



Layer7 API Security

Trusted API Security at Scale

Christian Oberlé – API Technical Lead EMEA

July 2025



APIs

A door to your applications and systems

- APIs are everywhere
- They power your apps and systems
 - Mobile, Web, IoT, ATM...
 - Private APIs, internal integrations
 - B2B

“The linchpin of digital business”

“Reshaping the way business operate in the digital era”

“Strategic imperative for modern enterprise”

FORRESTER

Gartner

IDC



APIs, APIs, APIs ...

←

→

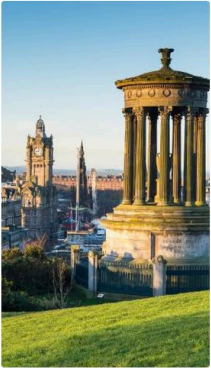
🏠

🔒 https://www.booking.com

☆ ↻

Escape the routine – for a week or a while

Our favorite destinations for getting away from it all




Edinburgh

United Kingdom

1,565 properties

Starting from € 50




Venice

Italy

2,673 properties

Starting from € 50




Bristol

United Kingdom

377 properties

Starting from € 56



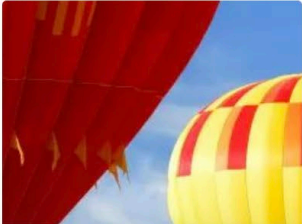
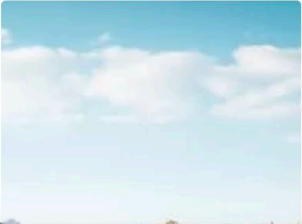
Dubrovnik

Croatia

2,456 properties

Starting from € 32

Get inspiration for your next trip



Inspector

Filter URLs

All HTML CSS

Status	Method	File	URL
302	GET	v2?client_id=vO1Kblk7xX9tUn2cpZLS&redi	https://account.booking.com/oauth...
302	GET	login.html?code=o5sG6eaOrkqdzjR4fL6Olt	https://secure.booking.com/login.ht...
200	GET	general.html?label=gen173nr-1FCAEoggl46	https://www.booking.com/general.ht...
200	GET	activityi;src=4228414;type=funne910;cat=c	https://4228414.fls.doubleclick.n...
200	GET	select?client_id=901905703382-m88jn1h9	https://accounts.google.com/gsi/ifra...
200	GET	i?nid=54f04dd9_4d34_47aa_87a6_989712	https://ltsnapchat.com/cm/i?nid=5...
11 requests		174.78 KB / 74.49 KB transferred	Finish: 16.08 min DOMContentLoaded: 1.80 s

Headers

Cookies

Request

Response

Timings

Security

Filter Headers

Block Resend

GET https://www.booking.com/general.html?label=gen173nr-1FCAEoggl46AdIM1gEaE2IAQGYATG4AQfIAQ_YAQHoAQH4AQKIAGGoAgO4Au3E-4oGwAIB0gIkMDJhY2EwNDAtMGU5Yi00MGVILWI1NmEtNjFiNmIwNDY3YmQz2AIF4AIB;sid=bb3f809a688567d5184cb37920f40cb5;iframe=1;tmpl=profile/login_callback_anon_sessio

n&=

Status 200 OK

Version HTTP/1.1

Transferred 1.32 KB (327 B size)

Referrer Policy origin-when-cross-origin

Response Headers (1.113 KB)

Raw

cache-control: private

content-encoding: br

content-length: 208

content-security-policy-report-only: frame-ancestors www.booking.com; report-uri https://reports.book

ing.com/csp_violation?type=report&tag=179&pid=749354f8256c0092&e=UmFuZG9tSVYkc2Rllyh9YUXi

zIM4n0j9zubmwcEJFBEJw63BpL1dnnlAN6fAMcQT&f=2&s=0;

content-type: text/html; charset=UTF-8

main.30b4c3f2.js

https://s.pining.com/ct/lib/main.30b...

268 requests

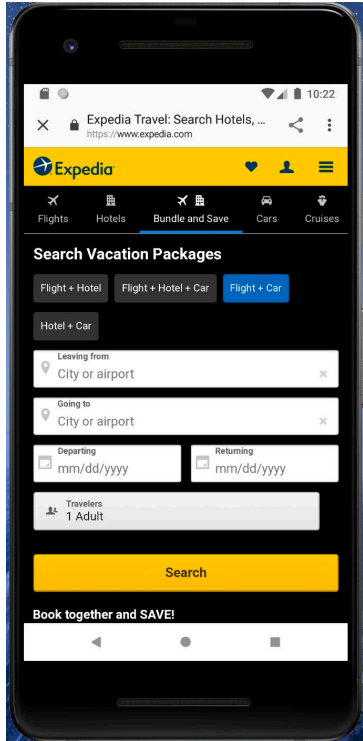
5.44 MB / 2.30 MB transferred

Finish: 1.03 min

DOMContentLoaded: 1.80 s

load

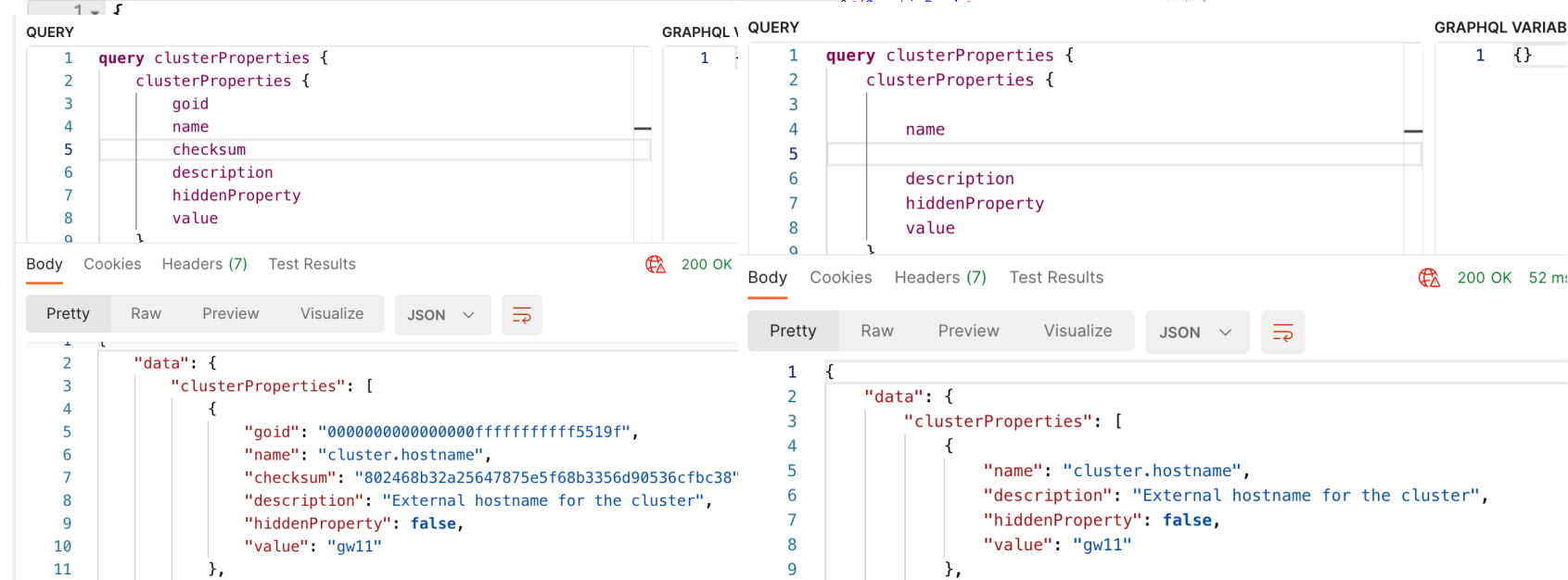
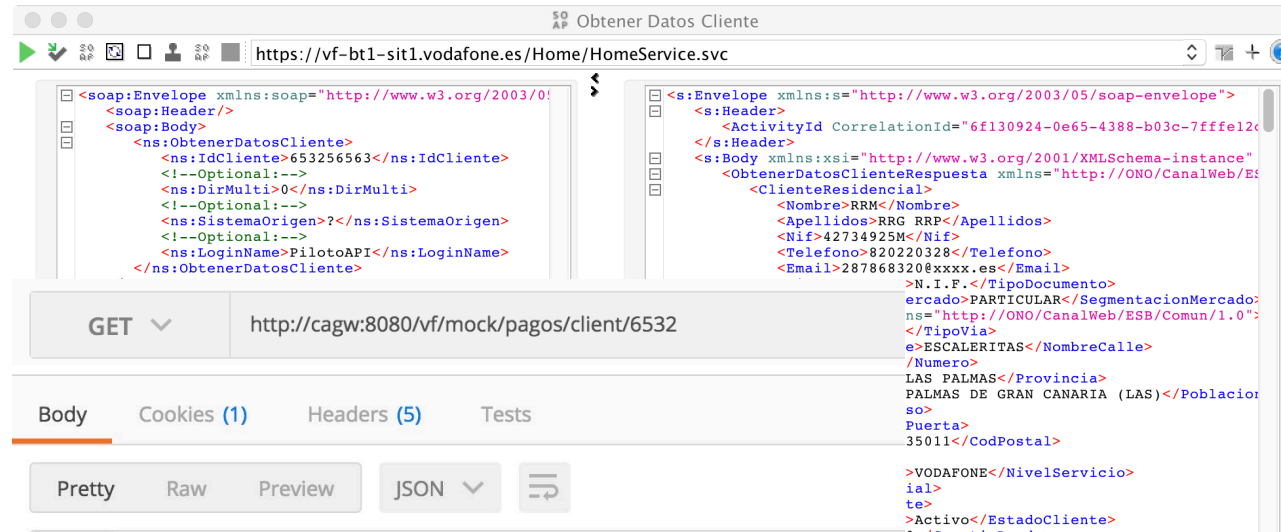
What is an API?



SOAP / XML

REST / JSON

GraphQL



API security is paramount

Securing your APIs is securing your applications



- APIs are an attractive attack target
- Breaches are on the rise
 - Cyber attacks exploit vulnerabilities in poorly secured interfaces
- Costly consequences
 - Financial loss
 - Reputation damage
 - Legal, regulatory consequences
 - Remediation costs
 - Human lives

API security struggles

What is hard about API security?

- Lack of authorization, weak authentication
- Compromised secrets, keys
- Unmanaged, unsecured shadow APIs
- Orchestrating API access control at scale, across clouds
- Security aware context of message content
- AI increases threat scale, humans can't keep up



API security
top-10 vulnerabilities

API1:2023 - Broken Object Level Authorization	API2:2023 - Broken Authentication	API3:2023 - Broken Property Level Authorization	API4:2023 - Unrestricted Resource Consumption	API4:2023 - Broken Function Level Authorization
API6:2023 - Unrestricted Access to Sensitive Business flow	API7:2023 - Server Side Request Forgery	API8:2023 - Security Misconfiguration	API9:2023 - Improper Inventory Management	API10:2023 - Unsafe consumption of APIs

Layer7 - Comprehensive API Security Infrastructure

Real-time Security & Integration

- Advanced security profile and zero trust through identity security
- Certified API infrastructure for high-value APIs allowing advanced security orchestration
- Advanced security, integration and transformation policy driven solution
- Powerful message and security introspection and transformation
- OWASP API security Top-10 vulnerabilities defense
- Secure API firewall & gateway security

APIOps at Scale

- Centralized governance for all API security stakeholders
- Automatic application of security across multi-clouds
- X-Region API metering
- Configure once/deploy anywhere

API Management

- Publish APIs, documentation
- Control API access across multi-cloud
- Discover APIs
- Advanced Developer Experience

API Intelligence

- Business insights from APIs usage
- Respond to threats and vulnerabilities
- Feed AI engines with context-enriched API traffic metadata

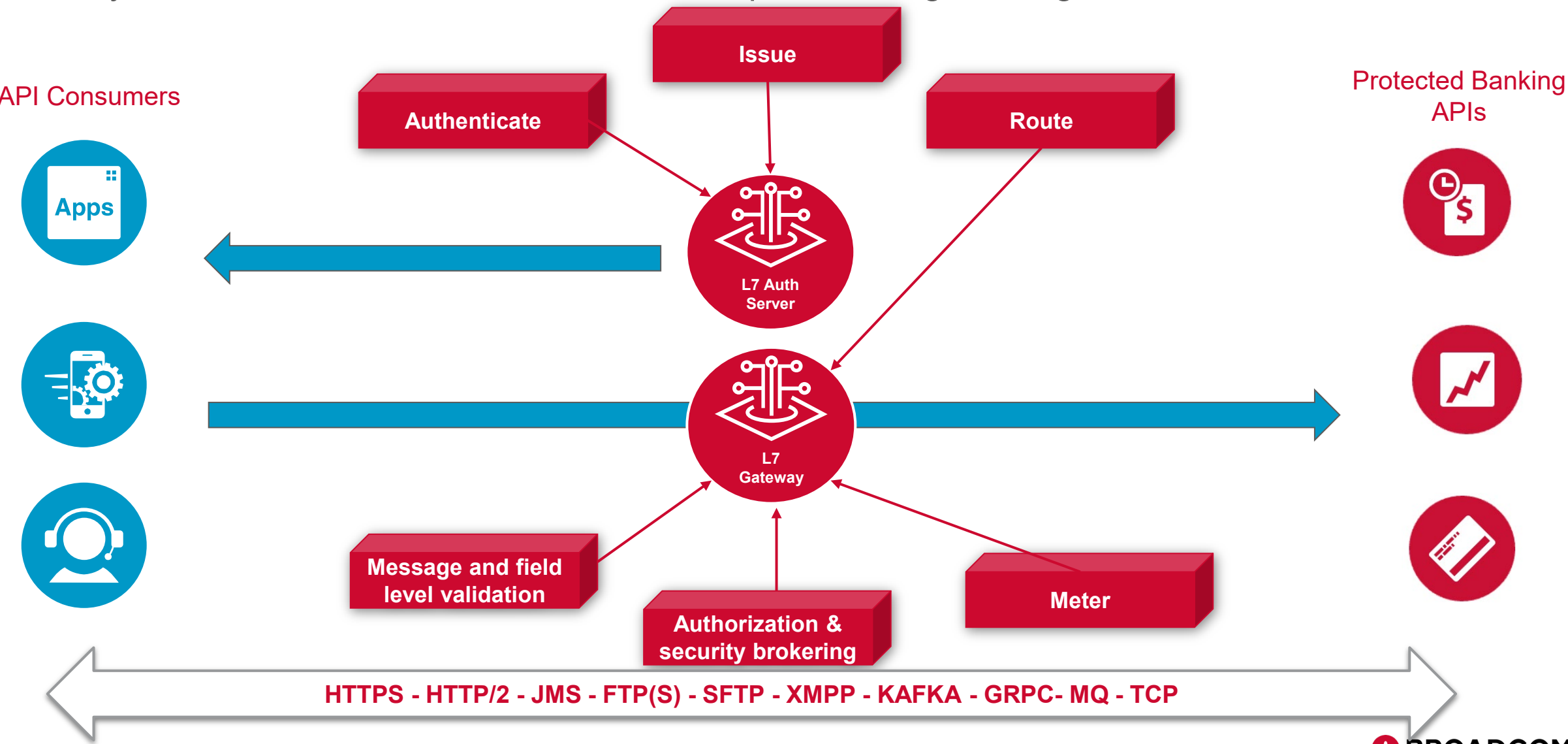
Real-time Security & Integration



Use case: Securing Banking APIs

200 Million API transactions/day
13M mobile banking users

Security rules enforced on behalf of internal and public facing banking APIs

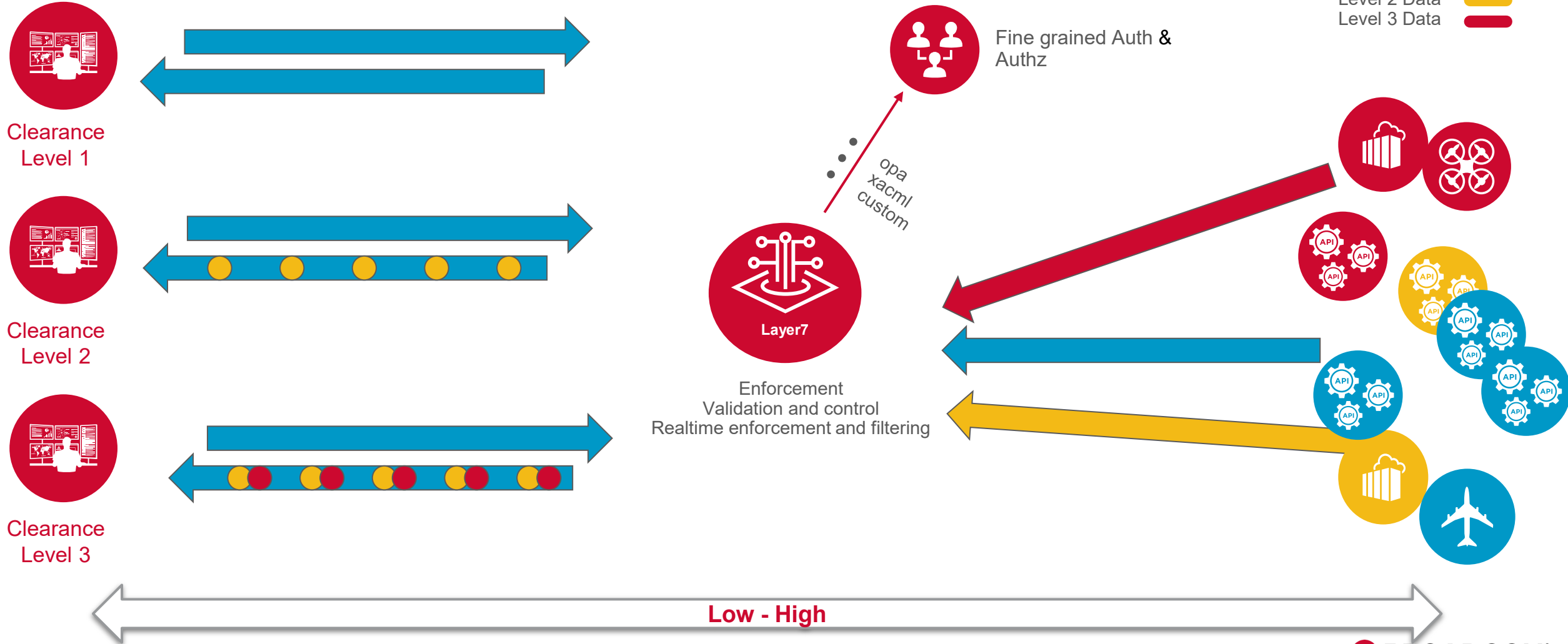


Use case: High/Low Guard

Security Community Use cases – One request with customized secured responses

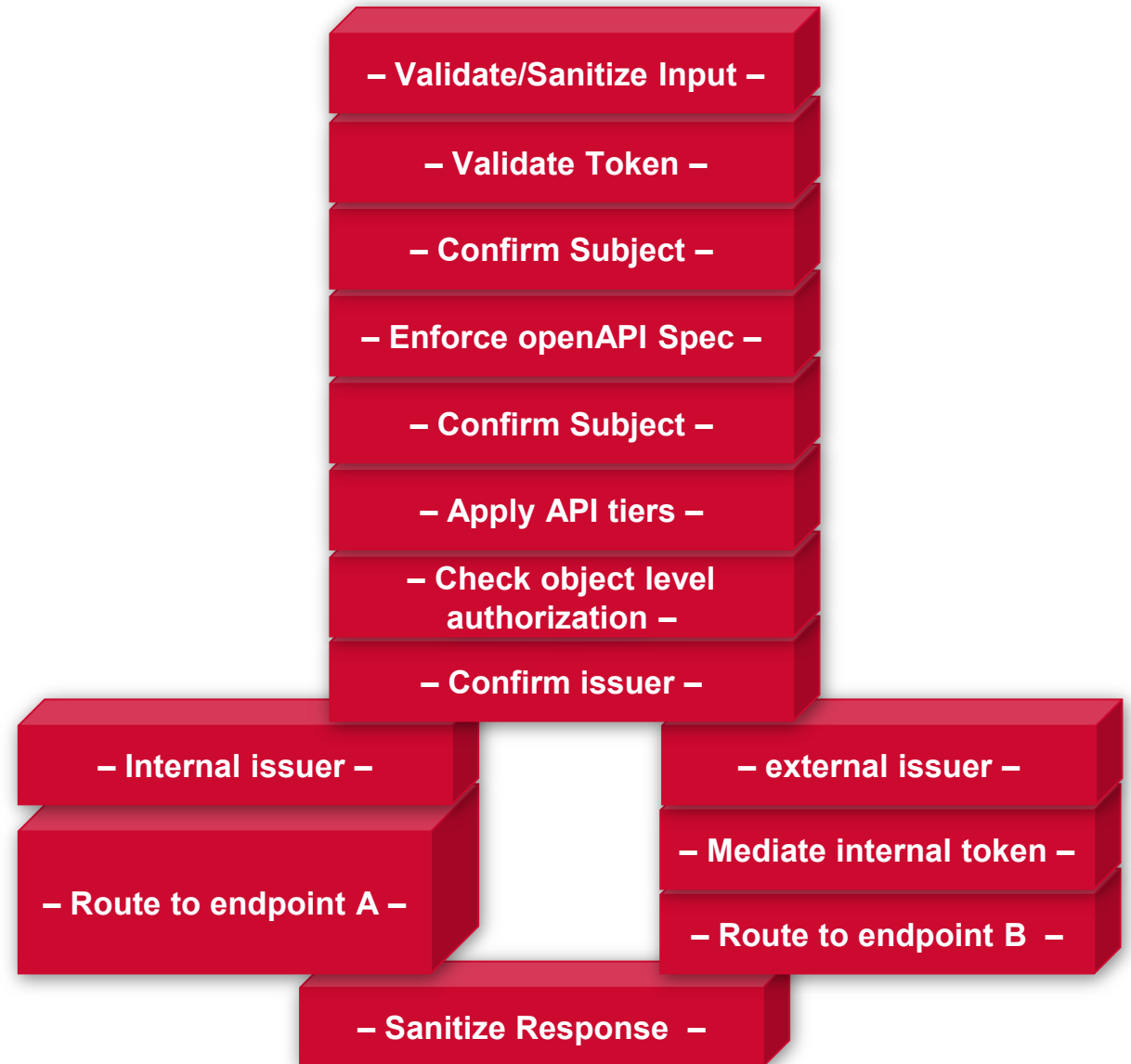


Level 1 Data 
Level 2 Data 
Level 3 Data 



API Policy

Low-code/no-code composable API policies



Implementation Sample

1

2 Include Policy Fragment: Service Security 2

2.2 # 3 Require SSL or TLS Transport

2.3 # 16 Request: Protect Against SQL Attacks [URL Path + URL Query String + Body]

2.4 # 17 Apply Rate Limit: up to 20 msg/sec per User or client IP

2.5 # 14 Customize Error Response CTRL+ALT+Y

2.6 # 13 OTK Require OAuth 2.0 Token

Security Governance

3 Split variable request.http.uri into splitURI on "/" [Ignore empty values]

Routing to SOAP back-end

4 At least one assertion must evaluate to true 3.1

5 All assertions must evaluate to true // product ID in the URL -> product details

3.2

6 Look Up Item by Index Position: find index 2 within \${splitURI}; output value to \${pld}

7 Set Context Variable m_soapRequest as Message to: <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org...

8 Route via HTTP to http://cagw:8080/ACMEWarehouse/services/WarehouseSoap

9 Response must match XPath /soapenv:Envelope/soapenv:Body/ns:getProductDetailsResponse/ns:getProductDetailsResult/*

10 Set Context Variable xml_productDetails as Message to: \${xpath_productDetails.elements}

11 \${xml_productDetails}: Apply JSON Transformation

12 All assertions must evaluate to true // no product ID in the URL -> list of products

13 Set Context Variable m_soapRequest as Message to: <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org...

14 Route via HTTP to http://cagw:8080/ACMEWarehouse/services/WarehouseSoap

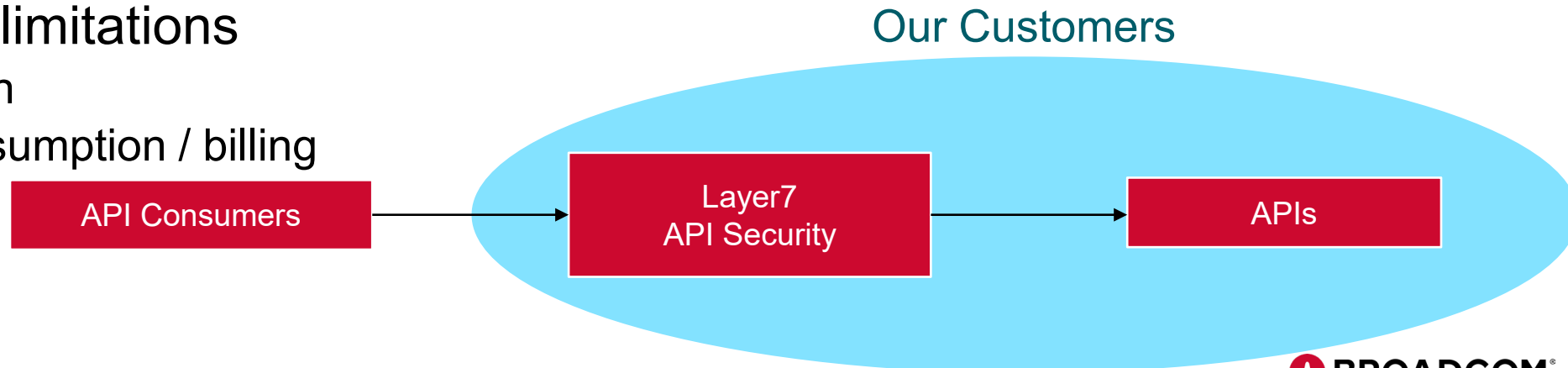
15 Response must match XPath /soapenv:Envelope/soapenv:Body/ns:listProductsResponse/ns:listProductsResult

16 Set Context Variable xml_productList as Message to: \${xpath_productList.elements}

17 \${xml_productList}: Apply JSON Transformation

Layer7 Use Cases – API Security

- Proxy / Integration
- Authentication / Authorization
 - Management of SAML, OAuth, JWT tokens
 - Integration with Federated Identity Management platforms (Siteminder, LDAP, OIDC, ...)
- XML and JSON Content Validation
- Content transformation (e.g. back-end legacy XML to front-end JSON)
- Protection against injections (SQL, Shells scripts)
- Rate and Quota limitations
 - Back-end protection
 - Monitoring the consumption / billing



Why AI Gateway?

Private LLM Challenges

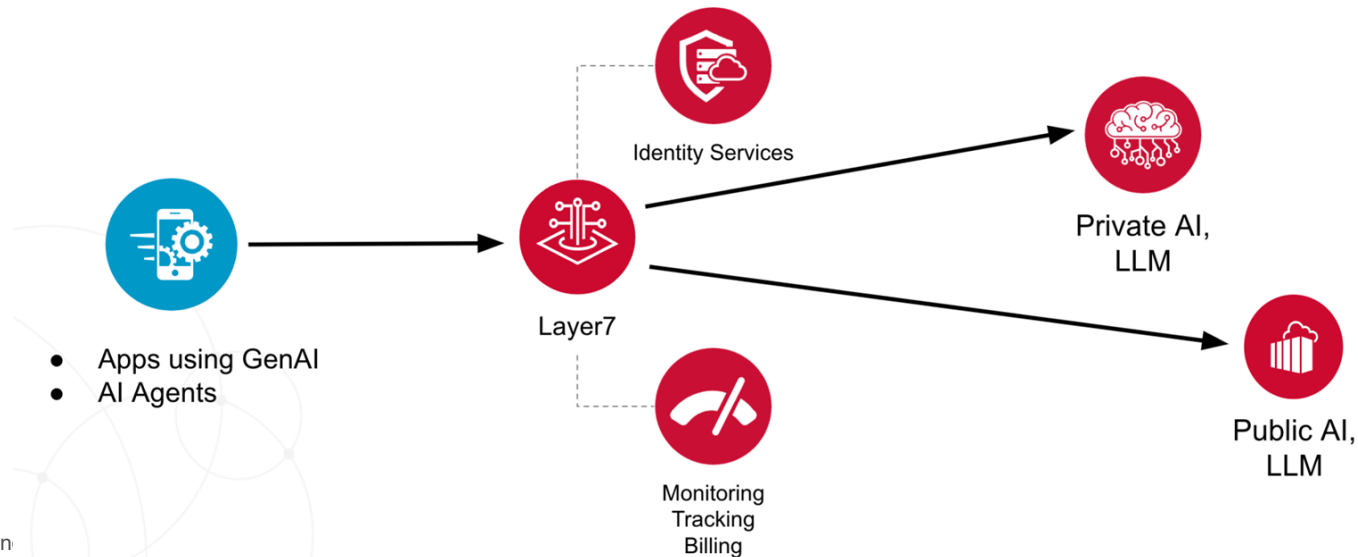
- How to run and operate?
- Prompt jailbreak, abuse
- Hosting and compute cost

3rd party LLM Challenges

- Privacy, information leakage
- Subscription costs
- Vendor locking

AI Gateway Solutions

- Integrate identity services, developer portal
 - Apply LLM guardrail rules
 - Track usage and enforce limitations
-
- Query filters and scrubbing
 - Track and limit outgoing calls
 - Broker public AI, switch on demand



Advanced API Security

- Common criteria certified solution
- Advanced API security profile
 - FAPI, DPOP, mTLS
 - Used in protecting high-value scenario APIs
- Preemptive quantum resistance
 - Demonstrated quantum resistance ahead of standard readiness for API signatures and key exchange protocols
 - Protect against harvest now, decrypt later
- Crypto agility
 - FIPS mode, pluggable crypto (hsm)
- Vulnerability management
 - Continuous scanning and remediation
 - Container hardening and shrinking, min -> micro -> distroless
- Latest authentication, authorization
 - OIDC, AuthZen



APIOps at Scale



APIOps at Scale

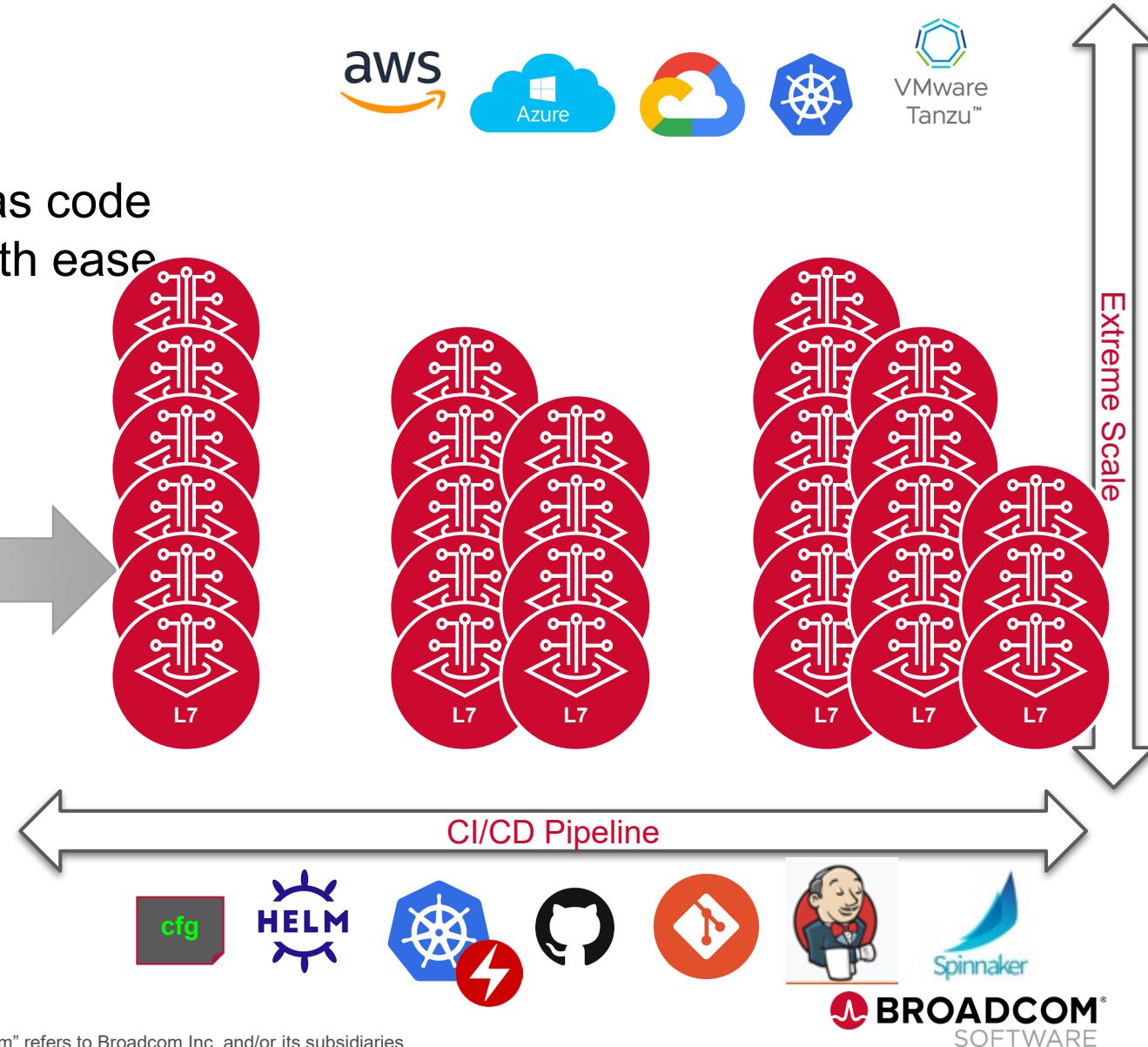
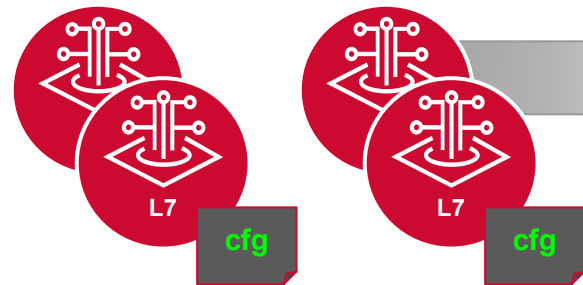
- Modern APIOps
 - Apply configuration-as-code and GitOps best practices
 - Collaboration between multiple API security stakeholders
 - Centralized governance, distributed enforcement
 - Kubernetes Operator Managed
- Unlock benefits of cloud-native deployments
 - Greater agility, availability and scalability
 - Faster times to market
 - Pain-free upgrades, reduced cost of ownership
- Licensed to promote API growth and success
- Proven large scale deployments



Use Case: APIOps at Scale

100,000 Requests per minute
across on-premises and cloud

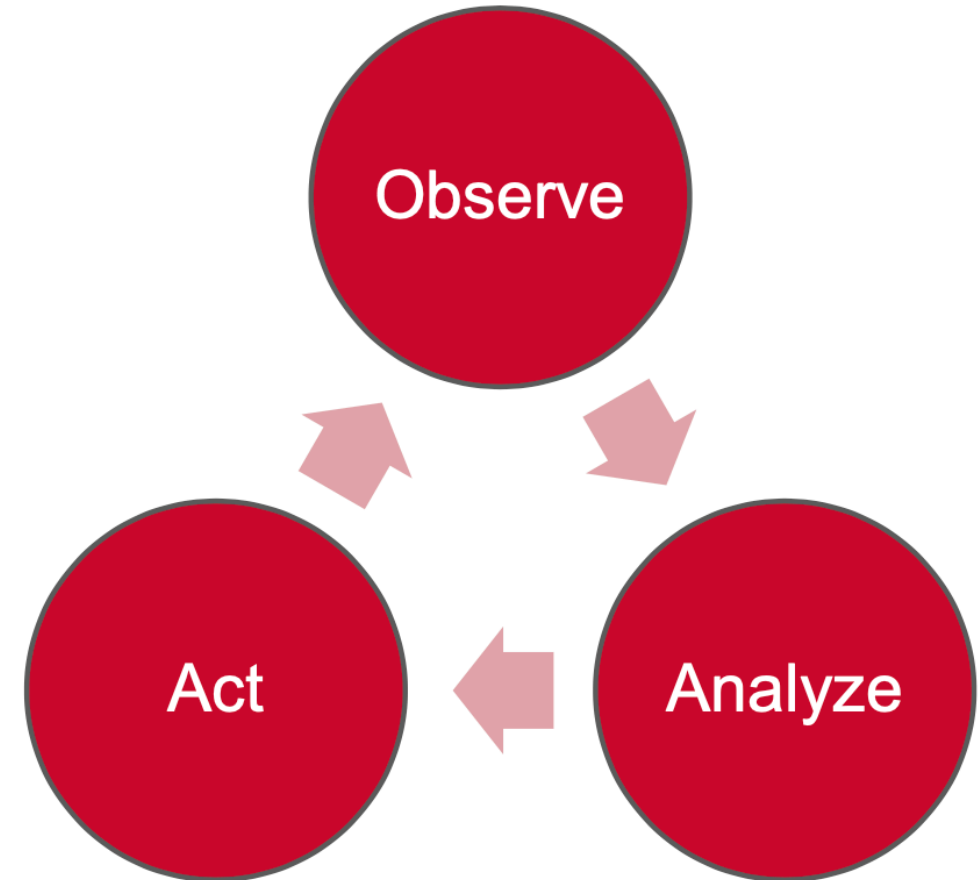
- API security in any architecture
- Proven scale and performance on premise
- Advanced security configuration managed as code
- Flexibility to grow, auto-scale and deploy with ease
- API security as infrastructure
- Migration to enable modern architectures



What is a Kubernetes Operator

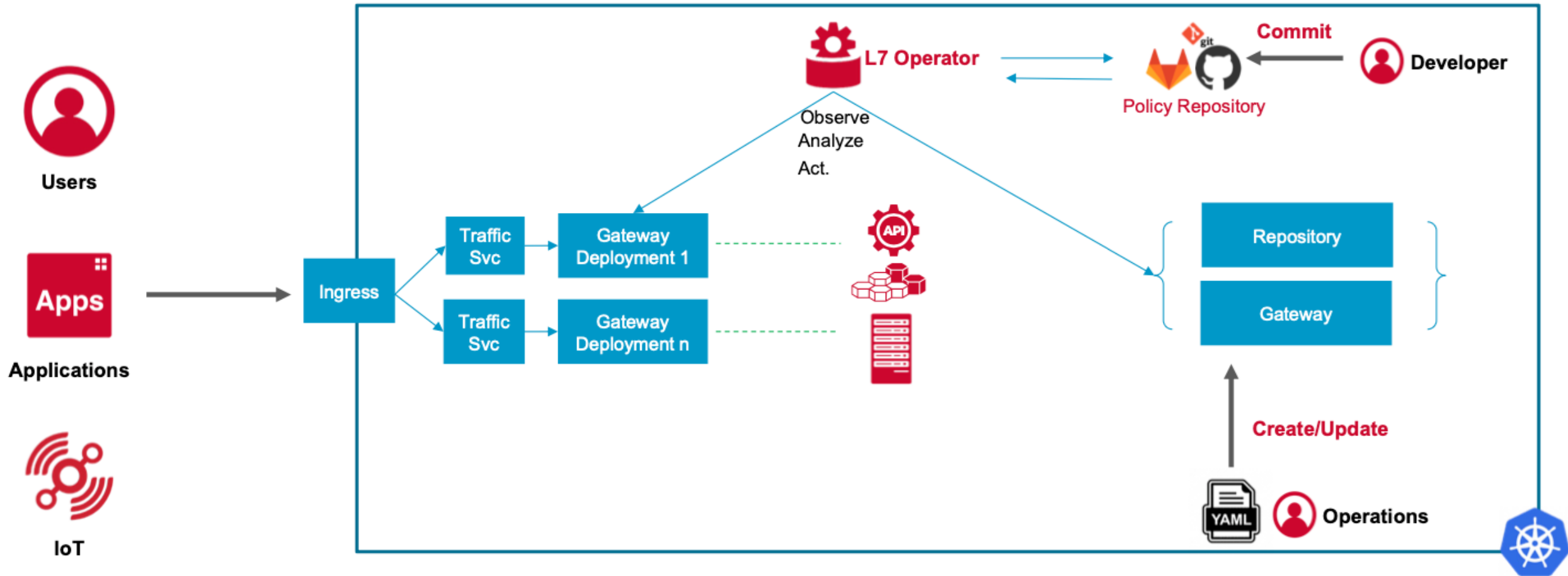
Operators are software extensions to Kubernetes that make use of **custom resources** to manage applications and their components. Operators follow Kubernetes principles, notably the **control loop**.

- The Operator pattern aims to capture the key aim of a human operator who is managing a service or set of services.
- Human operators who look after specific applications and services have deep knowledge of how the system ought to behave, how to deploy it, and how to react if there are problems.
- The Operator pattern captures how you can write code to automate a task beyond what Kubernetes itself provides



<https://kubernetes.io/docs/concepts/extend-kubernetes/operator/>

Cloud Native Architecture with Layer7 Operator

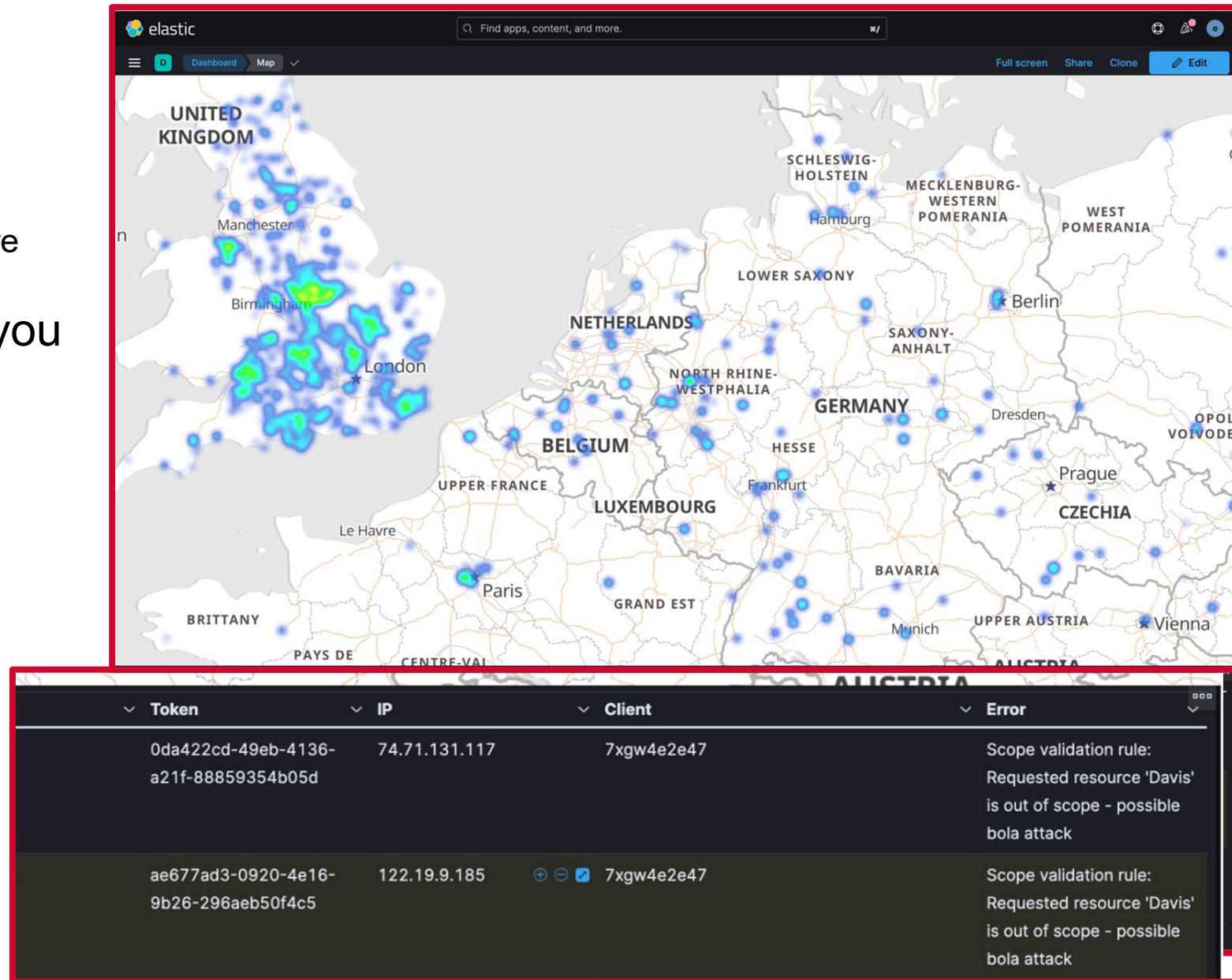


API Intelligence



Tapping into API signals

- API infrastructure emits signals
 - More context leads to richer signals
 - More security alerts lead to more secure APIs
- Deep level API security allowing you to extract the value from these signals
 - Business insights
 - Security insights
- Insights go beyond the API itself
 - The API as a window into your system/application



Use Case: Unlock application insight in public sector API

Enrich telemetry with Layer7 Policy context

Protecting
People



1. An agency code is derived as part of a Layer7 policy enforcement

Derive Agency Code

2. Policy tweak flags agency code variable as new telemetry to emit

Emit API insights

Telemetry Metric properties

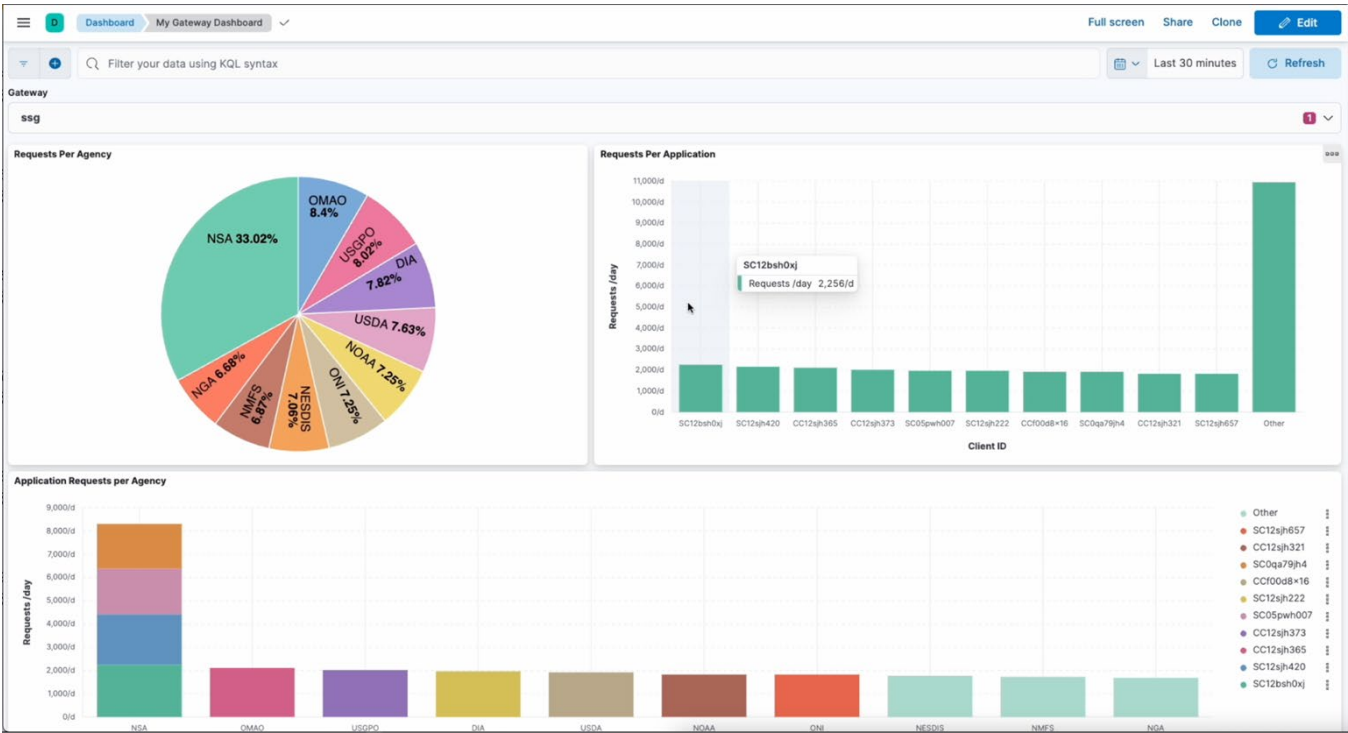
Name: Description:

Type:

Units: Measure:

Name	Value
agency-code	\$(agency-code)
client-id	\$(client-id)

3. Kibana dashboard reveals insight on which agencies consume the application for a given time period

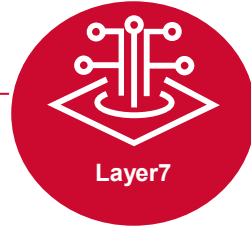


Layer7 API Intelligence

Runtime and intelligence layers working hand-in-hand



Layer7 API Runtime



Feed intelligence layer

- Built-in OpenTelemetry
- Specialized integrations

React to insights

- Block specific attack vectors
- Apply new policy
- Move unsecured API behind Layer7

capture, enrich, feed

strengthen

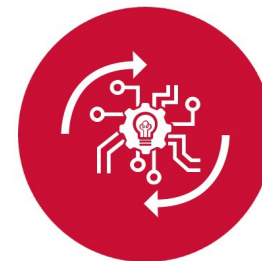
Traditional Observability



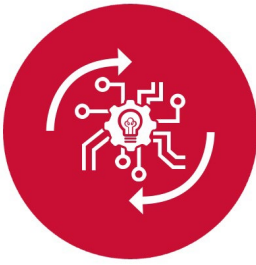
Specialized AI



API Management



API Management and Governance



- Securely managing APIs as Products
- Compliance - Enforcement and constant control
- Customized Developer user experience
- API Documentation
- API business monitoring



API Governance

HOME ▶ APIS ▶ EDIT HELLO ▶ POLICY TEMPLATES

Edit Hello

Policy Templates

Add Category ▼

Expand All Templates

Authentication	1+	Add Templates ▼
⋮ Standard Policy Template - API Key	▼	✕
API Foundation	ALL	Add Templates ▼
⋮ ThreatProtection - 1.0	▼	✕
⋮ BackendAuth - 1.0	▼	✕
⋮ BackendRoutingOptions - 1.0	▼	✕
⋮ LoggingAuditing - 1.0	▼	✕

Create Rate Limit & Quota

Name

Maximum length is 50 characters. Name must be unique.

Assignment Level

☒ API

Back end protection limit for the API, regardless of organization.

☐ Organization

Basic limit for an organization's entire usage, regardless of API application.

☐ API per Organization

Organization-specific API limit, shared by all applications.

☐ Product per Application

An application-level limit for a group of APIs that form a product.

Limit

☐ Rate

☐ Quota

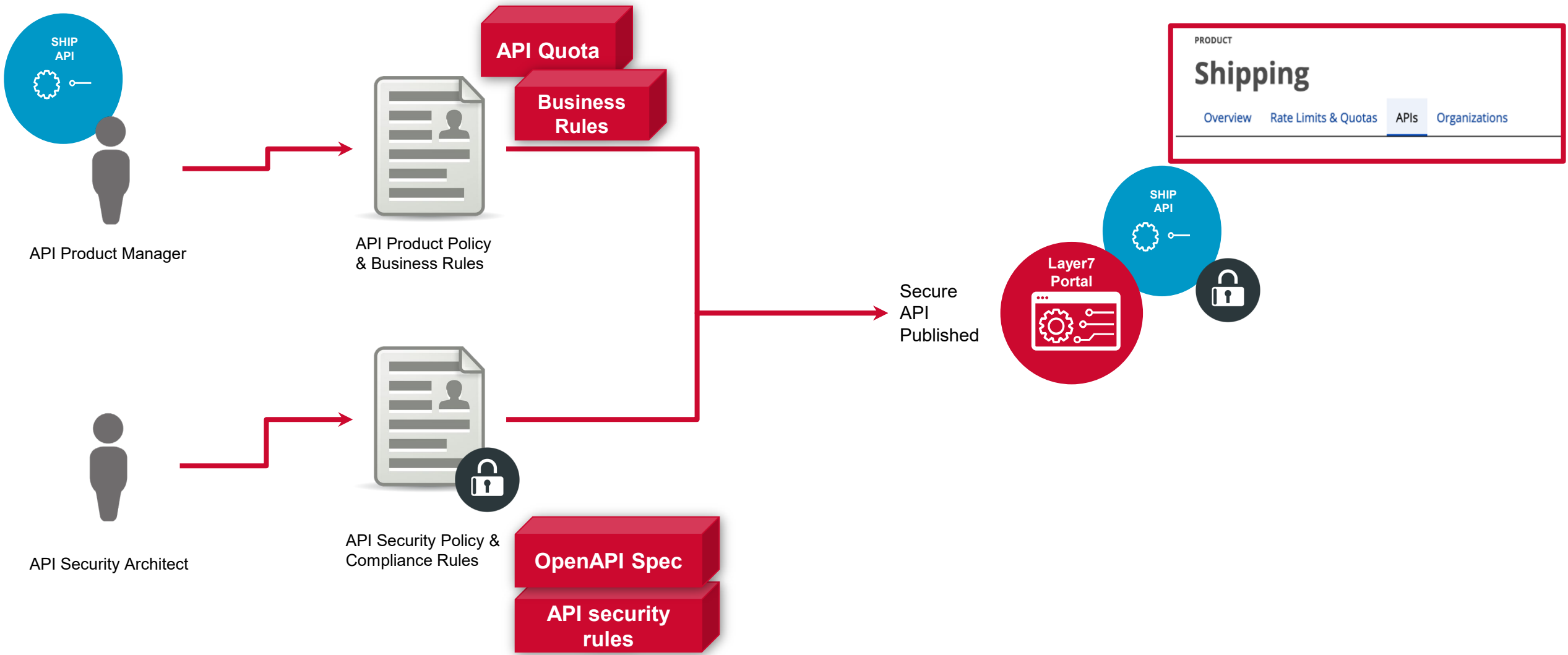
Description

Maximum length is 255 characters

Use case: API Management

API Product with Advanced Security

100,000 Applications
across 75 Regions



API Management

Secure Developer Experience

OVERVIEW

Ship API

● Enabled • Version: 1.0.0 • Private • Last Updated: Feb 02 2024 16:24

Overview Organizations Products Deployments **Spec** Documentation

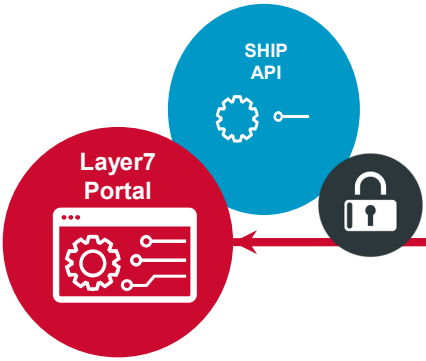
Authentication Details

Ship API 1.0.0 OAS3

Servers

default

POST	/ship/v1/shipments	Create Shipment
PUT	/ship/v1/shipments/cancel	Cancel Shipment
POST	/ship/v1/shipments/packages/validate	Validate Shipment
POST	/ship/v1/shipments/results	Retrieve Async Ship

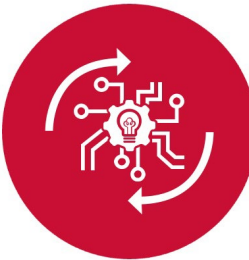


Internal API consumer
API Key
Enforced Security

External API consumer
API Key
Enforced Security

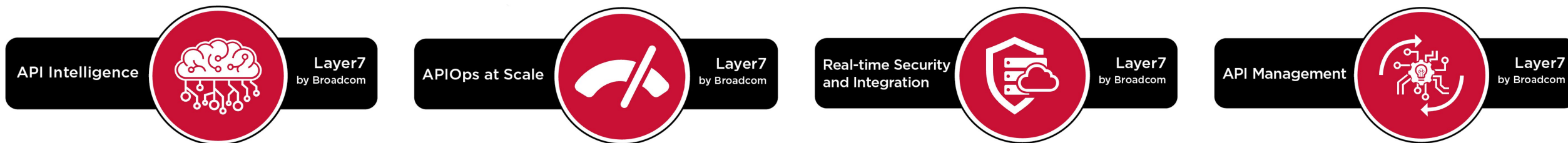
Secure Consumption
Tracked and Controlled API Access
Secure SDK access
API Discovery
Customised and Secure developer access
API documentation

Next



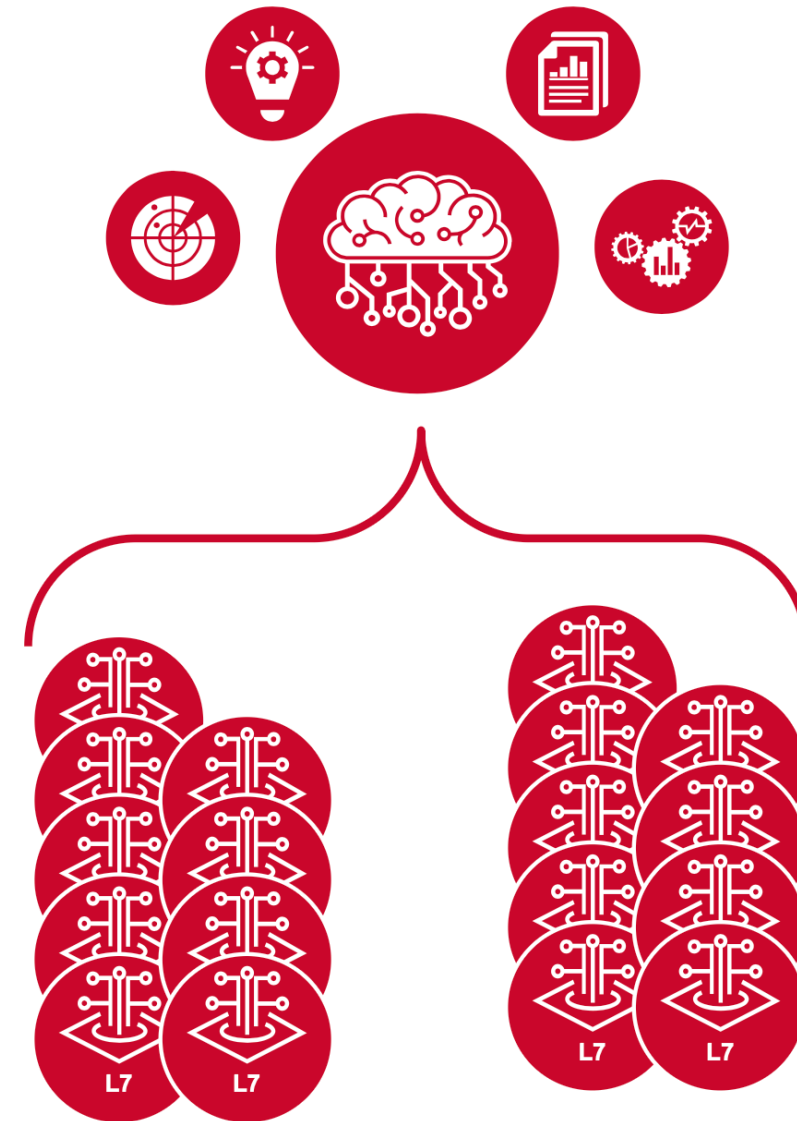
Vision Statement

The Layer7 solution is a securely deployable **API security** solution for all customers **regardless of where they are deploying** and where on the cloud deployment journey they are. **Scalable** API security infrastructure fully supporting **automation** and CI/CD integration where customer requirements mature. Secure API Management built on industry leading **real-time security**.



Layer7 API Security Intelligence

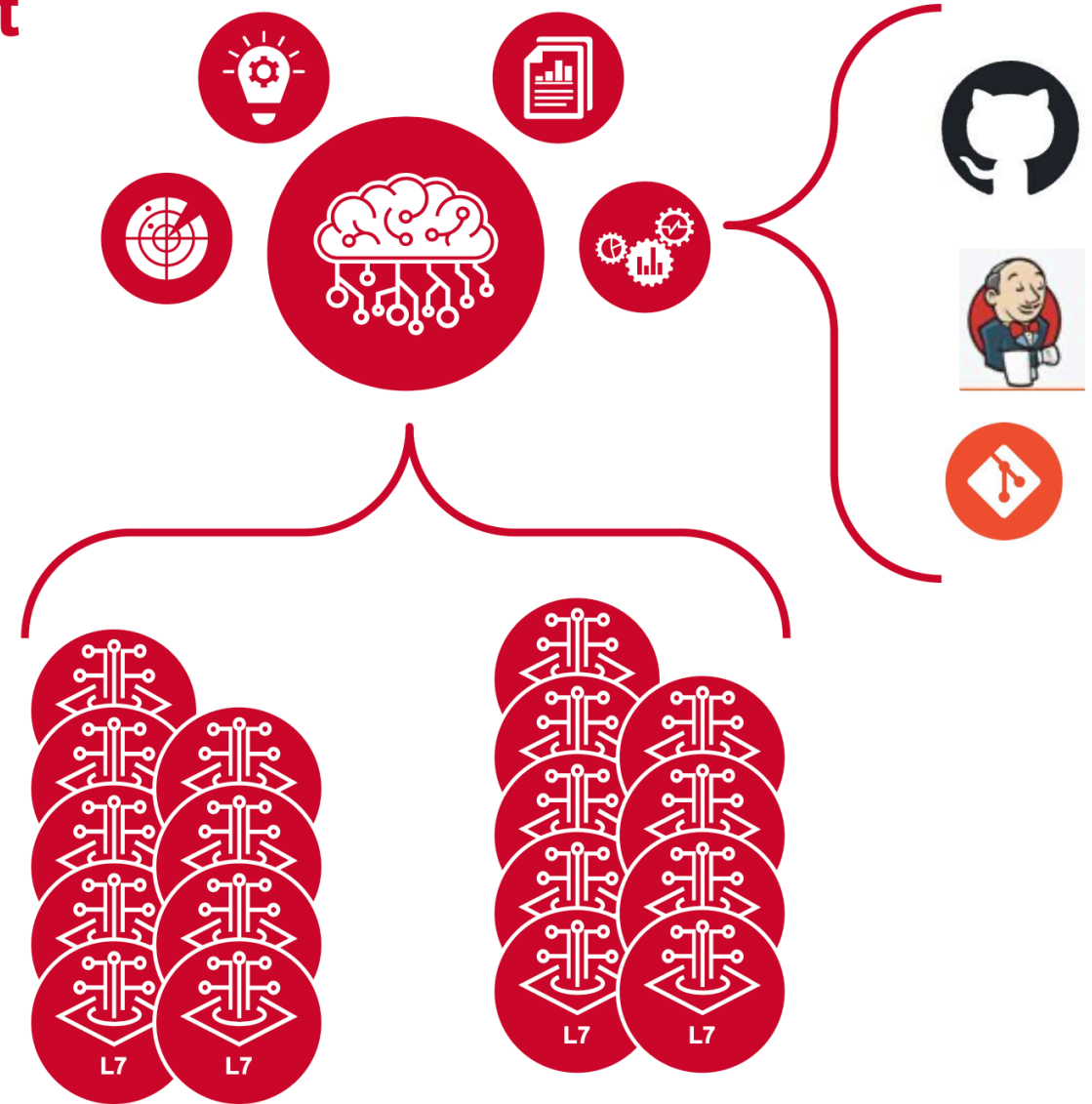
- Based on a highly configurable rules engine
- Provides the ability to gain insights into the entire Layer7 infrastructure
 - potential configuration problems
 - required maintenance tasks
 - observations about API traffic and patterns
 - and more...
- Customized dashboards and reporting via multiple channels



- Expiring Certs
- Missing security
- Unapplied patch
- Unusual latency
- ...

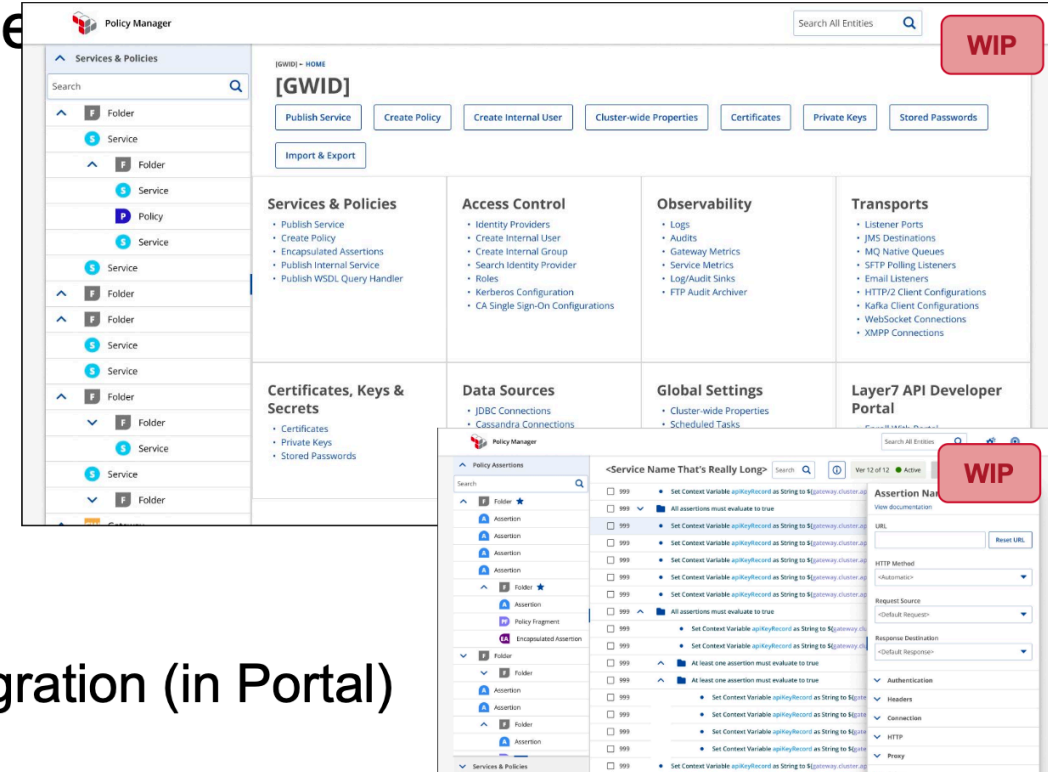
Layer7 Config & Infrastructure Mgmt

- Single point to manage Layer7 configuration (gw policy, entities, api mgmt, etc.)
- Provides ability to connect to remote repositories for CI/CD integration
- GW migration (policy, other entities)
- Patch Management
- Dev Ops Policy Authoring

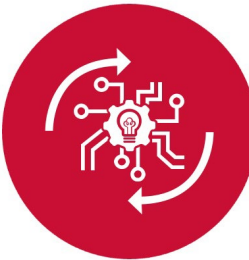


Policy Manager Replacement (PM2)

- Modern web UI replacement of Policy Manager
- Immediate Goals:
 - Deliver “must have” Policy Manager capabilities
 - Some enhancements of opportunity
 - Deployed with Gateways
 - **Experimental** in ~June
 - **Preview** in Gateway 11.2 in ~October
- Long Term Goals:
 - Integration with Portal
 - Integration with Multi-Gateway Management & Migration (in Portal)
 - New capabilities including:
 - SSO
 - Policy as Code
 - Git Integration
 - Test Automation
 - And more...



Final Words



Layer 7 API Security Leader

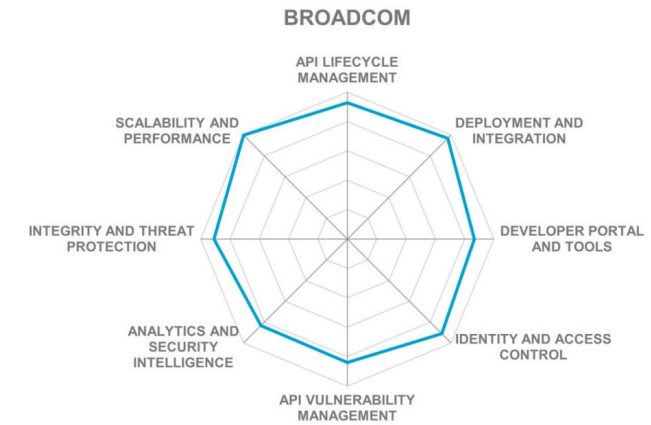


“API security has long become an industry of its own; with the scope of risks and challenges the industry confronts growing exponentially, API security solutions must expand their coverage and grow in complexity themselves”

“Broadcom provides a full range of management tools for API lifecycle management and microservices”

“Advanced security capabilities through Intelligent automation”

“OpenTelemetry support simplifies third-party observability tool integrations”



[KuppingerCole Leadership for API Security and Management, October 23, 2023](#)

Layer7 – Customer Validation

Real-time Security and Integration



Layer7
by Broadcom

“Layer7 API Management ensures standardization, security, and stabilization in a CI/CD pipeline for one of the worlds largest gambling operators.”

API Intelligence



Layer7
by Broadcom

“As far as the deployment and to the infrastructure, the hardware, the networks, those are all new. Our [new] data centers look like private cloud datacenters, which look like public cloud datacenters.”

“Layer7 is a critical component of our api-based banking applications allowing us to apply identity-based access control in a standardized way, and at scale.”

APIOps at Scale



Layer7
by Broadcom

“Layer7 provides a central way to identify and visualize business activity and security events during real-time security enforcement. Actions allow intelligent actions and enforcement”

API Management



Layer7
by Broadcom



A person wearing a red and blue plaid shirt is clapping their hands. In the background, a laptop is open on a wooden desk, displaying a website with blue and white elements. A smartphone is lying on a notebook in front of the laptop. The scene is dimly lit, suggesting an indoor office or meeting environment.

Thank you