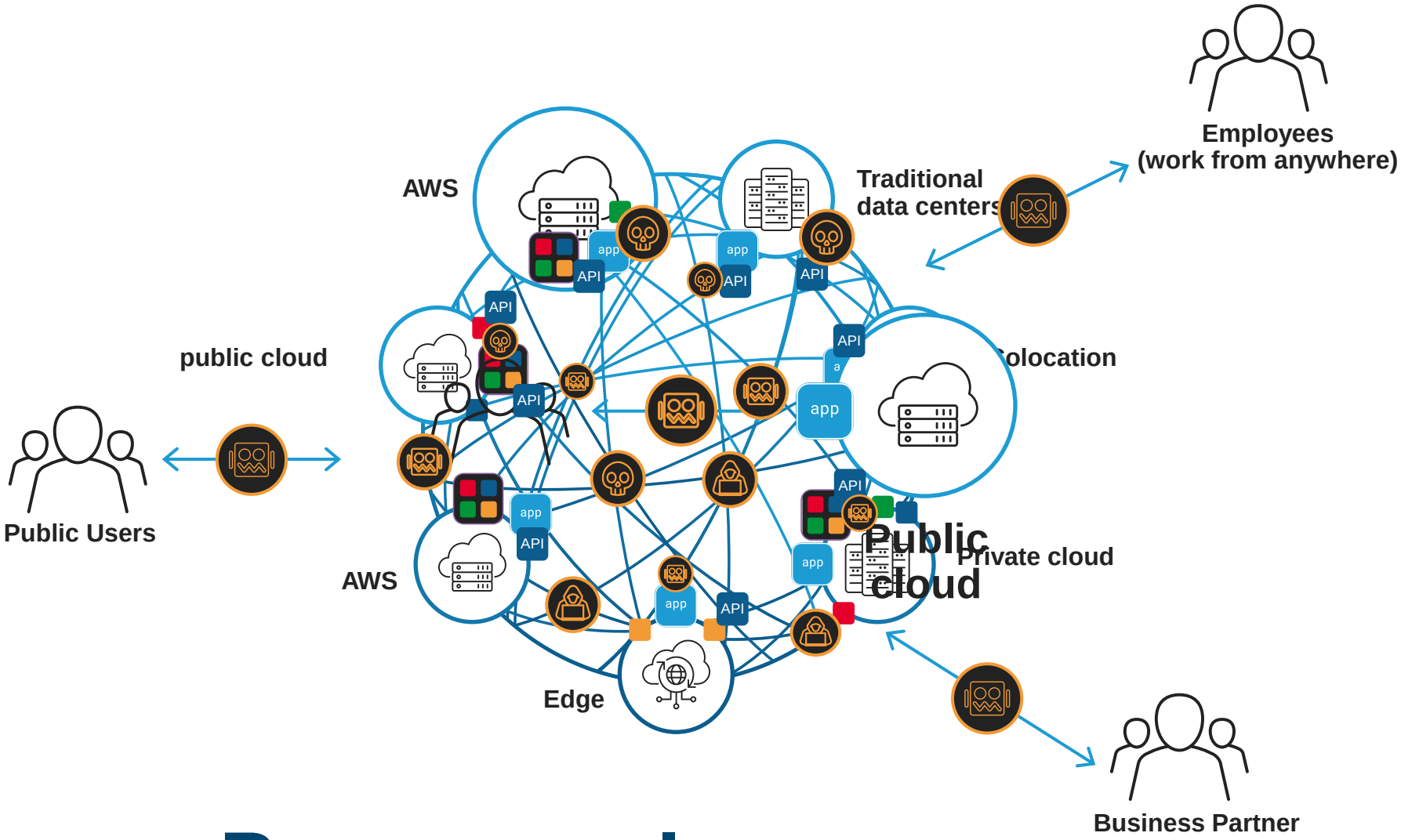
Journey to API Security

It-sa 2024 | 22.-24 October | Nuremberg

Stephan Schulz

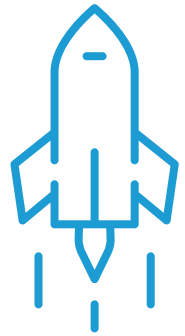
s.schulz@f5.com

The application world has changed / evolved



Application Programming Interface

over 200,000,000 APIs
are currently in use[1]



approaching 1,700,000,000 active APIs by 2030[1]

Source: [1]Continuous API Sprawl (F5 Office of the CTO)

- available – accessible from “anywhere”
- by design expose application logic – typically well-documented (not always exposed to everyone)
- provide access to sensitive data – such as personally identifiable information (PII)

What about Security?

APIs are vulnerable - just like WebApps

OWASP Top 10 API Security Risks – 2023

API1 – Broken Object Level Authorization

API2 – Broken Authentication

API3 – Broken Object Property Level Authorization

API4 – Unrestricted Ressource Consumption

API5 – Broken Function Level Authorization

API6 – Unrestricted Access to Sensitive Business Flows

API7 – Server Side Request Forgery

API8 – Security Misconfiguration

API9 – Improper Inventory Management

API10 – Unsafe Consumption of APIs

Source: https://owasp.org/API-Security/editions/2023/en/0x11-t10/

what we have today…

API-Management

- Define Policy
- Pushing Configurations
- Access Policy Management and Consumption Visualization
- Developer Portal

+

API-Gateway

- Easily Distributed
- Easily Scaled
- Heavy Lifting
- Request Processing

≠

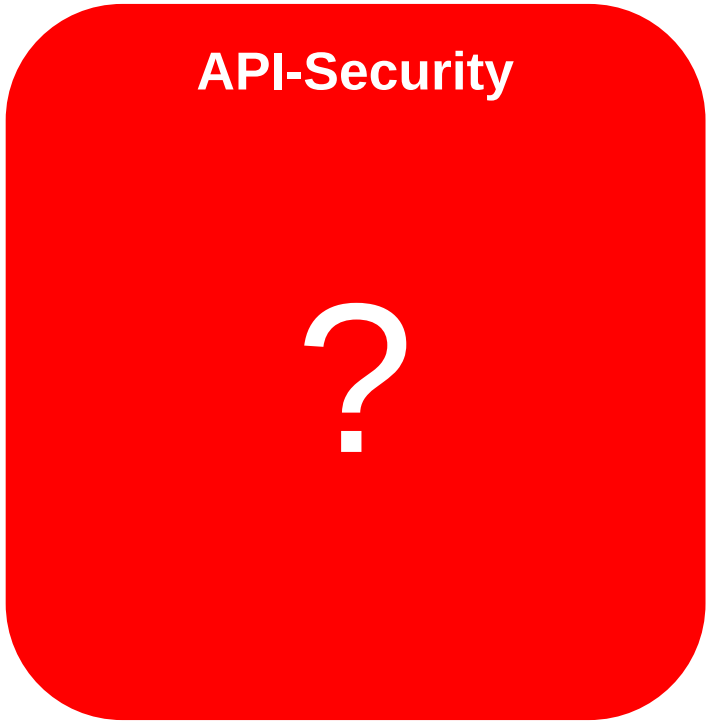
API-Security

?

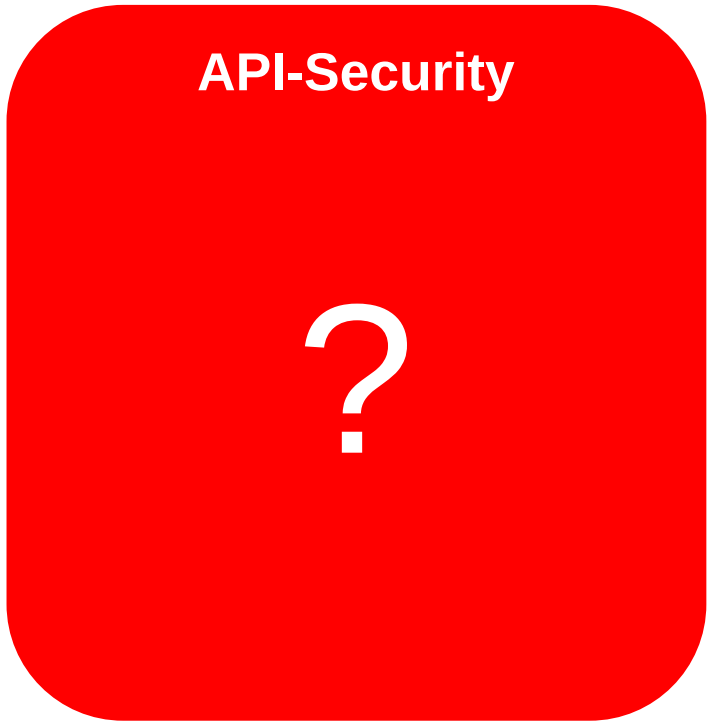
create and maintain

availability and access

What is API-Security?



API-Security Threats



- broken Authentication / Authorisation
- Vulnerabilities
- Data Breach / sensitive Data
- Brute Force / Denial of Service
- Fraud / Account Misuse
- automated Attacks / Scraping
- unusual API usage
- …

what we need today and in the future…

API-Management

- Define Policy
- Pushing Configurations
- Access Policy Management and Consumption Visualization
- Developer Portal

create and maintain

+

API-Gateway

- Easily Distributed
- Easily Scaled
- Heavy Lifting
- Request Processing

availability and access

+

API-Security

- Monitoring / Discovery
- Schema Validation
- Rate Limit / DDoS Protection
- BOT / Automation / Fraud
- Security Testing / Code Validation
- sensitive Data

detect, enforce and protect

bring it all together…

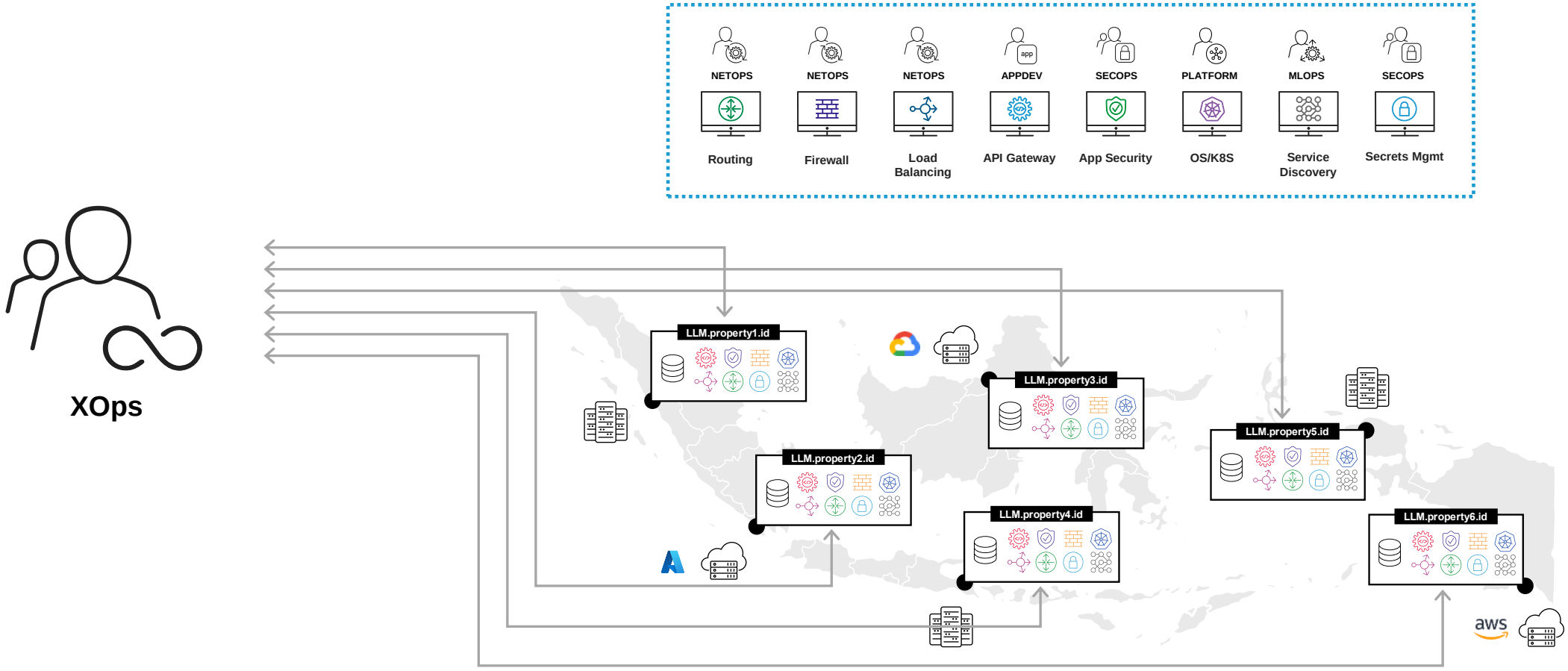
API-Security ≠ WebApp-Security

But without API-Security, there is no full WebApp-Security!

API-Security = AI-Security

AI workloads

The most modern of modern apps



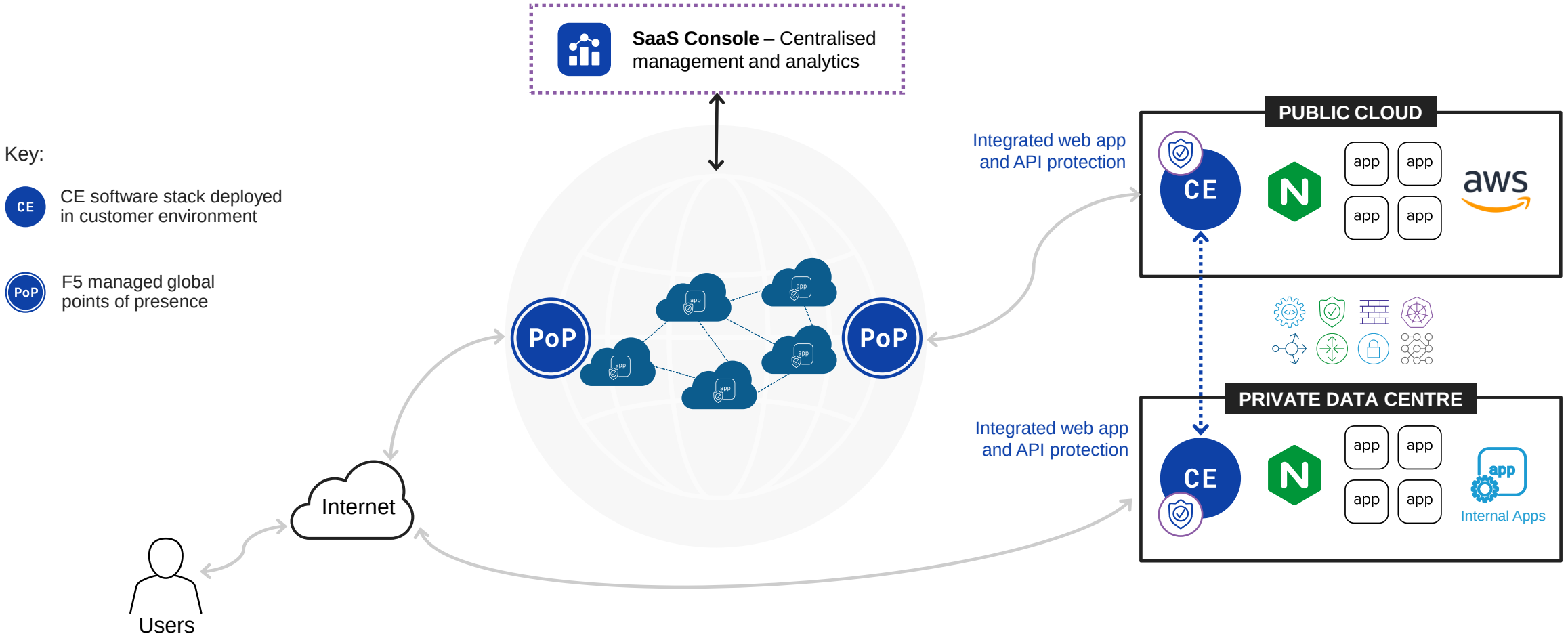
APIs require a dedicated approach for **Security** with

contiunesly **Monitoring, Discovery** and **Protection**

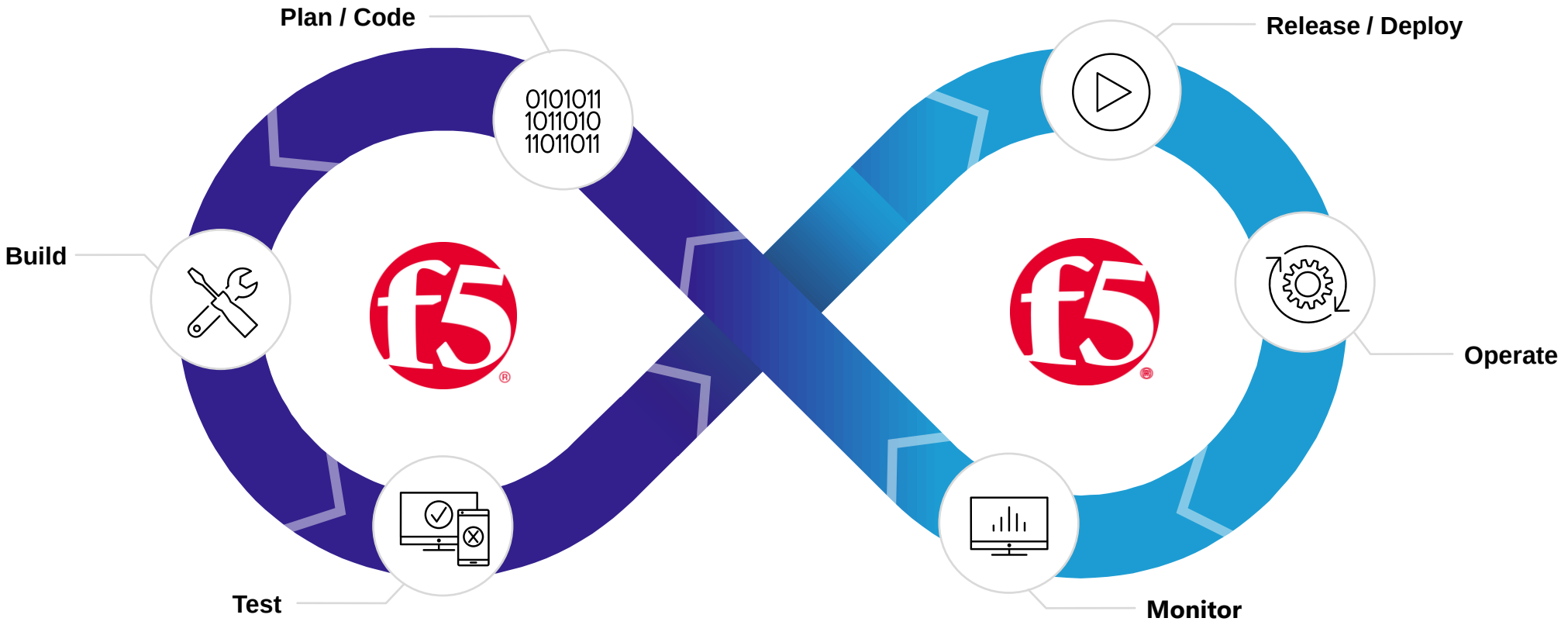
F5 Distributed Cloud (XC) - WAAP

F5 Distributed Cloud (XC) - WAAP

Scaling protection and workloads seamlessly



Integrating security earlier into the API dev pipeline is critical



API scanning and testing

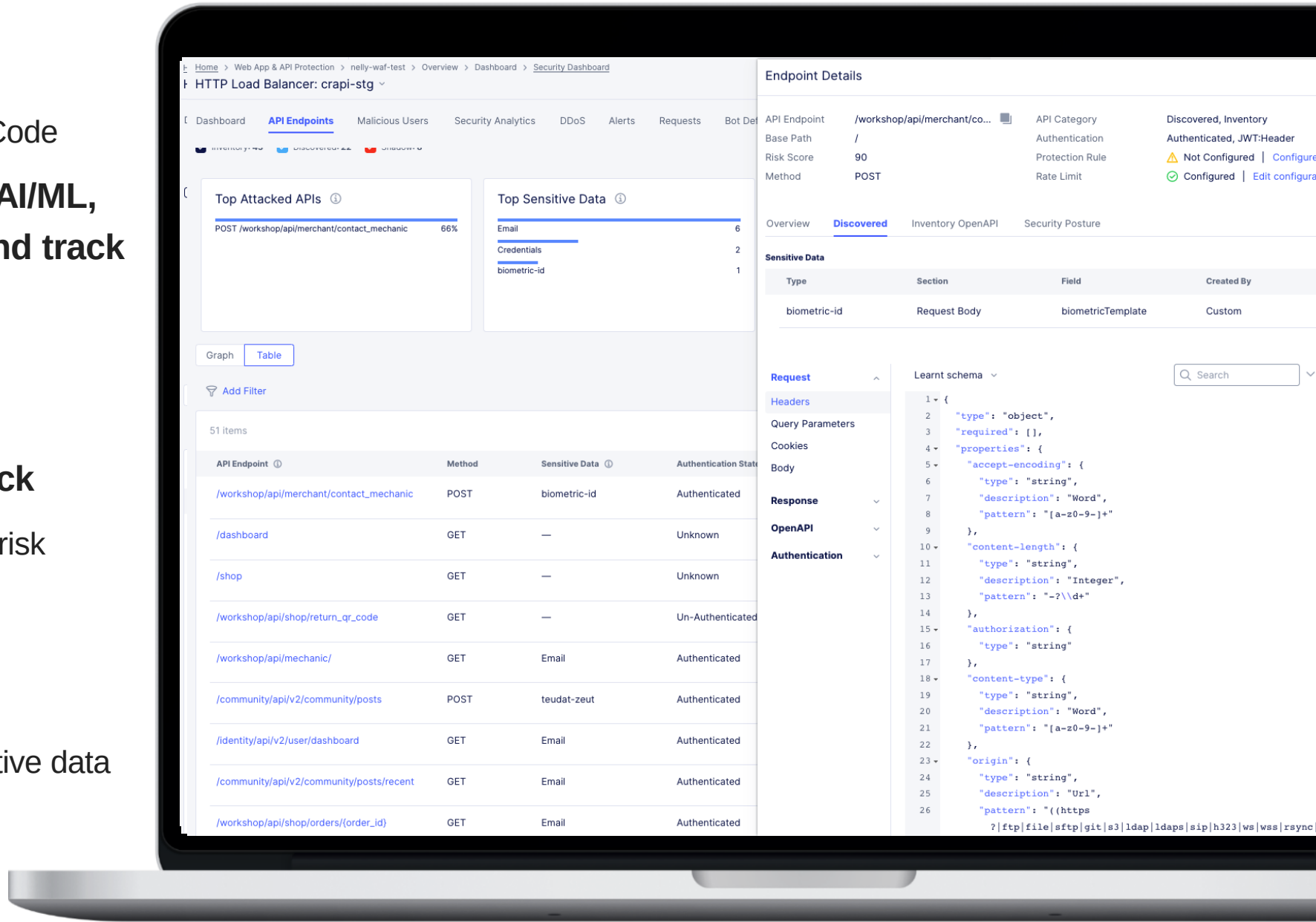
API code analysis

API discovery and traffic analysis

Runtime protection and enforcement

API Security – Key Features

- **API Discovery and Monitoring**
  - learning from Traffic and Source Code
- **Behavioral Analysis by using AI/ML, models are built to baseline and track API behavior**
  - detect outliers and shadow APIs
- **Discovery | Validation of API Authentication – option to block**
  - Authentication status, details and risk scoring for all API endpoints
- **Discovery and Monitoring for PII Data in APIs**
  - masking capabilities to hide sensitive data



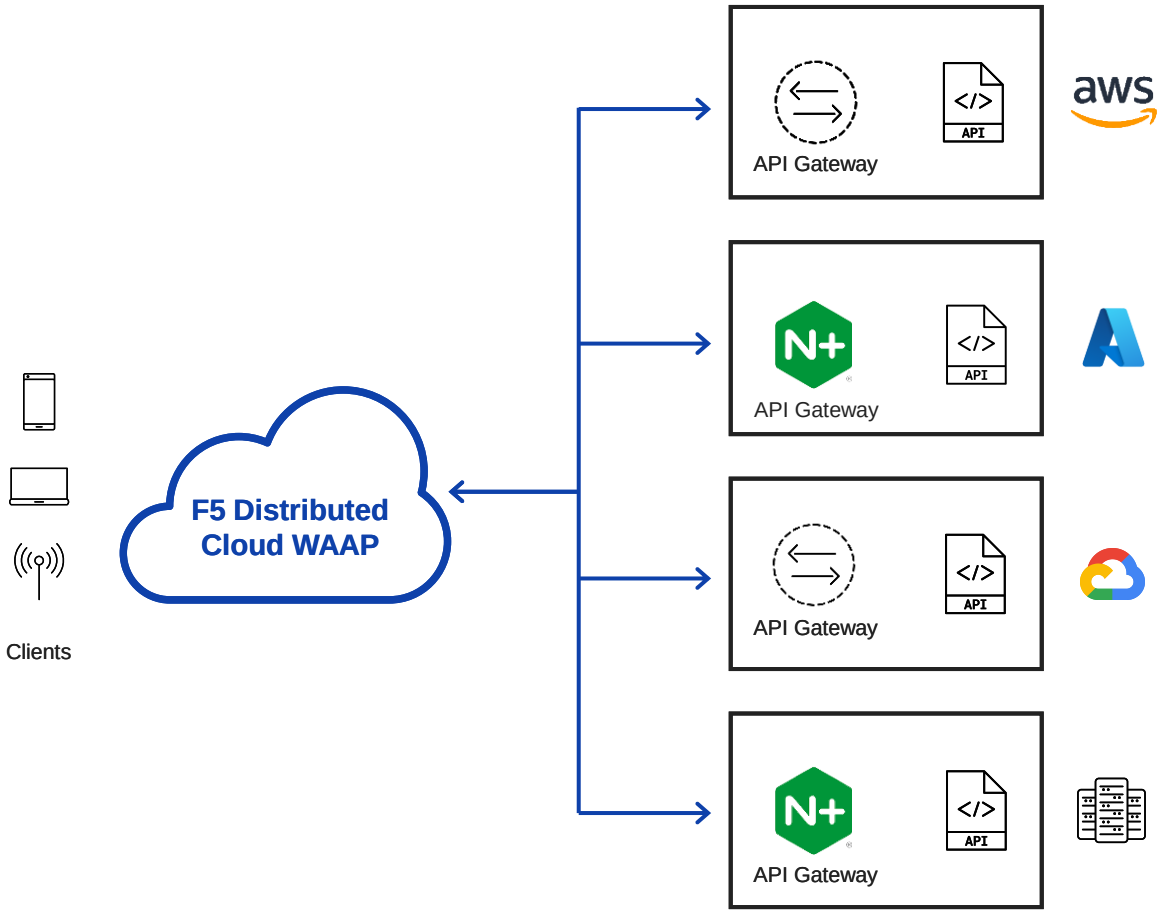
F5 Distributed Cloud comprehensive API Security

Discovery, Monitoring and Protection for any API

API-Security

- Monitoring / Discovery
- Schema Validation
- Rate Limit / DDoS Protection
- BOT / Automation / Fraud
- Security Testing / Code Validation
- sensitive Data

detect, enforce and protect



Discover

Dynamically learn and document API endpoints

Monitor

Continuously inspect and identify anomalies with API endpoints

Secure

Enforce API behavior and block/limit undesirable or malicious traffic