API-Schutz

Die Grundlage für umfassende KI-Sicherheit

Frank Thias, F5
Sr. Principal Solutions Engineer

17.09.2025, Congress Park Hanau

Agenda

Die wachsende Bedeutung von APIs und ihre Herausforderungen

Die Rolle von APIs in AI-getriebenen Umgebungen

API-Sichtbarkeit und Schutz in der Multi-Cloud-Welt

API-Learning und Anomalie-Erkennung

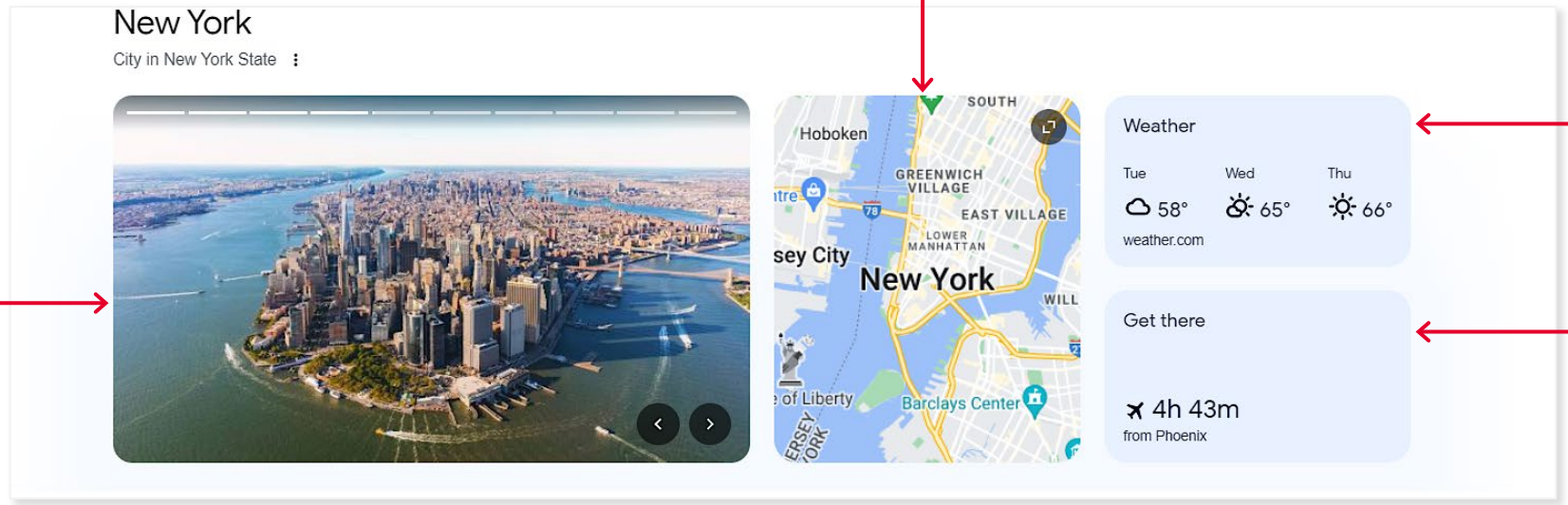
API-Abwehr gegen DDoS- und volumetrische Angriffe

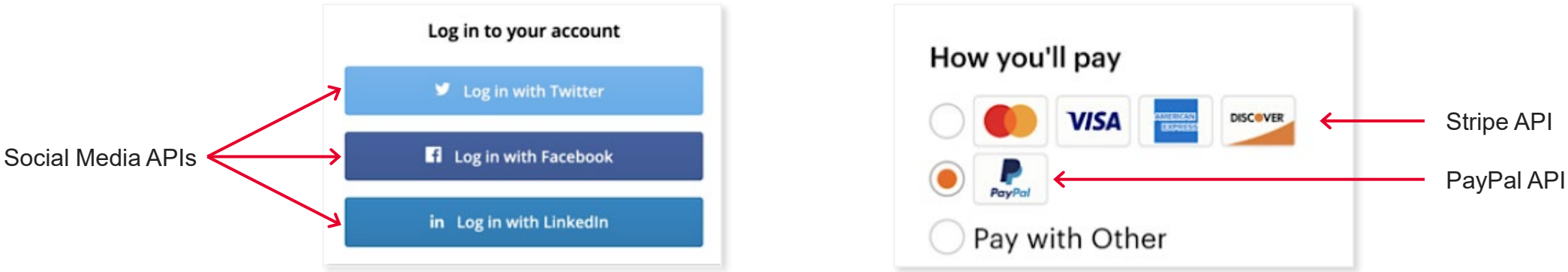
Die wachsende Bedeutung von APIs und ihre Herausforderungen

Die wachsende Bedeutung von APIs und ihre Herausforderungen

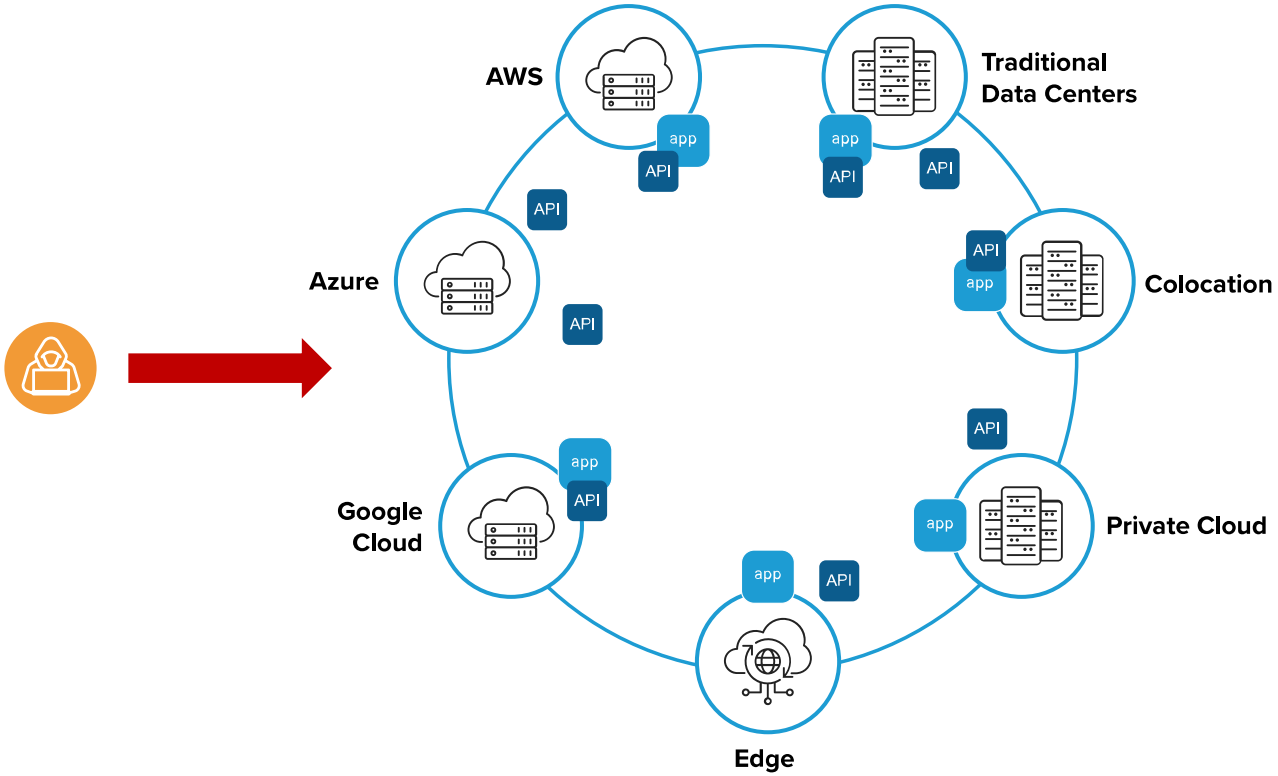
- APIs als Herzstück moderner IT-Architekturen (Multi-Cloud, SaaS und AI)
- Die Rolle von APIs in AI-Umgebungen
- Häufige Bedrohungen:
  - DDoS-Angriffe
  - API-Exploits
  - Credential Stuffing

Interacting with hundreds of APIs each day





API security is hard



- Attackers are increasingly targeting APIs
- APIs are driving untenable sprawl
- Security is a business imperative
- The Rise of Generative AI is top of mind

Die Rolle von APIs in AI-getriebenen Umgebungen

AI and API Security – Two sides of the same coin

APIs are a primary attack vector; you cannot secure your AI models without securing the APIs that serve them

> *No matter how you're using gen AI, at the end of the day, you're calling an endpoint either with an SDK or a library or via a REST API*

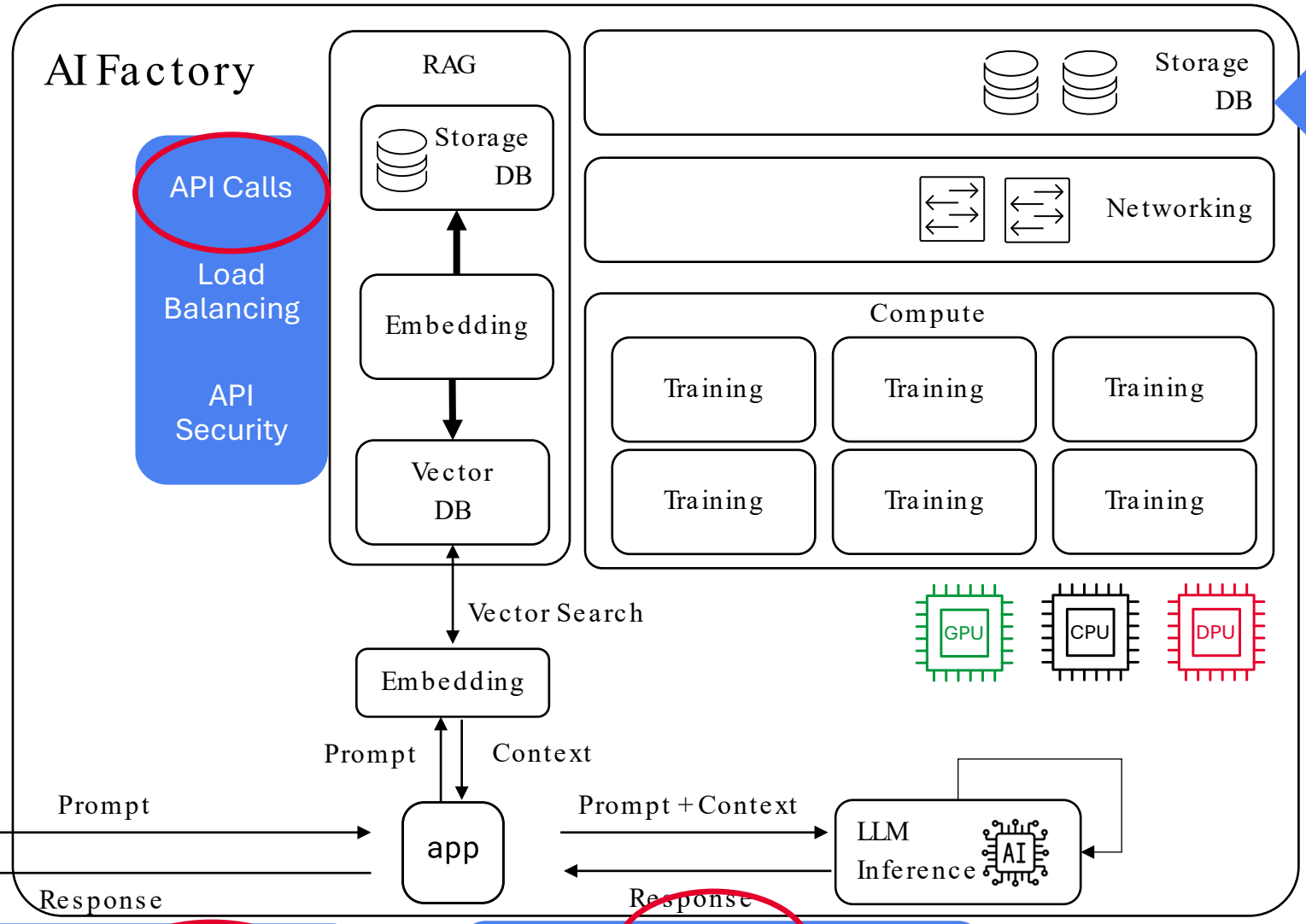
Mete Atamel
Developer Advocate, Google Cloud

Google Cloud

Protocols

Most of these services will run in Kubernetes

so they will need all the usual application delivery controller functionality F5 offers.



Massive amounts of data needs to be fed into these systems rapidly.

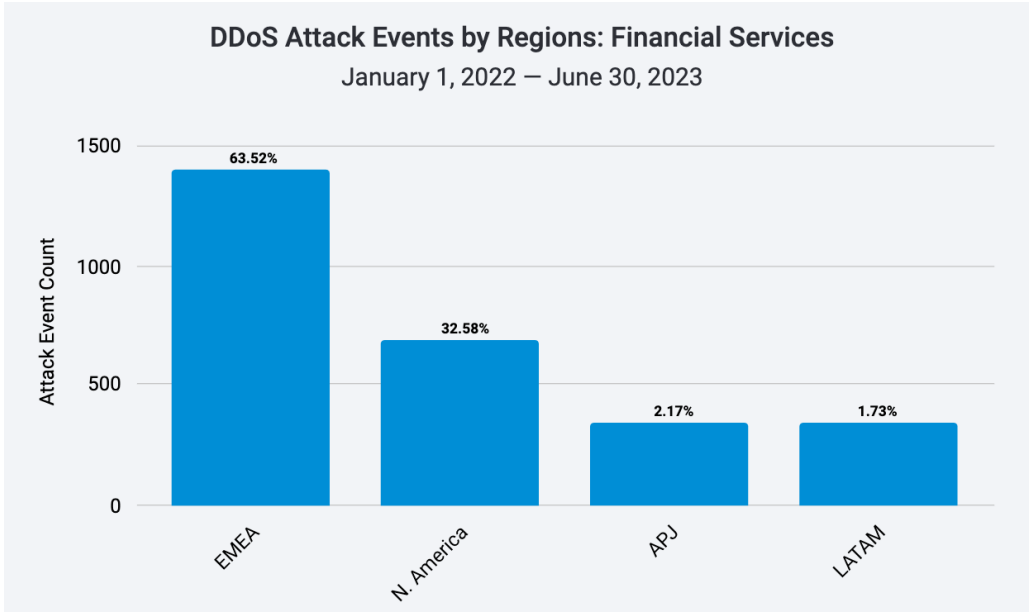
S3 storage

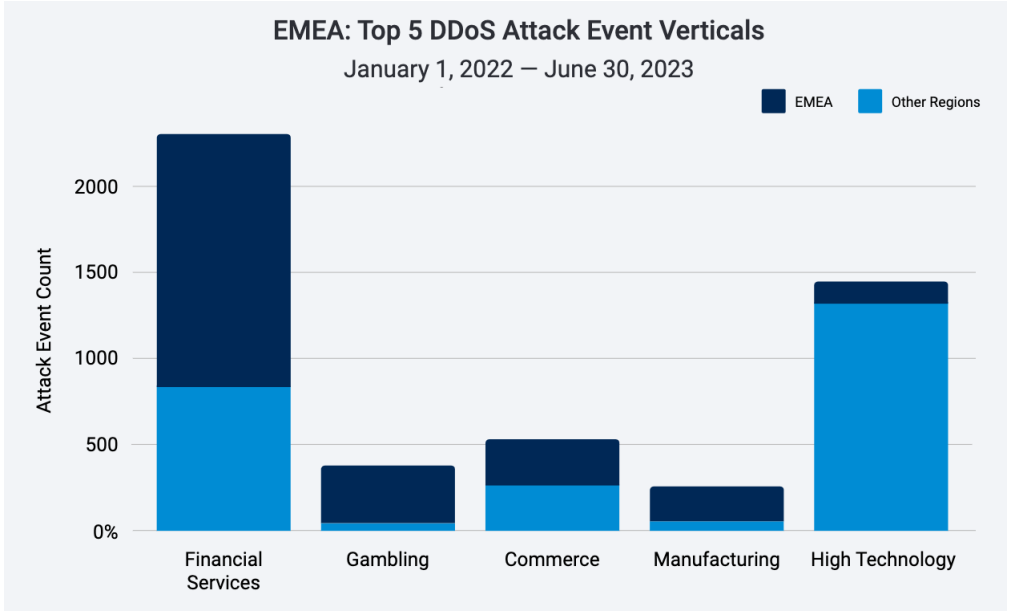
Looks like HTTPS, fed by API calls

Bedrohungen

EMEA DDoS Statistics

- EMEA experienced the most DDoS attack events, nearly double the amount in the next top region.
- UK tops the list at 29.2% of DDoS events, followed by Germany at 15.1%
- As of January 2025, the EU financial sectors should be prepared to comply with **DORA**.
- **NIS2** will go into effect on October 17, 2025.
- **PCI DSS v4.0** requires organizations to meet new requirements by March 2025.





API Exploits: The Primary Attack Vector for Modern Applications

1. Broken Object Level Authorization (BOLA):

•Exploiting weak identity and access controls.

•Example: Attackers retrieve sensitive data belonging to other users.

2. Injection Attacks:

•Code injections, such as SQL Injection, via API parameters.

•Example: Manipulating APIs to extract sensitive backend database content.

3. Excessive Data Exposure:

•APIs reveal too much data without adequate validation of what's necessary.

•Example: Leaking personal identifiable information (PII) unintentionally.

4. Lack of Rate Limiting:

•APIs are overloaded with unlimited requests.

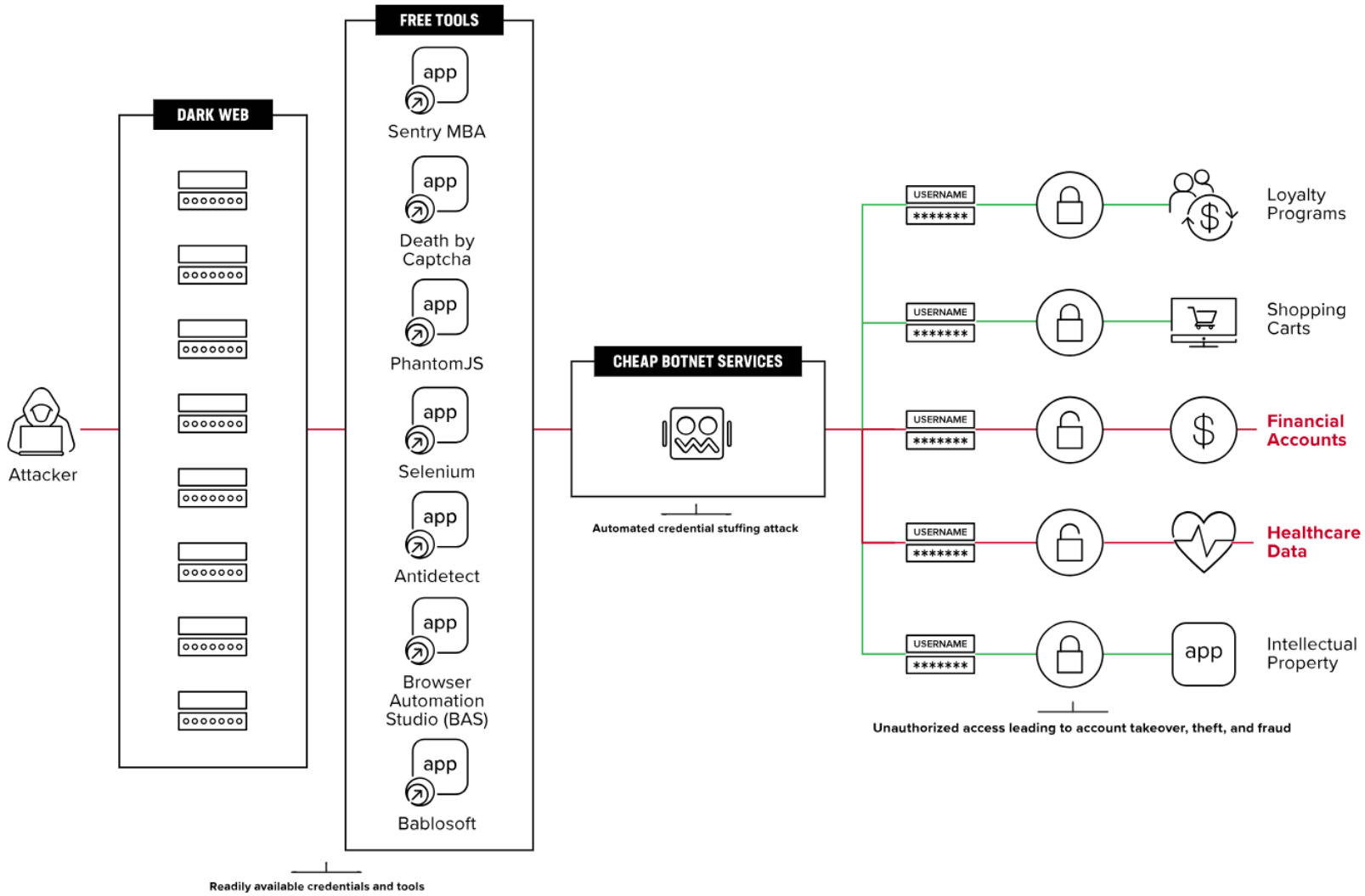
•Example: Bot attacks or Denial-of-Service (DDoS) targeting APIs.

5. Broken Authentication:

•Insufficient authentication mechanisms lead to credential stuffing or unauthorized API access.

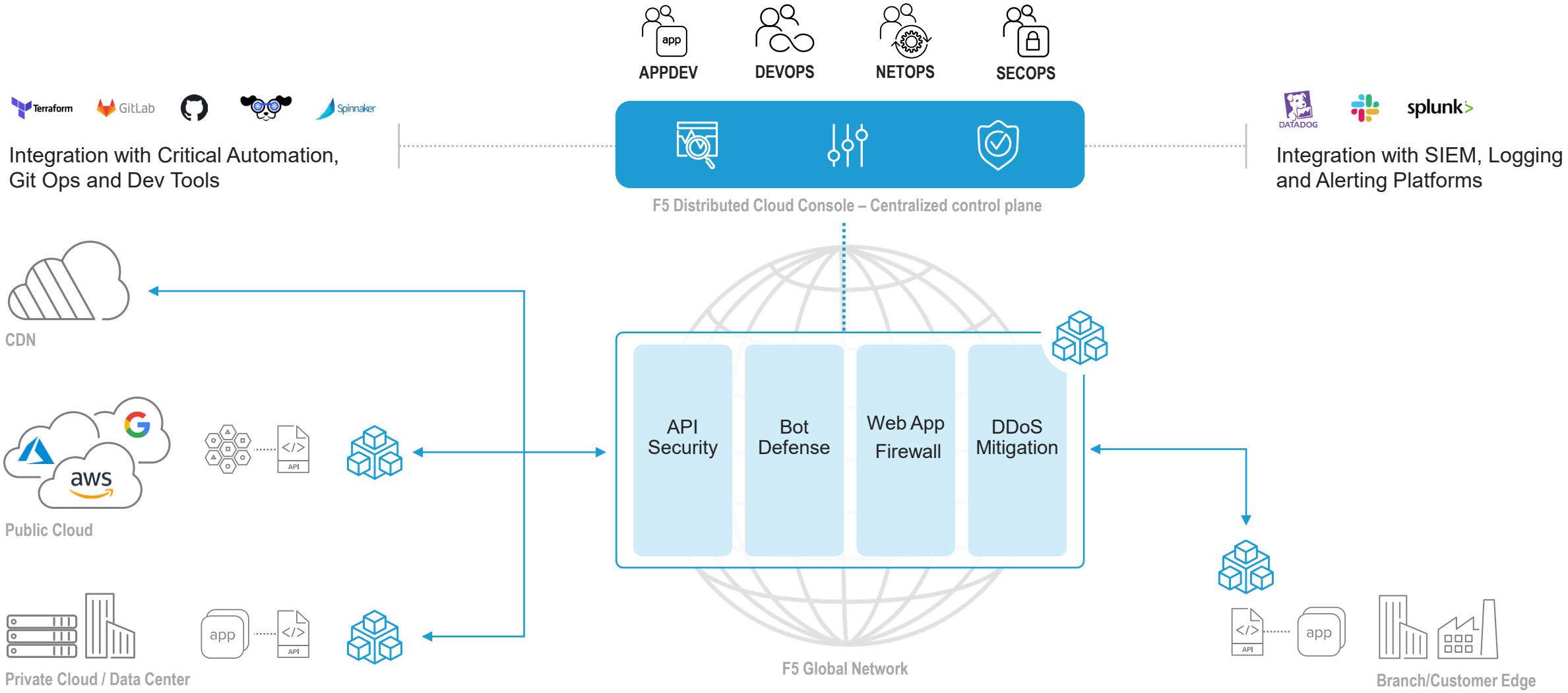
•Example: Attackers using stolen credentials to gain legitimate access to APIs.

Example of an credential stuffing architecture / Bot Attacks

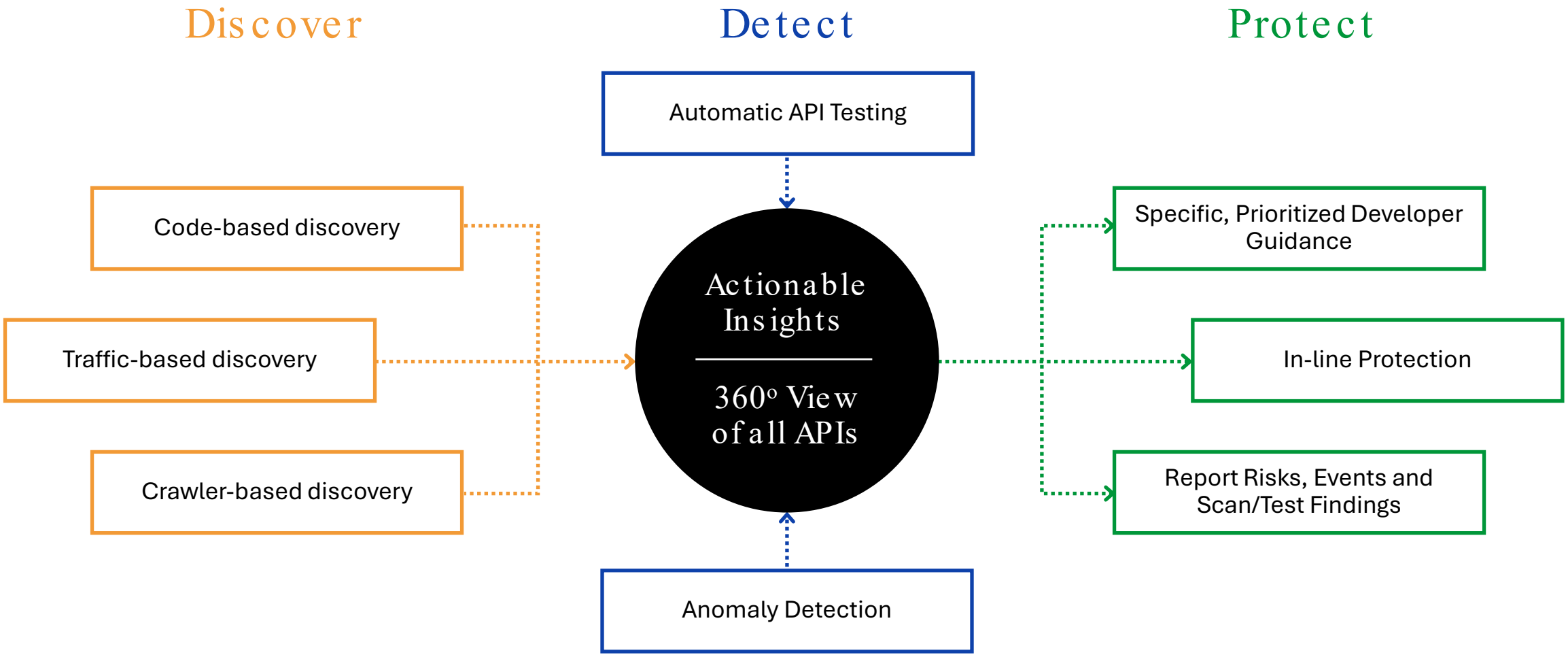


API-Sichtbarkeit und Schutz in der Multi-Cloud-Welt

F5 Distributed Cloud - Centralized control and flexible deployments



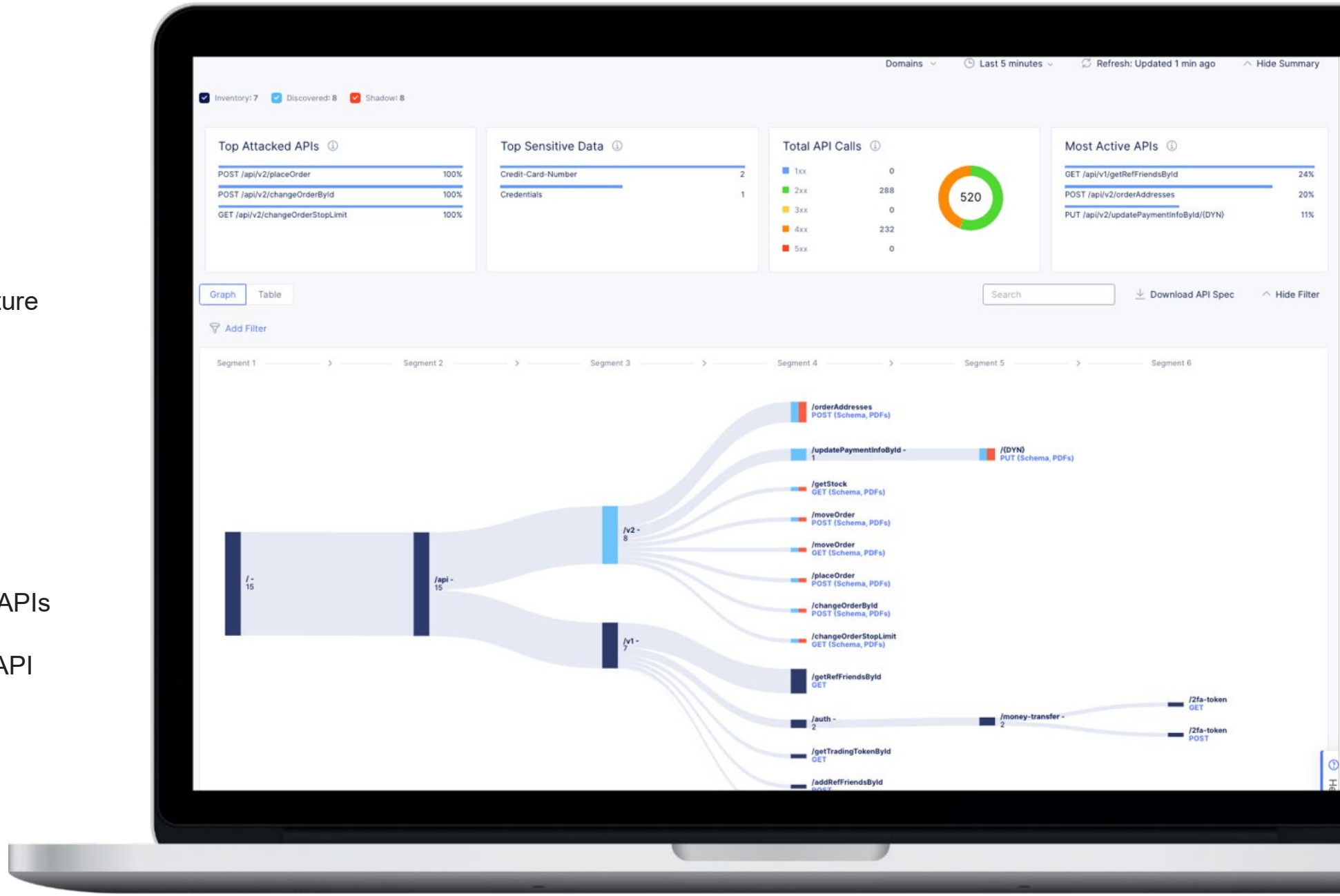
F5 delivers the most comprehensive API security solution on the market



API endpoint discovery

Continuous Defense

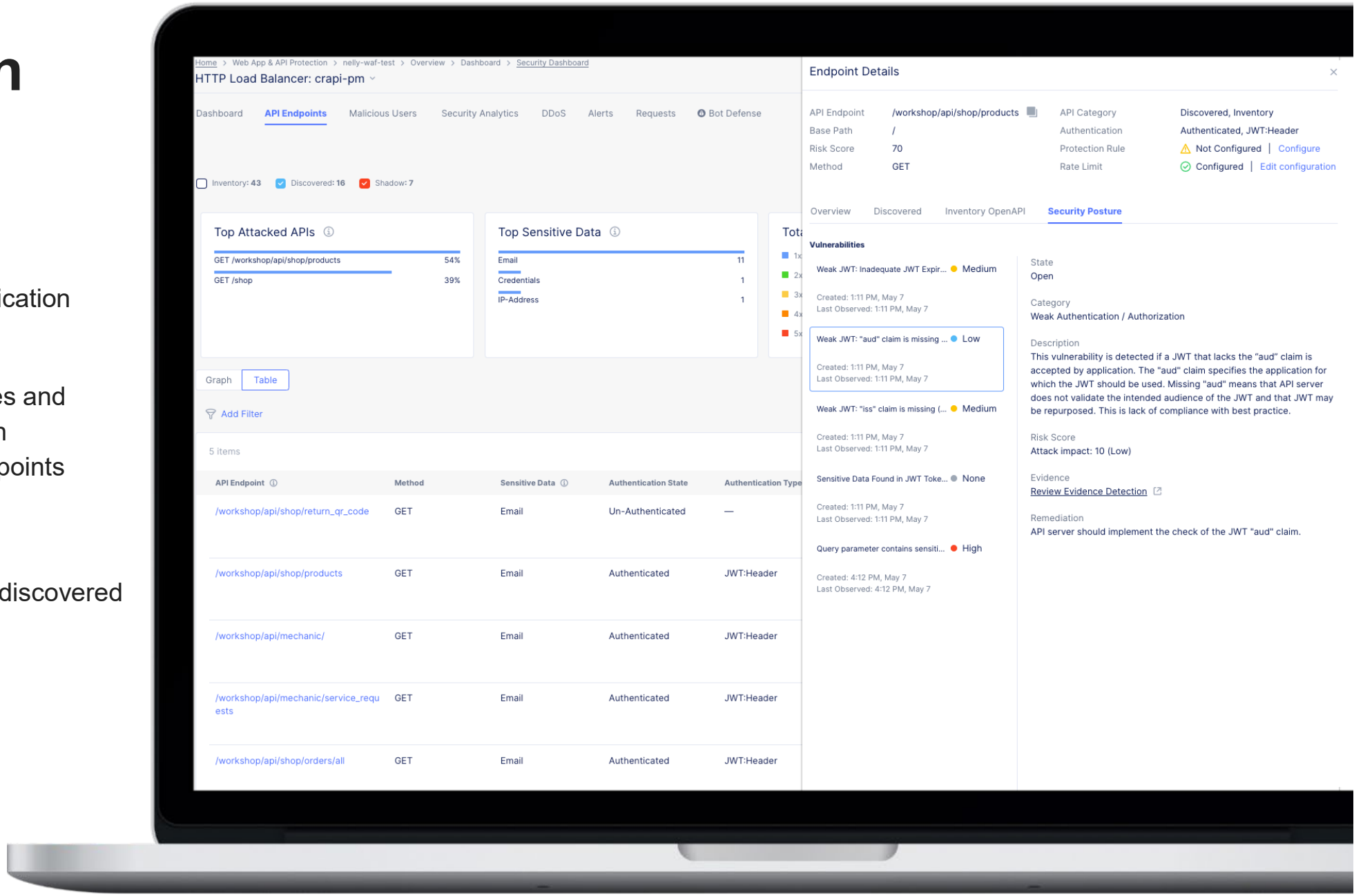
- ✓ Dynamically learn API structure
- ✓ Build a model for each API:
  - ➢ errors
  - ➢ latency
  - ➢ request metrics
- ✓ Detect outliers and shadow APIs
- ✓ Export swagger to improve API definitions/update inventory



Validate API authentication

Consistent Security

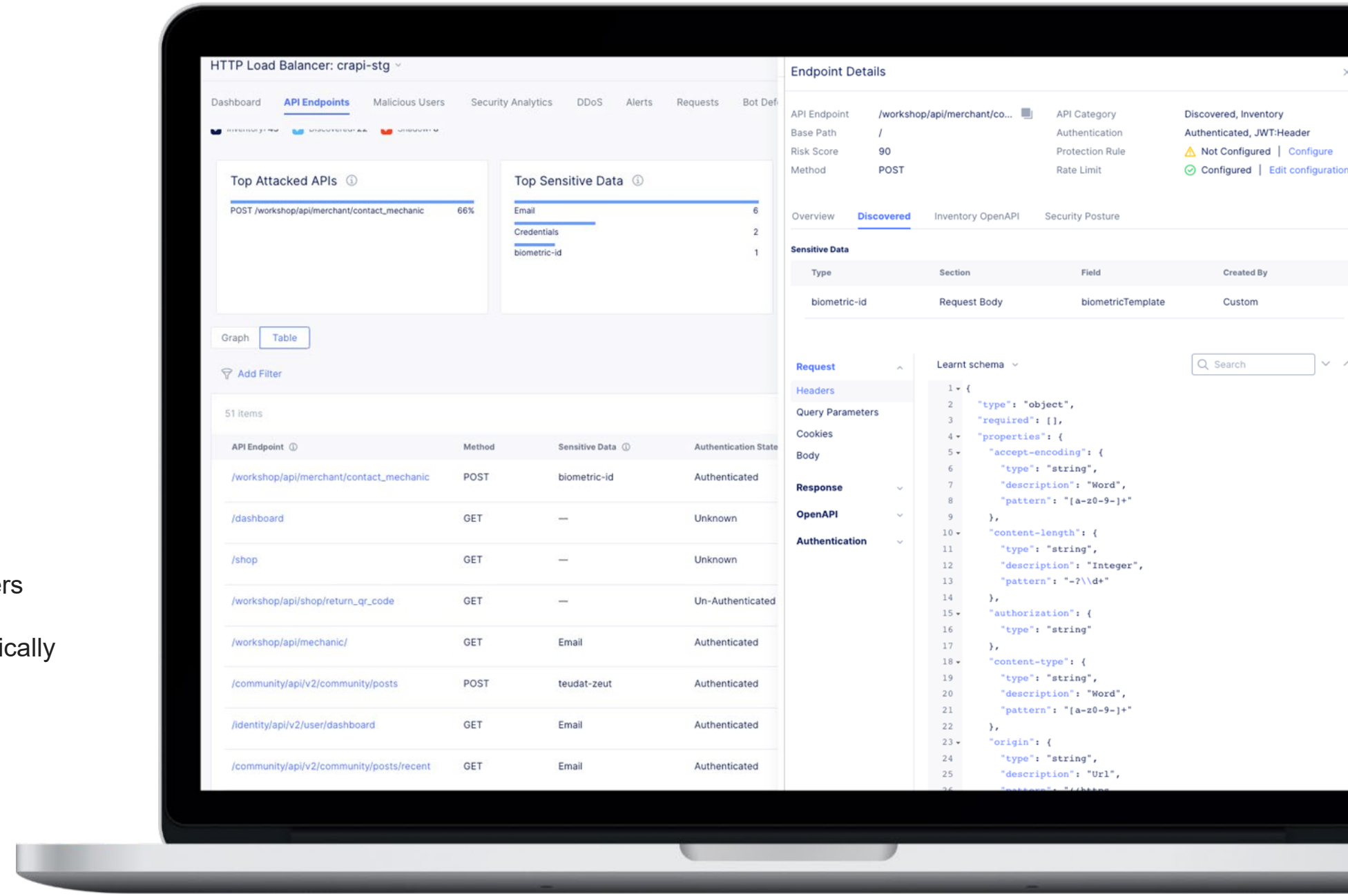
- ✓ Discover and view authentication status
- ✓ Gain insights into anomalies and potential vulnerabilities with authentication for API endpoints
- ✓ Includes JWT validation
- ✓ Create protection rules for discovered endpoints:
  - ➢ blocking
  - ➢ rate limiting



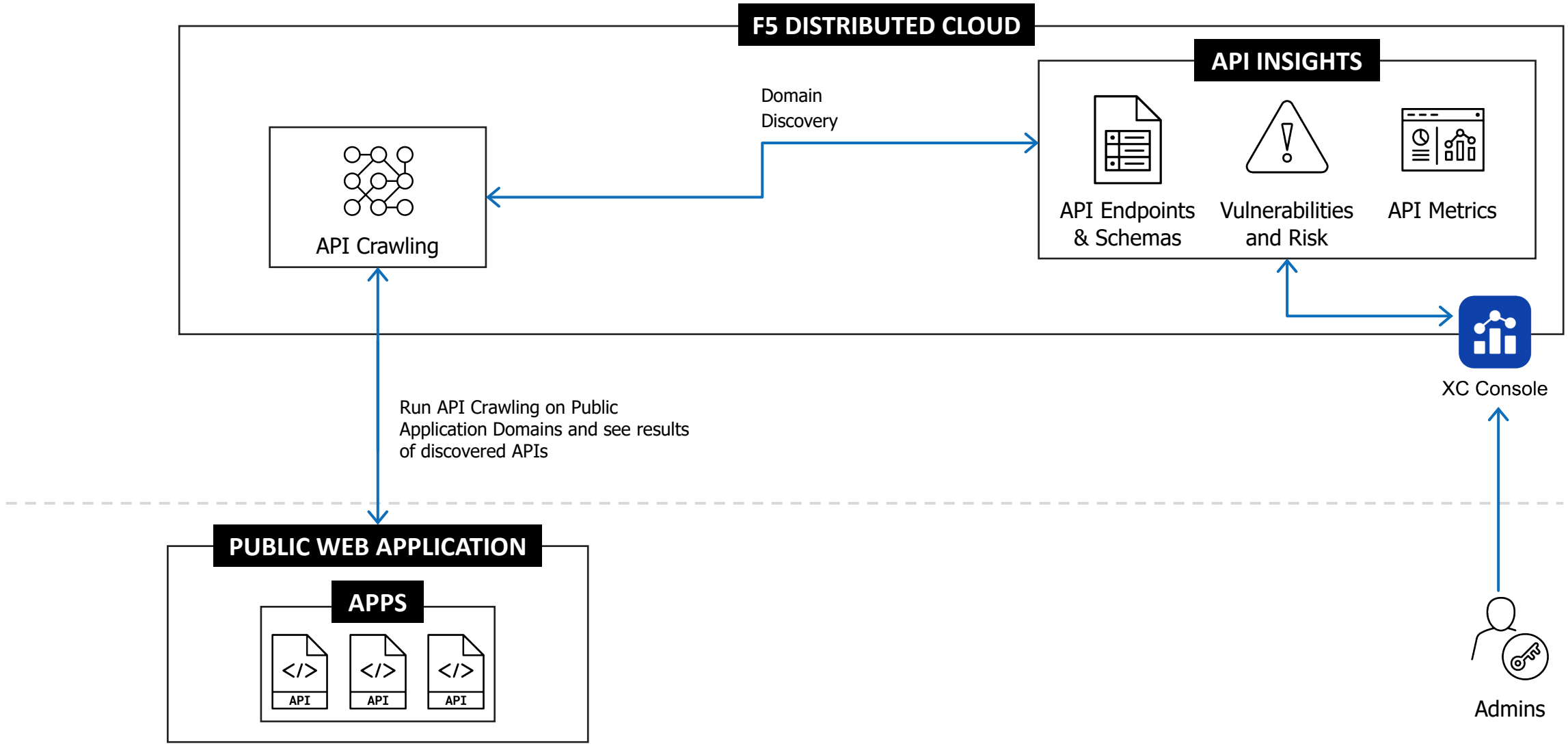
Prevent PII exposure

Consistent Security

- ✓ Detect and flag PII that is being exposed via APIs
  - ➢ names
  - ➢ addresses
  - ➢ phone numbers
  - ➢ social security numbers
- ✓ Mask sensitive data dynamically



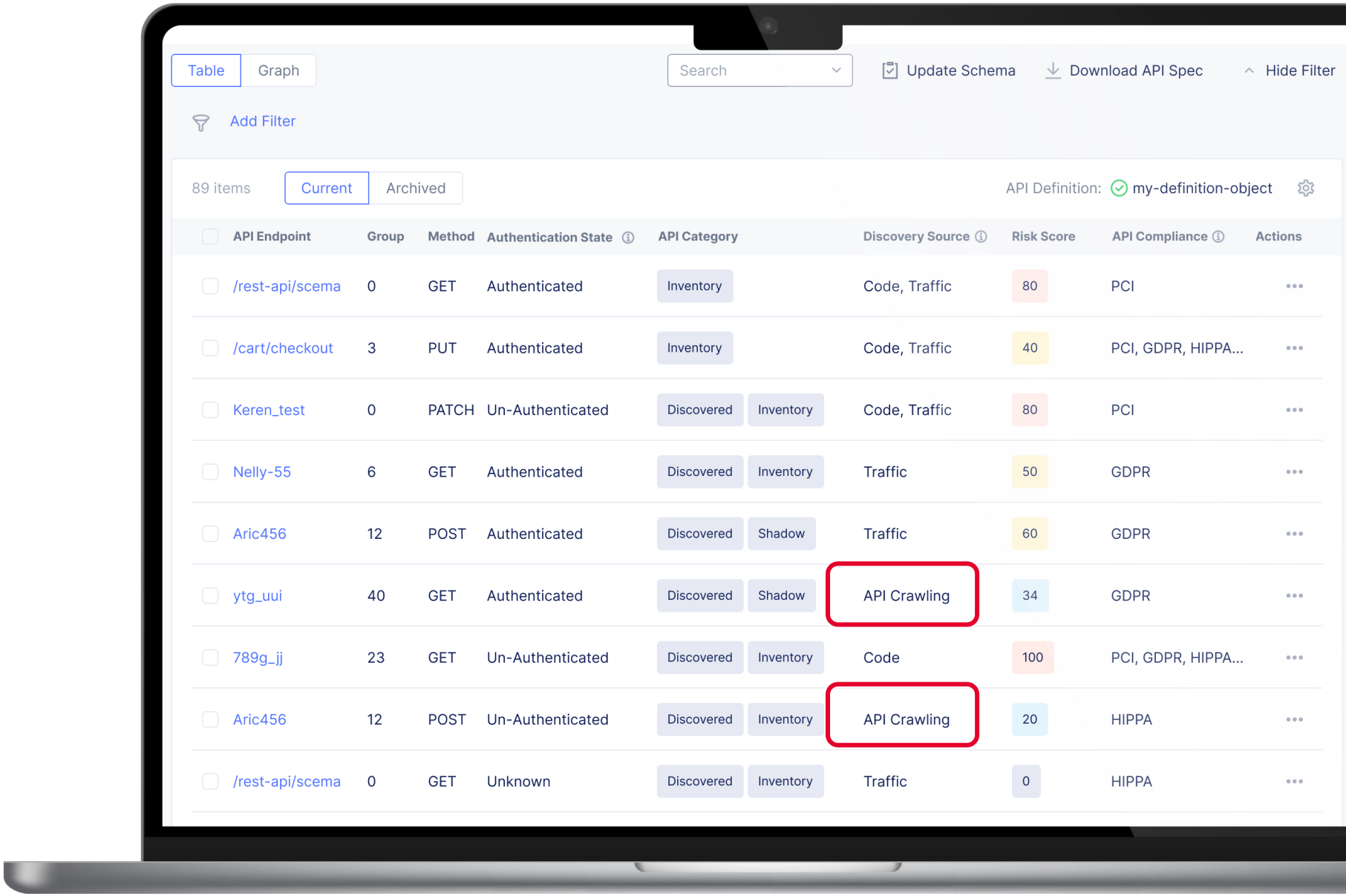
API Crawling for API Discovery



Crawler-based API Discovery

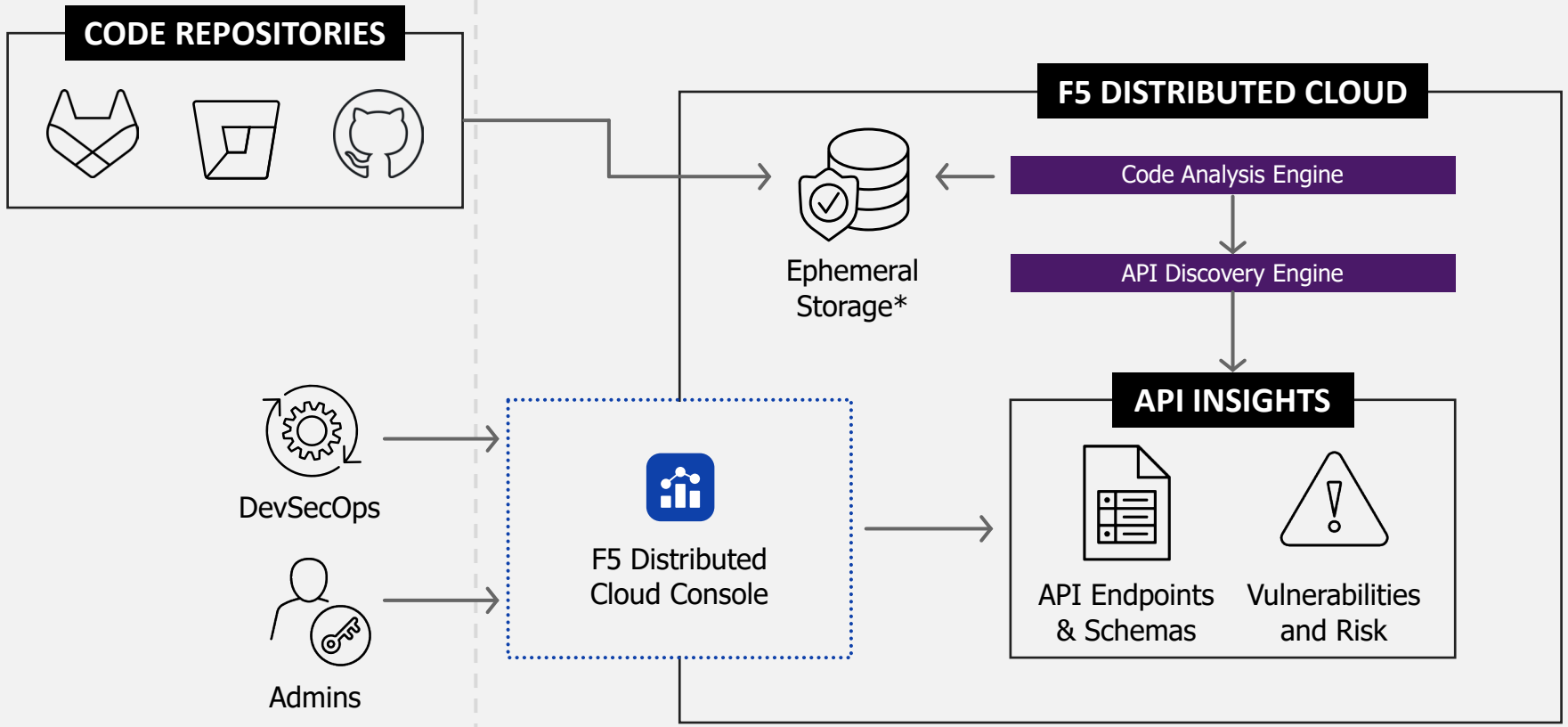
Why is this necessary?
Goes beyond traffic to find unmanaged APIs which are outside of any security proxy

- API Discovery lens using external domain crawling
- Scans subdomains for exposed API endpoints
- Findings fused with all other lenses of API Discovery into a rich API Inventory



API Endpoint	Group	Method	Authentication State	API Category	Discovery Source	Risk Score	API Compliance	Actions
/rest-api/scema	0	GET	Authenticated	Inventory	Code, Traffic	80	PCI	•••
/cart/checkout	3	PUT	Authenticated	Inventory	Code, Traffic	40	PCI, GDPR, HIPPA...	•••
Keren_test	0	PATCH	Un-Authenticated	Discovered, Inventory	Code, Traffic	80	PCI	•••
Nelly-55	6	GET	Authenticated	Discovered, Inventory	Traffic	50	GDPR	•••
Aric456	12	POST	Authenticated	Discovered, Shadow	Traffic	60	GDPR	•••
ytg_uui	40	GET	Authenticated	Discovered, Shadow	API Crawling	34	GDPR	•••
789g_jj	23	GET	Un-Authenticated	Discovered, Inventory	Code	100	PCI, GDPR, HIPPA...	•••
Aric456	12	POST	Un-Authenticated	Discovered, Inventory	API Crawling	20	HIPPA	•••
/rest-api/scema	0	GET	Unknown	Discovered, Inventory	Traffic	0	HIPPA	•••

How F5 discovers APIs by analyzing app source code



- **Repositories:** Azure, Bitbucket, GitLab, GitHub
- **Programing Languages:** Java – (EE, spring) , .Net, Python (flask, Django), JavaScript (express, hapi), GO - gin.
- **Github Tokens:** Classic and Fine-grained

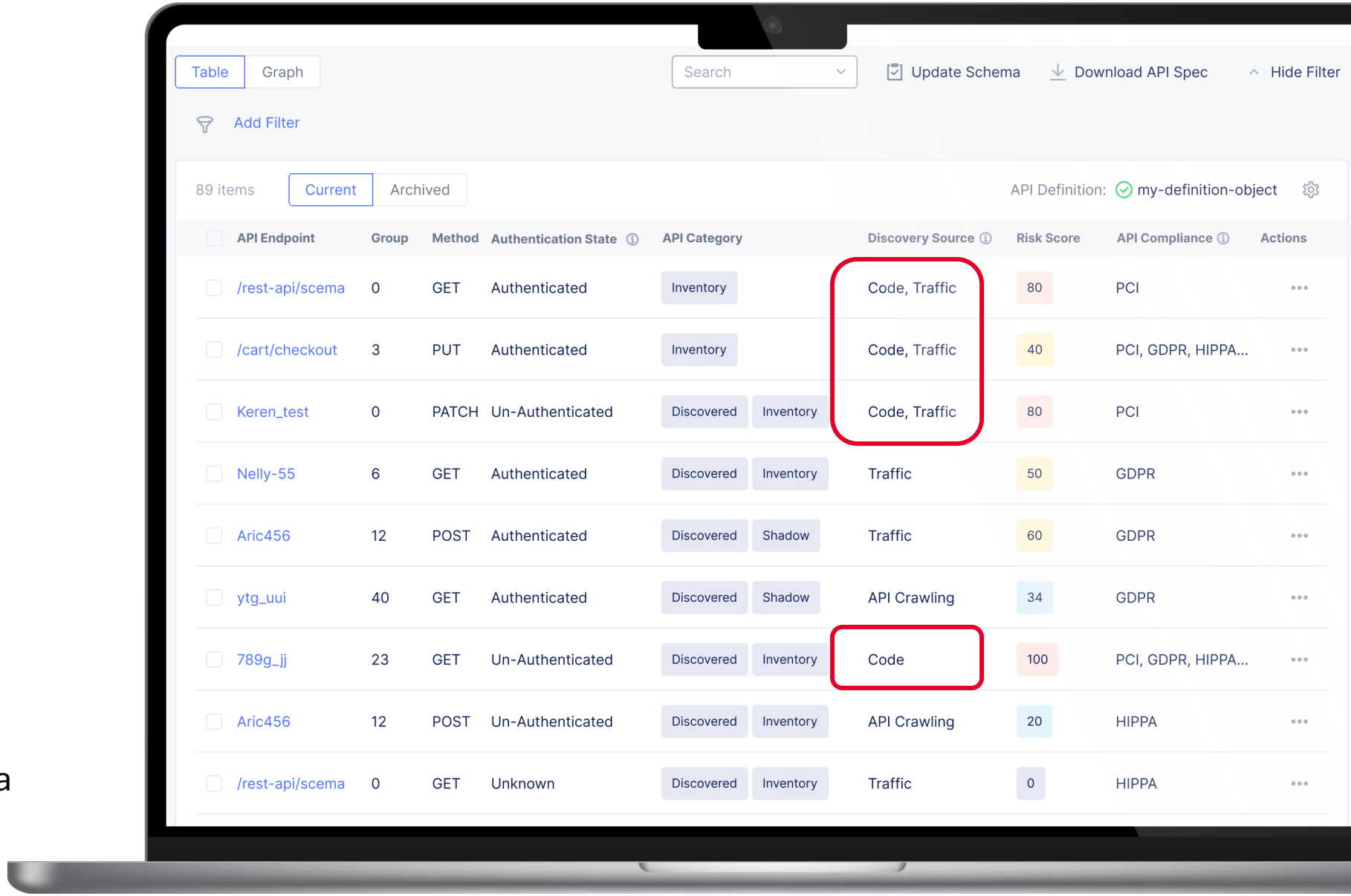
*Code is held only long enough to perform analysis.

API Discovery from Code

Why is this necessary?

Begin to document the API threat surface, find potential vulnerabilities and inform critical protections – before release to production, reducing risk posture

- Discover APIs directly from code repositories
- Findings fused with all other lenses of API Discovery into a rich, more complete API Inventory



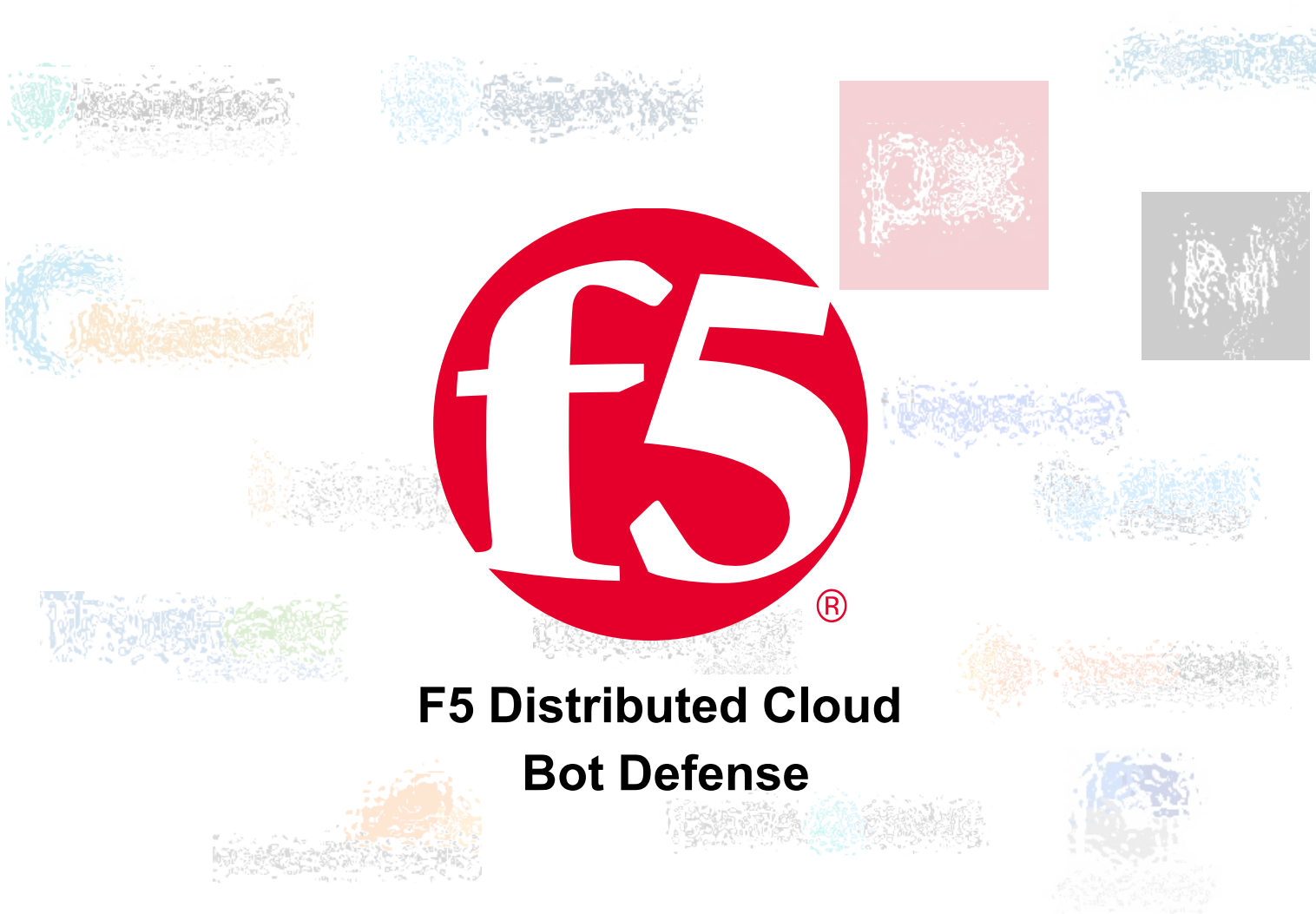
Industry's Most Effective Bot Solution

Eliminates 99%+
of unwanted automation

Zero Trust Model

Flexible Deployments

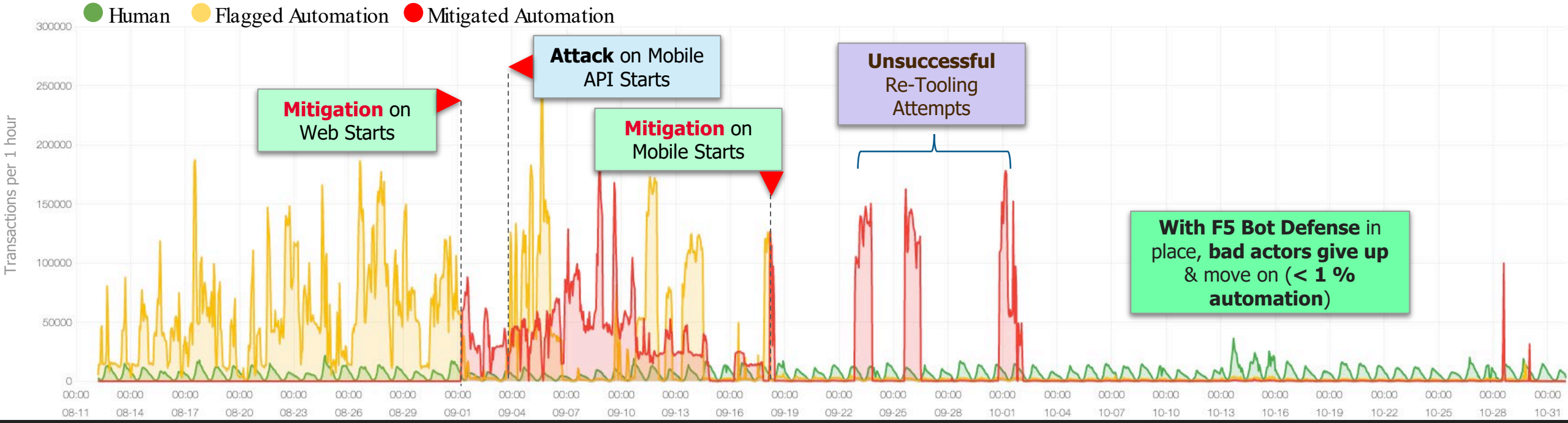
Managed Service



F5 Distributed Cloud
Bot Defense

Attacker Journey vs F5 Bot Defense

Immediate, durable & long-term efficacy with F5 Bot Defense Advanced



89M
Total Txns

4.3M IPs
19K ASNs
5.8M UAs

85%
Automation

Leveraging VPNs to attempt to bypass IP-reputation or rate limiting controls

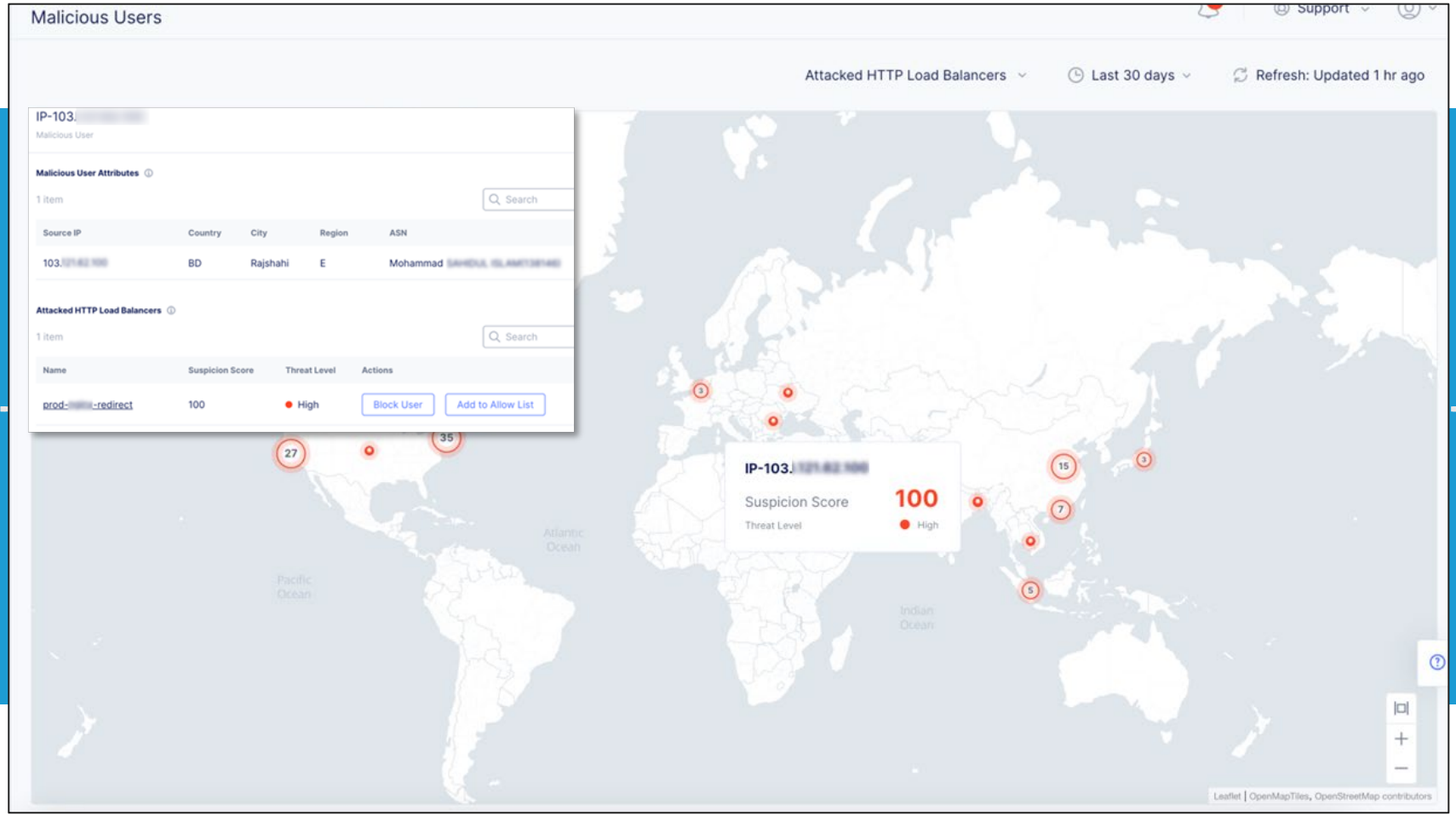
Spoofing User-Agents in attempt to bypass Signature-based tools

API-Learning und Anomalie-Erkennung

API-Learning und Anomalie-Erkennung

- Einsatz von Machine Learning und AI, um verdächtiges Verhalten frühzeitig zu identifizieren
- Dynamisches Lernen und Generierung von Sicherheitsrichtlinien
- Beispiele: Schutz vor fehlerhaften API-Aufrufen oder übermäßigen Traffic-Mustern

AI/ML Powered Anomaly Detection and Risk Scoring

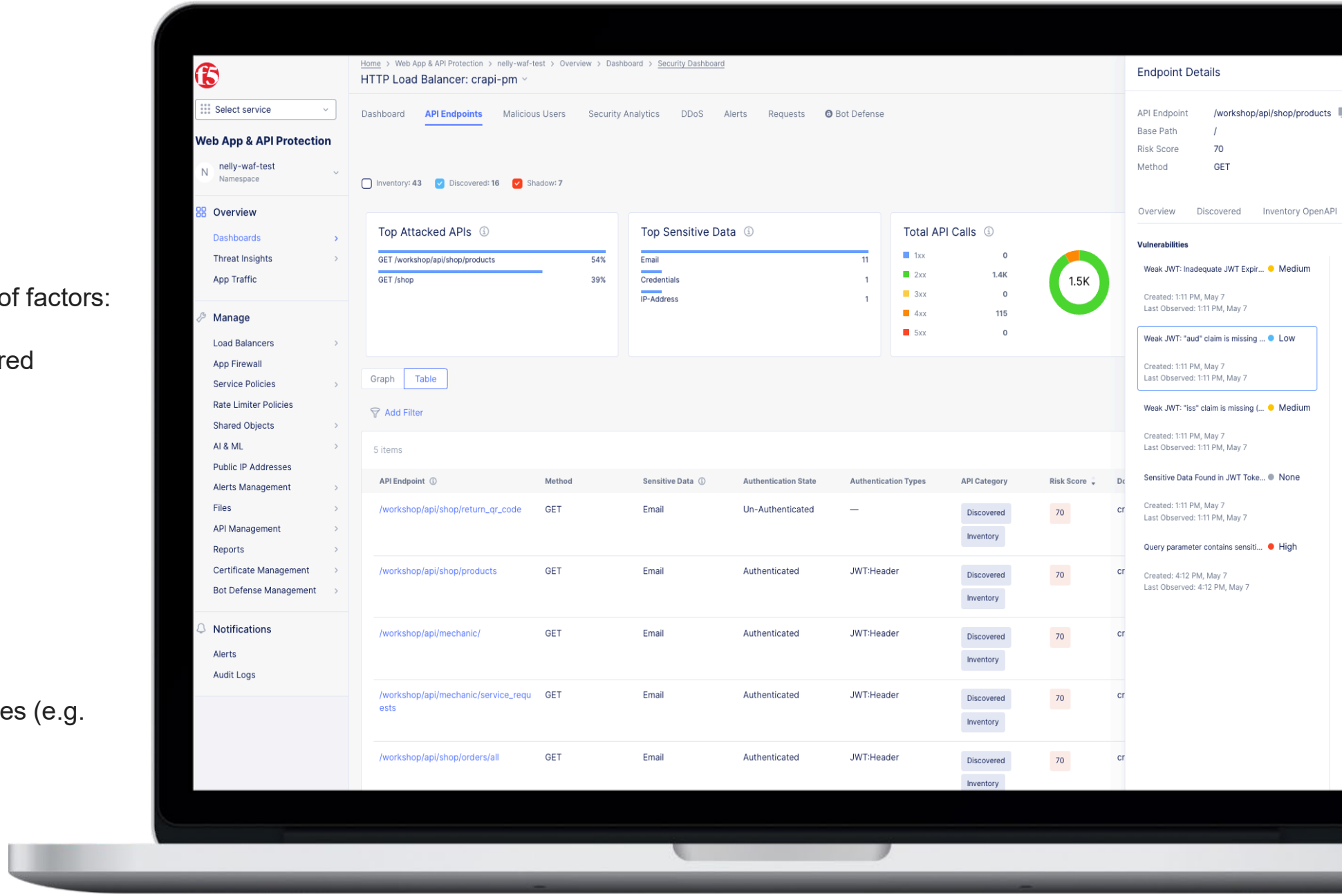


Comprehensive client analysis with **suspicion scoring** for rapid decision making

API endpoint risk scoring

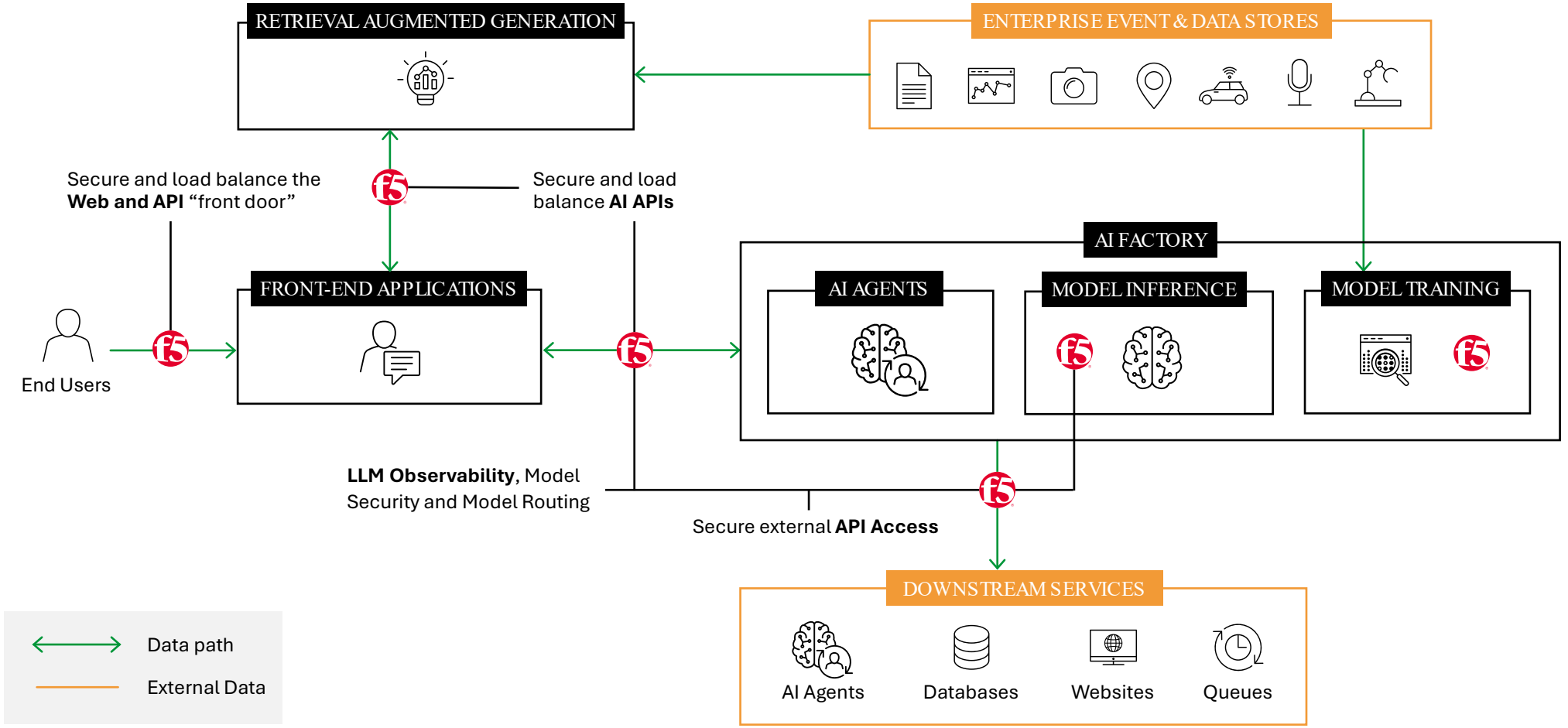
Consistent Security

- ✓ Score risk based on variety of factors:
  - ➢ vulnerabilities discovered
  - ➢ attack impact
  - ➢ attack likelihood
  - ➢ mitigating controls
- ✓ Provide guidance to aid in remediation efforts
- ✓ Inline enforcement capabilities (e.g. block, rate limit etc.)

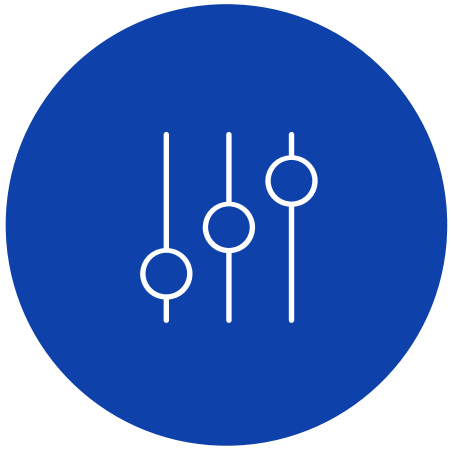


Zusammenfassung und Ausblick

Safeguard AI applications, APIs, and models while keeping them connected across highly distributed environments



F5 combines all critical API security capabilities into a single platform with centralized visibility and management



Complete API visibility from code to production

Continuous vulnerability and attack detection

Comprehensive enforcement and protection

Protect anywhere with flexible hybrid SaaS

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.