

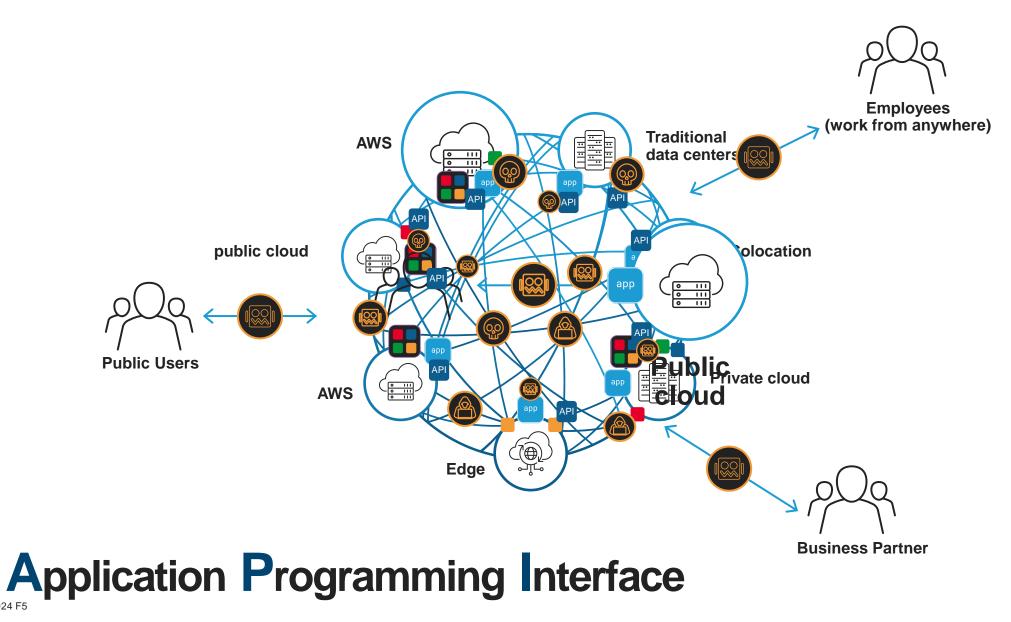
# Journey to API Security

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

Stephan Schulz

s.schulz@f5.com

## The application world has changed / evolved







### over 200,000,000 APIs are currently in use<sup>1</sup>

### approaching 1,700,000,000 active APIs by 2030<sup>1</sup>



• 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

API6 – Unrestricted Access to Sensitive Business Flows

API7 – Server Side Request Forgery

API3 – Broken Object Property Level Authorization

**API8 – Security Misconfiguration** 

API4 – Unrestricted Ressource Consumption

API9 – Improper Inventory Management

**API5** – Broken Function Level Authorization

API10 – Unsafe Consumption of APIs

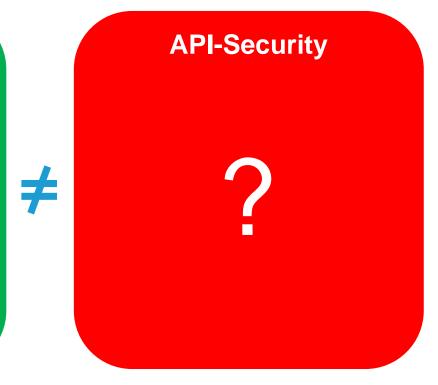
### what we have today...

#### **API-Management**

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

#### **API-Gateway**

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



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

#### **API-Gateway**

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

#### **API-Security**

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

create and maintain

availability and access

detect, enforce and protect

# bring it all together...

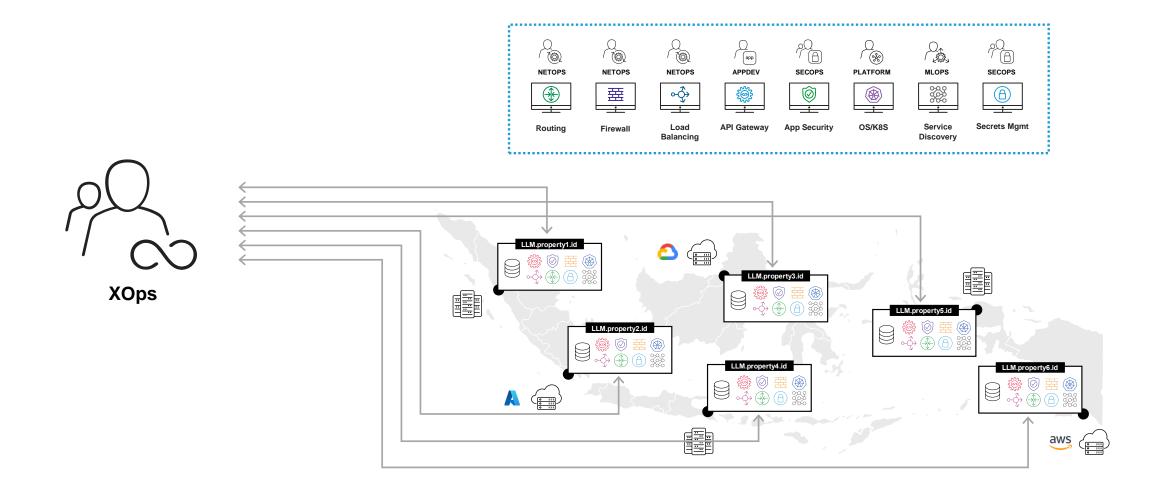
# API-Security **#** WebApp-Security

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

# API-Security AI-Security

# Al workloads

The most modern of modern apps



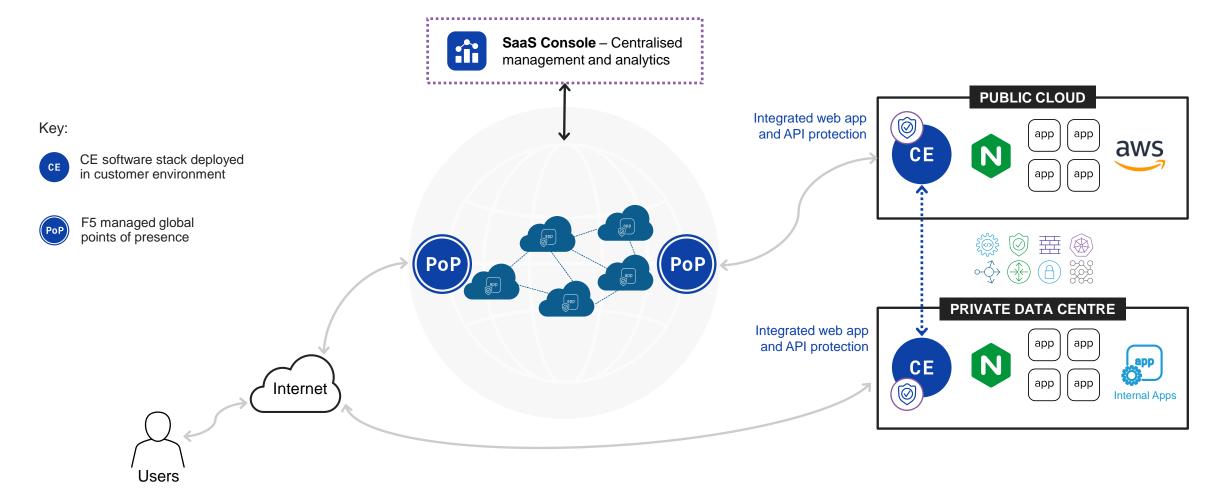
# APIs require a dedicated approach for **Security** with

# contiunesly Monitoring, Discovery and Protection

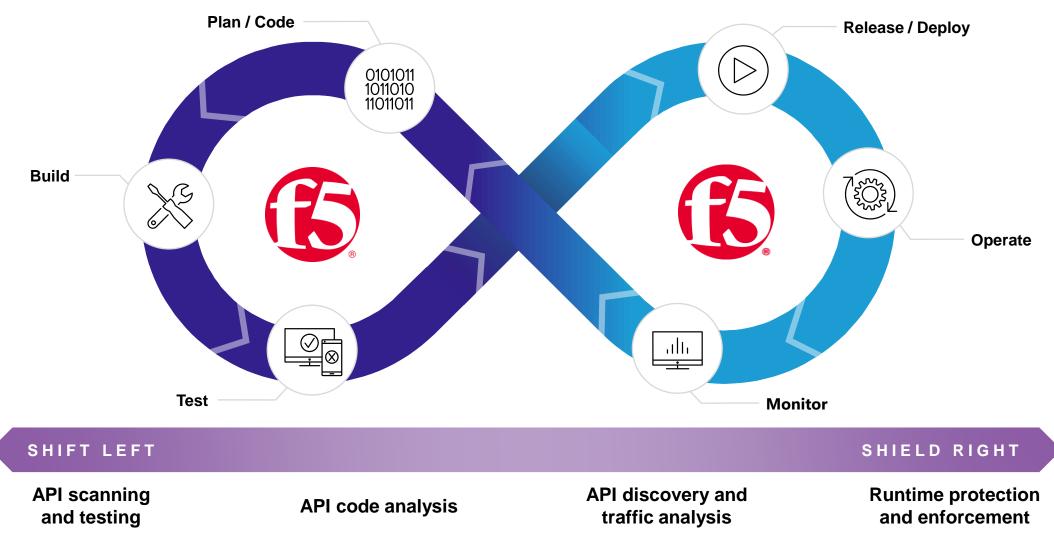
## F5 Distributed Cloud (XC) - WAAP

# F5 Distributed Cloud (XC) - WAAP

Scaling protection and workloads seamlessly



## Integrating security earlier into the API dev pipeline is critical



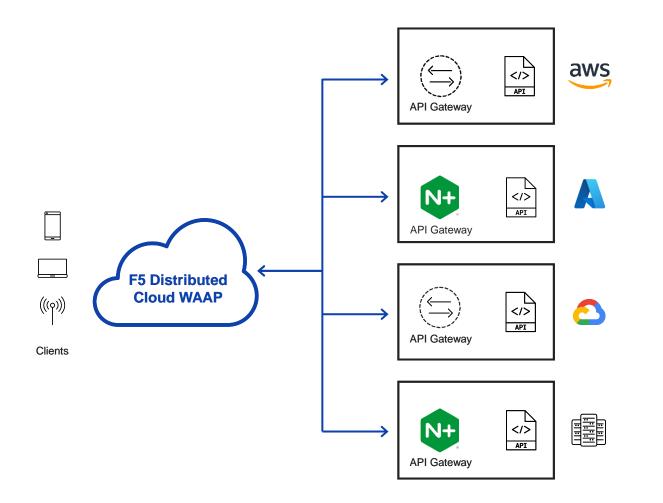
# **API Security – Key Features**

- API Discovery and Monitoring
  - learning from Traffic and Source Code
- Behavioral Analysis by using Al/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

|   | Home > Web App & API Protection > nelly-waf-test > Overview > Dashboard > Security Dashboard     HTTP Load Balancer: crapi-stg ~                        |            |                                  |                                   |  | Endpoint Details |  |  |   |  |
|---|---|------------|----------------------------------|-----------------------------------|--|------------------|--|--|---|--|
|   | E Dashboard API Endpoints Malicious Users Security Analytics DDoS Alerts Requests Bot De  |            |                                  |                                   |  | )                | o/api/merchant/co 📕  | API Category<br>Authentication<br>Protection Rule  | Discovered, Inventory<br>Authenticated, JWT:Header<br>Not Configured   Configured<br>Configured   Edit configured |  |
| C | Top Attacked APIs ③     Top Sensitive Data ③       POST /workshop/api//merchant/contact_mechanic     66%       Email     Credentials       biometric-id |            |                                  | 6<br>2<br>1                       | Method POST Overview Discovered Sensitive Data Type biometric-id |                  | Inventory OpenAPI<br>Section<br>Request Body               | Rate Limit<br>Security Posture<br>Field<br>biometricTemplate   | Created By<br>Custom  |  |
|   | Graph Table<br>Add Filter<br>51 items   |            |                                  |                                   | Request<br>Headers<br>Query Parameters                           | ^                | Learnt schema ~<br>1 ~ {<br>2 "type": "ob<br>3 "required": |  | Q Search  |  |
|   | API Endpoint ① /workshop/api/merchant/contact_mechanic  | Method     | Sensitive Data ①<br>biometric-id | Authentication State              | Cookies<br>Body<br><b>Response</b>                               | ~                | 6 "type":<br>7 "descri                                     | <pre>encoding": {     "string",     ppion": "Word",     n": "[a-20-9-]+" elength": {     "string",     ppion": "Integer",     n": "-?\\d+" encode the string" </pre> |   |  |
|   | /dashboard<br>/shop   | GET<br>GET | -                                | Unknown<br>Unknown                | OpenAPI ~<br>Authentication ~                                    | ~                | 11 "type":<br>12 "descri                                   |  |   |  |
|   | /workshop/api/shop/return_qr_code<br>/workshop/api/mechanic/  | GET<br>GET | —<br>Email                       | Un-Authenticated<br>Authenticated |  |                  | 14 },<br>15 - "authoriz<br>16 "type":<br>17 },             |  |   |  |
|   | /community/api/v2/community/posts<br>/identity/api/v2/user/dashboard  | POST       | teudat-zeut<br>Email             | Authenticated                     |  |                  | 20 "descrip  |  |   |  |
|   | /community/api/v2/community/posts/recent<br>/workshop/api/shop/orders/(order_id)  | GET<br>GET | Email                            | Authenticated                     |  |                  | 23 - "origin":<br>24 "type":<br>25 "descri<br>26 "patter   | "string",<br>ption": "Url",<br>n": "((https  | ldaps sip h323 ws wss rsynd   |  |

# 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

