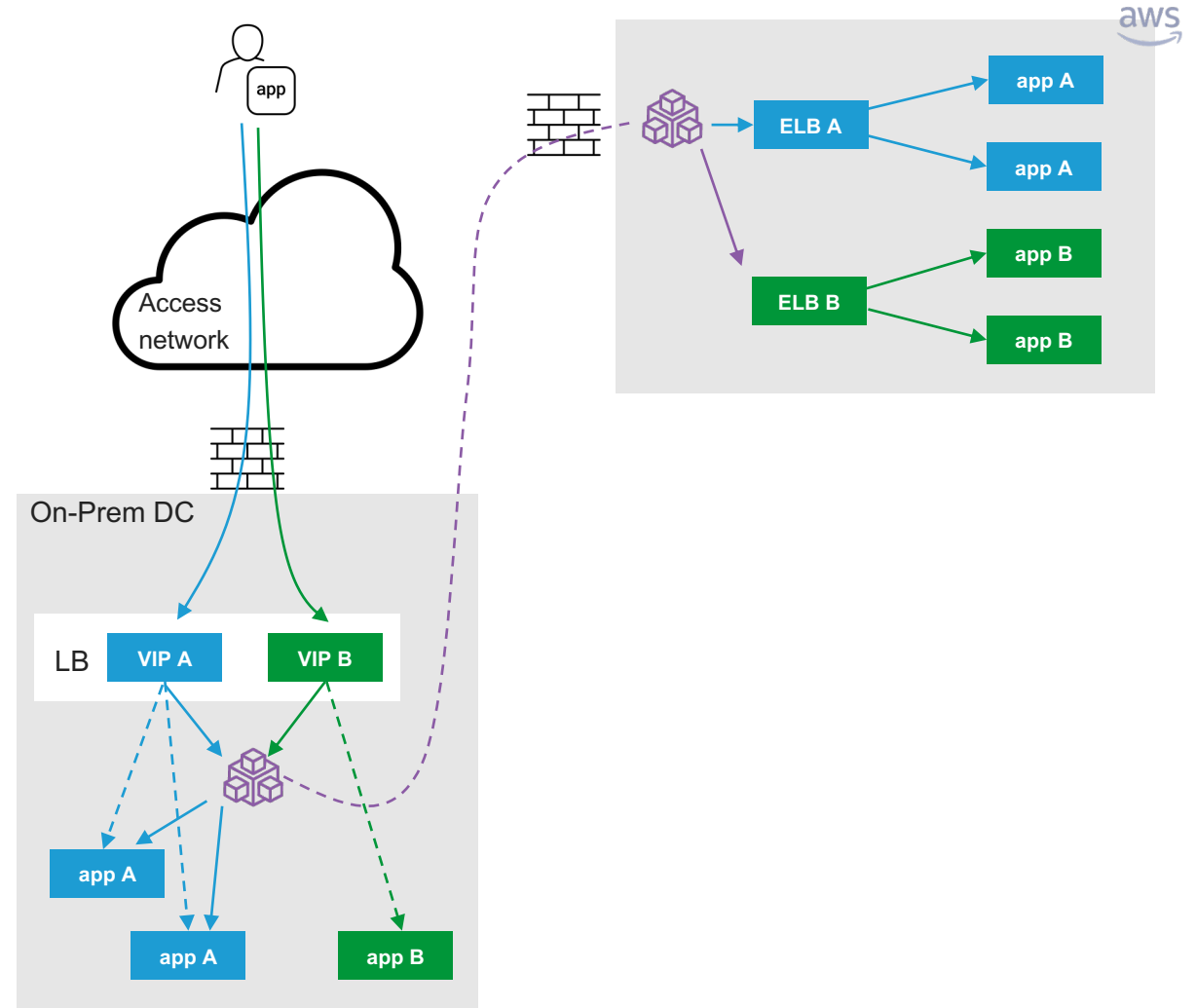
Migrating with F5 Distributed Cloud Mesh

Stage 1 – migrate workloads to cloud

- Direct traffic destined for DC workload to the cloud

- Transparent to clients

- Fully configured through Console
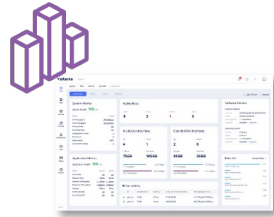
Benefits

- Standardized and low-touch DC to cloud connectivity

- One NAT/firewall burn between DC and cloud CEs

- App teams control traffic flow - "Try before you buy"

- Visibility of workload performance and security

Migrating with F5 Distributed Cloud Mesh

Stage 1 – migrate workloads to cloud (Alternate option)

- Hijack traffic destined for DC load balancers

- CE to advertise more specific routes for workload VIPs to DC router via BGP

- Simple rollback procedure – withdraw route advertisement
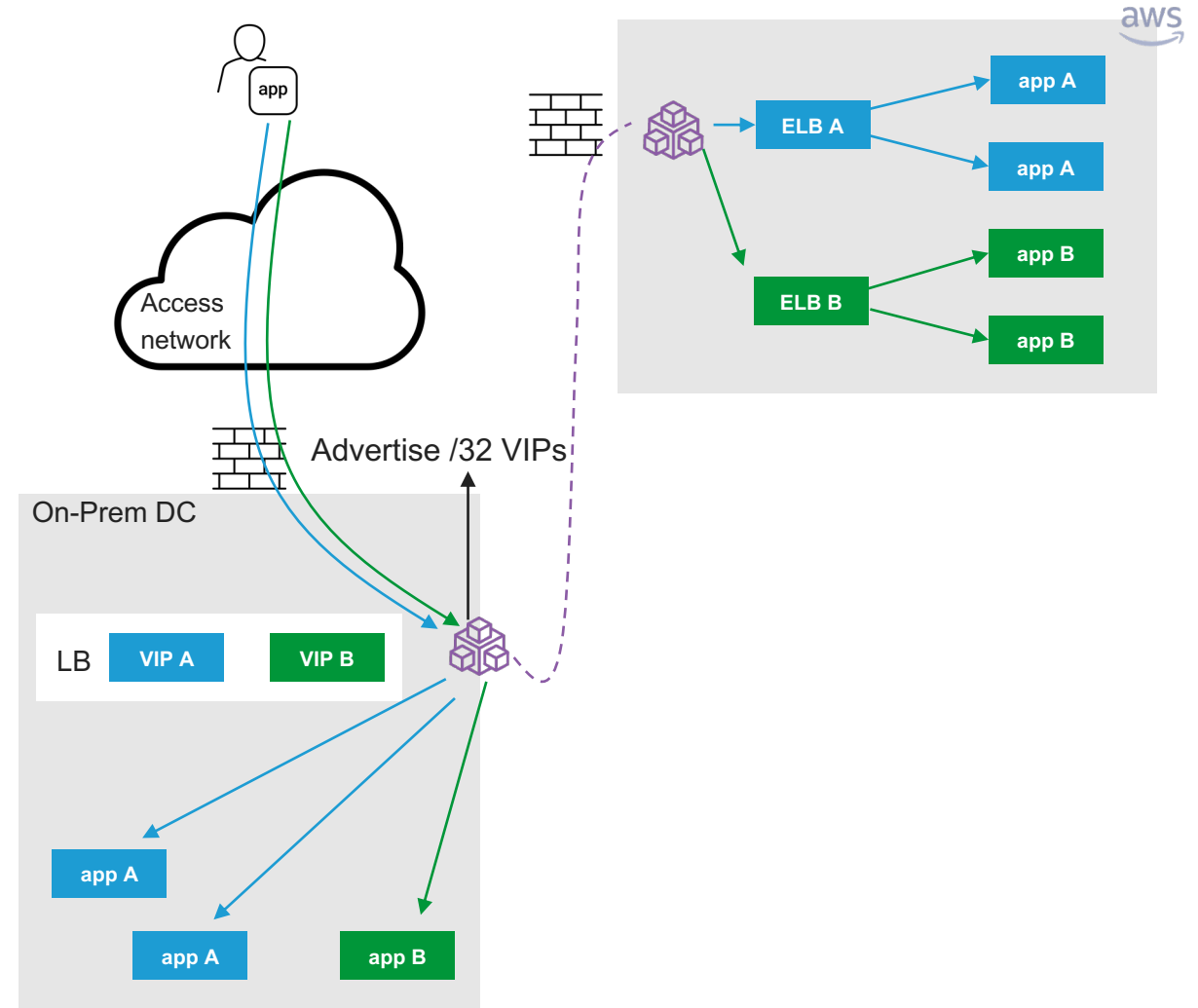
Migrating with F5 Distributed Cloud Mesh

Stage 2 – direct clients to cloud

- Once cloud workload is performing satisfactorily, migrate clients to new VIP on CE

- Any CE can be ingress

    - Direct access through VIP on cloud CE

    - Deploy CE in access network

- Seamless introduction of workloads in new environment
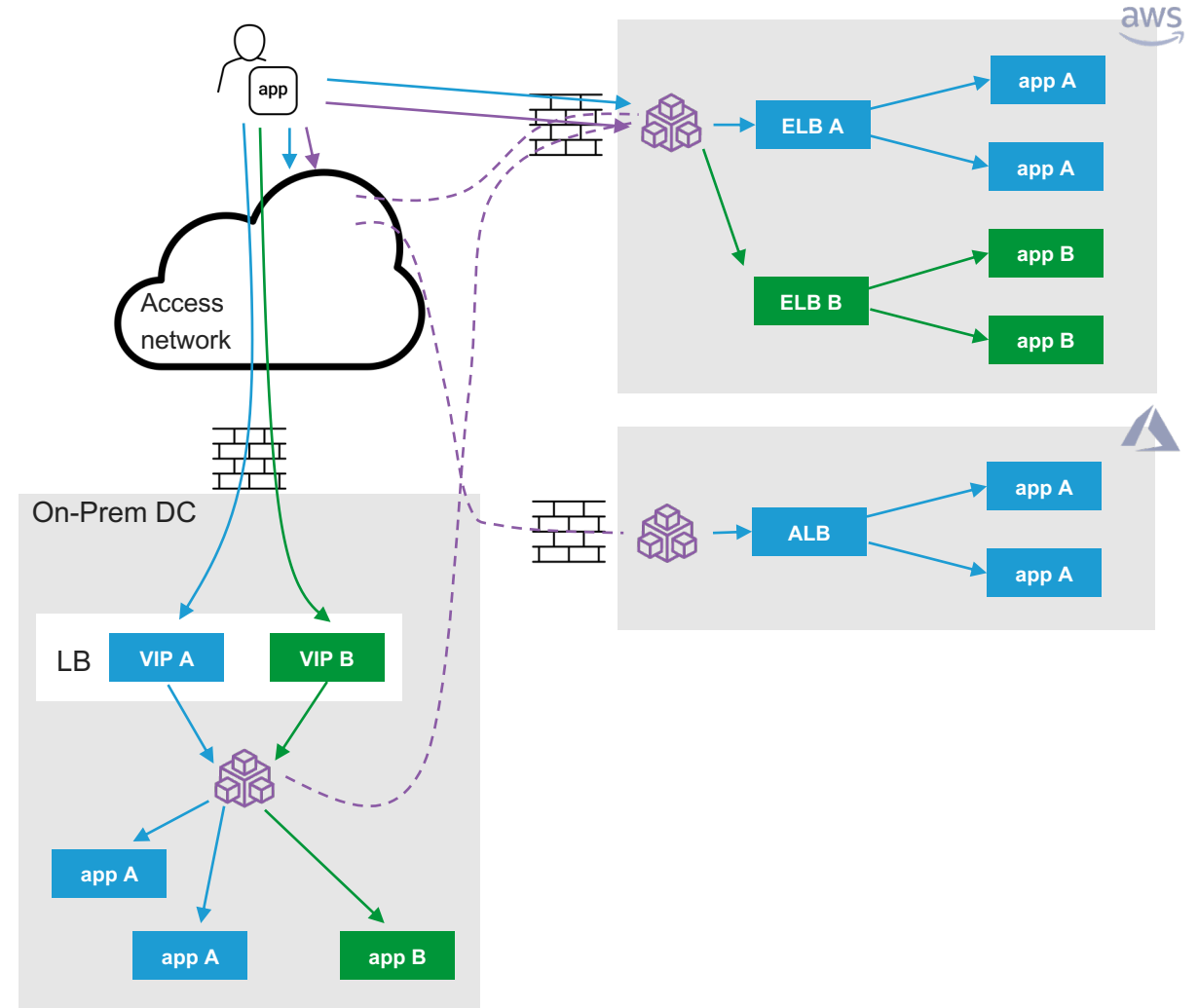
Outcome
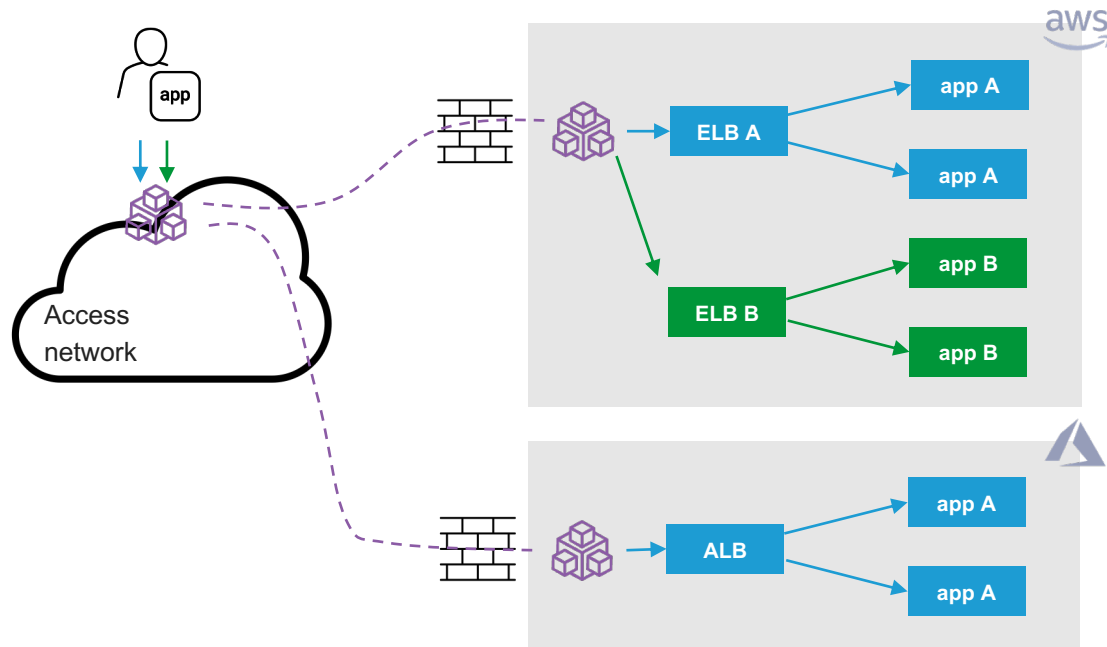
- Standardized workload migration to any cloud

- Application teams can control where the workloads are running, and where to access them

- Security teams can implement common security policies across all environments

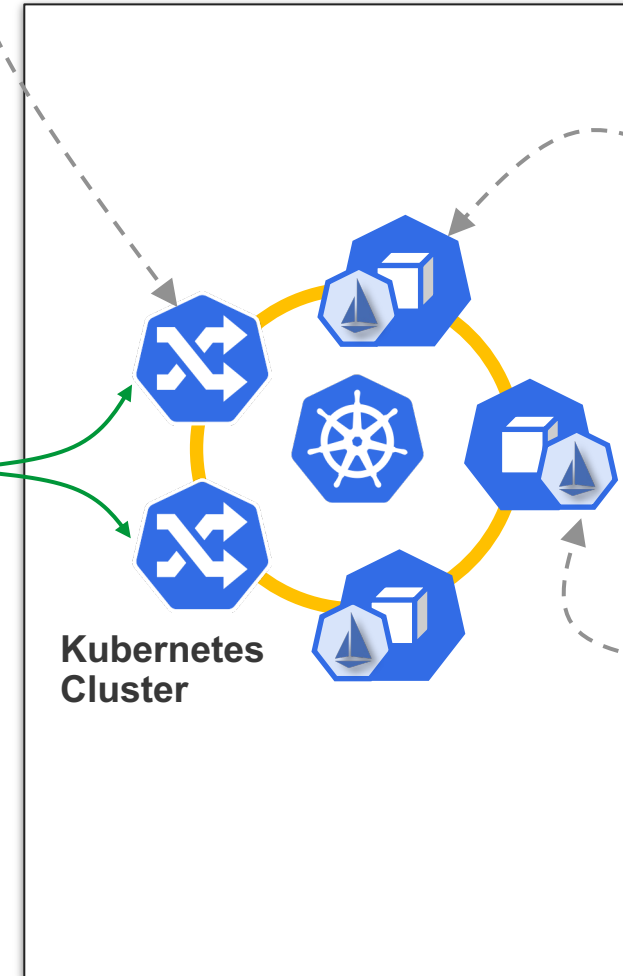- Single pane of glass to monitor workload performance and security

©2023 F5

Use Case – Protecting microservices
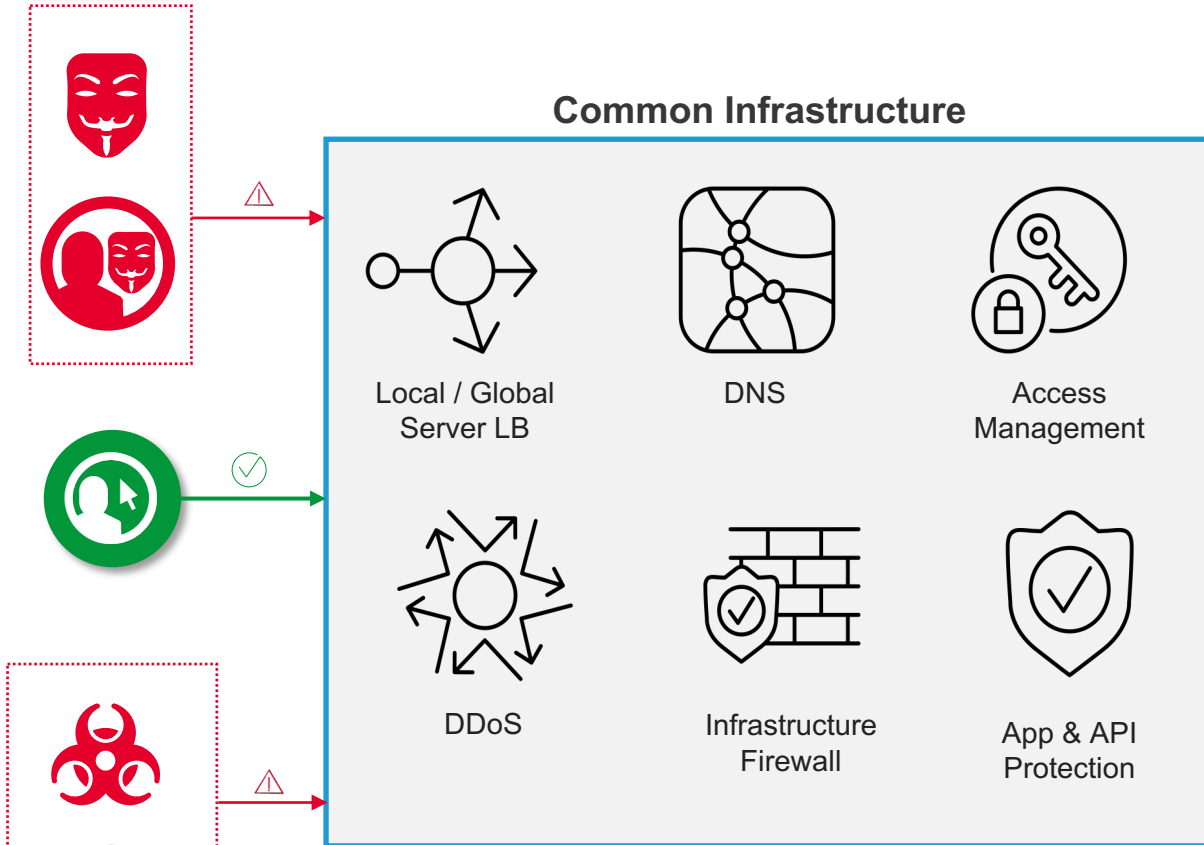
App Services in a Modern Architecture

Ingress (with API Gateway)
- Layer 7 routing for traffic entry point coming into Kubernetes
- Built for HTTP traffic. TCP/UDP for non-HTTP traffic
- May include API Gateway implementation

Common Infrastructure

Local / Global Server LB

DNS

Access Management

DDoS

Infrastructure Firewall

App & API Protection

Kubernetes Cluster
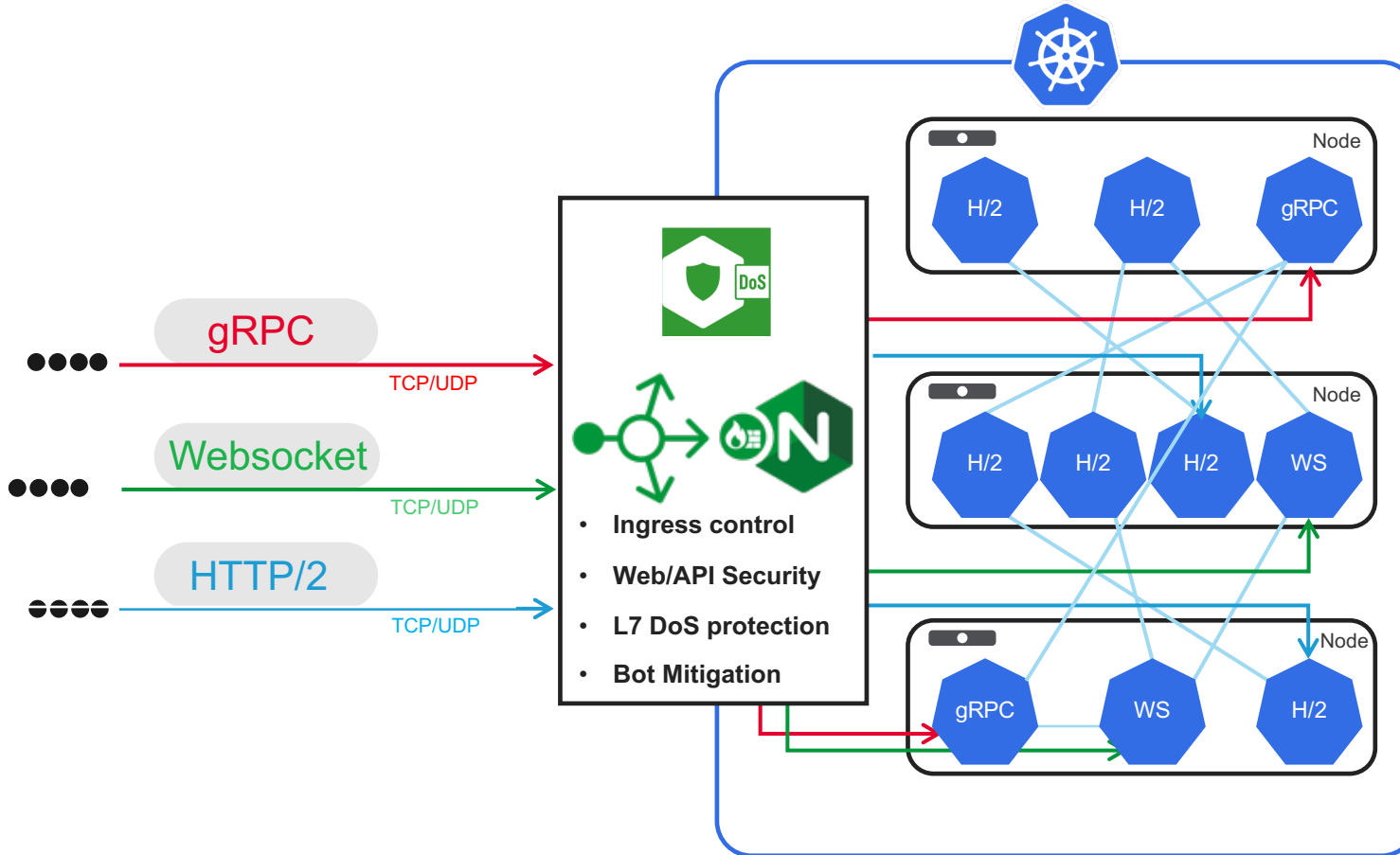
Pods
- Runs app in a container / CNF

Service Mesh
- Open Source Service Mesh implementation (Istio)
- Injects Sidecar to every pod
- Enforces routing, security with mTLS, etc.
- Provides traceability of pod communication

Cloud Microservices PaaS
- On-prem private cloud (e.g: VMware)
- Public cloud (e.g: AWS, Azure, GCP)

App Services in micro-service environment

Capabilities:

- DoS protection for:
  - HTTP
  - gRPC
  - Websocket
- Web application and API security
- Bot Mitigation
- OpenAPI Spec (Swagger) enforcement
- Attack Signature/Schema Validation inside:
  - HTTP
  - XML
  - JSON
  - gRPC
  - Websockets
  - GraphQL
- TCP SYN flood protection via eBPF
- Comprehensive Ingress and AuthN/AuthZ capabilities

Deployment:

- NGINX Ingress Controller
  - (Kubernetes native manifest)

©2023 F5

Protecting services at ingress and globally

Domestic (country-level request)

DNS Query: app.domain.com

DNS Response: app.domain.com X.X.X.X

app.domain.com CNAME app.global.domain.com

GSLB NS ns1.f5clouddns.com

NS ns2.f5clouddns.com

DNS Query: app.domain.com

DNS Response: app.domain.com Y.Y.Y.Y

Rest of the world

Y.Y.Y.Y (Anycast globally)

Volumetric L3/L4 protection using TCP proxy

F5 Distributed Cloud

26 Global PoPs
21 metro cities
Dedicated IX connectivity

18+ Tbps capacity
Top 50 IPv4 Global Peering
Top 10 IPv6 Global Peering

X.X.X.X

Ingress, WAF, Bot and L7 DoS protection

SNAT from global F5 Distributed Cloud POPs

Ingress Server: nginx-ingress-controller
Namespace: nginx-ingress

N+

Origin Server: app service
Namespace: app

A force for a better digital world