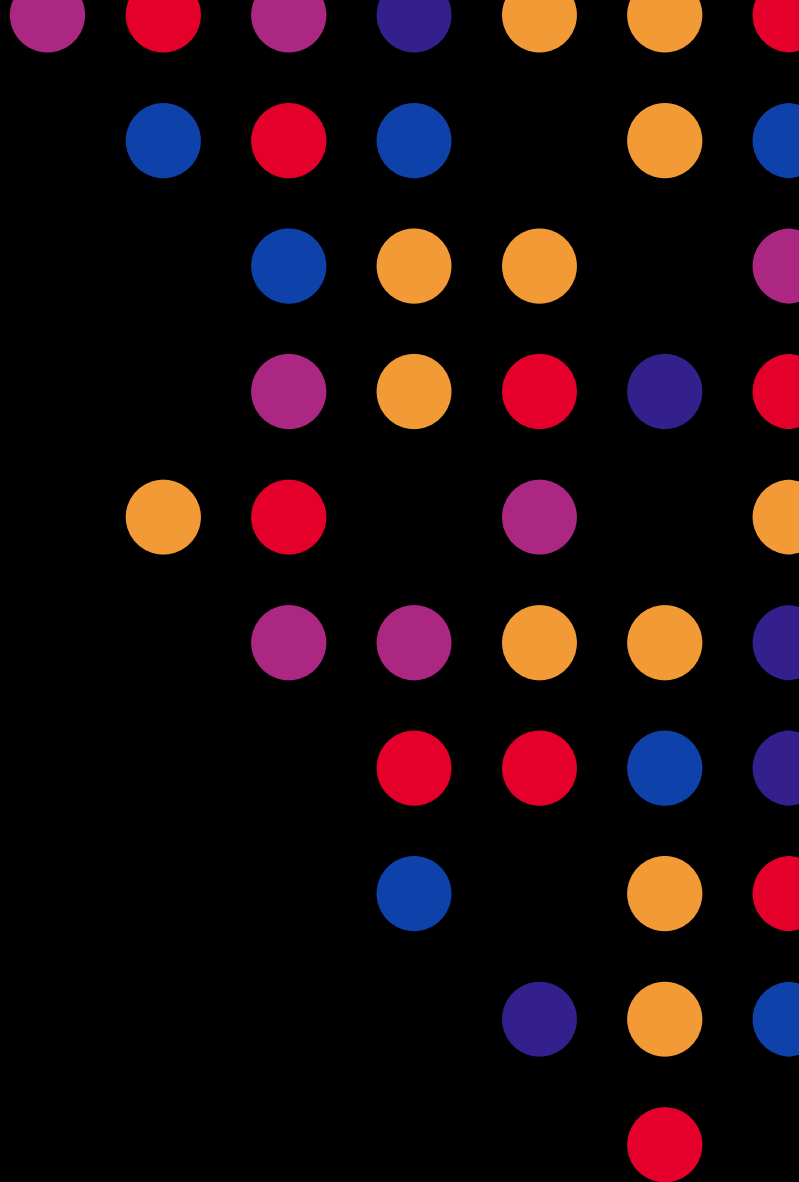




# Securing APIs

Josh Goldfarb, Global Solutions Architect – Security

Brad Otlin, Sr Solutions Engineer



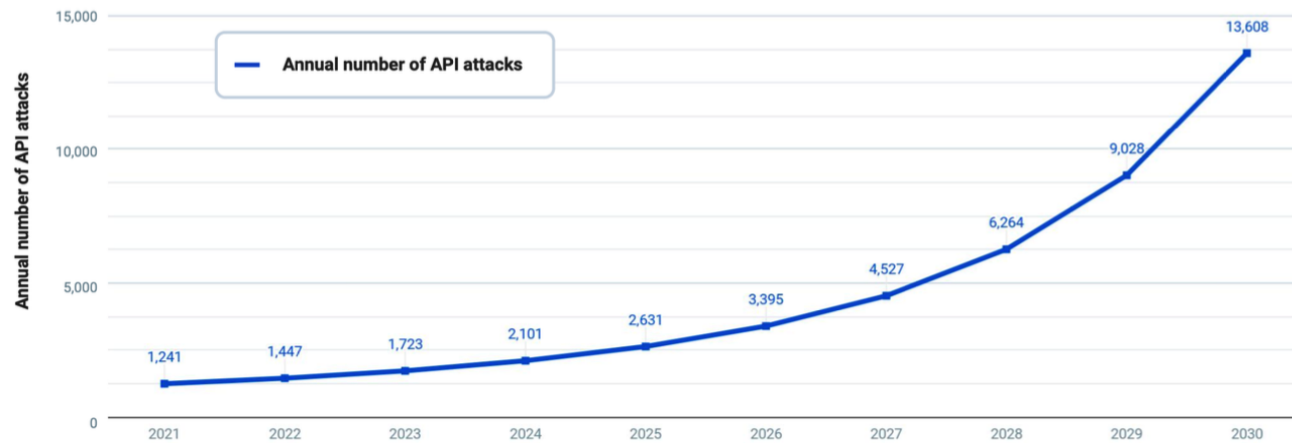
# The State of API Security

# APIs are under Attack

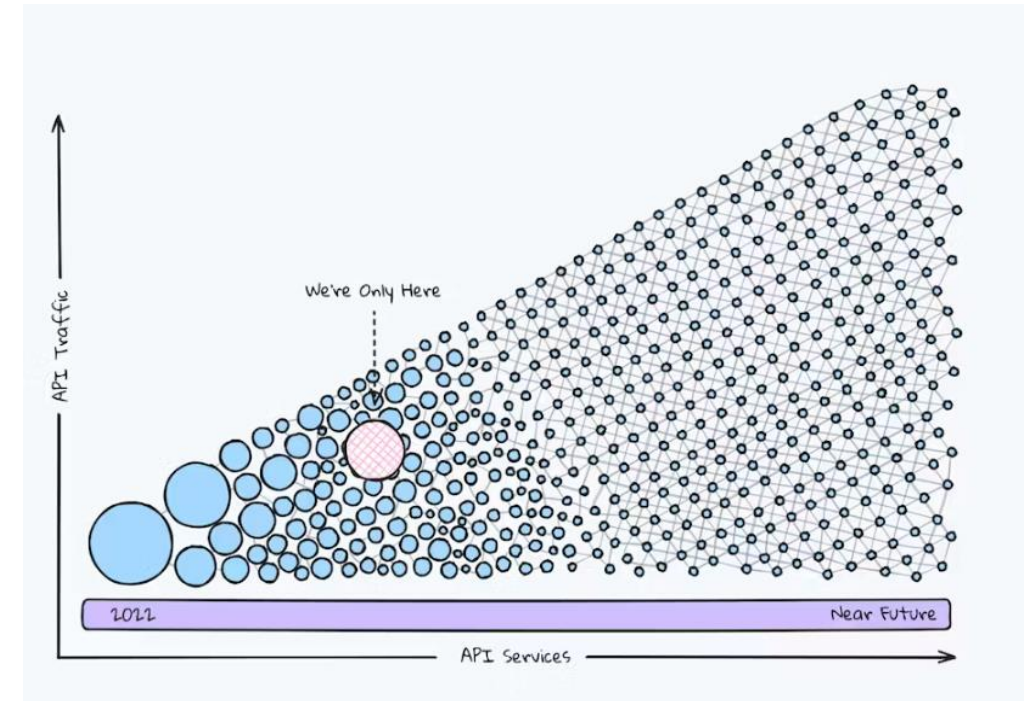
API Security Research

## API Attacks

**996%** growth in forecasted API attacks between 2021 and 2030



Source – Kong API Security Research



# APIs are risky by definition



**Open by design** – APIs are created to share access to data and applications



**Larger attack surface** – Every API and endpoint expands the potential attack surface



**Difficult to observe** – API attacks can evolve slowly with small requests over weeks or months



**Expose extra data** – Developers build flexible APIs that provide more data than is required

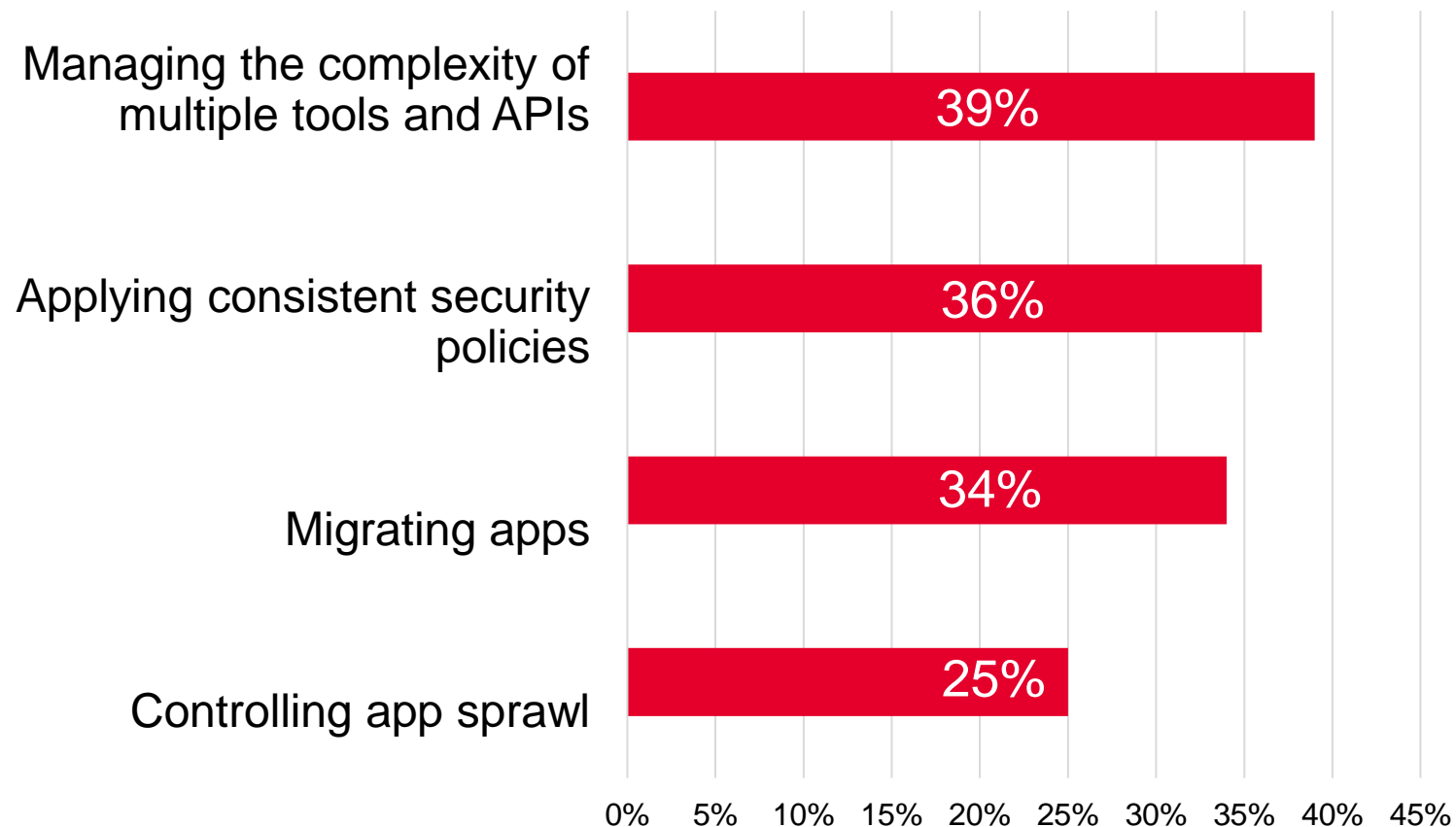


**Predictable structure** – APIs adhere to logical architectures (REST) making them easy to probe



**Lack protections** – APIs are often deployed without basic protections like access control

# Managing and securing APIs continues to be a challenge



*More than 9 out of 10 enterprises have experienced an API security incident*

SOURCES: State of Application Strategy Report (F5, 2023); Continuous API Sprawl (F5, 2021)

# Why use AI/ML to protect APIs?

- Modern Payments like BNPL require immediate pro-active Security screening
- API security requires data-driven analysis to identify malicious usage patterns.
- Top-tier threat actors are themselves using AI in their recon and attack campaigns—this will be arms race.
- Rapid growth of API adoption makes manual approaches to API security impractical, slow and costly
- Enables continuous traffic inspection, behavioral analysis and anomaly detection – security evaluation at machine speed
- Inform Decision Making – create new tools like risk scoring – aggregating insights to aid in analyst review for remediation

# Use Cases: Applying AI to API Security

# API Visibility and Discovery



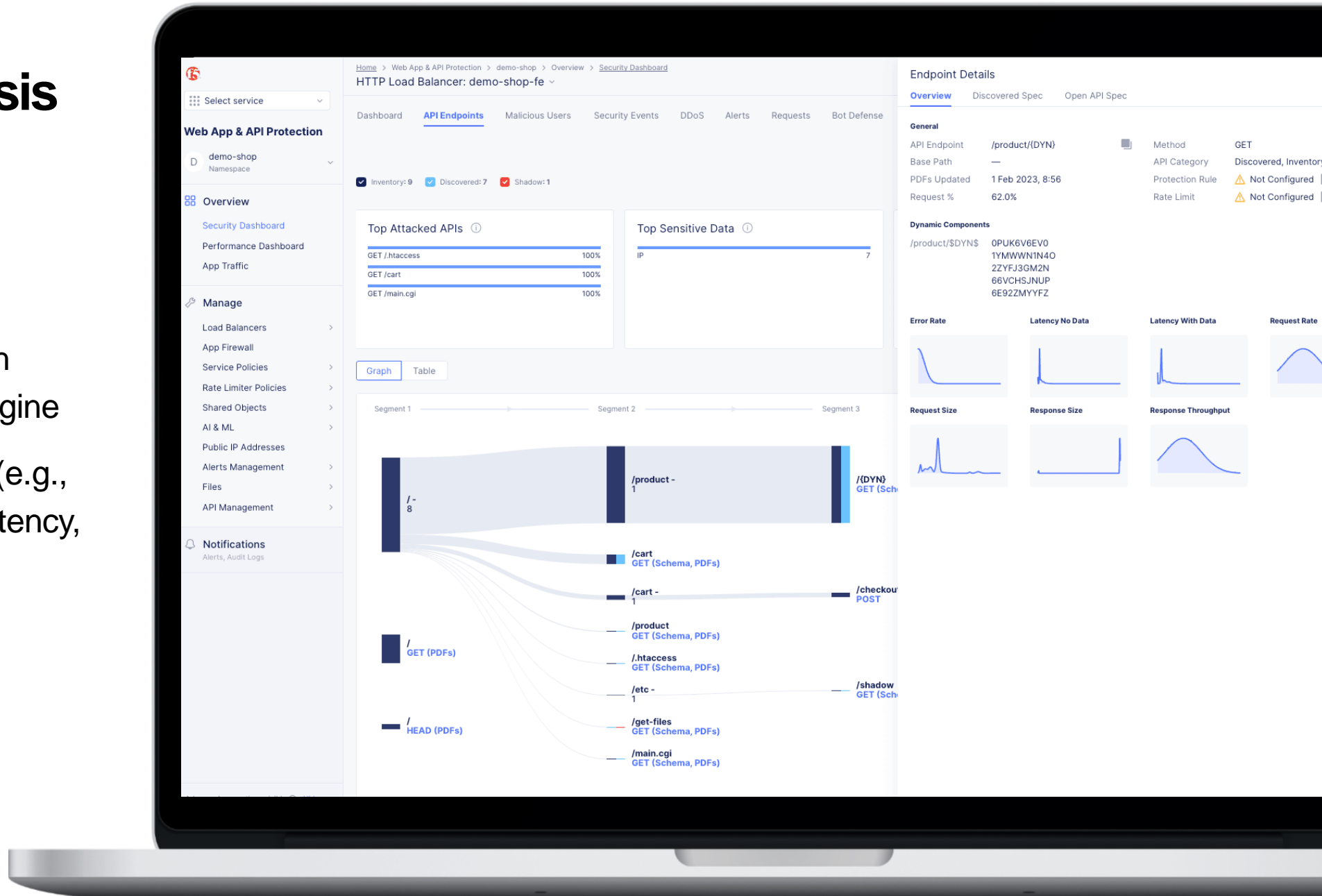
# How?

- Begin with inventory, management, and security of known API endpoints
- Study traffic to learn of additional API endpoints
- Include legitimate API endpoints in inventory, management, and security
- Decommission illegitimate API endpoints
- Work with the business to reduce the number of unknown API endpoints
- Continually iterate

# F5 XC

## Behavioral Analysis of API Endpoints

- Monitor and baseline API behavior continuously with machine learning (ML) engine
- Easily identify anomalies (e.g., spikes in request rates, latency, response size, etc.)



# Demo

# Schema Enforcement



# How?

- Begin with policy
- Learn schemas by analyzing traffic
- Detect departures from policy
- Detect drift
- Mitigate/enforce schema compliance

# F5 XC

## OpenAPI Spec Import and Enforcement

Automatically enforce API schema and a Positive Security Model

- Upload existing API schema for enforcement of appropriate API behavior
- No wasted time spent configuring and deploying APIs
- Easily allow valid requests and block any method that the schema doesn't support
- Import via UI or the API and integrate into a CI/CD Pipeline

The screenshot displays the F5 OpenAPI Spec Import and Enforcement interface. At the top, a Swagger Petstore schema is imported from a source URL. The schema is displayed in a code editor, showing the OpenAPI specification for the Swagger Petstore API. The interface includes a sidebar with a list of API endpoints and their methods. The main area shows the Swagger Petstore API endpoints, including /pet, /store, and /user. The interface also includes a 'Source' field with the URL 'https://swagger.io/'. Below the schema, the 'API Endpoints' section shows a list of endpoints with their methods and status. The 'API Endpoints' section includes a table with columns for 'Endpoint', 'Method', and 'Status'. The table lists endpoints such as /pet, /store, and /user, with their respective methods and status. The interface also includes a 'Download Swagger' button and an 'Auto-Refresh' option. The bottom section shows a list of API endpoints with their methods and status, including /pet, /store, and /user.

# Demo

# Access Control



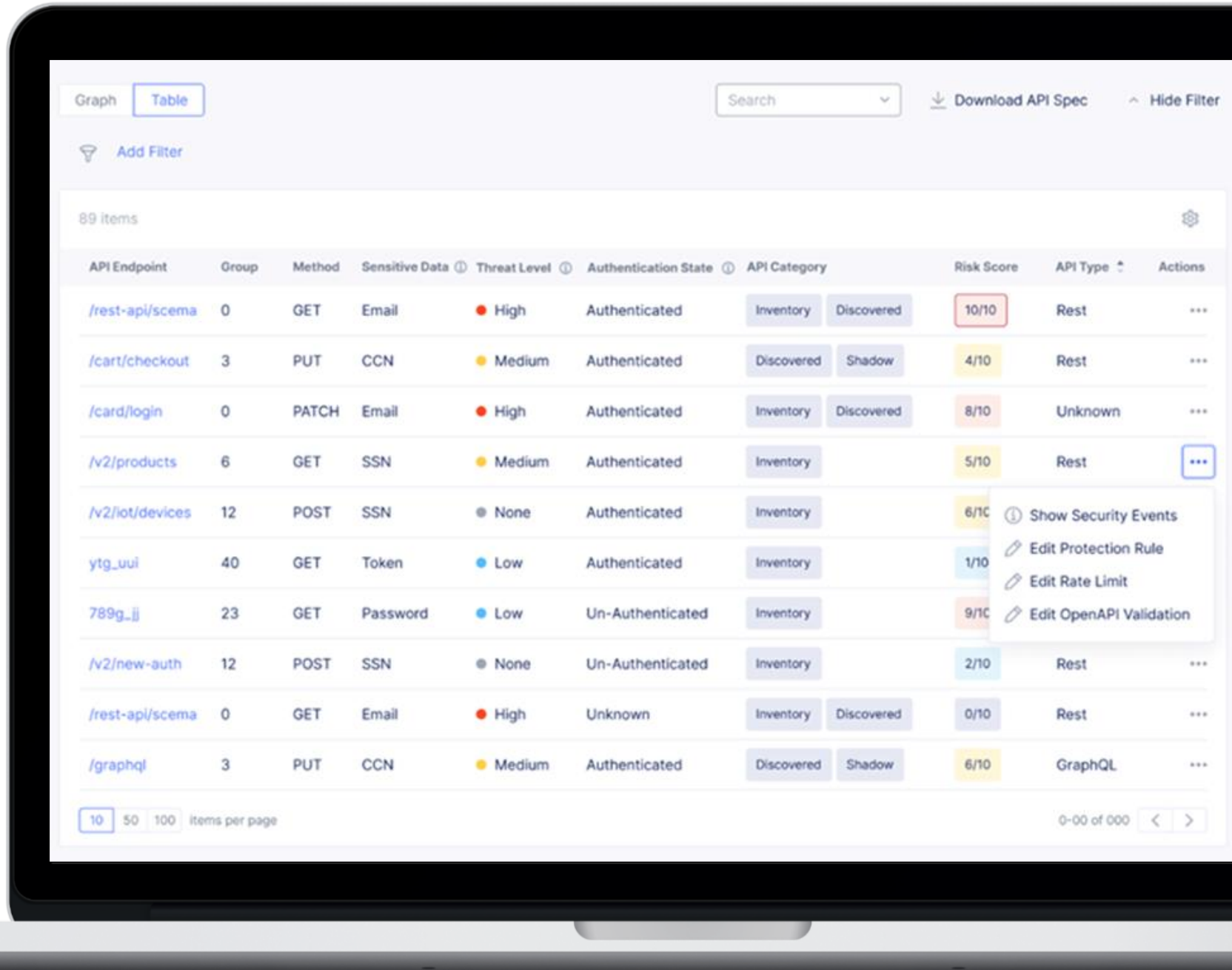
# How?

- Map APIs and identify gaps in API authentication and authorization
- Baseline authentication state of all APIs
- Evaluate existing authorizations
- Produce a threat level and risk score for each API
- Mitigate/refine access control as required

# F5 XC

## Discovery and Validation of API Authentication

- Discover and view authentication status, details for all API endpoints
- Easily create protection rules (e.g., Blocking, rate limiting etc.)



The screenshot displays the F5 XC API Discovery and Validation interface. At the top, there are tabs for 'Graph' and 'Table', a search bar, and links for 'Download API Spec' and 'Hide Filter'. Below the tabs, there is a section for '89 items' with a settings icon. The main table lists API endpoints with columns for API Endpoint, Group, Method, Sensitive Data, Threat Level, Authentication State, API Category, Risk Score, API Type, and Actions. A context menu is open for the endpoint '/v2/iot/devices', showing options like 'Show Security Events', 'Edit Protection Rule', 'Edit Rate Limit', and 'Edit OpenAPI Validation'.

API Endpoint	Group	Method	Sensitive Data	Threat Level	Authentication State	API Category	Risk Score	API Type	Actions
/rest-api/scema	0	GET	Email	High	Authenticated	Inventory Discovered	10/10	Rest	...
/cart/checkout	3	PUT	CCN	Medium	Authenticated	Discovered Shadow	4/10	Rest	...
/card/login	0	PATCH	Email	High	Authenticated	Inventory Discovered	8/10	Unknown	...
/v2/products	6	GET	SSN	Medium	Authenticated	Inventory	5/10	Rest	...
/v2/iot/devices	12	POST	SSN	None	Authenticated	Inventory	6/10	Rest	Show Security Events Edit Protection Rule Edit Rate Limit Edit OpenAPI Validation
ytg_uui	40	GET	Token	Low	Authenticated	Inventory	1/10	Rest	...
789g_ii	23	GET	Password	Low	Un-Authenticated	Inventory	9/10	Rest	...
/v2/new-auth	12	POST	SSN	None	Un-Authenticated	Inventory	2/10	Rest	...
/rest-api/scema	0	GET	Email	High	Unknown	Inventory Discovered	0/10	Rest	...
/graphql	3	PUT	CCN	Medium	Authenticated	Discovered Shadow	6/10	GraphQL	...

At the bottom, there is a pagination bar showing '10 50 100 items per page' and a status bar showing '0-00 of 000'.

# Demo

# Safeguarding Sensitive Data



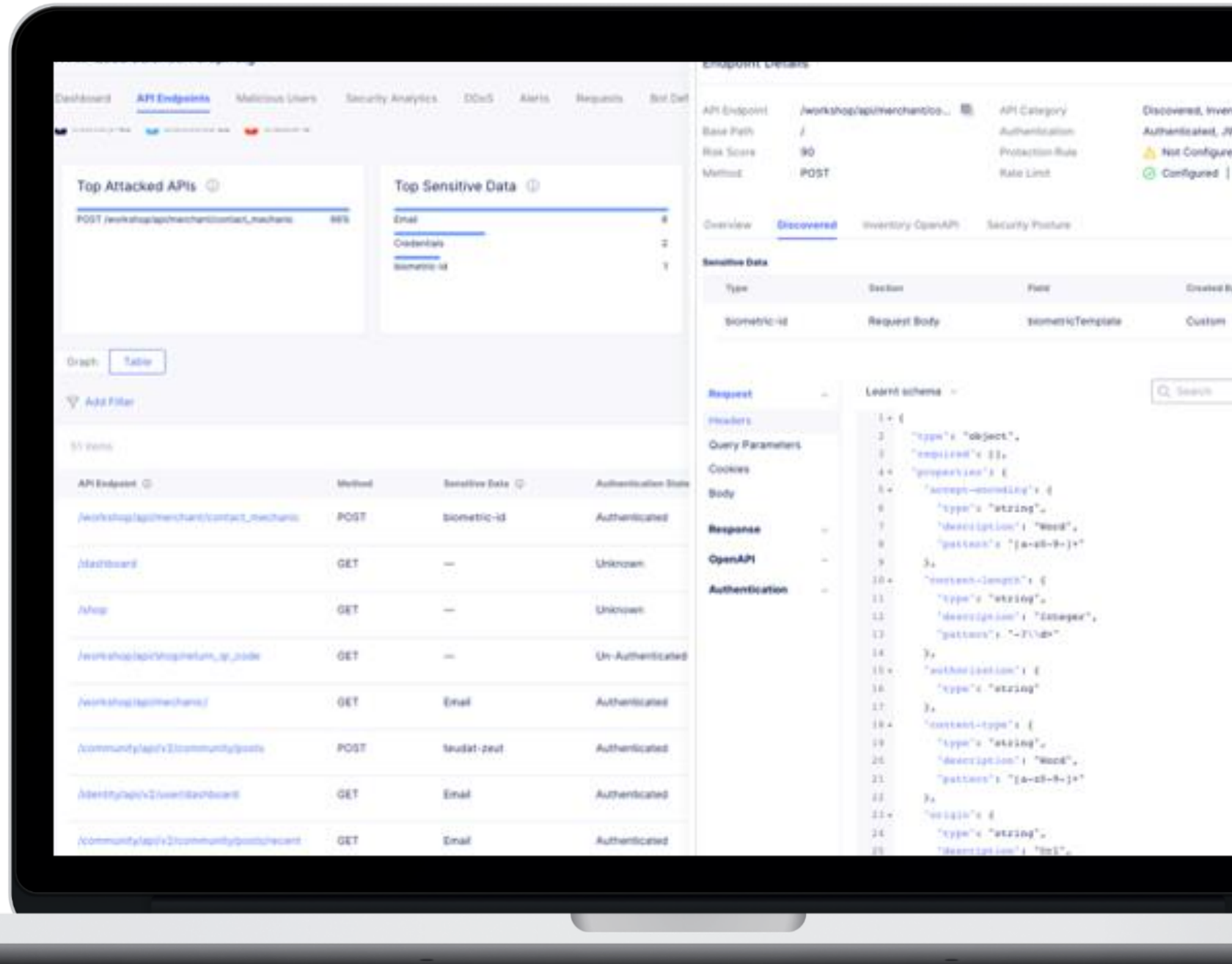
# How?

- Identify API endpoints where PII and other sensitive data is transferred
- Detect and flag PII and other sensitive data that is exposed
- Mitigate and/or mask

# F5 XC

## Discovery and Monitoring for PII Data in APIs

- Detection and flagging of PII that is being exposed
- Quickly and easily identify any critical PII that is being shared for any API, so remediation can be put in place



# Demo

# Layer 7 DDoS Protection



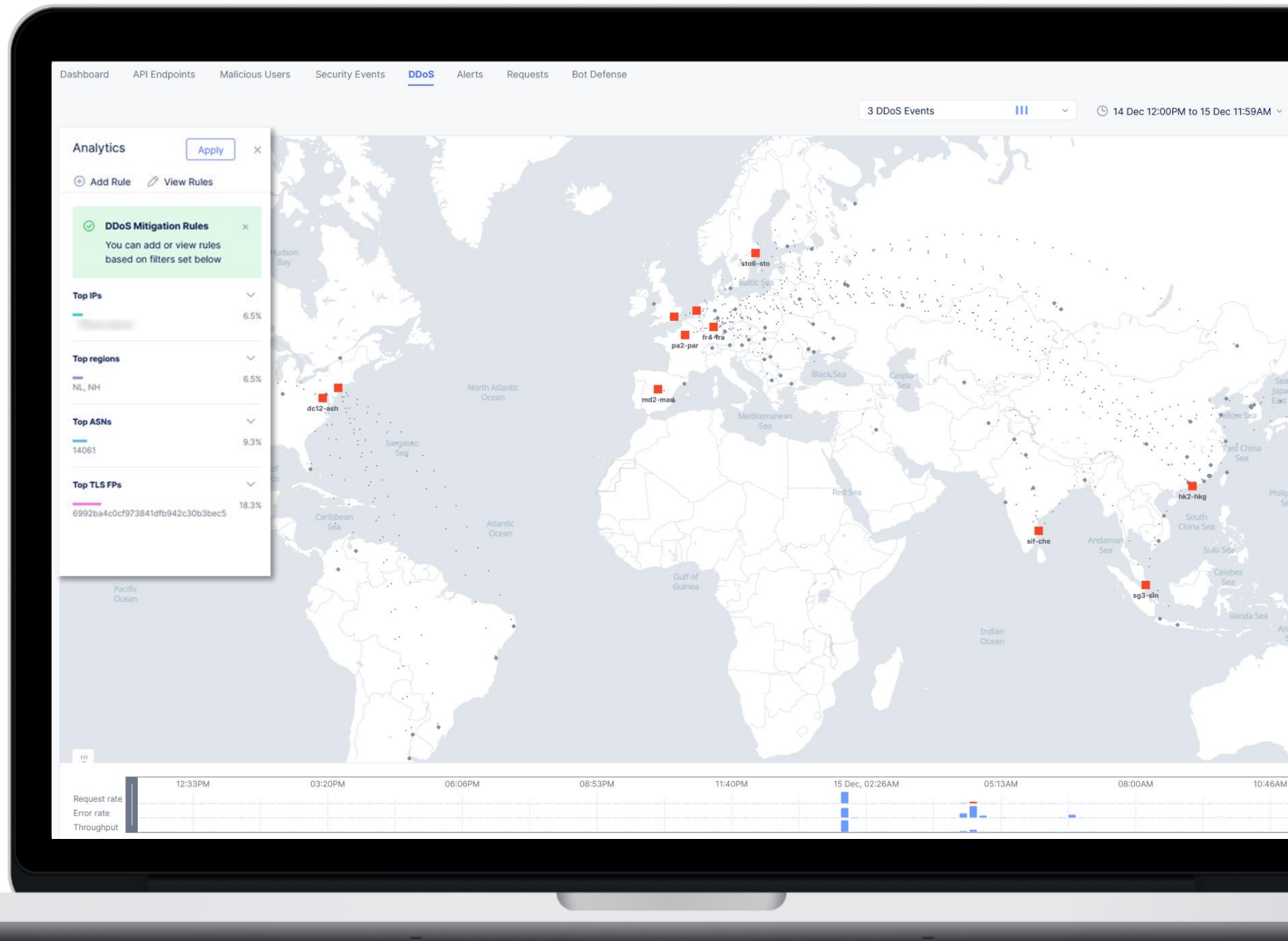
# How?

- Begin with rate limiting as a first step
- Detect abuse of APIs at layer 7 (application layer)
- Use granular controls – one size does not fit all APIs
- Continually analyze and baseline each API's traffic
- Deny or limit based on IP address, region/country, ASN or TLS fingerprint, HTTP method, path, query parameters, headers, cookies, and more

# F5 XC

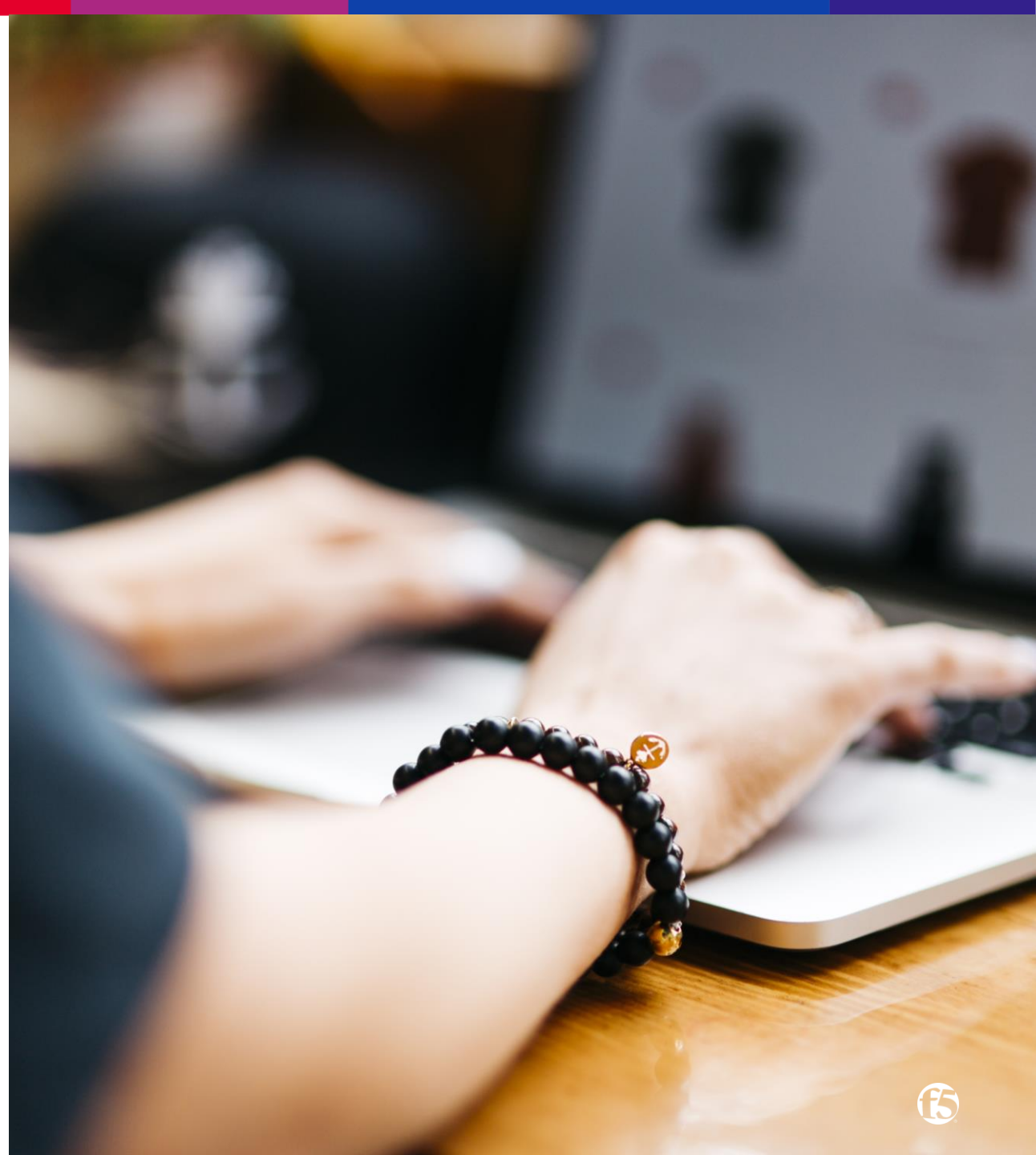
## Layer 7 DoS

- Detection and alerting on abnormal traffic patterns & trends
- Advanced machine learning (ML) to detect spikes, sudden drops and more
- Analyzes request rate, error rate, and throughput of app and API endpoints
- Deny with auto mitigation or Rate limit endpoints



# Demo

# Malicious User Detection



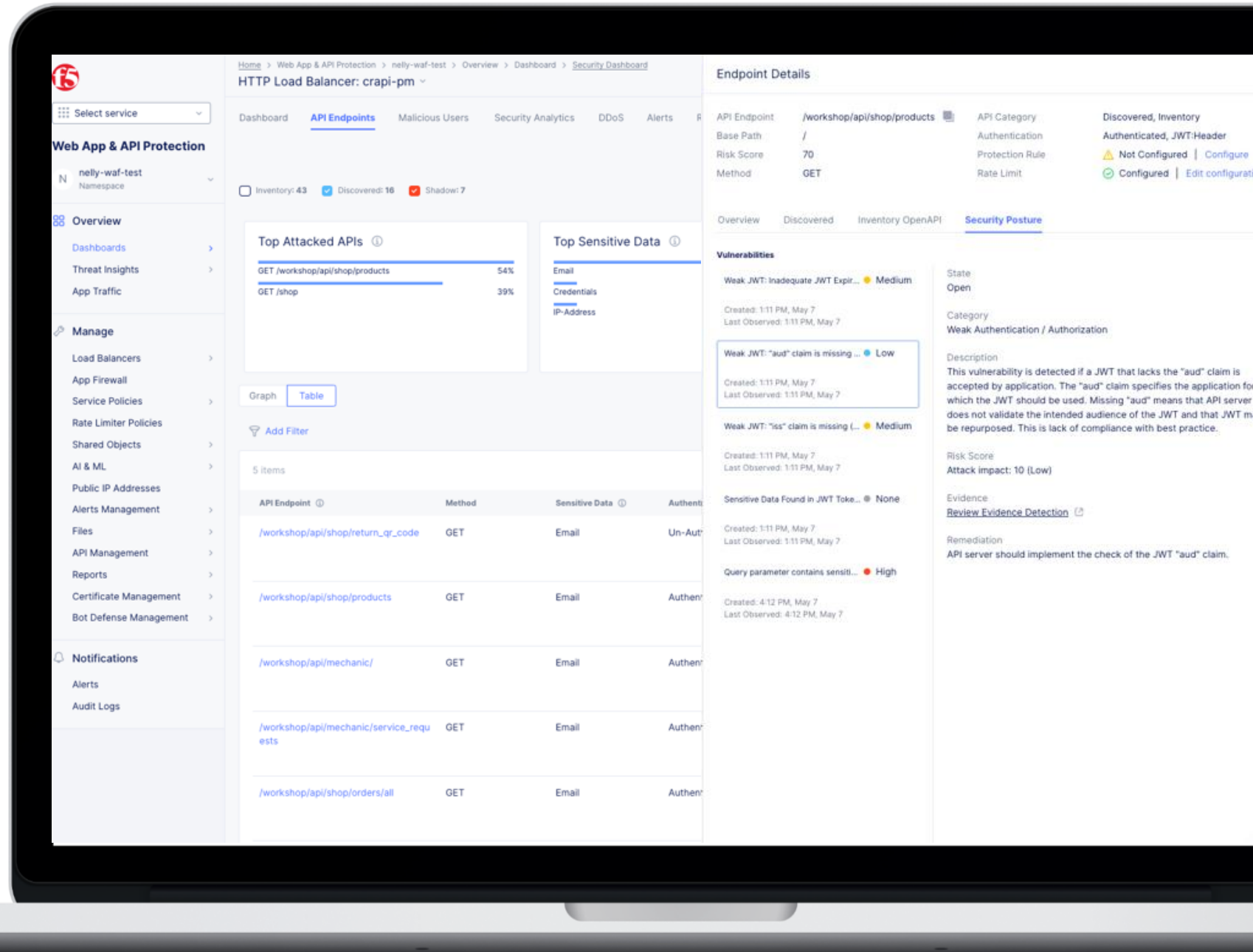
# How?

- Analyze all client interactions, including with APIs
- Identify outliers
- Produce threat level and risk score for each client
- Continually adjust threat level and risk score based on subsequent interactions
- Continually adjust client access and permissions based on threat level and risk score

# F5 XC

## API Endpoint Risk Scoring

- Scores based on variety of factors including vulnerabilities discovered, attack impact, attack likelihood and mitigating controls
- Includes guidance with instructions and evidence to aid in remediation efforts



# Demo

