Next-Gen API Infrastructure

Halim Fadhli
F5 Solutions Engineer

Agenda

- Introduction on API Trends
- Recent News on API Breaches
- Architectural Consideration
  - Generic App & Network Services Architecture in Today's Standard (covering Global-Site-App Tier)
  - Industry Recommendation on Enterprise Architecture of API
- Key Requirements for Secure API Architecture
- Demo #1: API Gateway with NGINX
- Demo #2: API Security with F5 Distributed Cloud

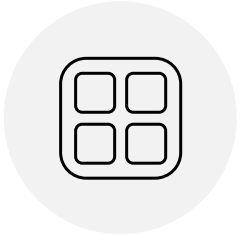
Introduction

Industry trend with API adoption

Changes in the business are forcing changes in the technologies

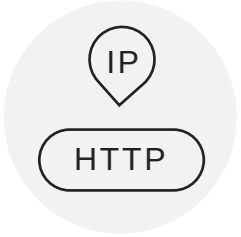
Modern Apps Characteristics

Monolithic Apps

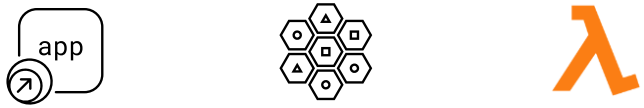


One Cloud Provider

Network-based Communication



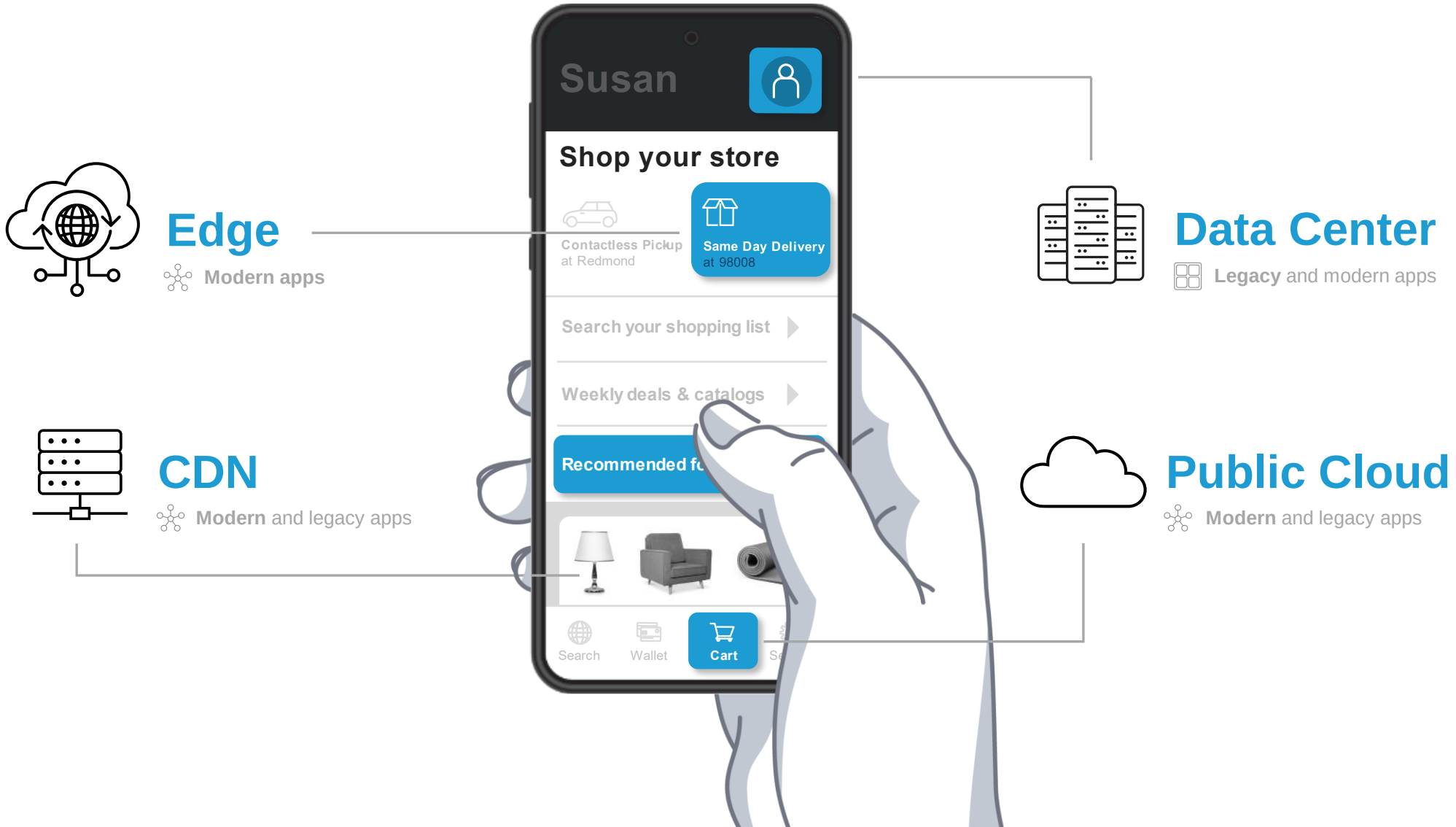
Microservices-based Apps



Multi-cloud and Edge Computing

API-based Communication

Digital experiences are comprised of legacy and modern apps, with multiple app sources spanning on premises to the edge



Landscape of API Traffic

Over 90% of developers use APIs

91% of Organizations Had An API Security Incident in 2020

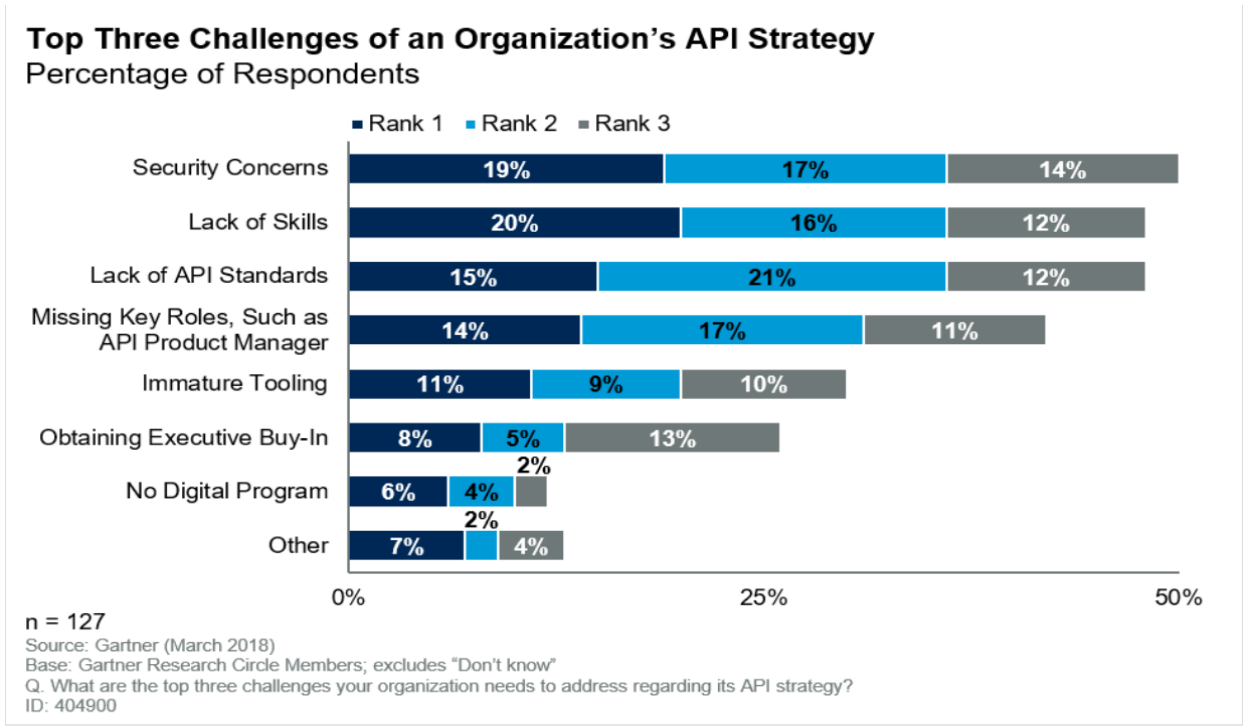
83% of All Internet Traffic Belongs to API-Based Services

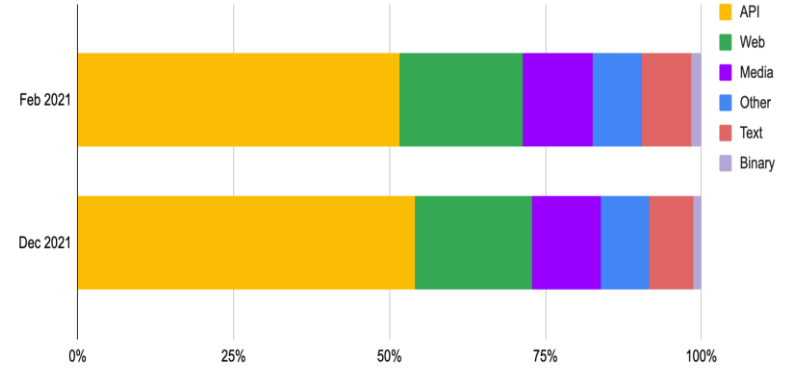
93.4% of API Developers Are Still Using REST

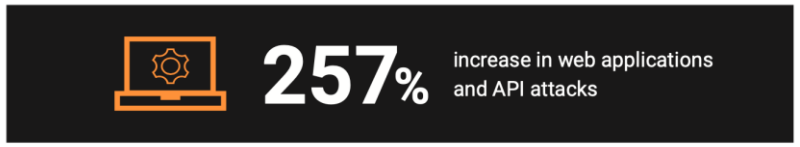
GraphQL Is Used By 22.5% of API Developers

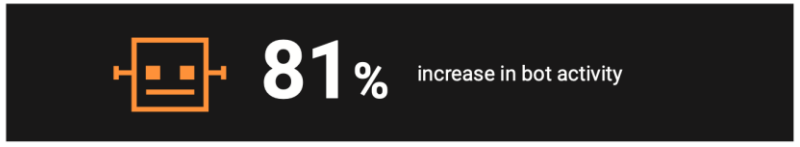
> GraphQL is still sometimes susceptible to broken object-level authorization, which is the number one API vulnerability

https://nordicapis.com/20-impressive-api-economy-statistics/



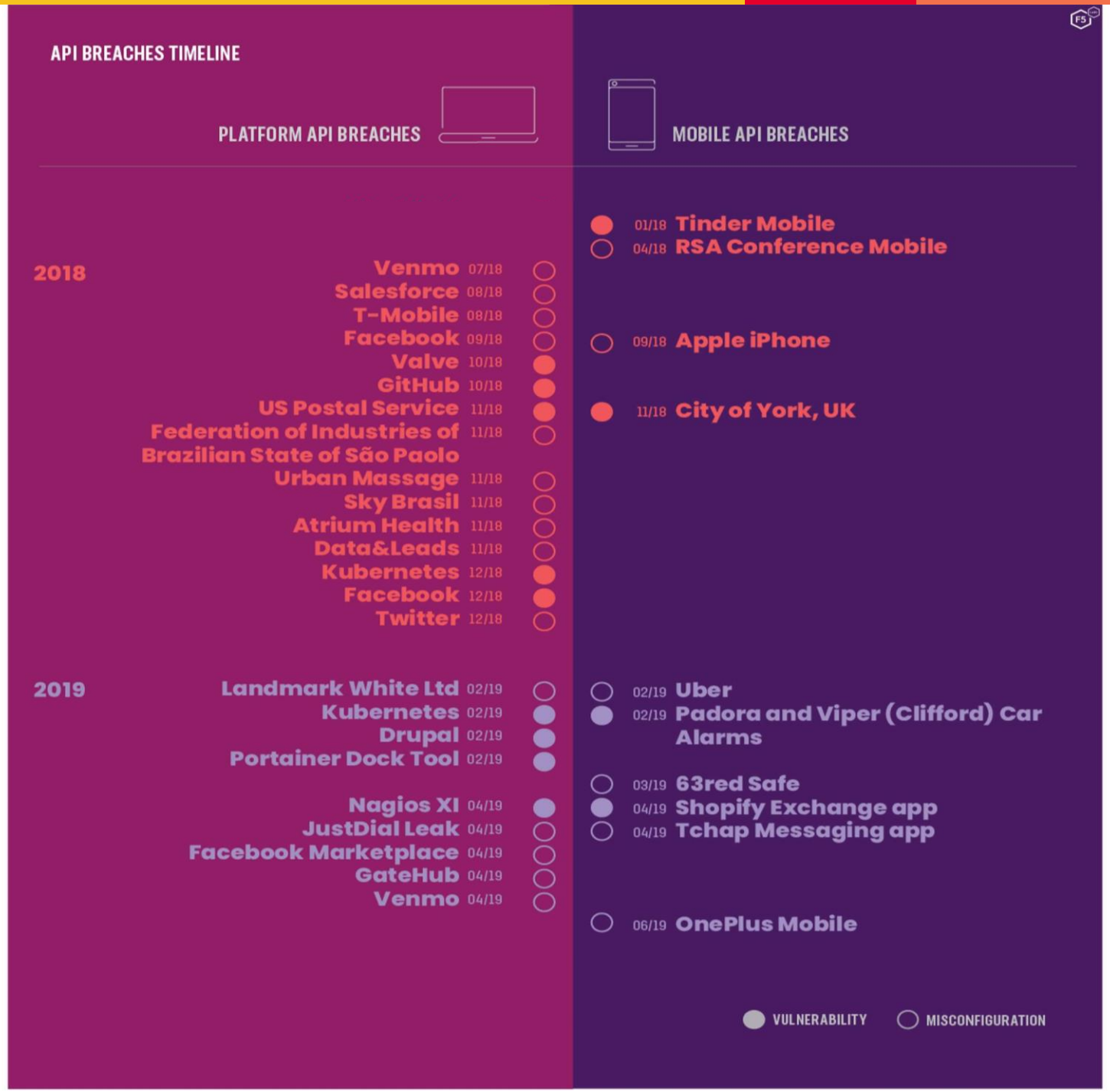






Recent News

API related breaches



Notable API breaches

Vulnerabilities

Lack of proper access controls

Misconfigurations

Inadequate controls for API specific security

2019

- Bounceshare

2021

- Linkedin

Sep, 2022

- Optus

Nov, 2022

- Twitter

Oct, 2022

- Toyota

Jan, 2023

- T-Mobile

Jan, 2023

- BMW, Mercedes and Ferarri

Breaches from lacking of API Security has been on the rise

Coincidentally? Or Naturally?

#9.1 Devastating data breaches rock the industry in 2022

OPTUS

- Personal details of 11 million customers were accessed. The information included names, dates of birth, phone numbers, email and home addresses, driver's license and/or passport numbers, etc.

tpg TELECOM

- Experienced a hack of its Hosted Exchange service, which compromised the email accounts of 15,000 customers. The attackers targeting financial and cryptocurrency data of TPG Telecom's iiNet and Westnet clients.

TM

- Breech affected 250,248 Unifi Mobile customers. It involved customer names, phone numbers and emails.

Telstra

- The personal information of more than 130,000 Telstra customers has been exposed in a privacy breach.
- The company attributed the breach to a "misalignment of databases" rather than hacking

Singtel

- Subsidiary of SingTel, IT services consulting company, Dialog, had its servers hacked in September 2022, and a small sample of its data, including some employee personal information, was published on the dark web on October 7th.

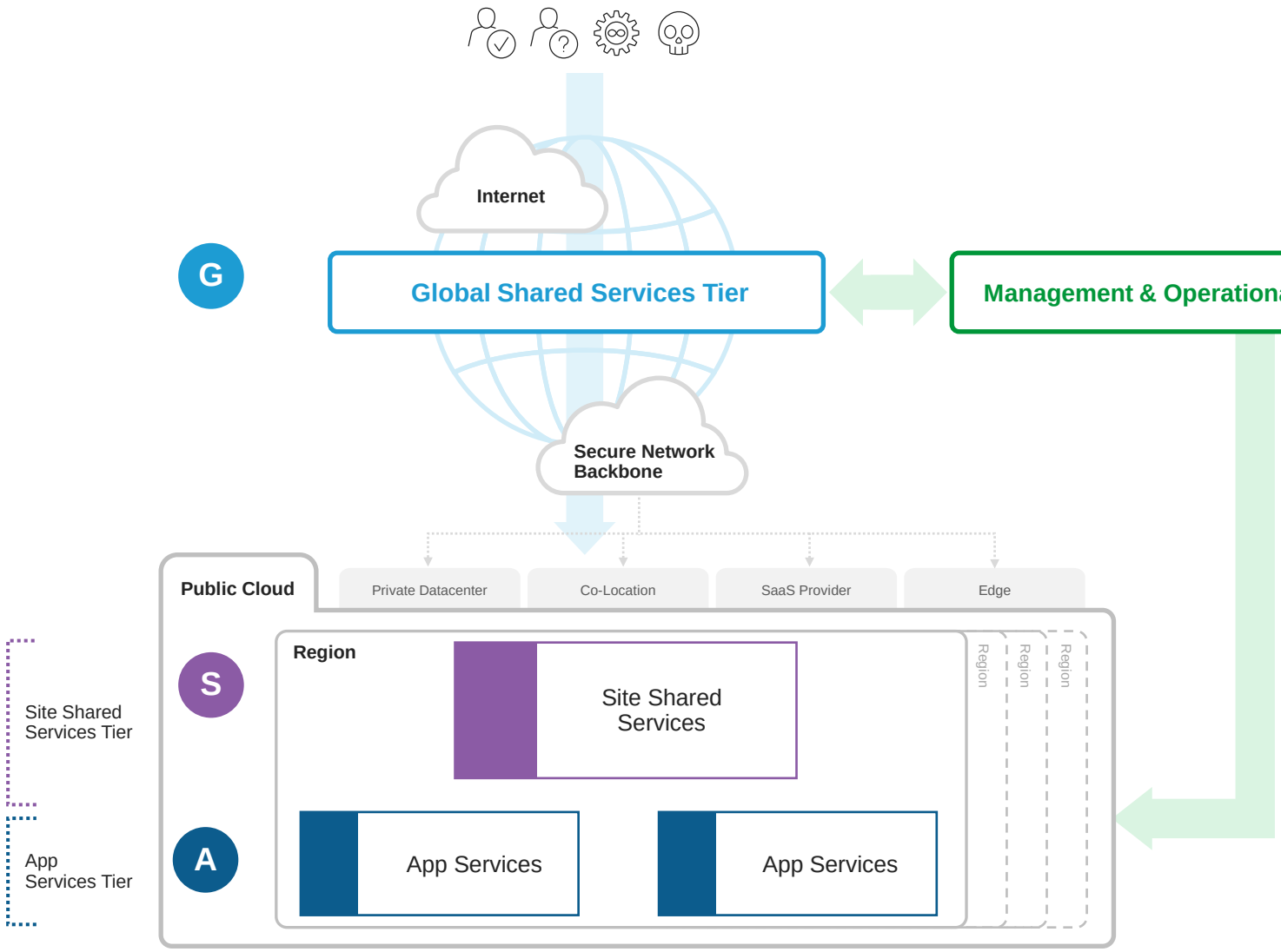
Telkom Indonesia

- Data leak involving Indihome, a subsidiary of Telkom Indonesia in which personal data of 26,730 Indihome customers, including their names, addresses, surfing history on the internet, such as dates, passwords, domains, platforms, browsers and URL links was accessed

Source: twimbit analysis, industry reporting

Architectural Consideration

Generic App & Network Services Architecture



Management & Ops Tier

- System Source of Truth
- Integration and Testing
- Automated Delivery
- Operational Observability and Insights
- Business Workflow Management

Global Service Tier

- Scalable App Delivery
- Anti-Abuse
- Global Connectivity Services
- Global App Health
- Global App Protection

Site Shared Service Tier

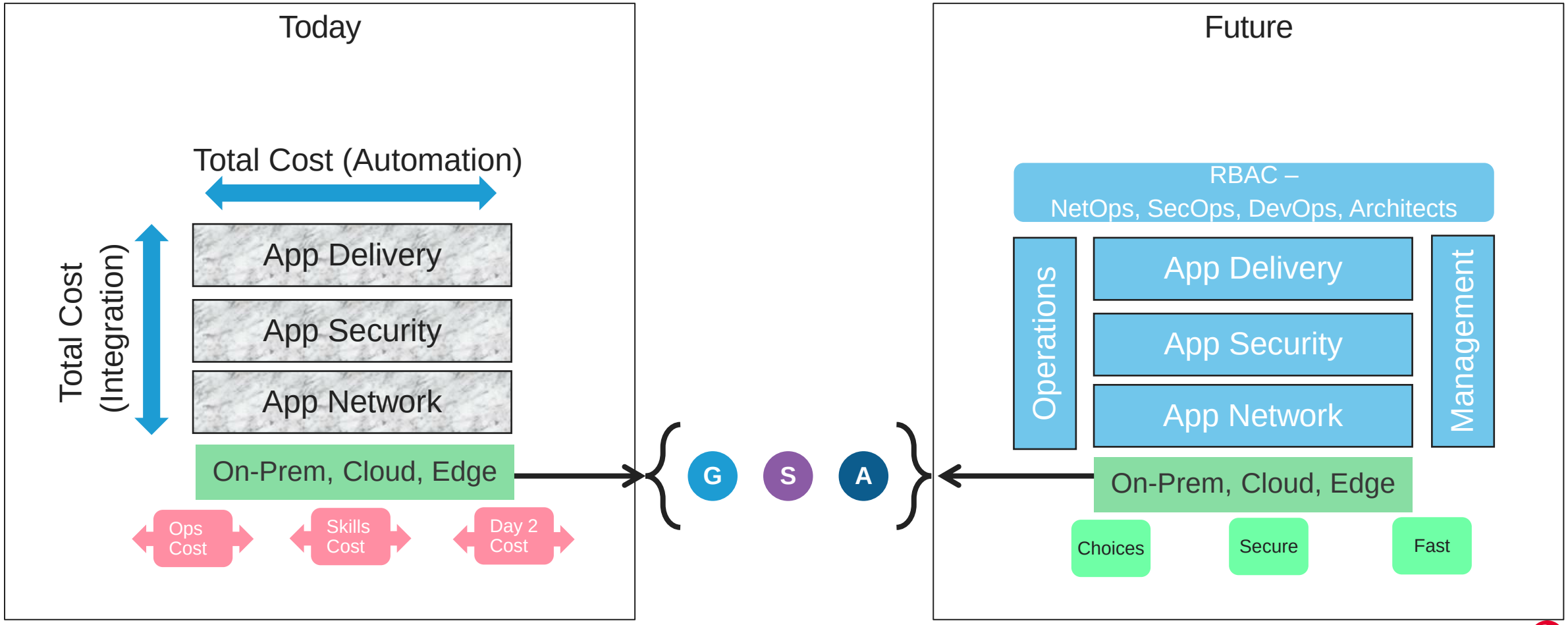
- Scalable App Delivery
- Site Security
- Site Connectivity
- Site App Health

App Service Tier

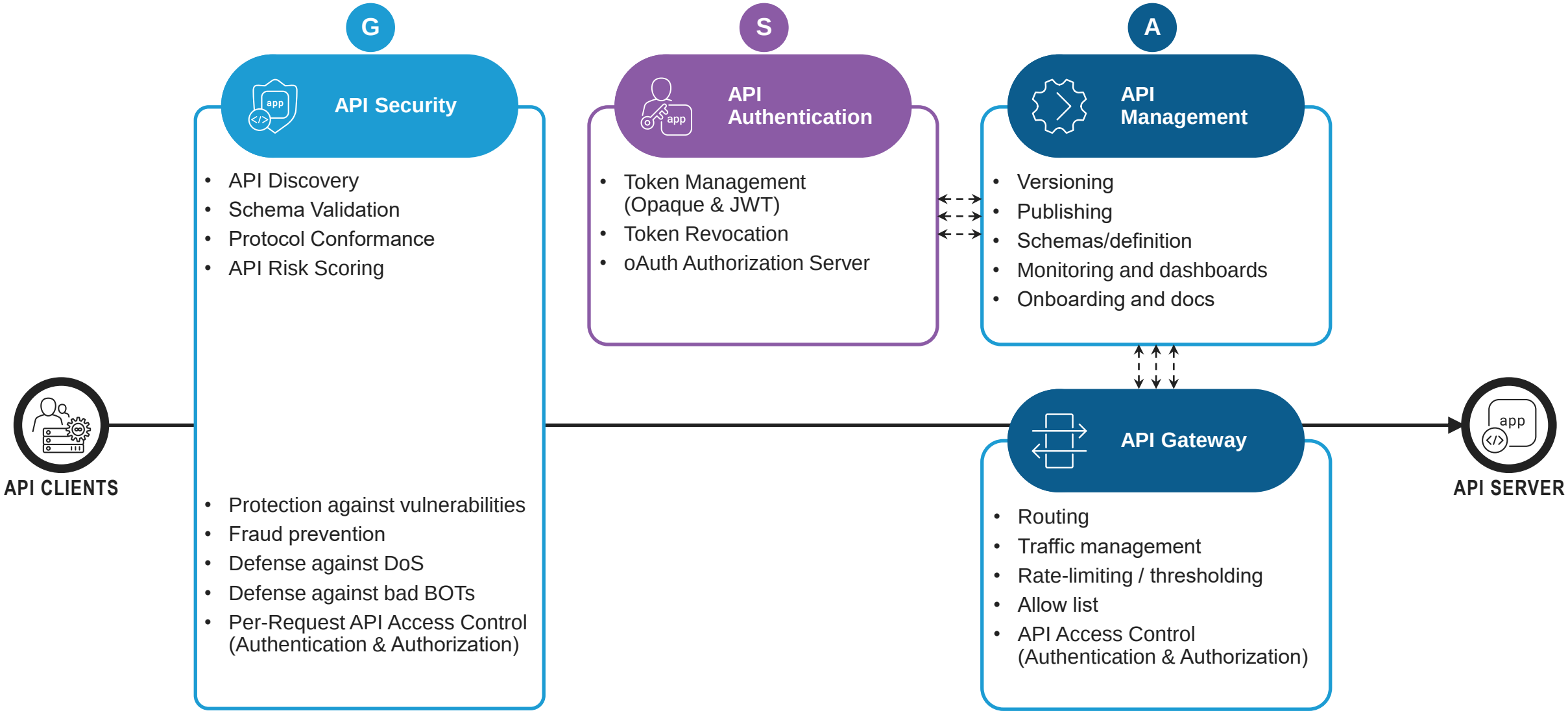
- Scalable App Delivery
- Instance Security
- Instance Connectivity
- Instance App Health

Benefits of Modern App Architecture

Common App Infra Services Platform

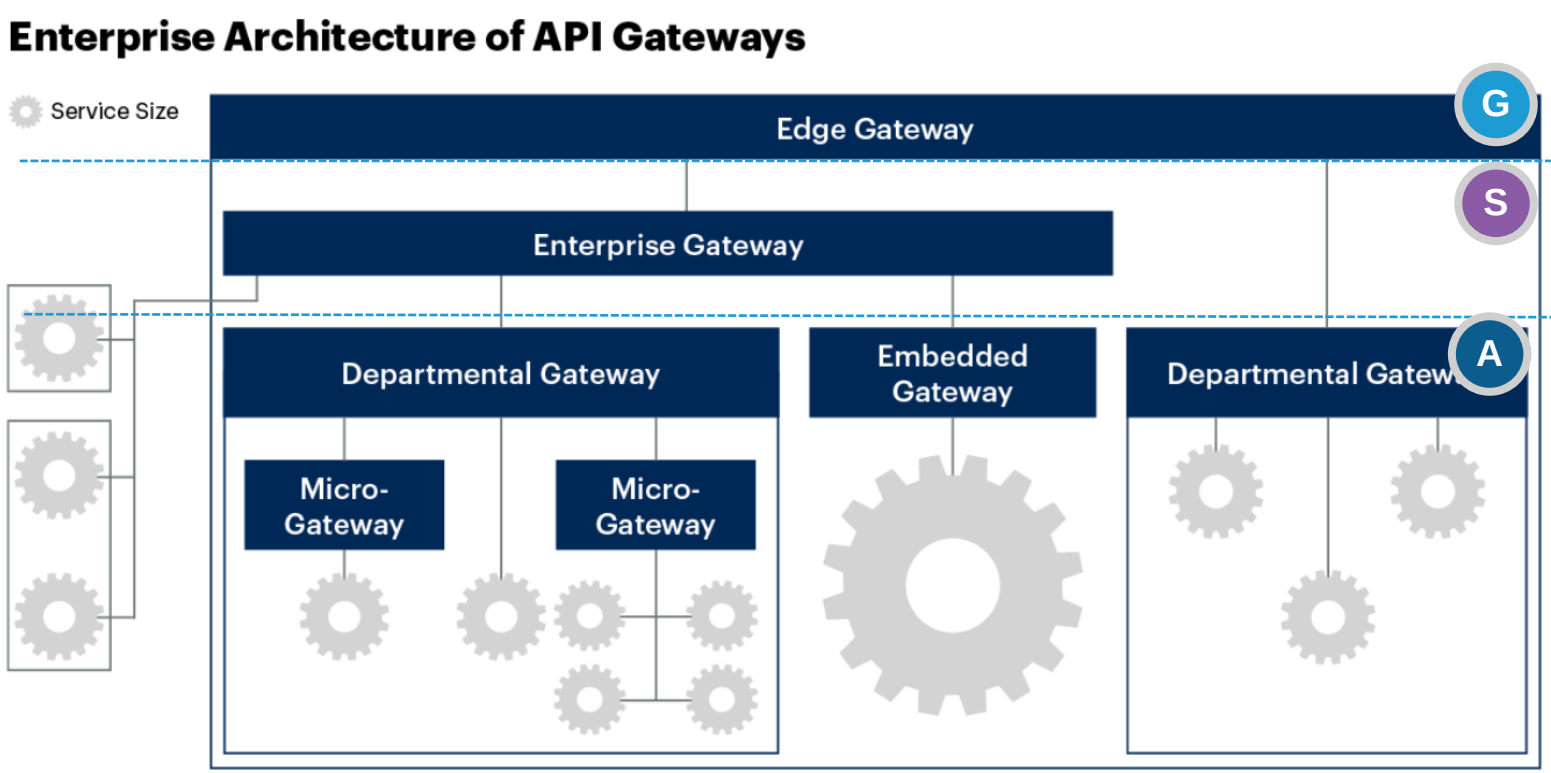


Key Requirements for ~~Standard~~ Secure API Architecture



Gartner on 3 Tiers of “Enterprise Architecture of API”

Figure 3: Enterprise Architecture of API Gateways



- C-WAAP
- H-WAAP
- D-WAAP

Distributed Cloud Services · Akamai · imperva · CLOUDFLARE

- OAuth
- Legacy API GW

BIG-IP · axway · apigee · 3SCALE · Tyk · WSO2 · MASHERY · mashape · ca technologies · amazon web services · akana

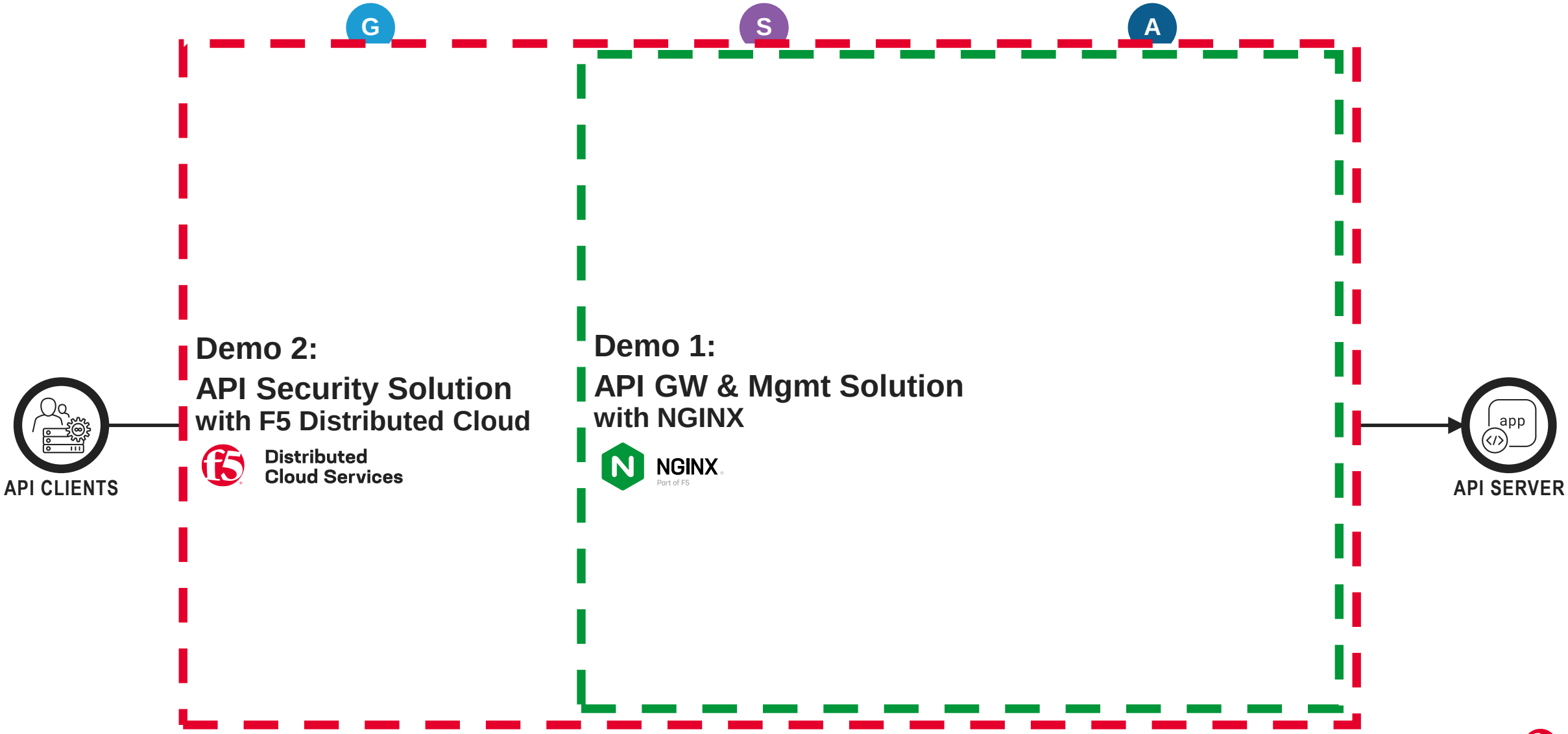
- Realtime API GW
- Light Weight
- Per App

NGINX · NGINX · ambassador

Source: Gartner
777062_C

Gartner

Key Requirements for ~~Standard~~ Secure API Architecture



Demo

Quick Introduction on

NGINX API Connectivity Stack

NGINX API Connectivity Stack

Simplify API management in multi-cloud and hybrid environments

API Connectivity Manager

Connect, govern, and secure APIs in microservices and multi-cloud environments

Instance Manager

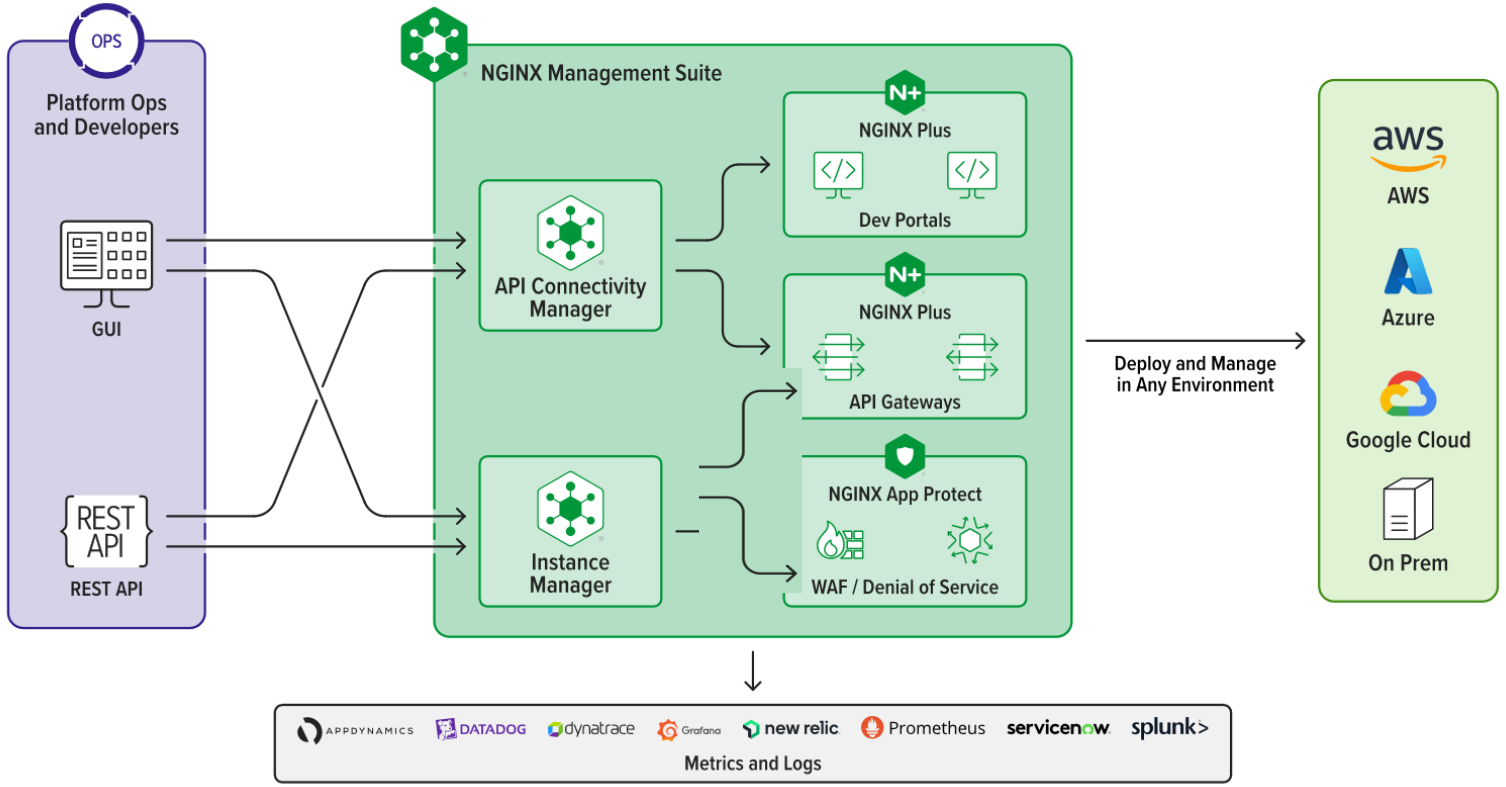
Track and configure NGINX Open Source, NGINX Plus, and NGINX App Protect WAF instances

NGINX Plus

Deliver unparalleled performance with the world's most trusted API gateway

NGINX App Protect

Apply positive security with schema validation, URI request validation, and more



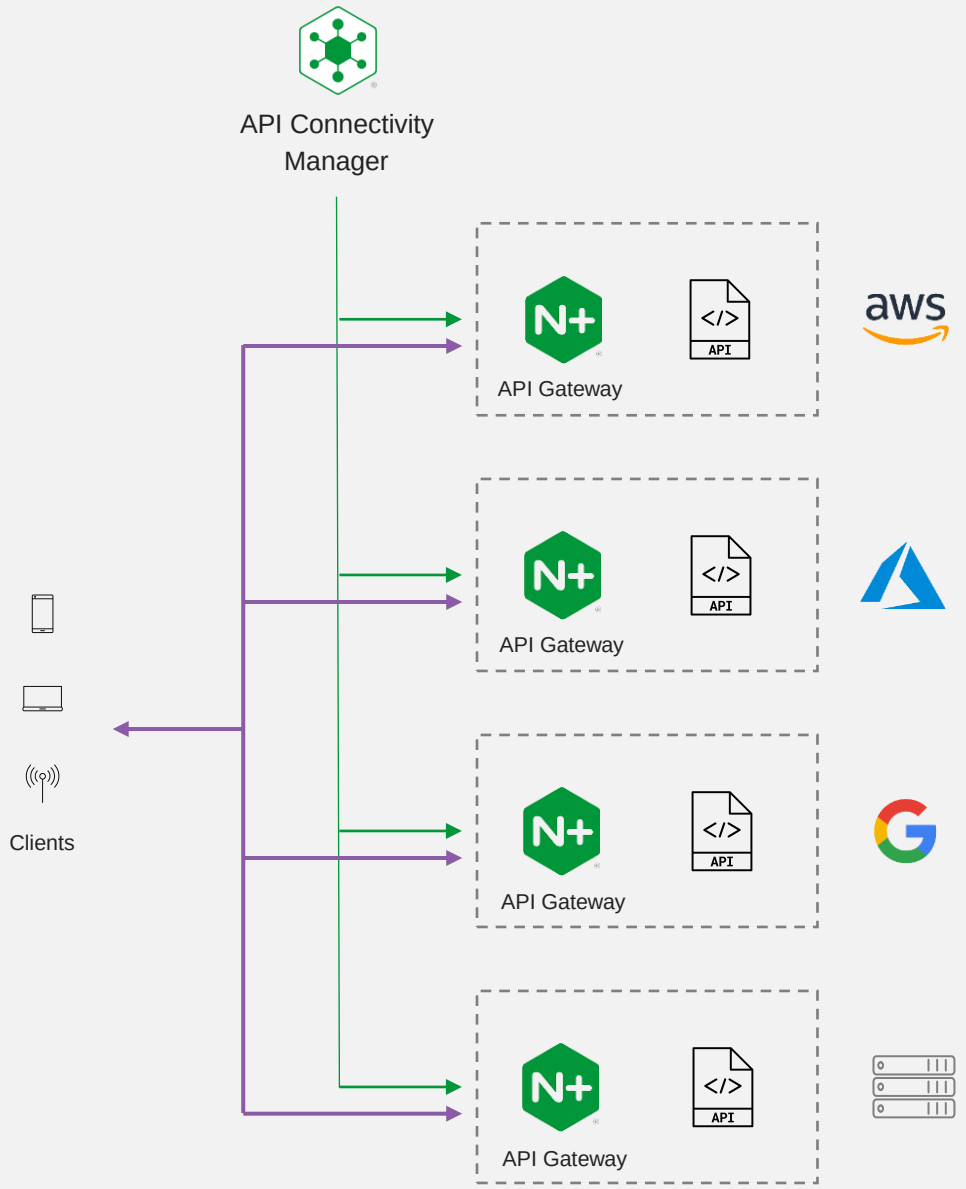
Gain architectural freedom

Platform agnostic
Run wherever your APIs are – in the cloud, at the edge, in Kubernetes, or on hardware

Unified management
Manage APIs deployed across clouds and data centers from a single pane of glass

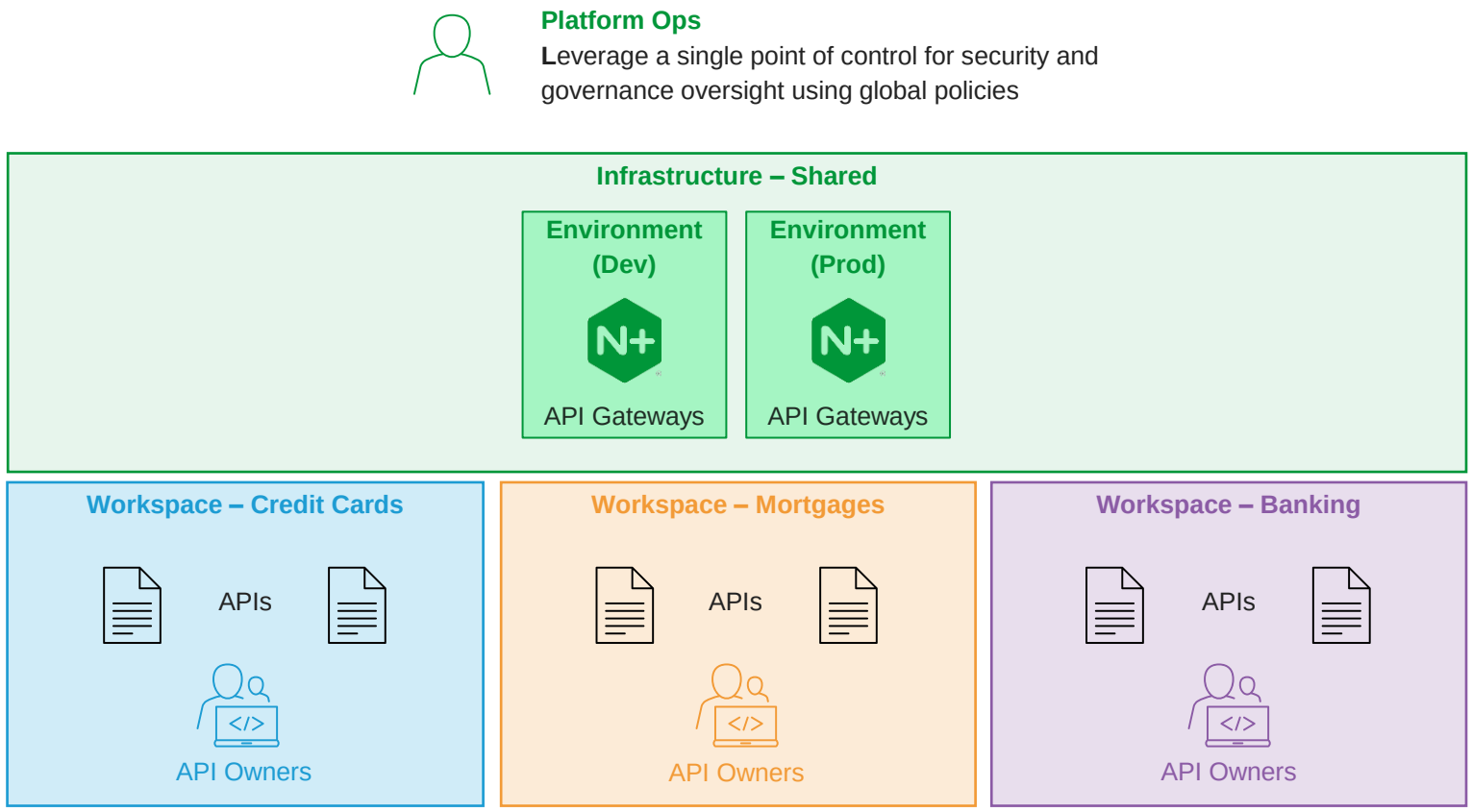
Flexible deployments
Deploy as many gateways, services, and environments as you need without restriction

Fair pricing
Pay only for successful API calls with no hidden fees for additional gateways or regions



Shared operating model

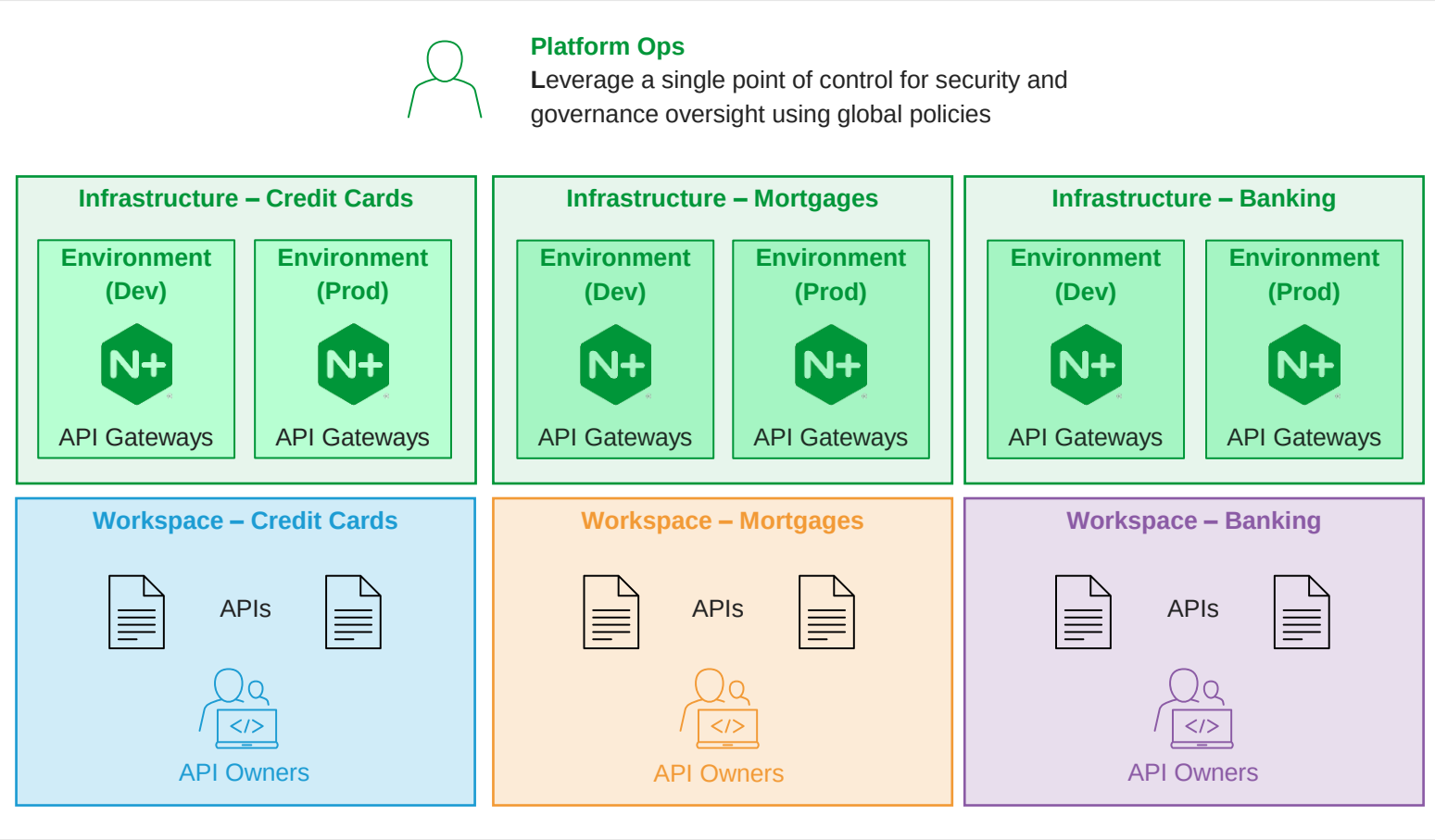
Impose uniformity across teams with a shared API Gateway cluster



- Enables **standardization** across teams and lines of business
- It is easier to observe APIs and configurations through a single API gateway cluster
- Less flexible to meet the needs and compliance requirements of different teams

Decentralized operating model

Physically separate API gateway clusters per teams and environments



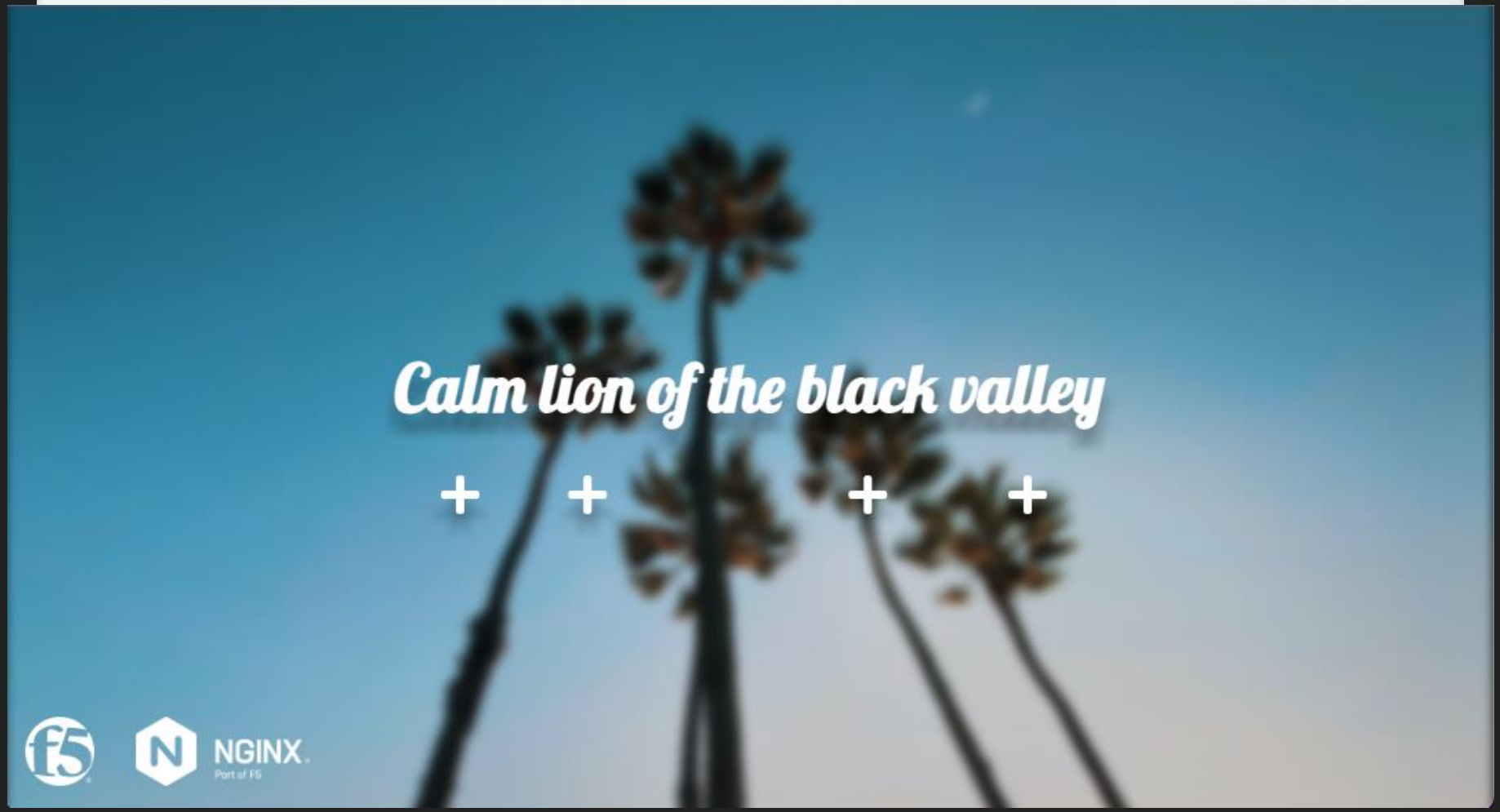
- Enables **adaptive governance** – requirements are set by team and line of business
- Greater resilience across teams and the business as a whole
- Requires greater automation so Platform Ops teams can manage infrastructure

Demo #1

API GW and Mgmt Solution with NGINX

Sample Application

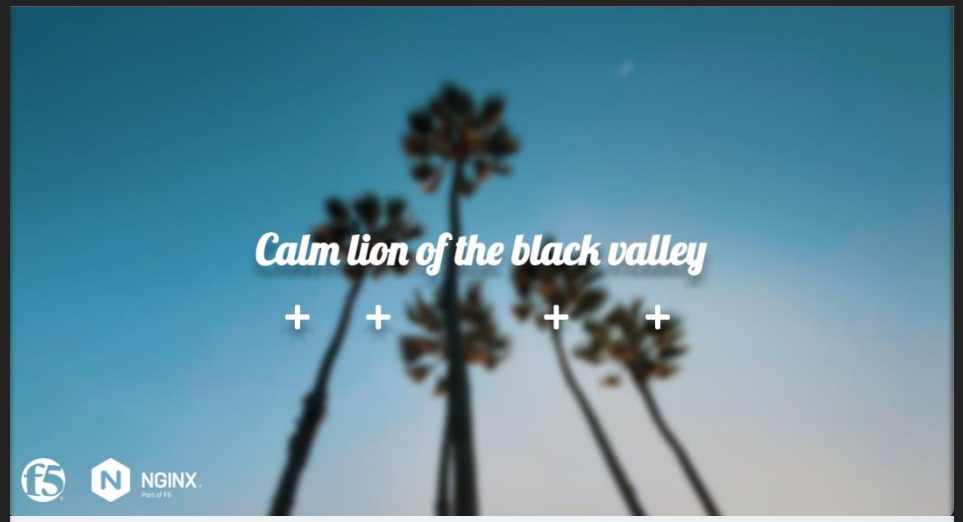
Sentence Demo App

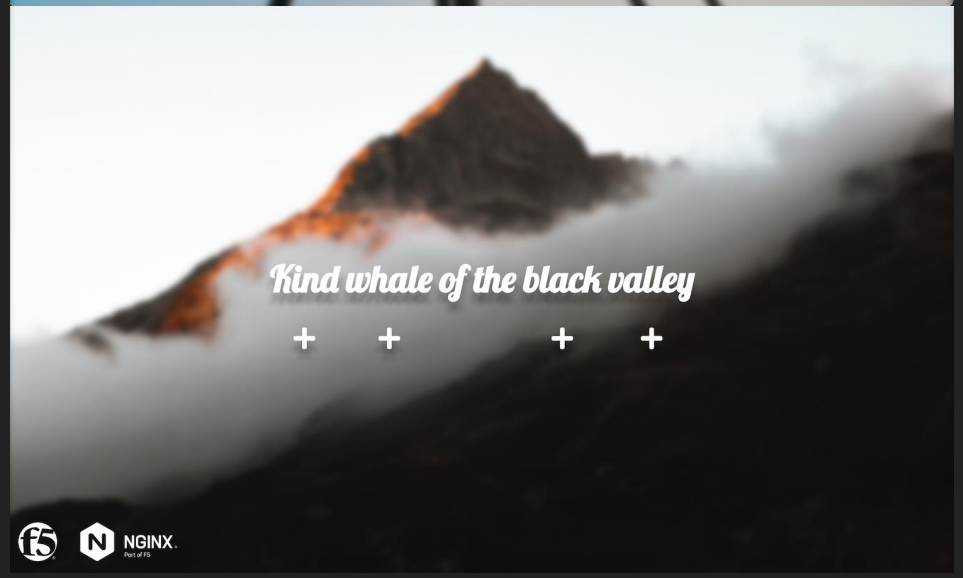


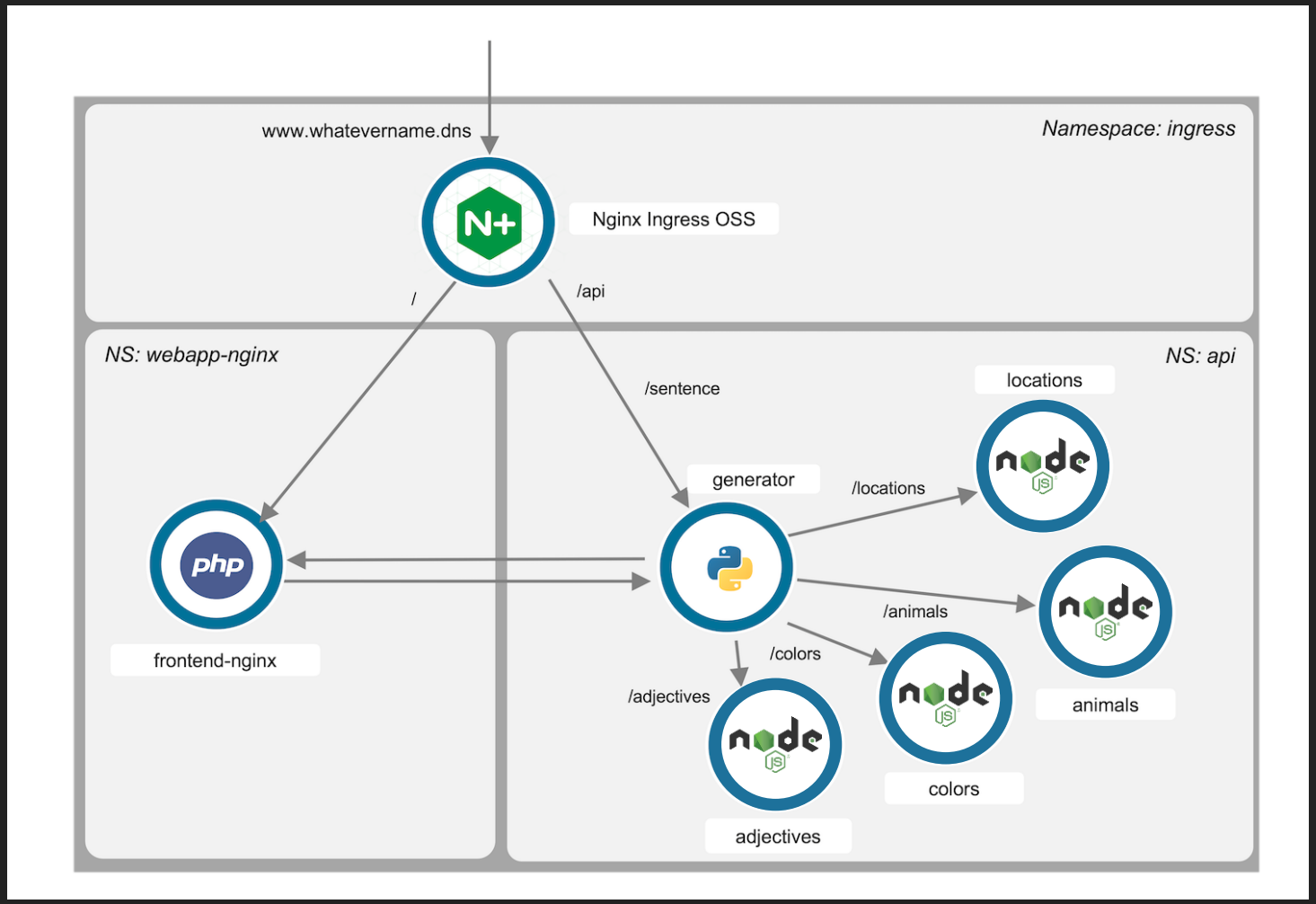
- This app will generate a sentence :)
- It consists of multiple WORD microservices pod
- Every WORD pod delivers a list of WORDS. Then, the GENERATOR select one WORD per POD, and generates a SENTENCE in a JSON format

ARHICTECTURAL DIAGRAM

Sample Application – Sentence Demo App



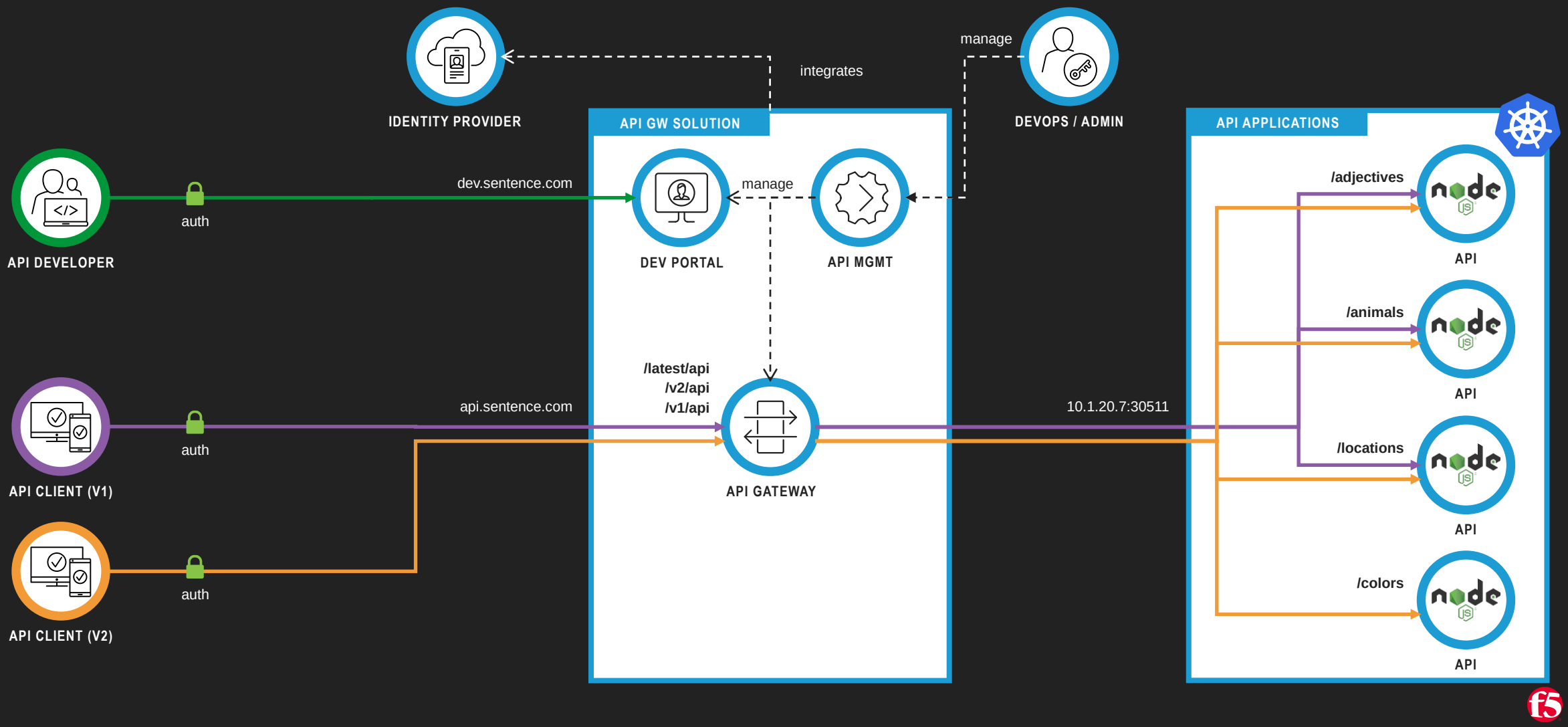




* Note: Deploy yourself at https://github.com/f5devcentral/sentence-demo-app

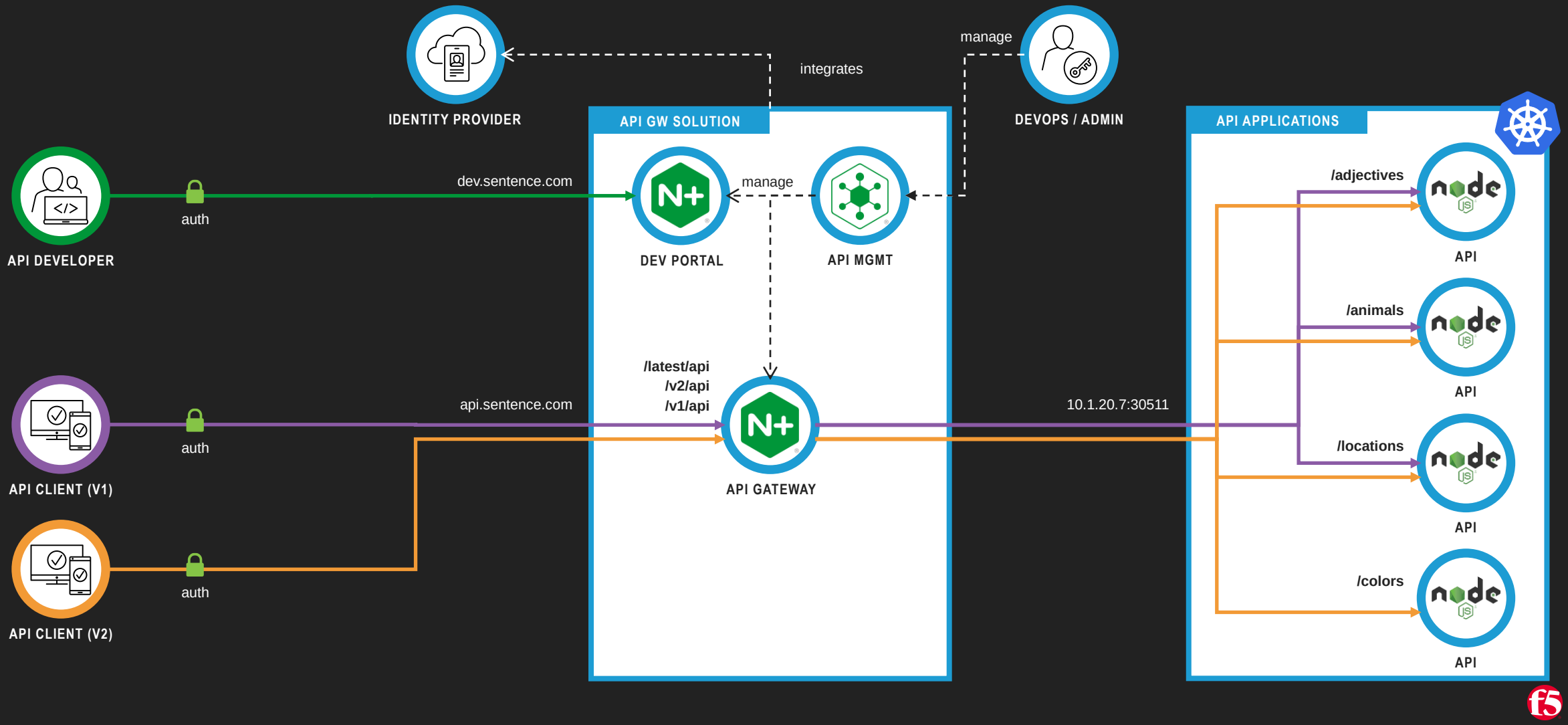
ARHICTECTURAL DIAGRAM

Demo Setup



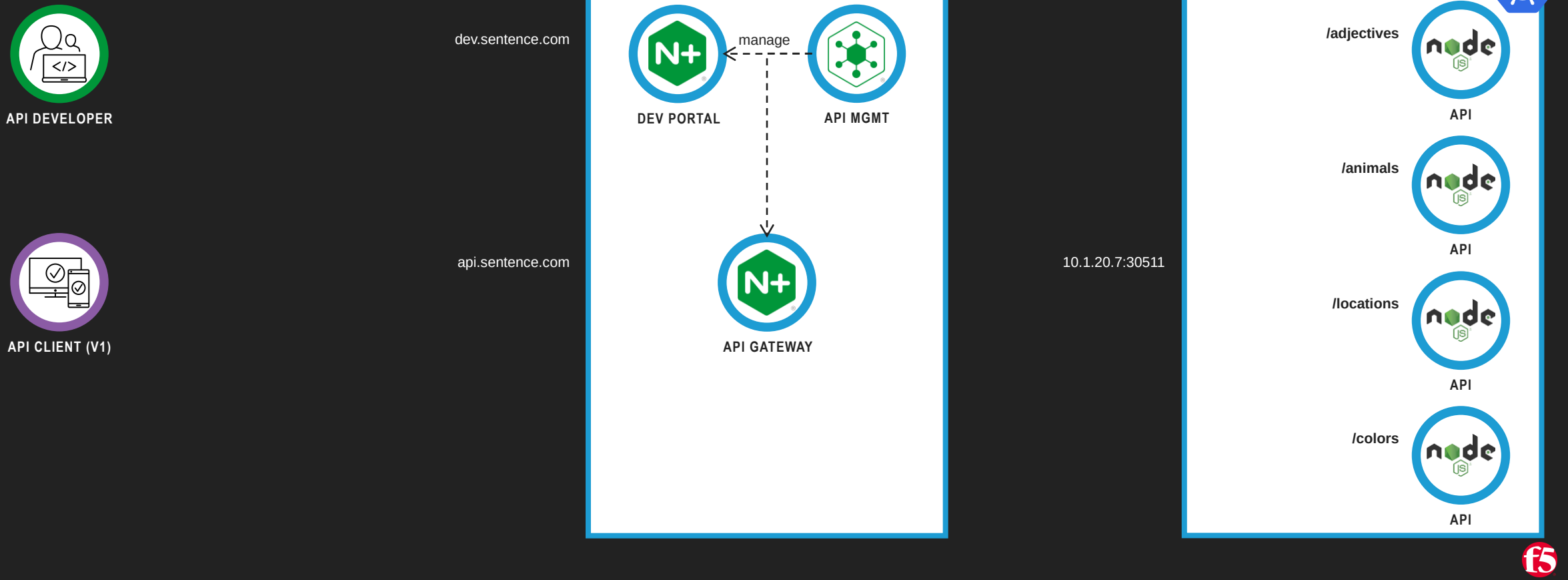
ARHICTECTURAL DIAGRAM

Demo Setup



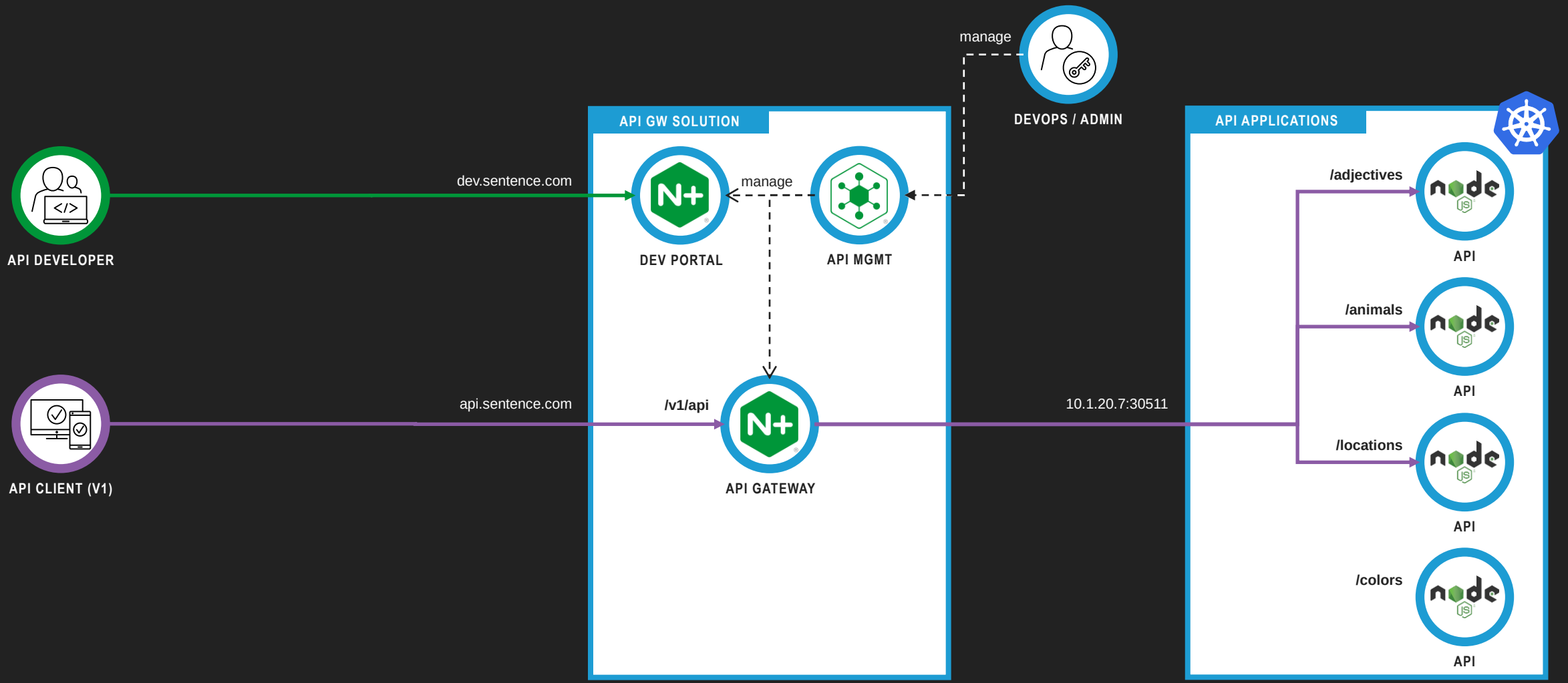
API GATEWAY DEMO

#1 – Initial Setup



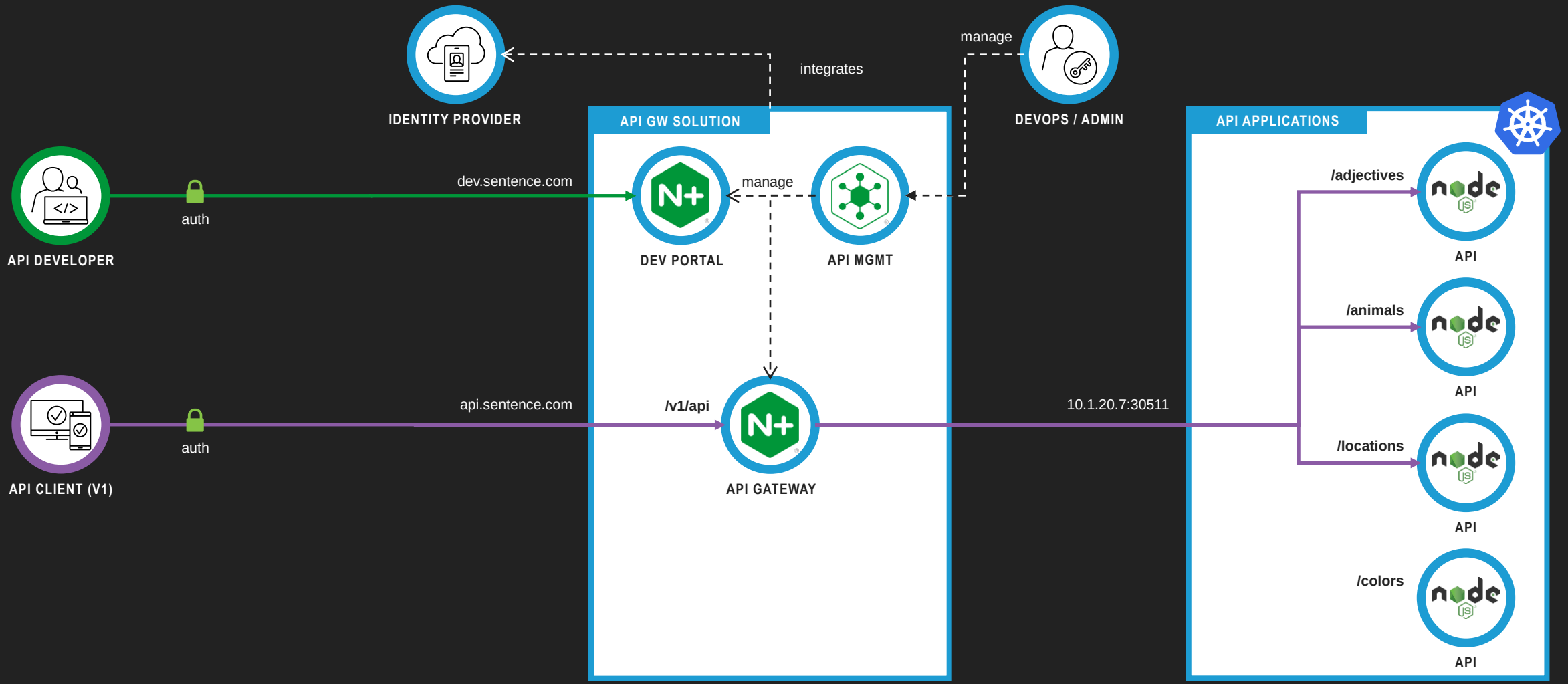
API GATEWAY DEMO

#2 – Publish initial API service (v1)



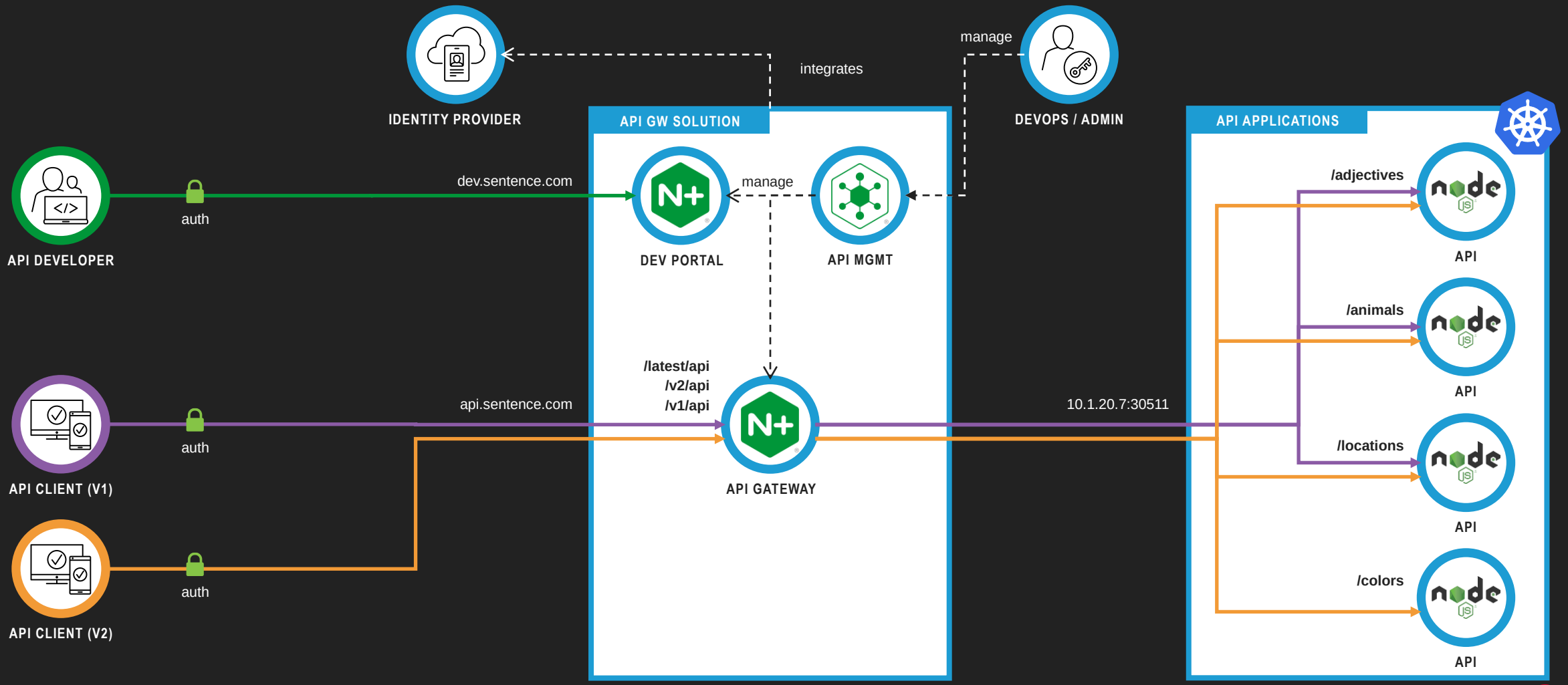
API GATEWAY DEMO

#3 – Integrate with IdP for API Auth and Mock API in DevPortal



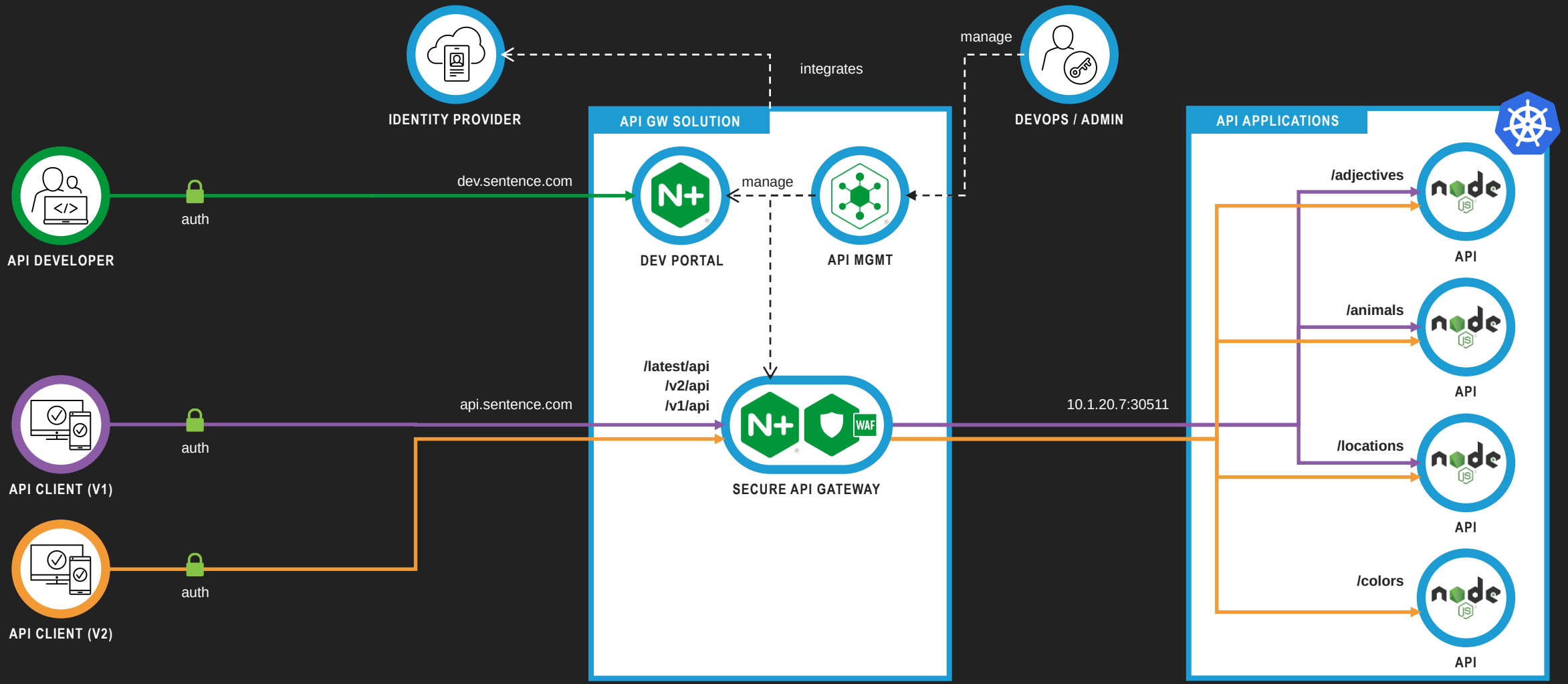
API GATEWAY DEMO

#4 – Publish multiple API Services (v2 and latest)

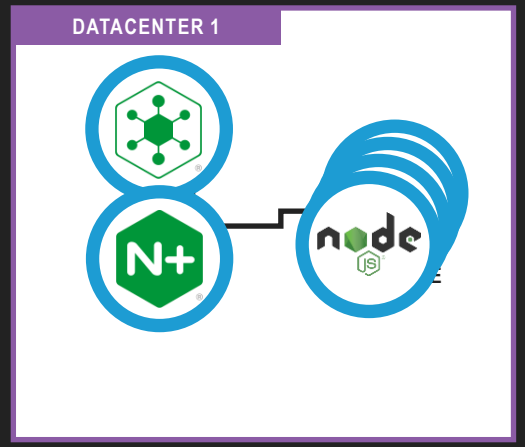


API GATEWAY DEMO

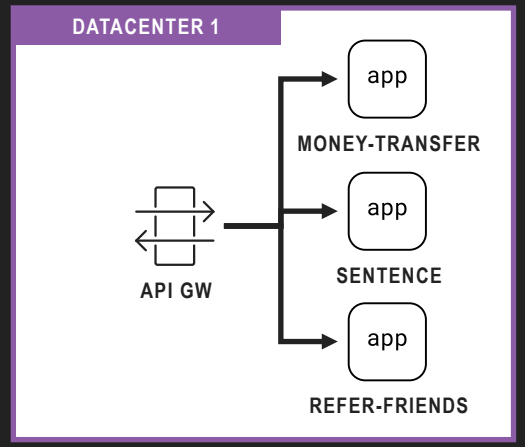
#5 – Advanced Security (Rate Limiting and WAF)



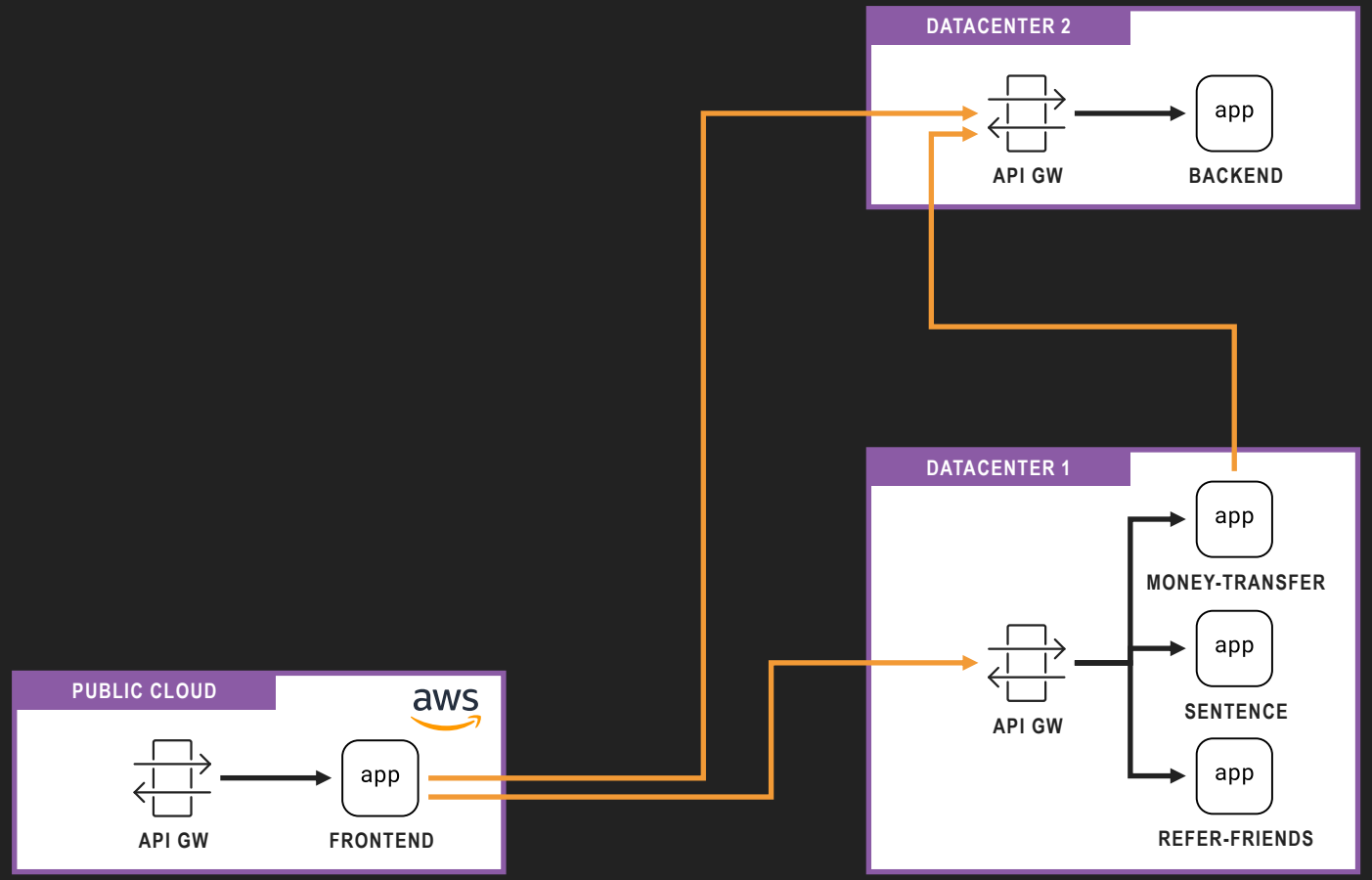
Sentence Microservices only represents 1 Module/Service



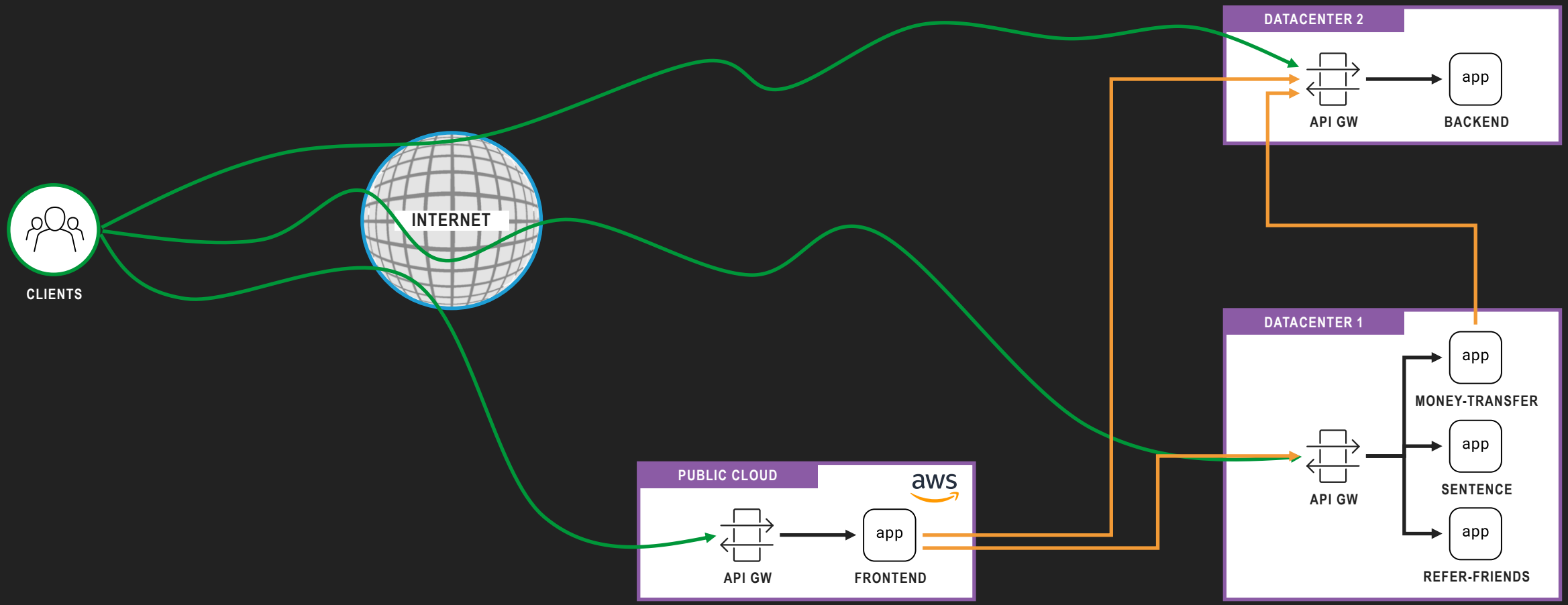
To deliver a fully functioning Modern Application, multiple microservices is required…



And all the microservices may span across Hybrid Cloud, stitched via API…



While microservices increases application resiliency, it also complicates API traffic visibility and security…

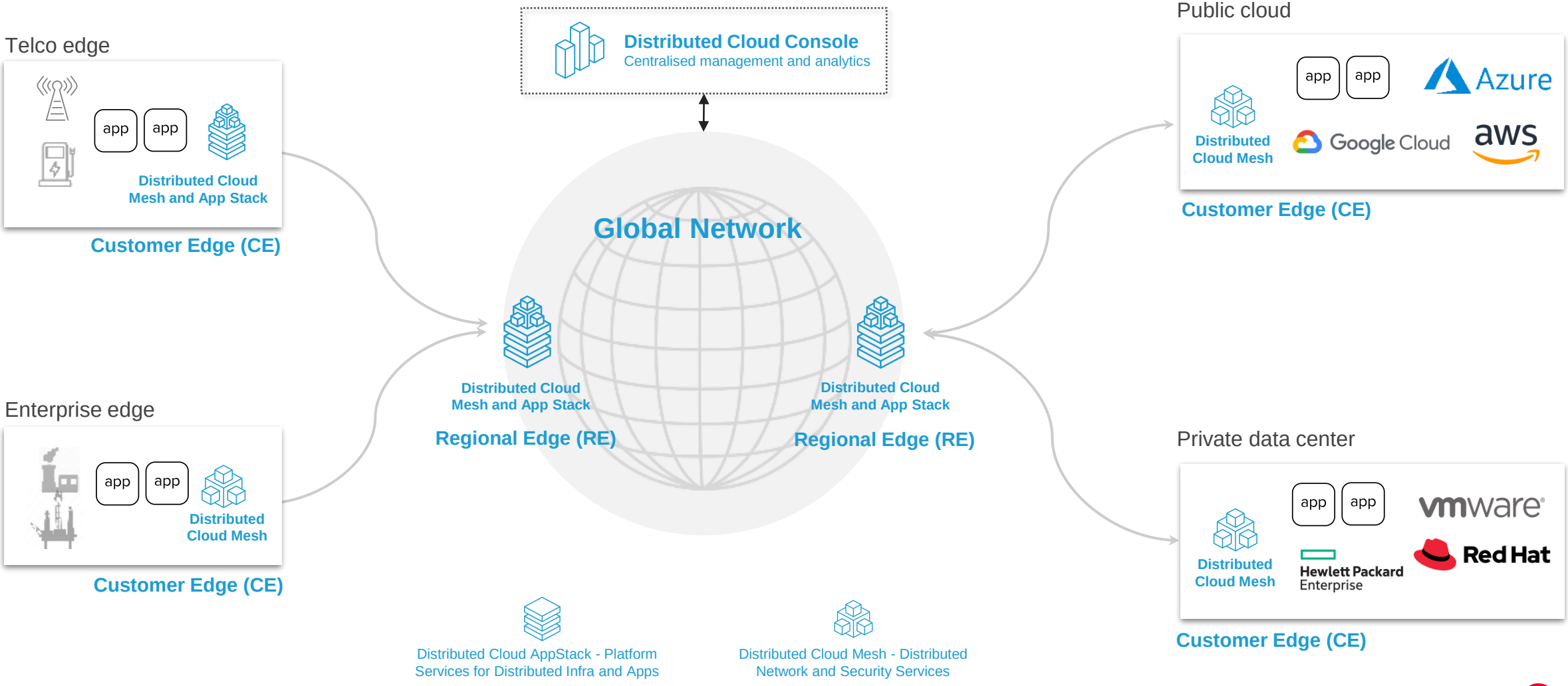


Quick Introduction on

F5 Distributed Cloud (F5 XC)

F5 Distributed Cloud – Platform Overview

Scaling to infinite number of Points of Presence (PoPs)

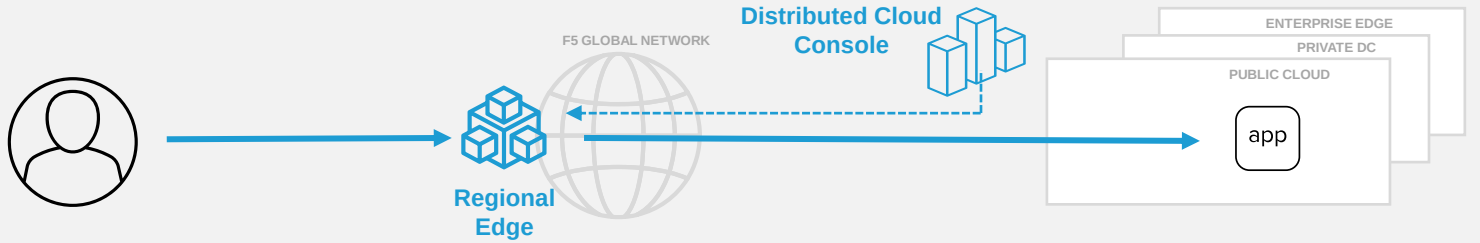


Distributed Cloud – Deployment Flexibility

Enable and consume services from global network or on premises

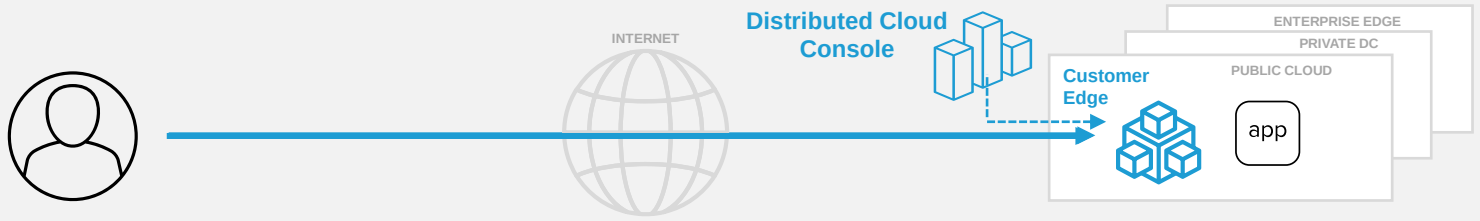
Regional Edge (RE)

Hosted in Global Network
Shared node (many customers)

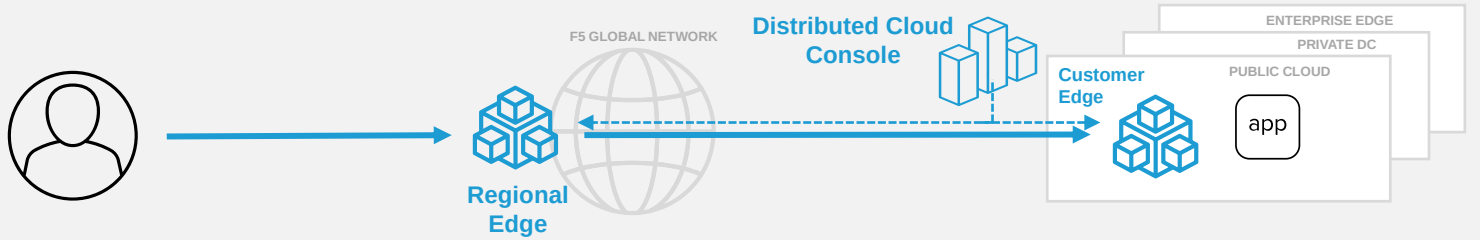


Customer Edge (CE)

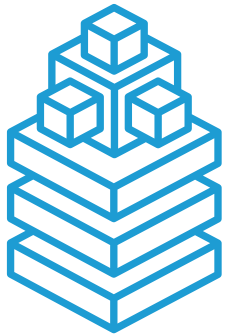
Hosted in customer premises / public cloud
Dedicated node (single customer)

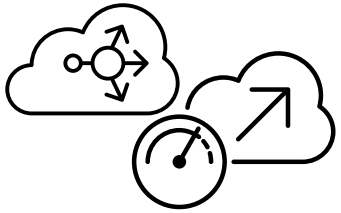


Hybrid (RE+CE)



F5 Distributed Cloud – Use Cases





Application delivery and optimisation:

DNS, Global DNS and CDN

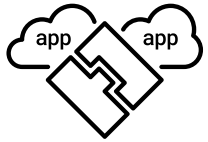
DNS delegation, primary or secondary, and global DNS for high availability

Content caching and delivery

Application Security:

Web App and API Protection

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



Application Networking:

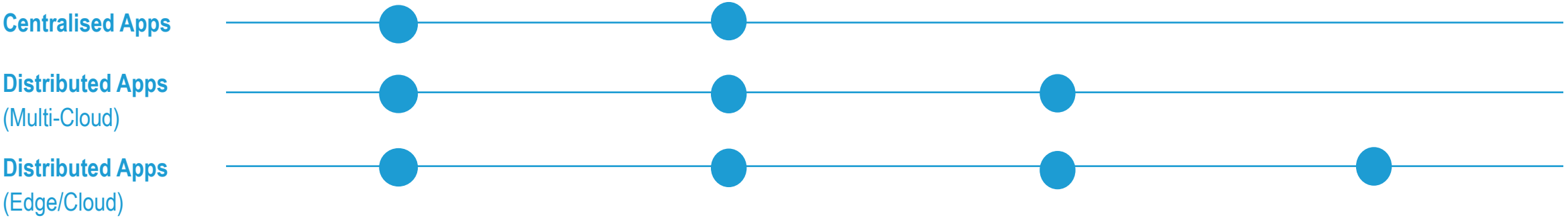
Hybrid and Multi-cloud

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

Application Deployment:

Cloud and Edge

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

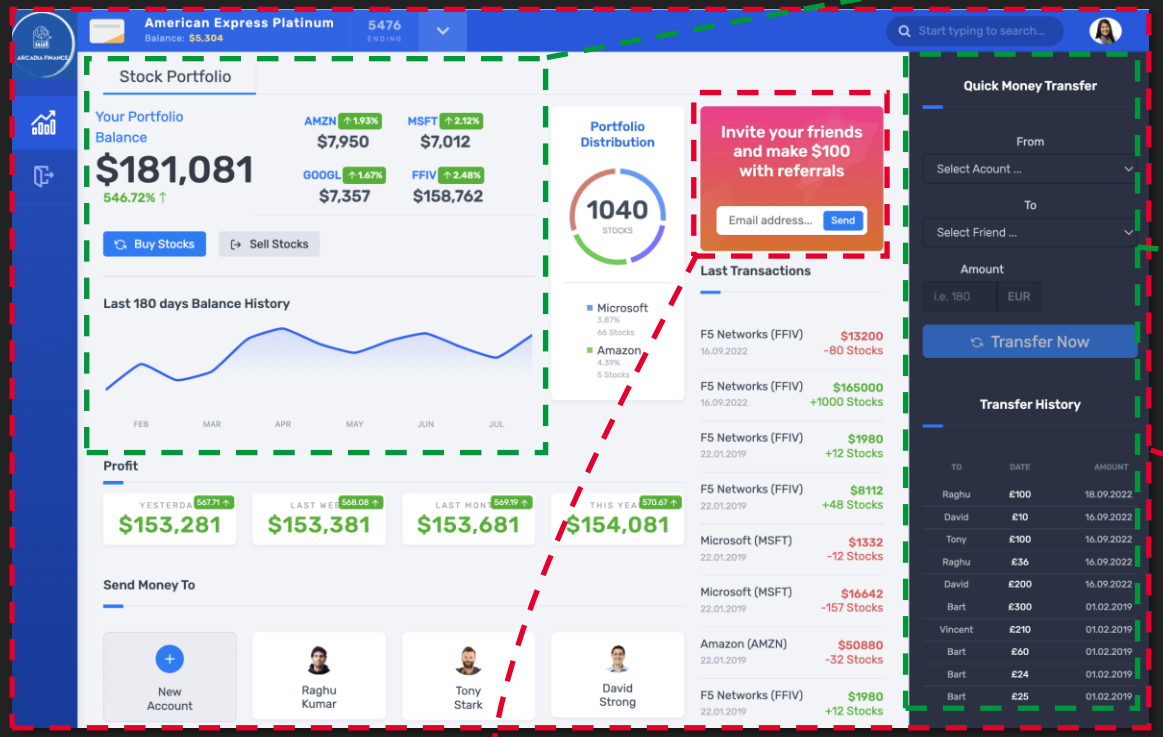


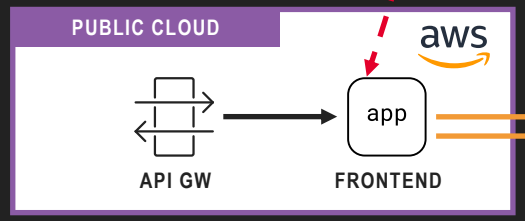
Demo #2

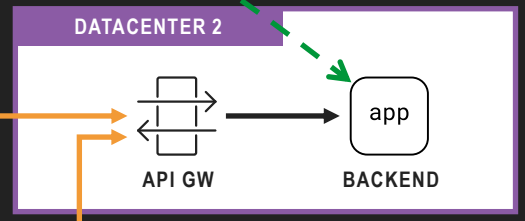
API Security Solution with F5 Distributed Cloud (F5 XC)

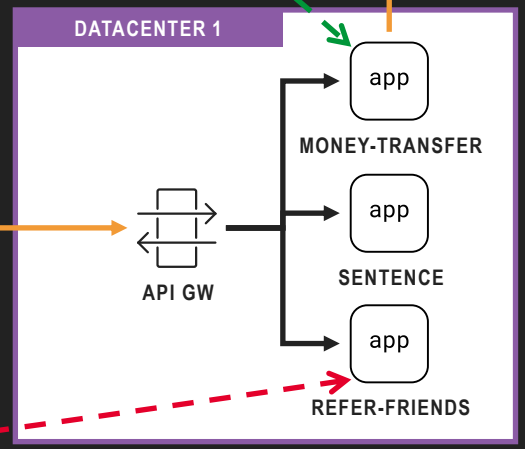
Another Sample Application

Arcadia – Financial Demo Application





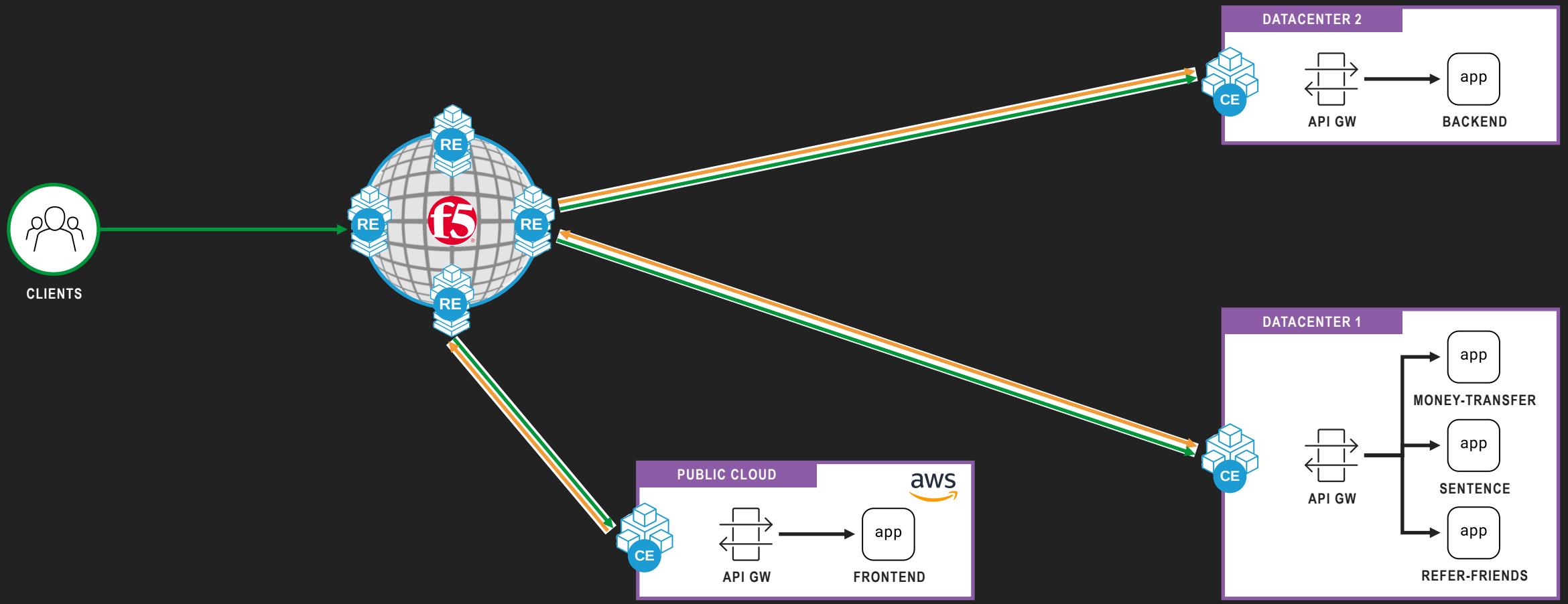




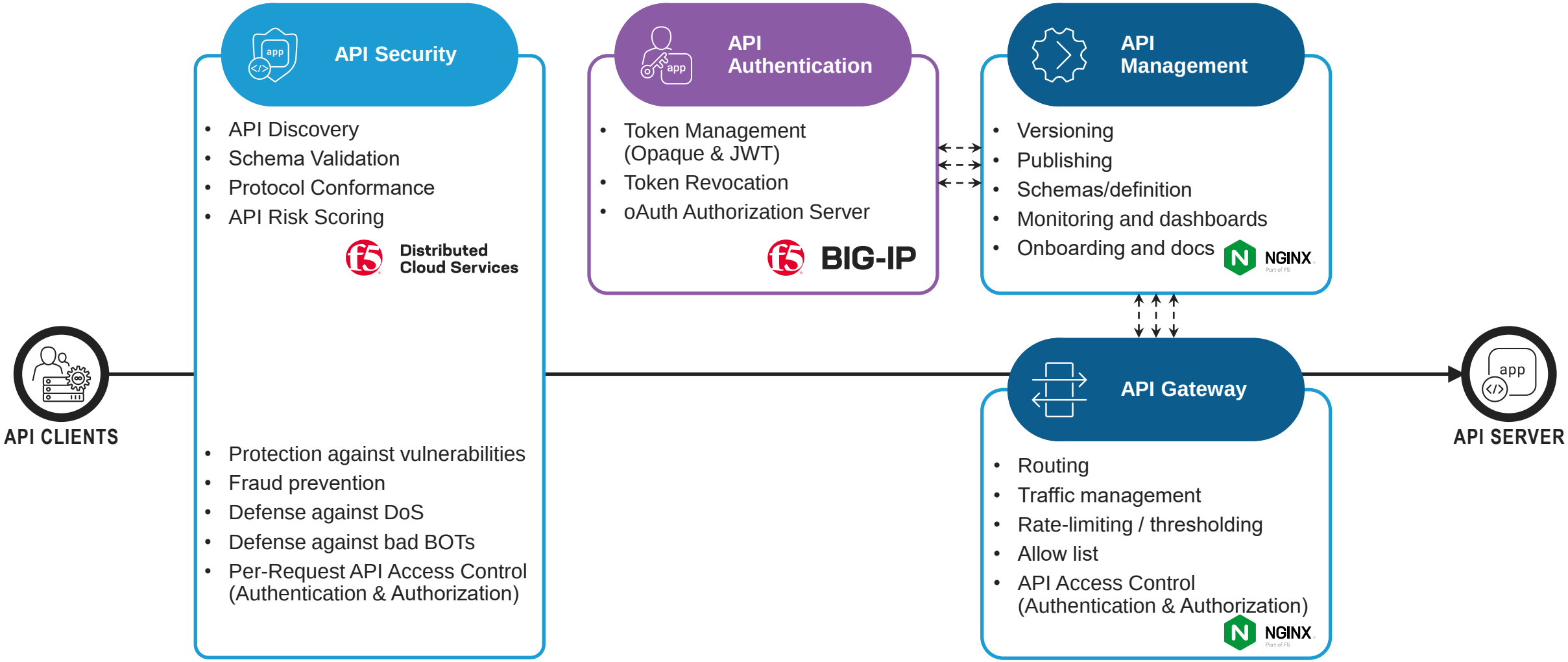
API SECURITY DEMO

#1 – API Discovery for Modern Application

Hybrid deployment mode – Regional Edge (RE) and Customer Edge (CE)



Key Requirements for ~~Standard~~ Secure API Architecture



Have more question? Reach out to us!

Or email us at: ask_marketing@f5.com