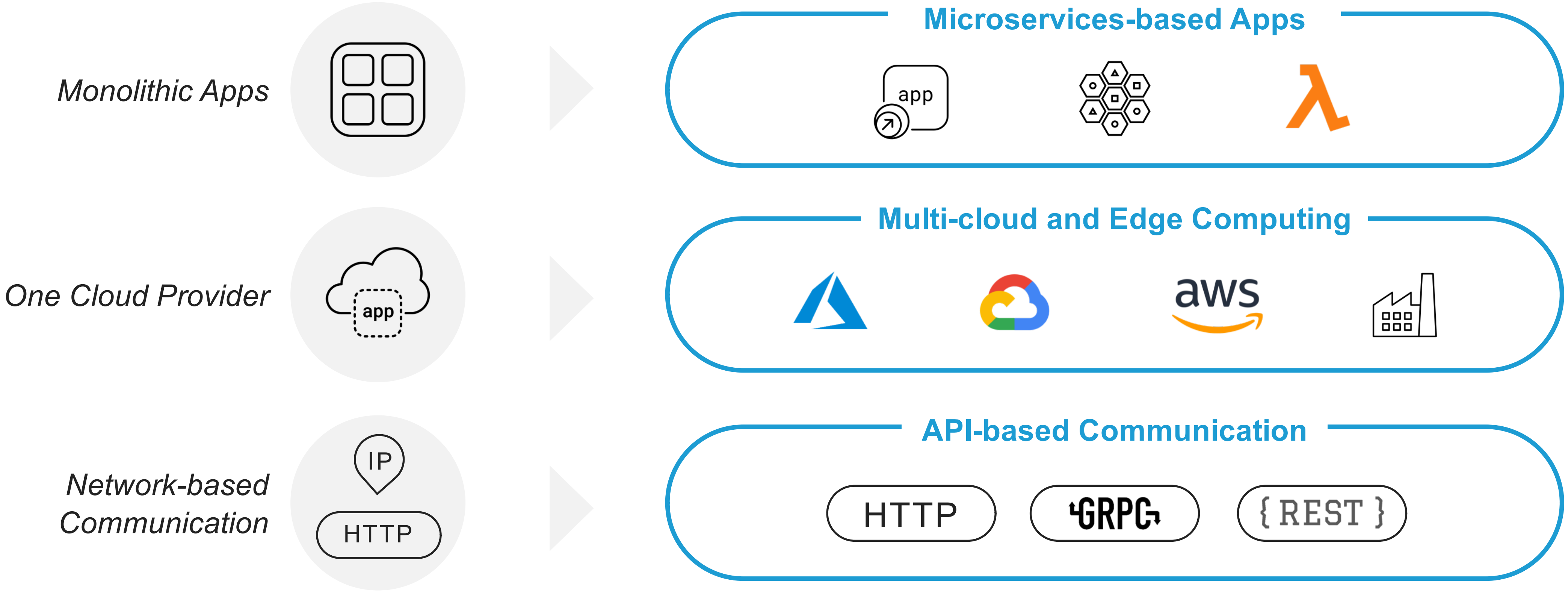
F5 Distributed Cloud

Martin Oravec
Systems Engineer

Fundamental shift in how apps are designed & deployed



Monolithic Apps

Microservices-based Apps

One Cloud Provider

Multi-cloud and Edge Computing

Network-based Communication

API-based Communication

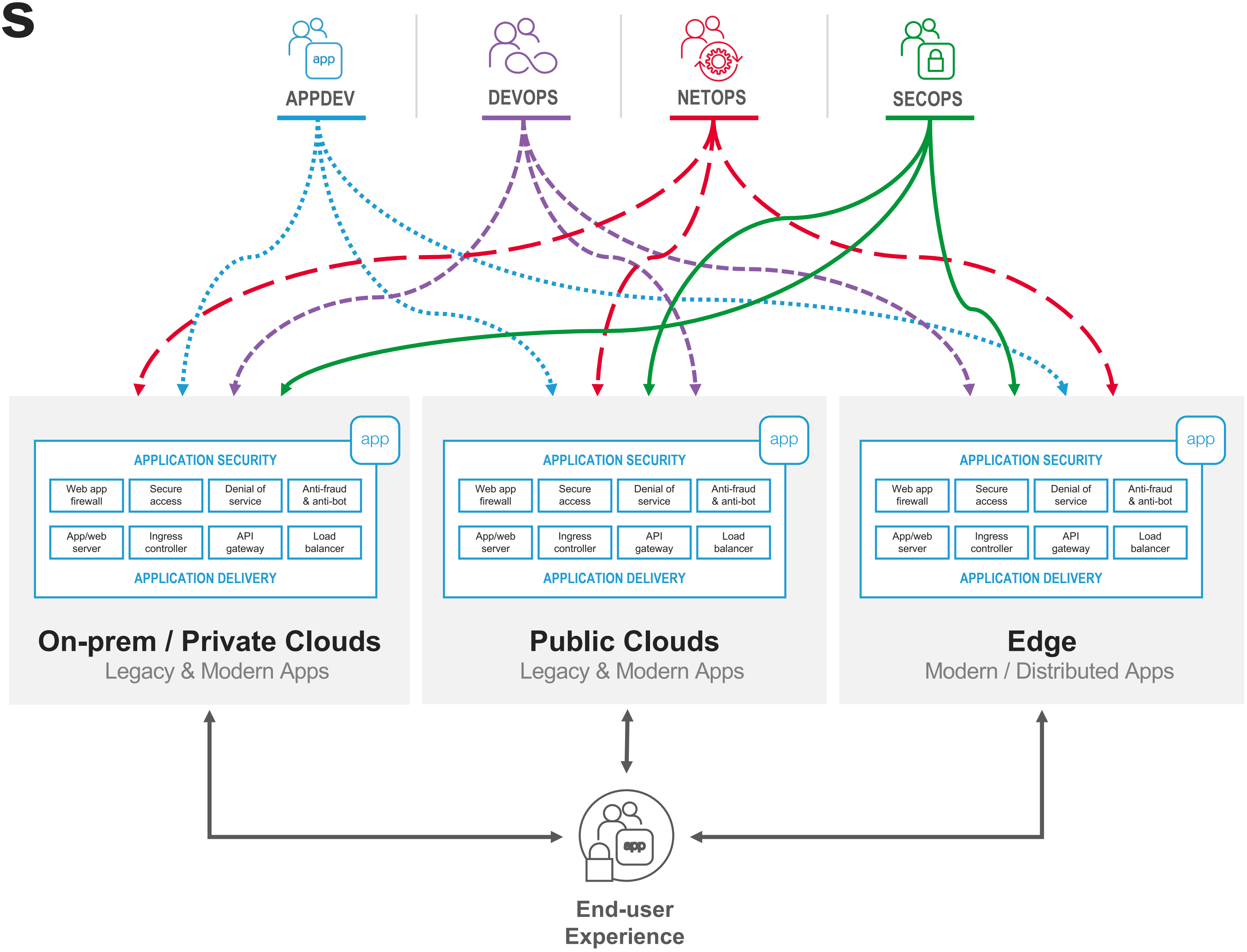
Technical challenges of delivering apps

#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’d telemetry trapped in disjointed systems & environments



APPLICATION SECURITY

Web app firewall	Secure access	Denial of service	Anti-fraud & anti-bot
App/web server	Ingress controller	API gateway	Load balancer

APPLICATION DELIVERY

On-prem / Private Clouds
Legacy & Modern Apps

APPLICATION SECURITY

Web app firewall	Secure access	Denial of service	Anti-fraud & anti-bot
App/web server	Ingress controller	API gateway	Load balancer

APPLICATION DELIVERY

Public Clouds
Legacy & Modern Apps

APPLICATION SECURITY

Web app firewall	Secure access	Denial of service	Anti-fraud & anti-bot
App/web server	Ingress controller	API gateway	Load balancer

APPLICATION DELIVERY

Edge
Modern / Distributed Apps

End-user Experience

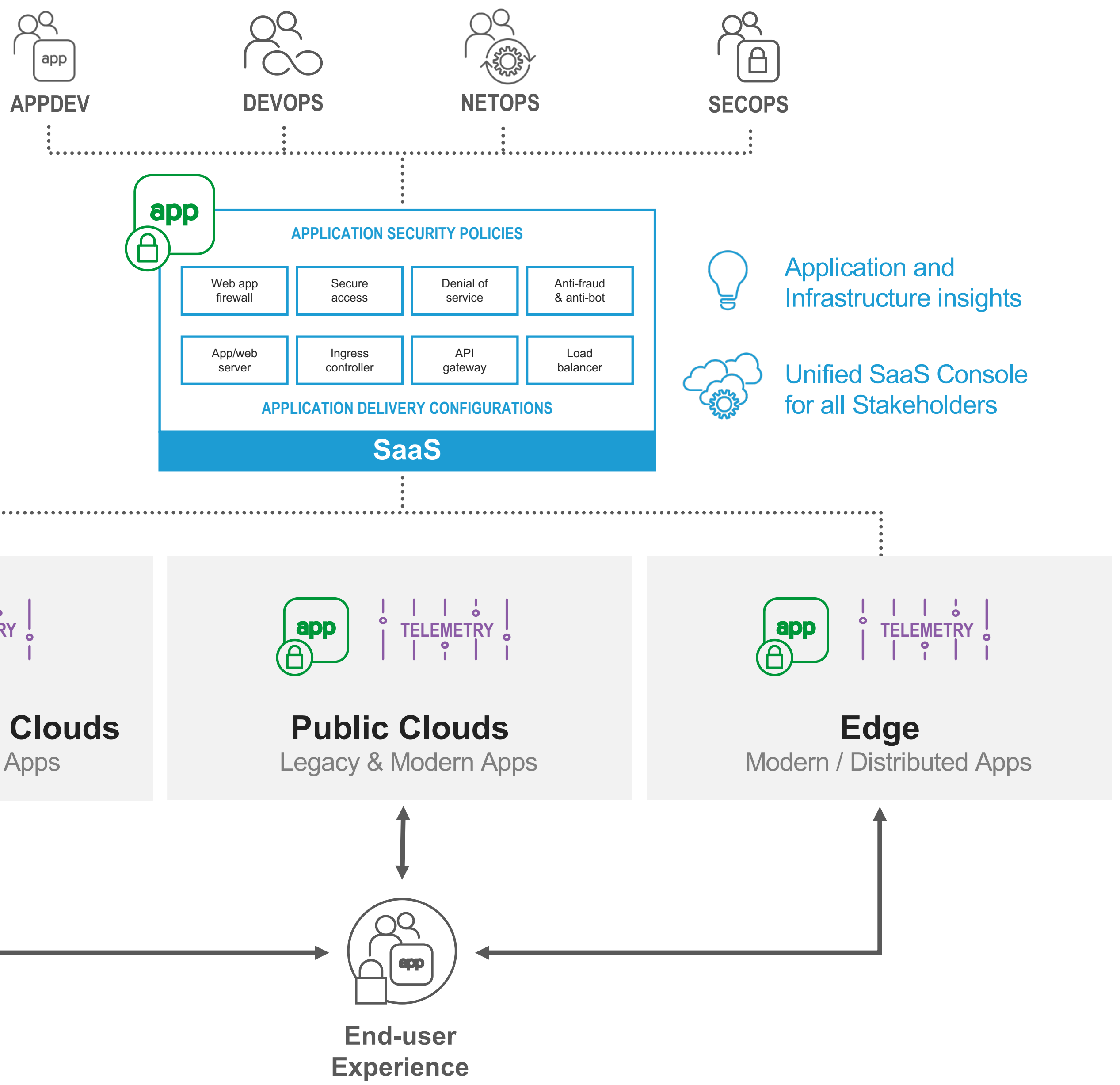
Distributed Cloud Services
for Modern App Delivery

#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



APPDEV

DEVOPS

NETOPS

SECOPS

app

APPLICATION SECURITY POLICIES

Web app firewall	Secure access	Denial of service	Anti-fraud & anti-bot
App/web server	Ingress controller	API gateway	Load balancer

APPLICATION DELIVERY CONFIGURATIONS

SaaS

Application and Infrastructure insights

Unified SaaS Console for all Stakeholders

app TELEMETRY

On-prem / Private Clouds
Legacy & Modern Apps

app TELEMETRY

Public Clouds
Legacy & Modern Apps

app TELEMETRY

Edge
Modern / Distributed Apps

app

End-user Experience

F5 BIG-IP

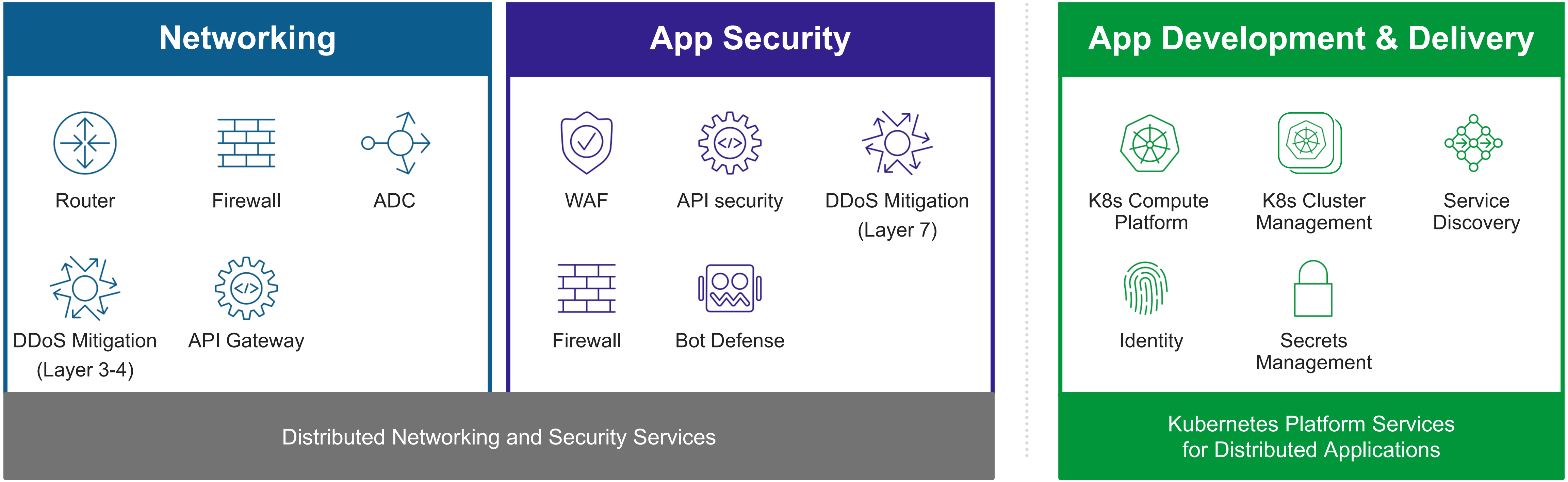
F5 Distributed Cloud Services

F5 NGINX

https://www.f5.com/company/news/press-releases/f5-protection-digital-world-f5-distributed-cloud-services

Key Building Blocks

Understanding the Critical Components



Networking

- Router
- Firewall
- ADC
- DDoS Mitigation (Layer 3-4)
- API Gateway

App Security

- WAF
- API security
- DDoS Mitigation (Layer 7)
- Firewall
- Bot Defense

Distributed Networking and Security Services

App Development & Delivery

- K8s Compute Platform
- K8s Cluster Management
- Service Discovery
- Identity
- Secrets Management

Kubernetes Platform Services for Distributed Applications

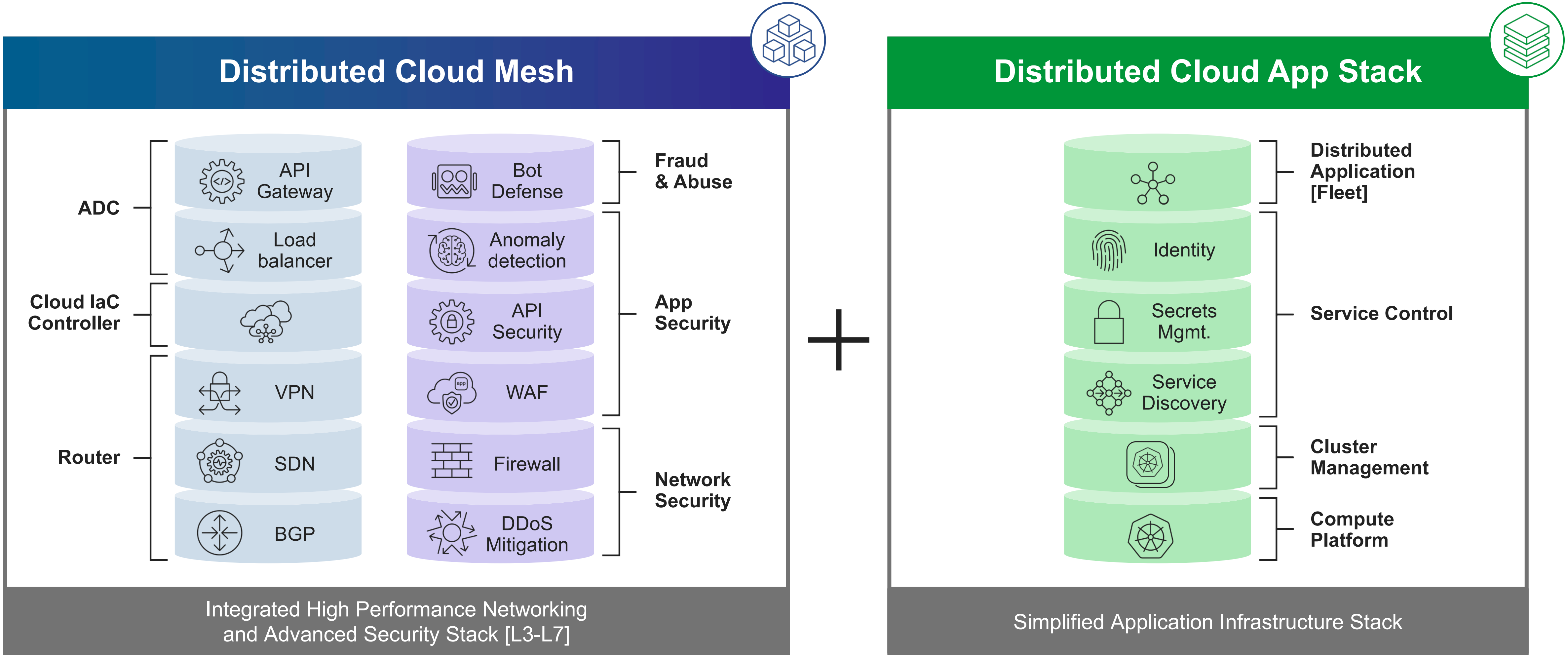
Distributed Cloud Console

SaaS-based centralized console managing application lifecycle and visibility

- Visibility and Analytics
- Centralized Operations
- Artificial Intelligence/ Advanced Insights

A Distributed Node Architecture

Flexible deployment options across cloud and edge sites



Distributed Cloud Mesh

ADC
- API Gateway
- Load balancer

Cloud IaC Controller

Router
- VPN
- SDN
- BGP

Fraud & Abuse
- Bot Defense

App Security
- Anomaly detection
- API Security
- WAF

Network Security
- Firewall
- DDoS Mitigation

Integrated High Performance Networking
and Advanced Security Stack [L3-L7]

+

Distributed Cloud App Stack

Distributed Application [Fleet]

Service Control
- Identity
- Secrets Mgmt.
- Service Discovery

Cluster Management

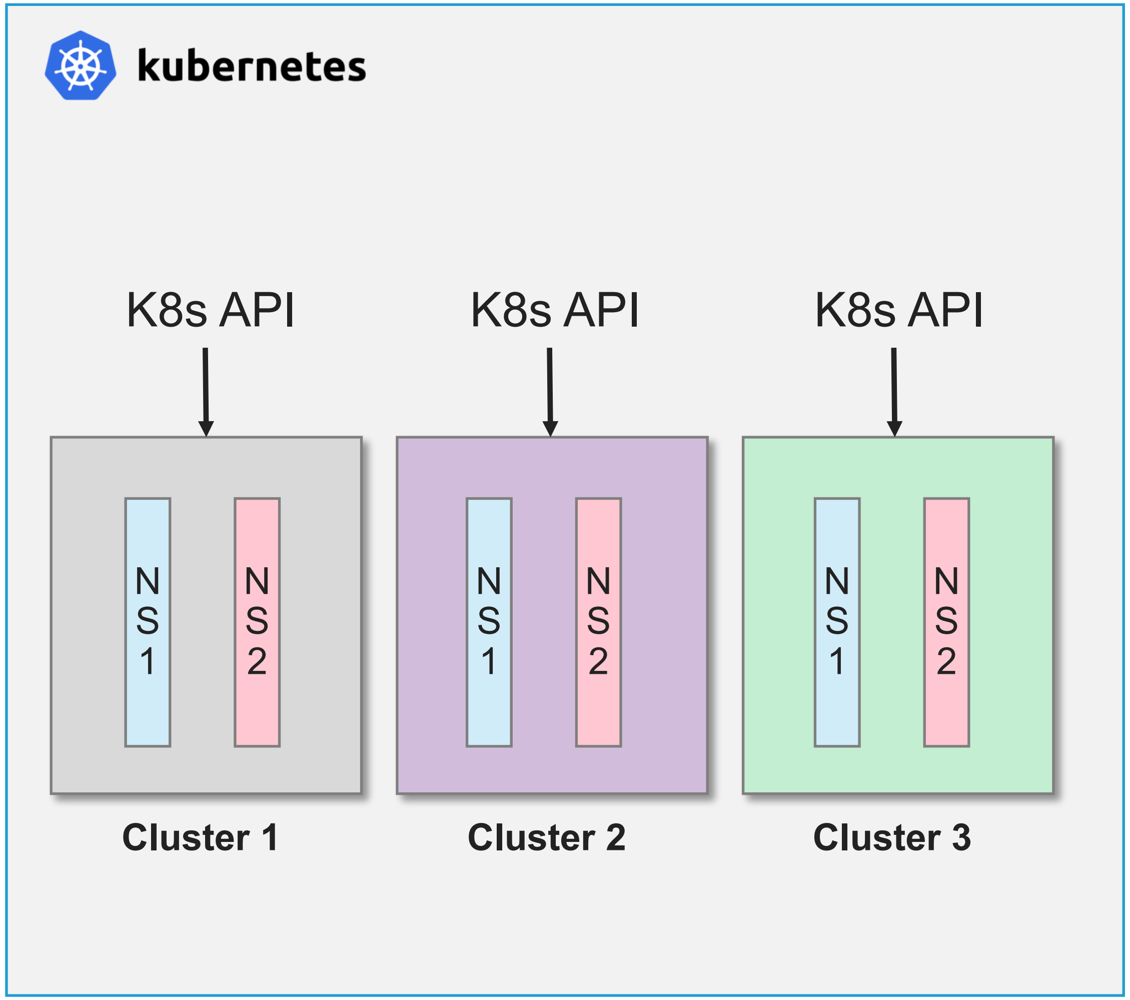
Compute Platform

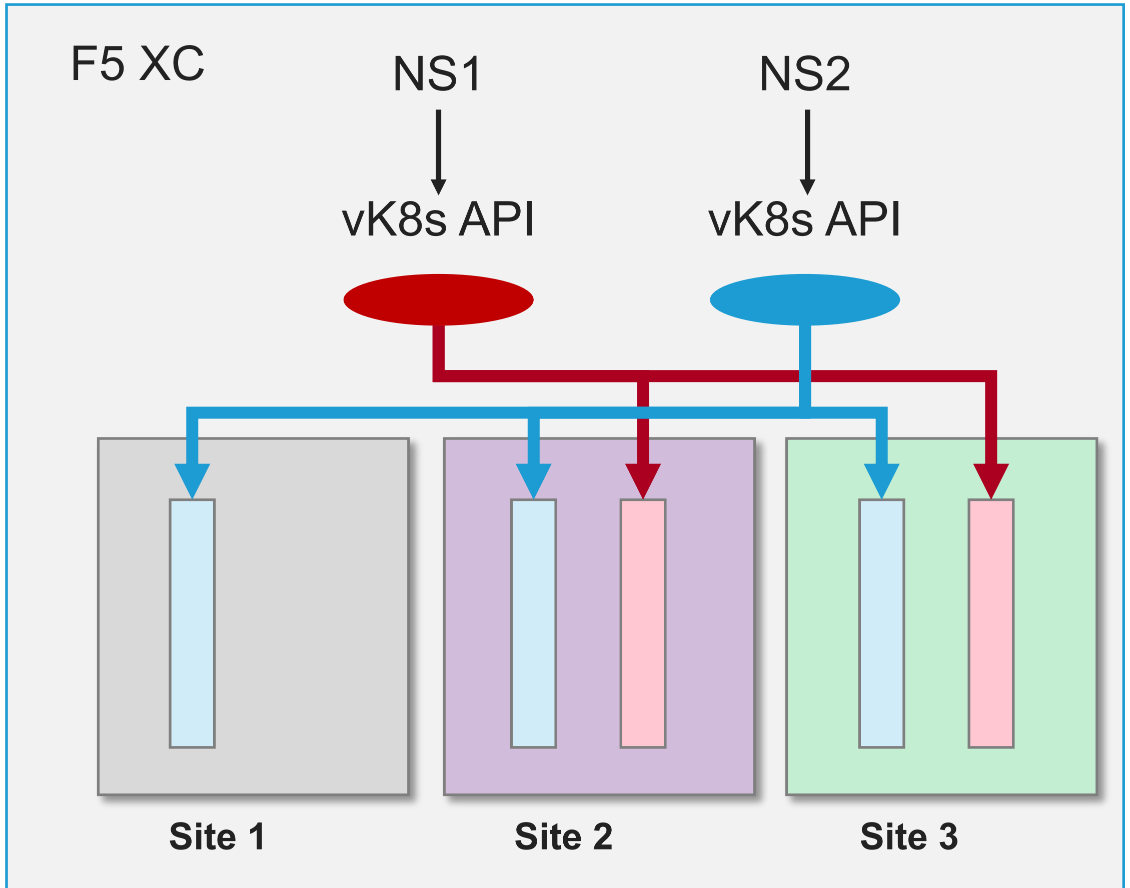
Simplified Application Infrastructure Stack

Standard K8s versus vK8s

App Stack

INTERACT WITH MULTIPLE CLUSTERS THROUGH A SINGLE API

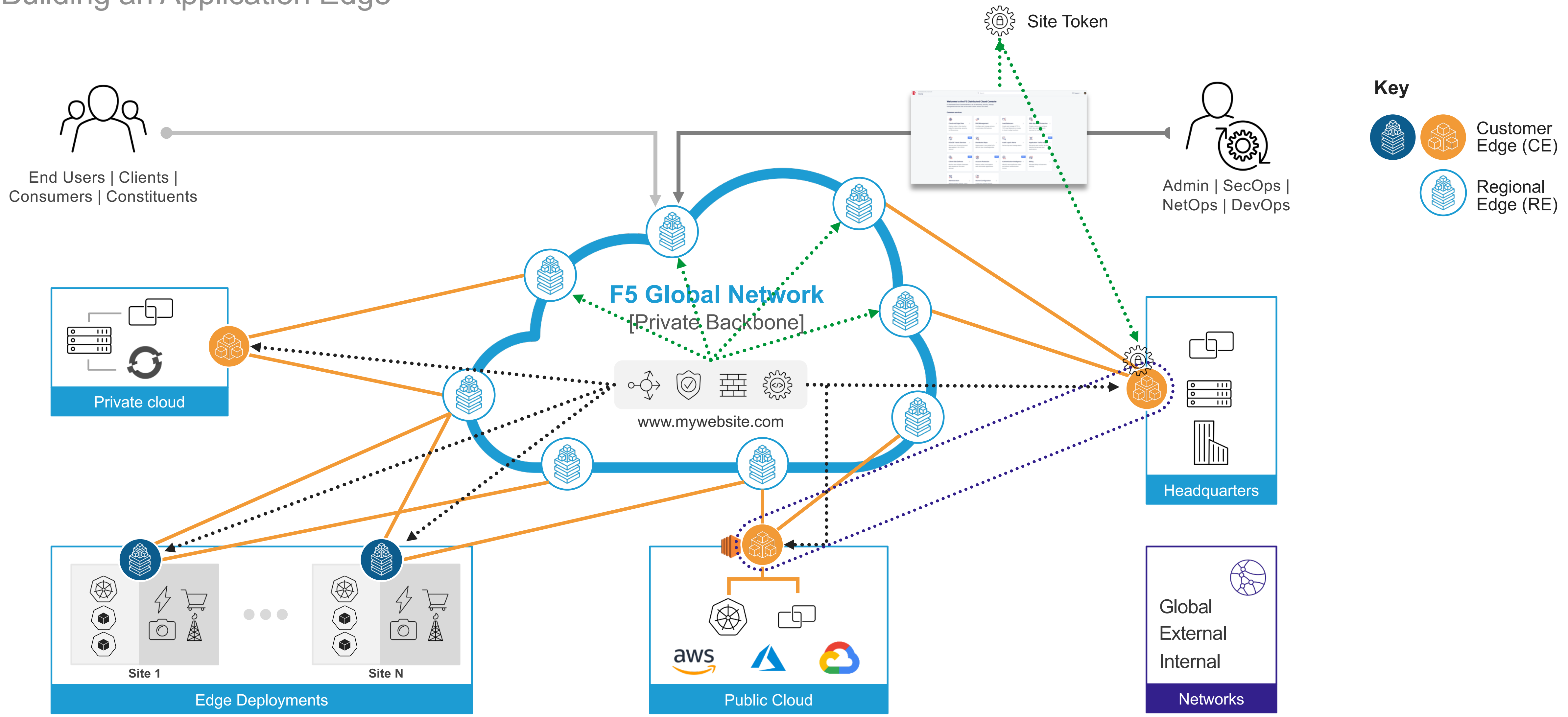




NS1 vK8s – Virtual Site with Sites 1, 2 and 3
NS2 vK8s – Virtual Site with Sites 2 and 3

Linking everything together

Building an Application Edge



F5 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

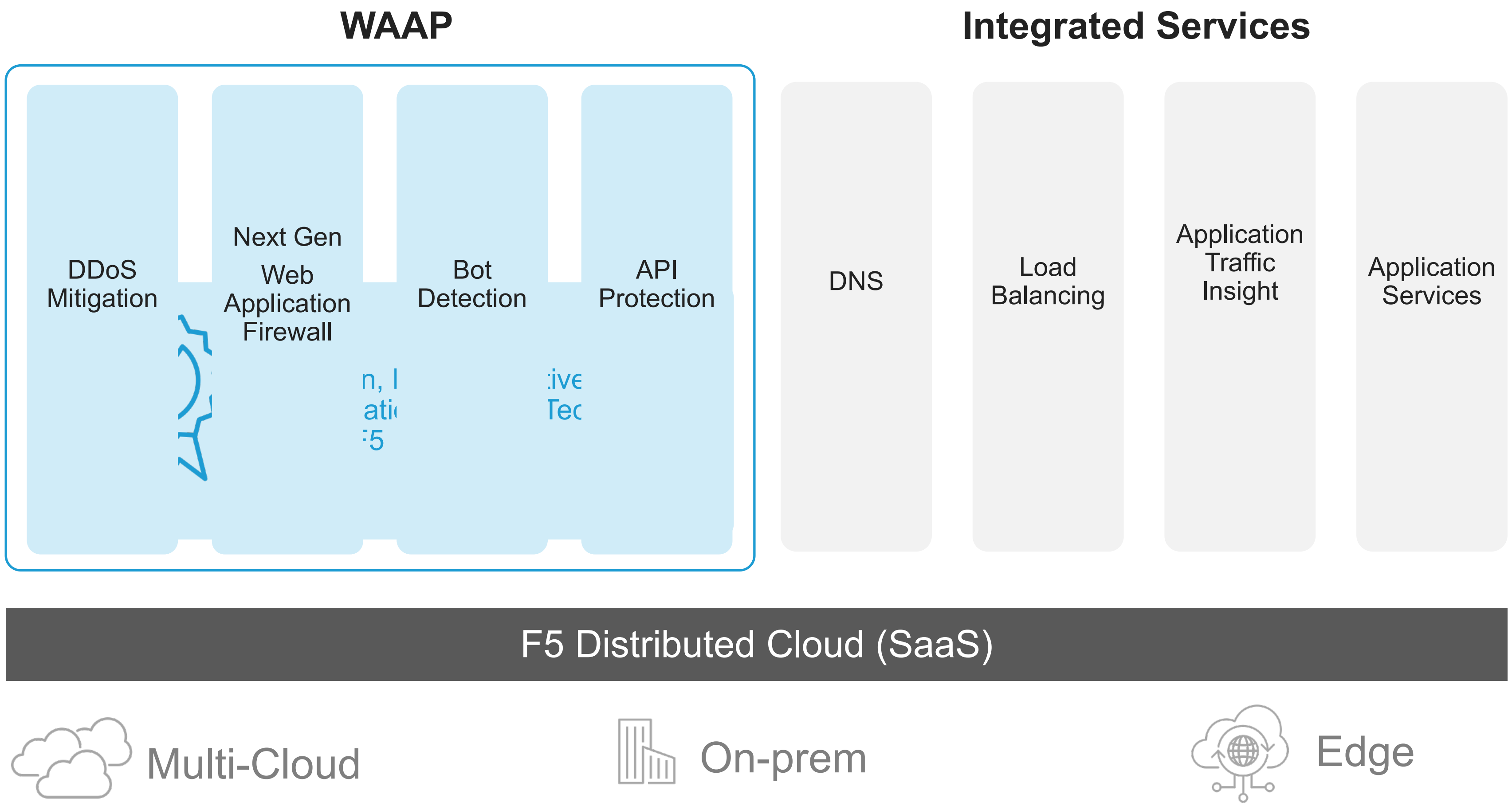
Application Delivery: Cloud and Edge

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

WAAP-as-a-Service

MULTI-LAYERED, HIGHLY EFFECTIVE MODERN APP SECURITY BRINGING TOGETHER THE BEST OF F5 APPLICATION SECURITY



WAAP

DDoS Mitigation

Next Gen Web Application Firewall

Bot Detection

API Protection

Integrated Services

DNS

Load Balancing

Application Traffic Insight

Application Services

F5 Distributed Cloud (SaaS)

Multi-Cloud

On-prem

Edge

DDoS Mitigation

DDoS Mitigation

Next Gen Web App Firewall

Bot Detection

API Protection

L3-L7 DDoS mitigation

Ensure the availability of critical application and network resources.

- Ensure application and network availability during DDoS attacks
- Block the malicious traffic while allowing the good, ensuring good user experience for applications and services
- Identify and mitigate sophisticated Layer 7 DoS attacks that exploit application & infrastructure weaknesses
- Block the attack where it originates with a global backbone and distributed DoS mitigation technology
- Protect small facility and cloud-based applications and services with DNS-based redirection

Mitigate Large, Sophisticate DoS Attacks

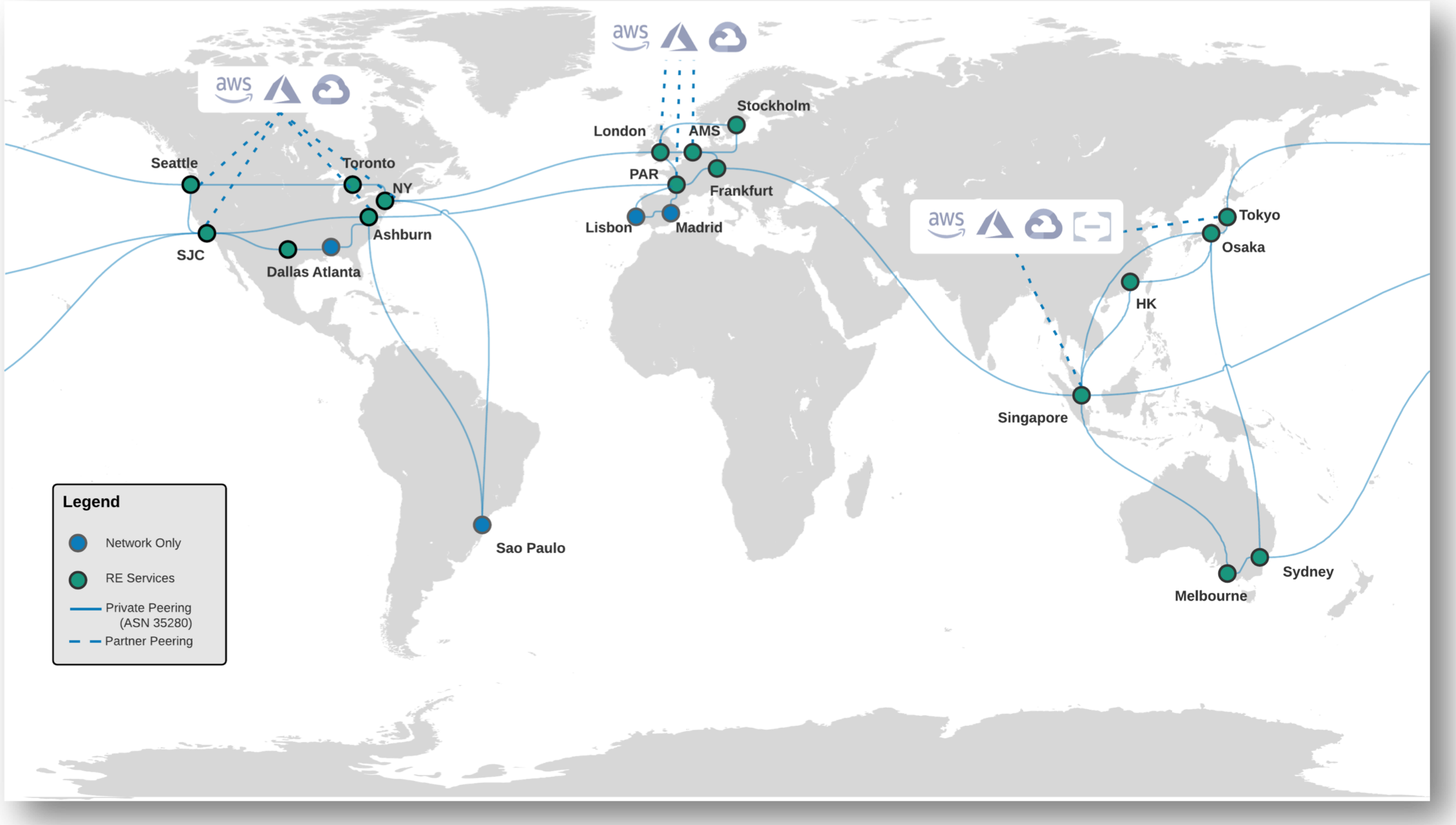
MITIGATE CLOSER TO THE ORIGIN AWAY FROM CRITICAL APPS AND INFRASTRUCTURE

World Class Global Security Operations Center responds to DDoS attacks in < 2 minutes on average.*

Global DDoS Protection Network with 12+ Tb of scrubbing capacity**.**

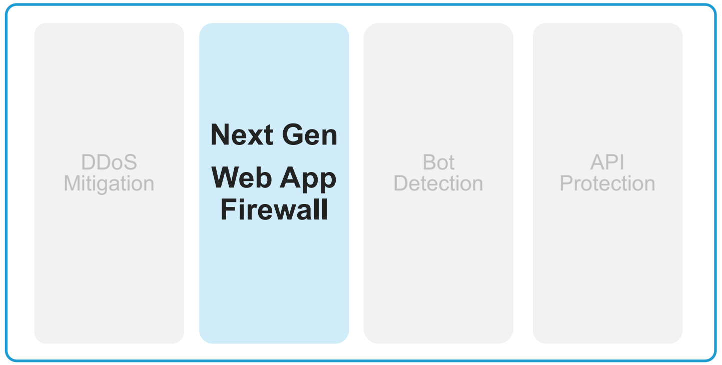
Flexible Service Options including Always Available or Always On deployments

Connect how and where you need with BGP-based traffic redirection and direct connections, peering or GRE tunnels.



Next Gen WAF - Identifying new threat actors

MOVING BEYOND SIGNATURE-BASED DETECTION



Signature based identification

Identifies a bad request based on a match to one or more signatures in a database

- Protection against known attack signatures
- Live signature feed so you're always up to date with the changing threat landscape
- Threat campaigns that help you reduce false positives based on actor intent
- Evasion detection support finds potentially malicious requests that signatures alone don't find

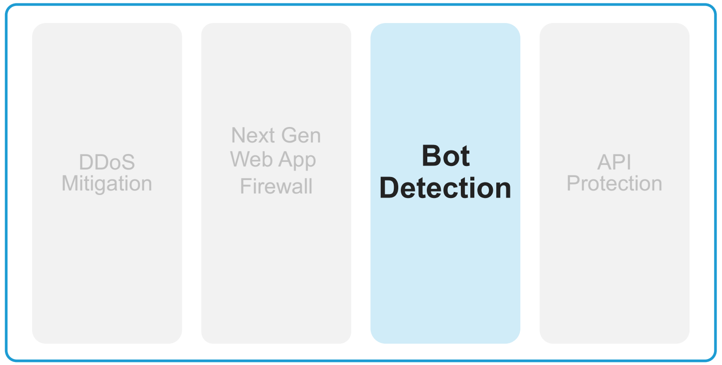
Behavior based to identify threat actors and false positives

Identifies a client and follows their behavior

- Identifies anomalous user behavior and blocks malicious attacks
- Recognizes non-human, automated requests that can potentially be harmful
- Reduces the time spent resolving false positives

Bot Detection

ENHANCED BOT DETECTION POWERED BY SHAPE

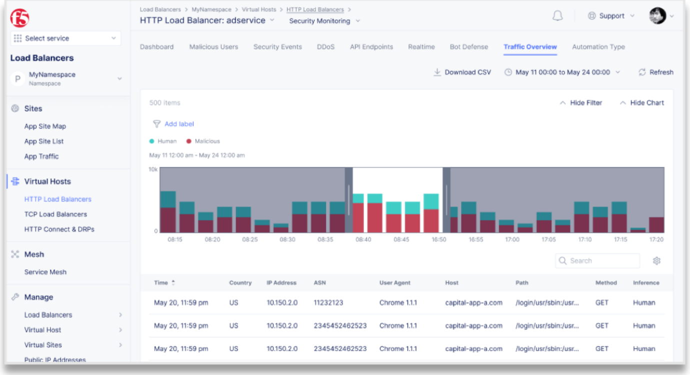


DDoS Mitigation

Next Gen Web App Firewall

Bot Detection

API Protection



HTTP Load Balancer: adservice

Security Monitoring

May 11 00:00 to May 24 00:00

500 items

May 11 12:00 am - May 24 12:00 am

Time	Country	IP Address	ASN	User Agent	Host	Path	Method	Inference
May 20, 11:59 pm	US	10.150.2.0	11232123	Chrome 1.1.1	capital-app-a.com	/login/usr/sbin:/usr...	GET	Human
May 20, 11:59 pm	US	10.150.2.0	2345452462523	Chrome 1.1.1	capital-app-a.com	/login/usr/sbin:/usr...	GET	Human
May 20, 11:59 pm	US	10.150.2.0	2345452462523	Chrome 1.1.1	capital-app-a.com	/login/usr/sbin:/usr...	GET	Human

Bot detection and mitigation

Identify automated, non-human attacks that can flood your digital infrastructure

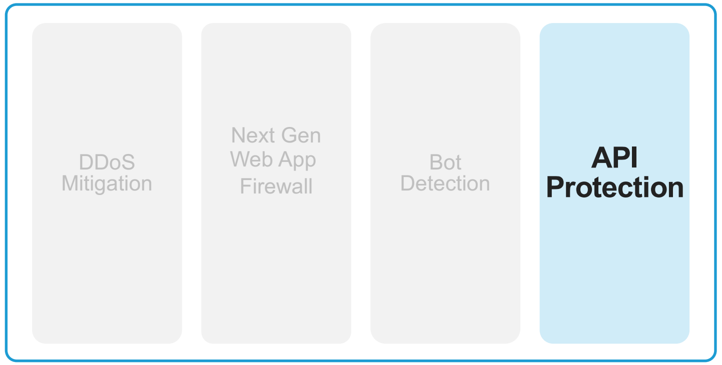
- Best of breed bot detection
- Identify fraudulent requests and transactions
- Minimize impact on user experience due to false positives

Part of F5

Client meta data is sent to SHAPE bot protection service

API Protection

DISCOVER, ENFORCE AND OBSERVE

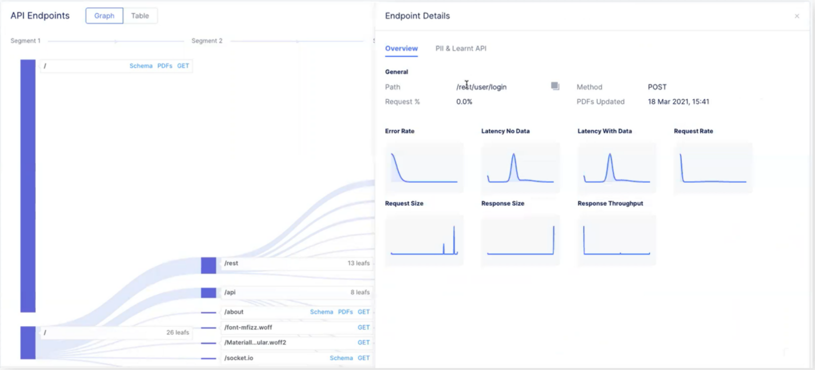


DDoS Mitigation

Next Gen Web App Firewall

Bot Detection

API Protection



/ Schema PDFs GET

/rest 13 leafs

/api 8 leafs

/about Schema PDFs GET

/ 26 leafs

/font-mfizz.woff GET

/Materiall...ular.woff2 GET

/socket.io Schema GET

General

Path /rest/user/login

Method POST

Request % 0.0%

PDFs Updated 18 Mar 2021, 15:41

API discovery and security

Easily identify all API endpoints mapped to your applications and anomalous activities

- Generate API schema and Swagger files to minimize manual tracking of API endpoints
- Block suspicious requests and prevent data leakage
- Reduces the time spent to configure and deploy API security policies

CUSTOMER NEED - EDGE TO CLOUD APPLICATION MGMT

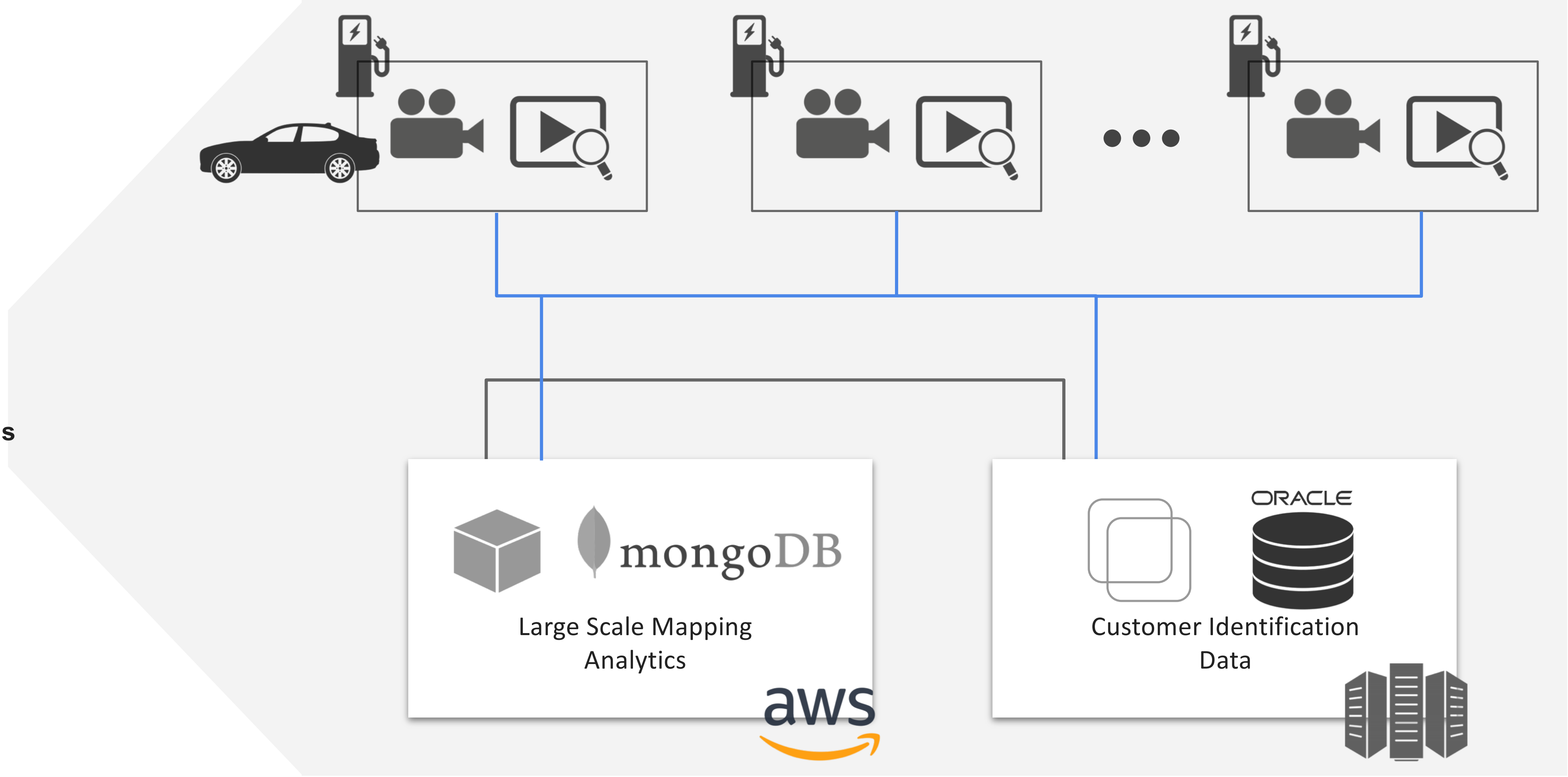
Automotive

Top-3 Global Automaker

Data Mgmt for EV Stations

Continuous Upgrades

Production Automation



HD Mapping Data from EVs

Video Analytics at EV Station

Centralized Data Lake

Data Analytics in Cloud

TRADITIONAL APPROACH → SCALE & OPEX CHALLENGES

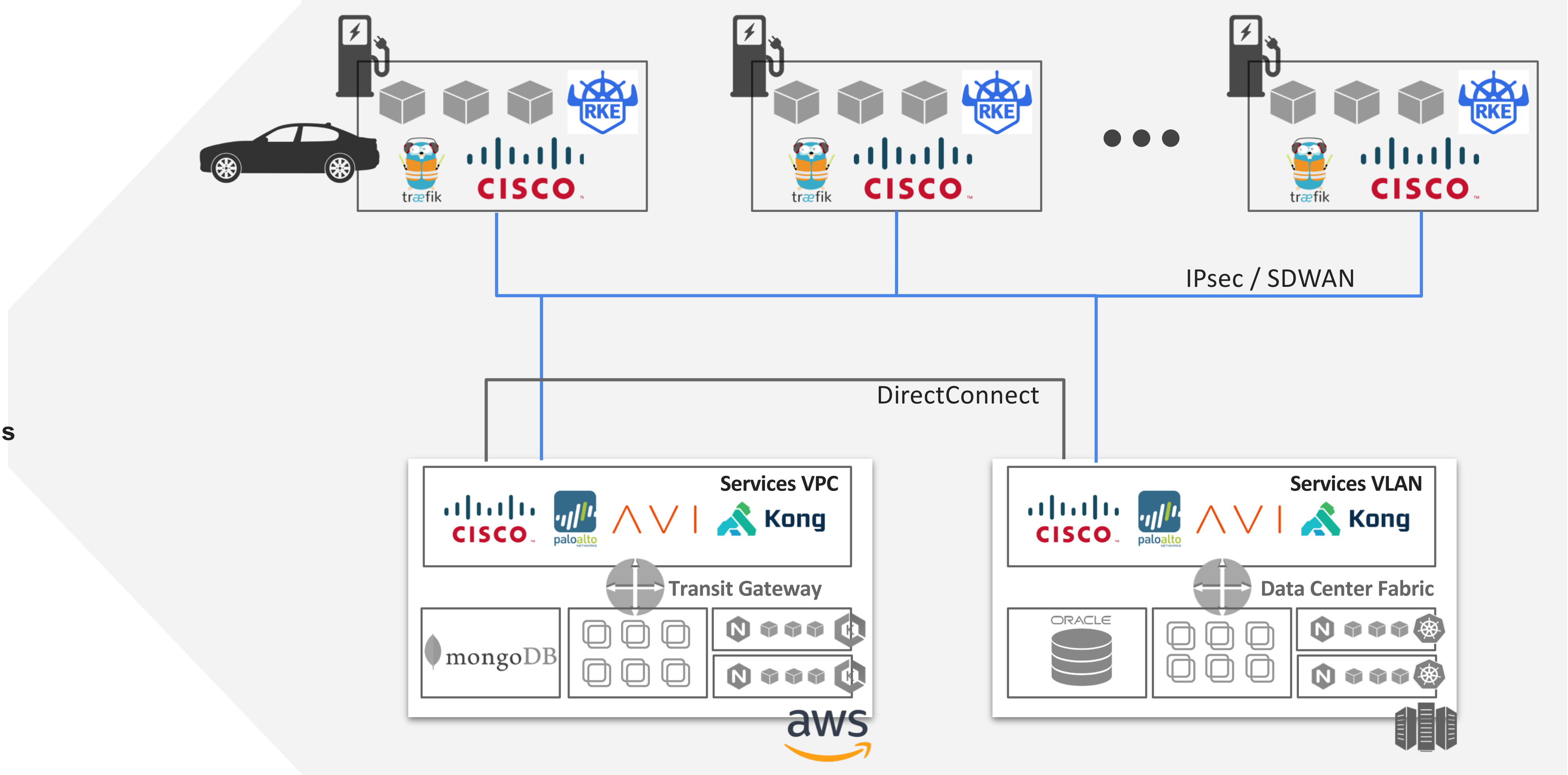
Automotive

Top-3 Global Automaker

Data Mgmt for EV Stations

Continuous Upgrades

Production Automation



12 Months - Rollout

6K/yr Truck Rolls

Large Operations Cost

F5 APPROACH - GLOBAL SCALE & SIMPLIFIED OPS

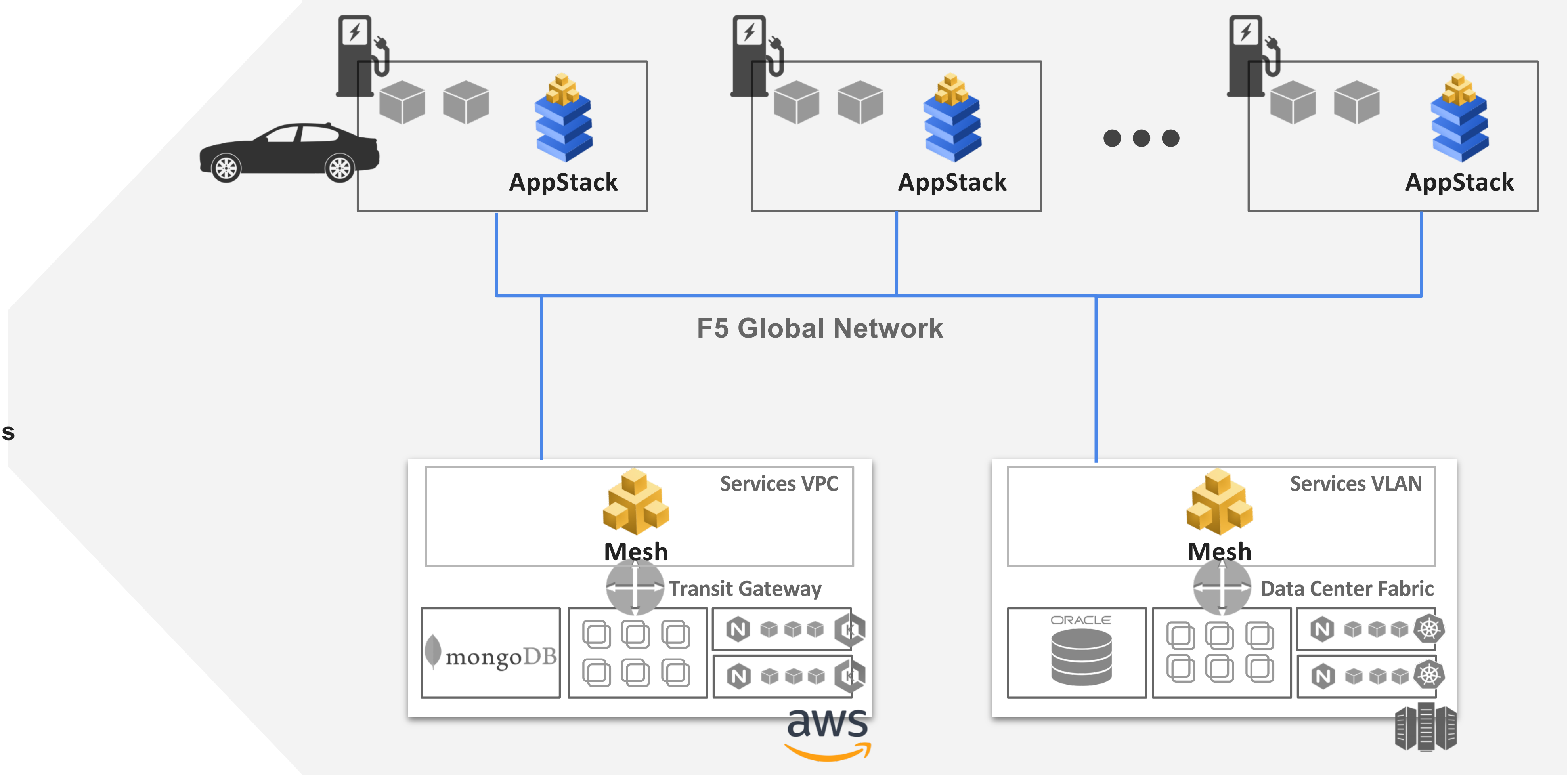
Automotive

Top-3 Global Automaker

Data Mgmt for EV Stations

Continuous Upgrades

Production Automation

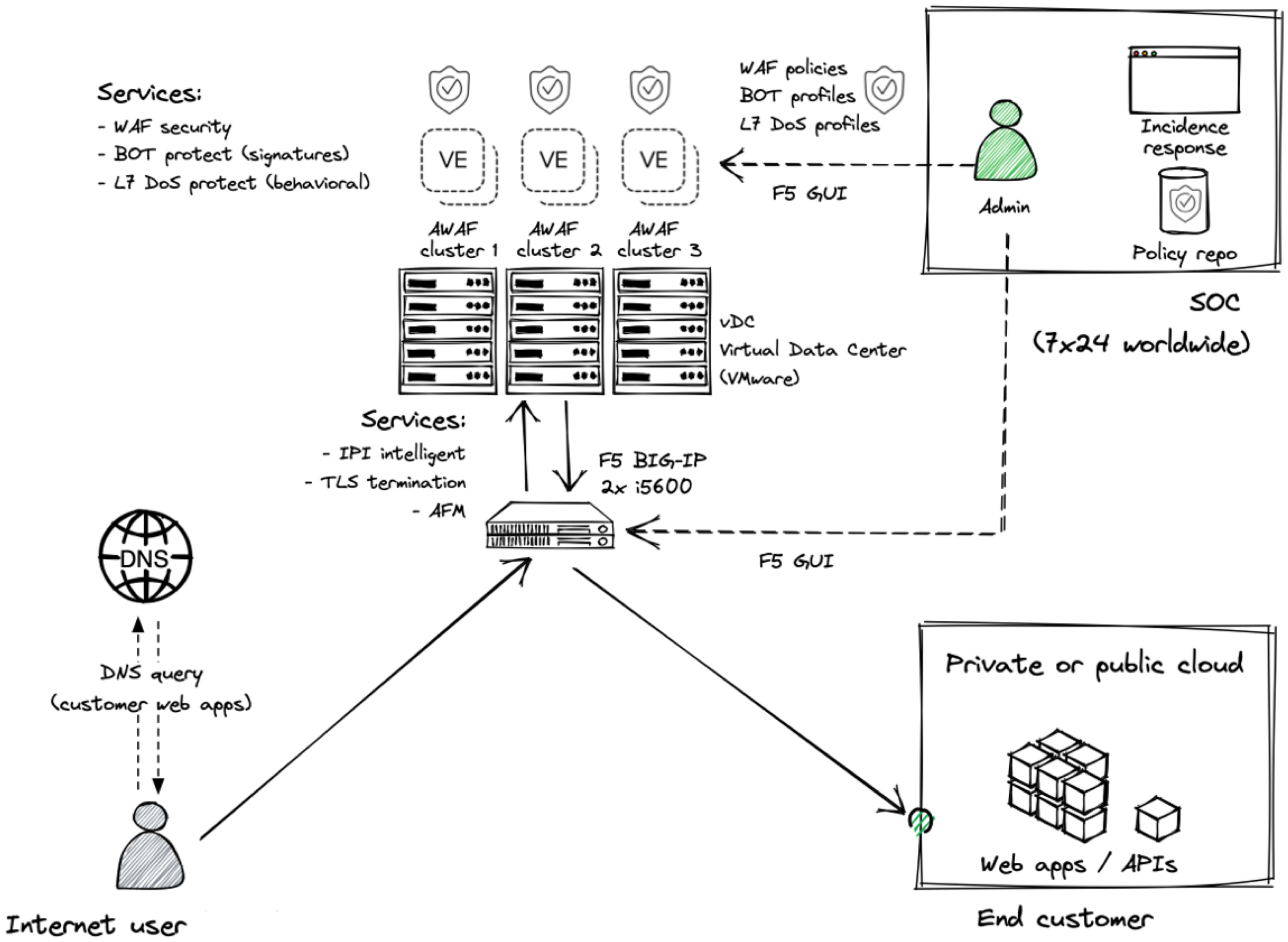


1 Month Rollout (vs 12 months)

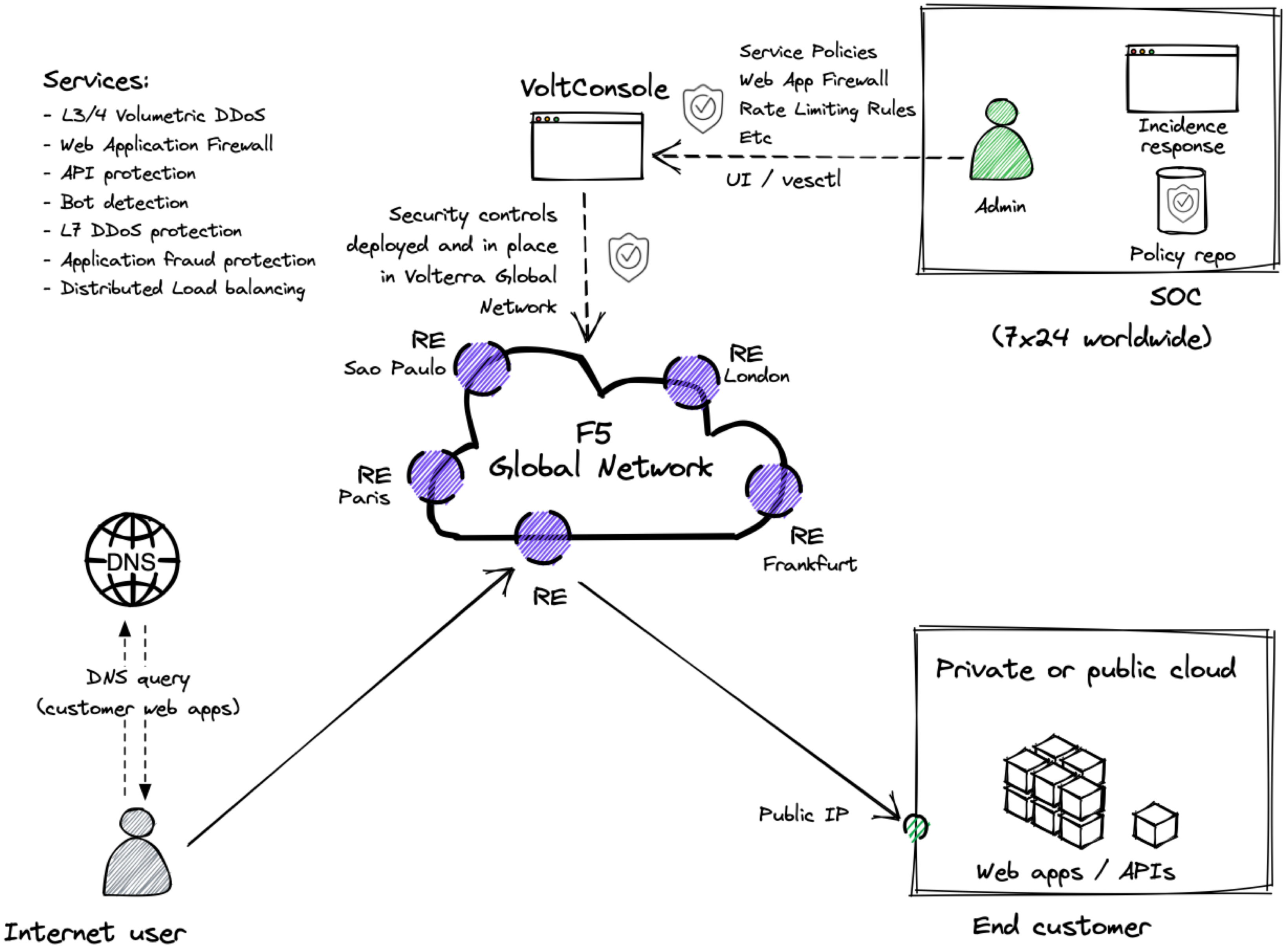
<1K/yr Truck Rolls (vs 6K/yr)

>$5M/yr Opex Reduction

MSP - WAF current model



MSP - WAF new SaaS model



Services:

- L3/4 Volumetric DDoS
- Web Application Firewall
- API protection
- Bot detection
- L7 DDoS protection
- Application fraud protection
- Distributed Load balancing

https://simulator.f5.com/distributedcloud

https://www.f5.com/cloud

https://www.f5.com/cloud/pricing

And many other solution also for SP‘s
Advanced WAF also on dedicated HW appliances, hypervisors or in containers
anti-DDoS, FWW, CGNAT with data retention
DNS solutions and DNS cache with DoH/DoT and DDoS protection
Policy enforcement with DPI
Signalling solutions – Radius, GTP, Diameter, SIP, HTTP2, ...