

Securing APIs

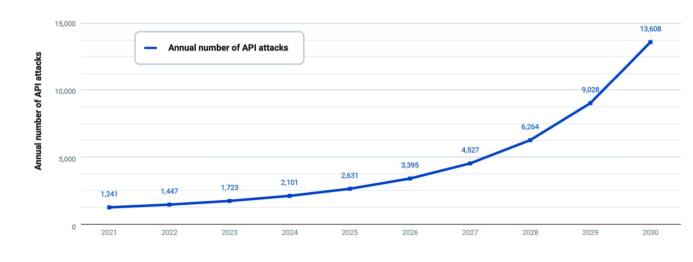
Josh Goldfarb, Global Solutions Architect – Security

Brad Otlin, Sr Solutions Engineer

The State of API Security

3 ©2024 F5

Source – Kong API Security Research

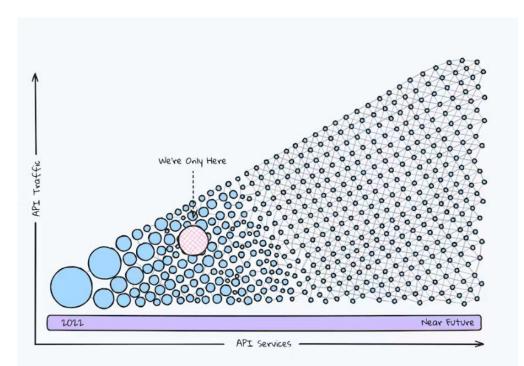


API Security Research API Attacks

996% growth in forecasted API attacks between 2021 and 2030

API Security Research

APIs are under Attack



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

0101011 1011010 11011011

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

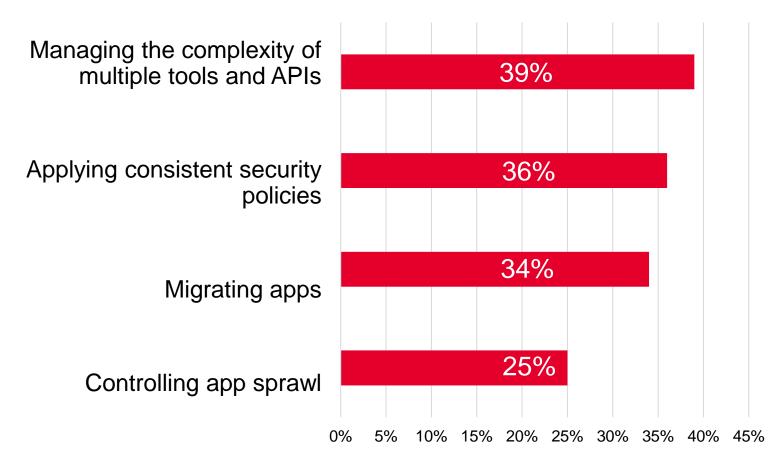


Predictable structure – APIs adhere to logical architectures (REST) making them easy to probe



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

Managing and securing APIs continues to be a challenge



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

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

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

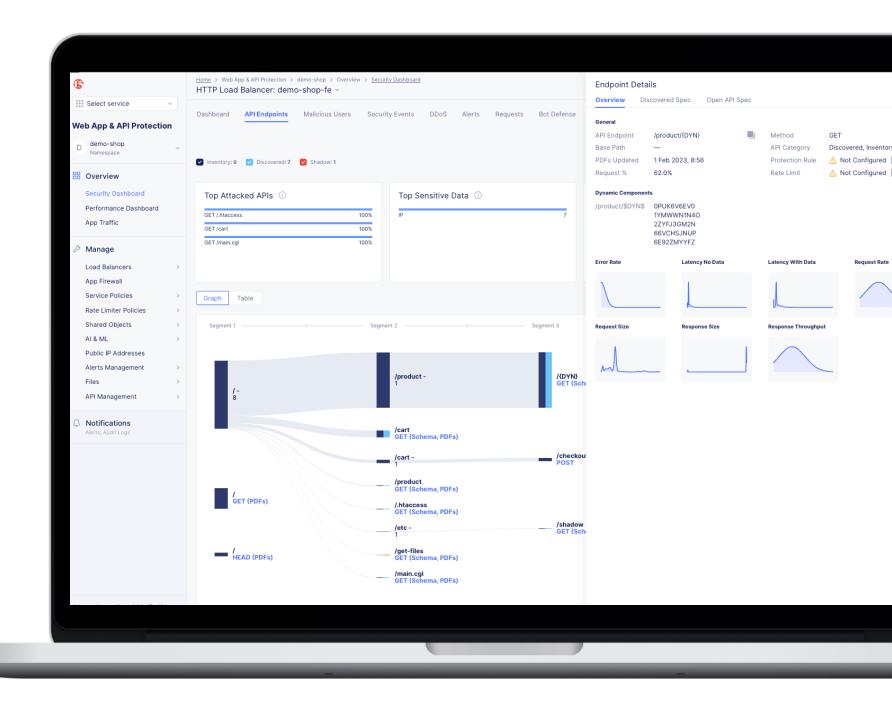


How?

- 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



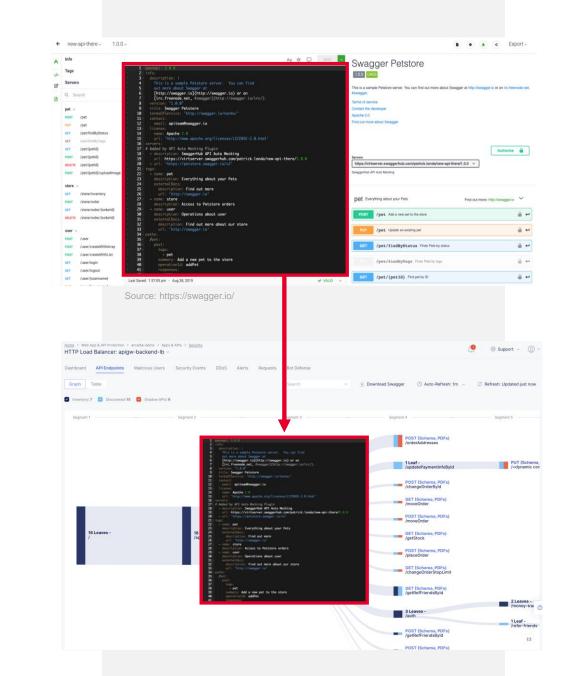
How?

- 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

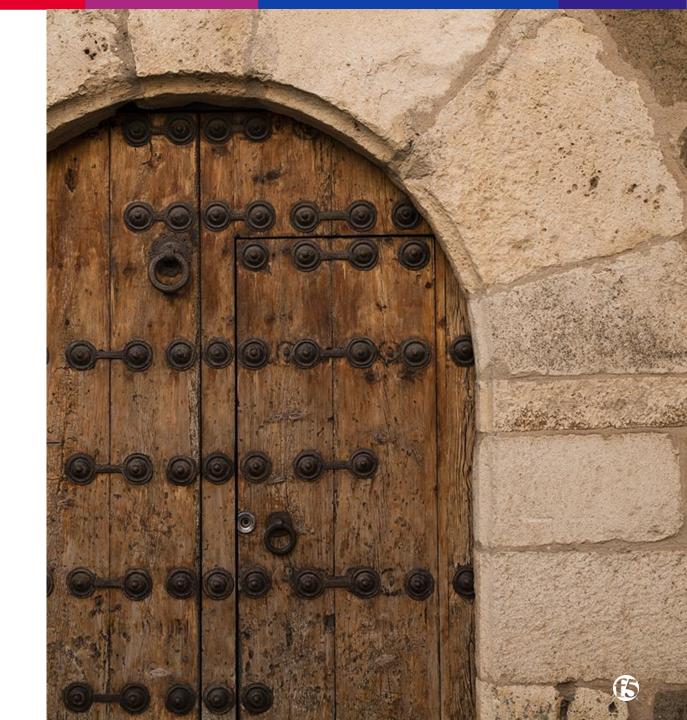
Automatically enforce API schema and a Positive Security Model

- 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



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.)

Fraph Table					5	Search	×)		ad API Spec	Hide
Add Filter										
89 items										
API Endpoint	Group	Method	Sensitive Data ①	Threat Level ①	Authentication State ①	API Category		Risk Scor	API Type 🕈	Act
/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		6/1C (③ Show Security Ev	vents
ytg_uui	40	GET	Token	• Low	Authenticated	Inventory		1/10	 Edit Protection Ri Edit Rate Limit 	ule
789g_jj	23	GET	Password	• Low	Un-Authenticated	Inventory		_	C Edit OpenAPI Vali	idatic
/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	
10 50 100 iter	ms per pag	,e							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

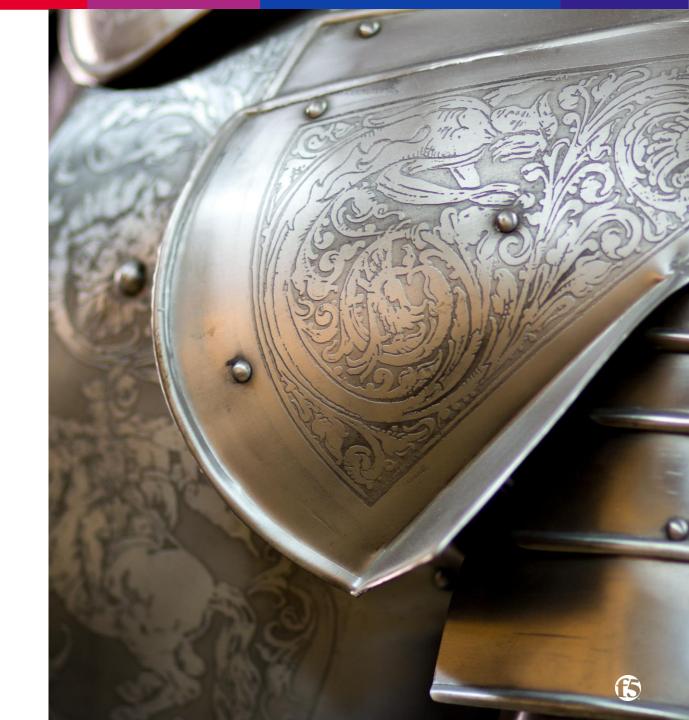
F5 XC Discovery and Monitoring for PII Data in APIs

- 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

				Endpoint D	tiaca.			
Danhament Aff Endpoints Malicinus Union Sacurity Analytics DCmS Alartis Requests Bot Dat 					/worksho / 90 POST	gʻapimerchantica B	API Category Authentication Protection Bale Rate Limit	Discovered, Inver Authenticated, JR
Top Attacked APIs ①		Top Sensitive Data		Matting	(and		Construction of the second	O canadrasa 1
POST /workshop/api/metchanticontiact_machante	445				Discovered	Inventory OpenAPs	Security Pointine	
		Codenitais Bornetite M		Seculture Data	_			
				740-		Sector	Free	Deatest B
				bonetic	ж	Request Body	TriometricTemplate	Custom
Drach <u>Table</u> © Add Filter (1) Dense				Request Proders Overy Param	nes -	Learnt schema (+ + 		Q, Seauth
API Reducted	. Wetterd	Banative Data 😳	Autorituation Date	Cookes		die Sproparks		
/winking/apprestant/contact_mechanic	POST	biometric-id	Authenticated	Body		a fayya 9 fakat	"s "wtring", Hiptics": "Weed", sat's "(seat-b-)""	
Mastrouwi	GET		Unicroam.	OpenAM		3 34		
No.	GET	-	Unknown.	Authenticati	on	13 Tepe	-length": { 's "etriog", tiplics": "Estagar",	
Increasing Increasing Instance, process	061	<u> </u>	Un Authenticated			14 34	int's "-Filds"	
(with the destine there)	067	Enal	Authenticated			17 34	"« "etring"	
Accounted players Discountering Sector	POST	teudist-peut	Authenticated			19 Tappe	Litops's ("s "atalog", rigtion's "Weed",	
Adviting/apply2/sources/docard	GET	Email	Authenticated			88 P.a	ers") "[4-25-8+]*"	
A community legits 2 to one only bound accent	GET	Enal	Authenticated			24 ⁽⁴⁾ 1414	"e "etring";	

Demo

Layer 7 DDoS Protection

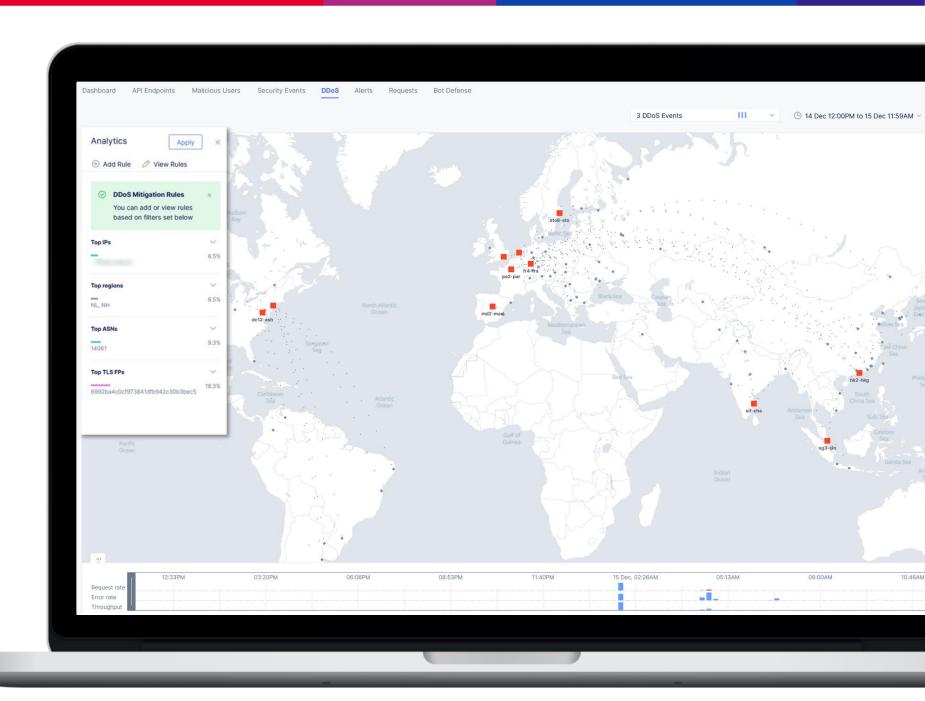


How?

- 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, latency, and throughput of app and API endpoints
- Deny with auto mitigation or Rate limit endpoints



ILLUSTRATIVE

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

6	Home > Web App & API Protection > nelly-waf HTTP Load Balancer: crapi-pm ~	-test > Overview > Dash	board > Security Dashboard		Endpoint Details					
III Select service Web App & API Protection N nelly-waf-test Namespace	Dashboard <u>API Endpoints</u> Malicio	us Users Security	API Endpoint /workshop/api/shop/products Base Path / Risk Score 70 Method GET	API Category Authentication Protection Rule Rate Limit	Discovered, Inventory Authenticated, JWT:Header Not Configured Configure Configured Edit configuret					
Overview Dashboards Threat Insights App Traffic	Top Attacked APIs ① GET /workshop/api/shop/products GET /shop	54% 39%	Top Sensitive Data Email Credentials	3	Overview Discovered Inventory OpenAP Vulnerabilities Weak JWT: Inadequate JWT Expir Medium Created: 111 PM, May 7	State Open				
Manage Load Balancers App Firewall Service Policies Rate Limiter Policies	Graph Table		IP-Address		Last Observed: 111 PM, May 7 Last Observed: 111 PM, May 7 Weak JWE: "aud" claim is missing • Low Greated: 111 PM, May 7 Last Observed: 111 PM, May 7 Weak JWT: "iss" claim is missing (• Medium	Category Weak Authentication / Authorization Description This vulnerability is detected if a JWT that lacks the "aud" claim is accepted by application. The "aud" claim specifies the application f which the JWT should be used. Missing "aud" means that API serve does not validate the intended audience of the JWT and that JWT r be repurposed. This is lack of compliance with best practice.				
Shared Objects 33 Al & ML 32 Public IP Addresses Alerts Management 33 Files 32 API Management 32 Reports 33	S items	Method	Sensitive Data ① Authen	Authenti	Created: 1:11 PM, May 7 Last Observed: 1:11 PM, May 7 Sensitive Data Found in JWT Toke None	Risk Score Attack impact: 10 (Low) Evidence <u>Review Evidence Detection</u> (2) Remadiation API server should implement the check of the JWT "aud" claim.				
	The second states of the second states of the second	GET	Email	Un-Aut	Greated: 1:11 PM, May 7 Last Observed: 1:11 PM, May 7 Query parameter contains sensiti • High					
Certificate Management >> Bot Defense Management >>	/workshop/api/shop/products	GET	Email	Authen:	Created: 4-12 PM, May 7 Last Observed: 4-12 PM, May 7					
 Notifications Alerts Audit Logs 	/workshop/api/mechanic/	GET	Email	Authen						
	/workshop/api/mechanic/service_requests	GET	Email	Authen						
	/workshop/api/shop/orders/all	GET	Email	Authen						

Demo

