

Identity Week | 2023

The complete platform for
API Security.



What?

Why?

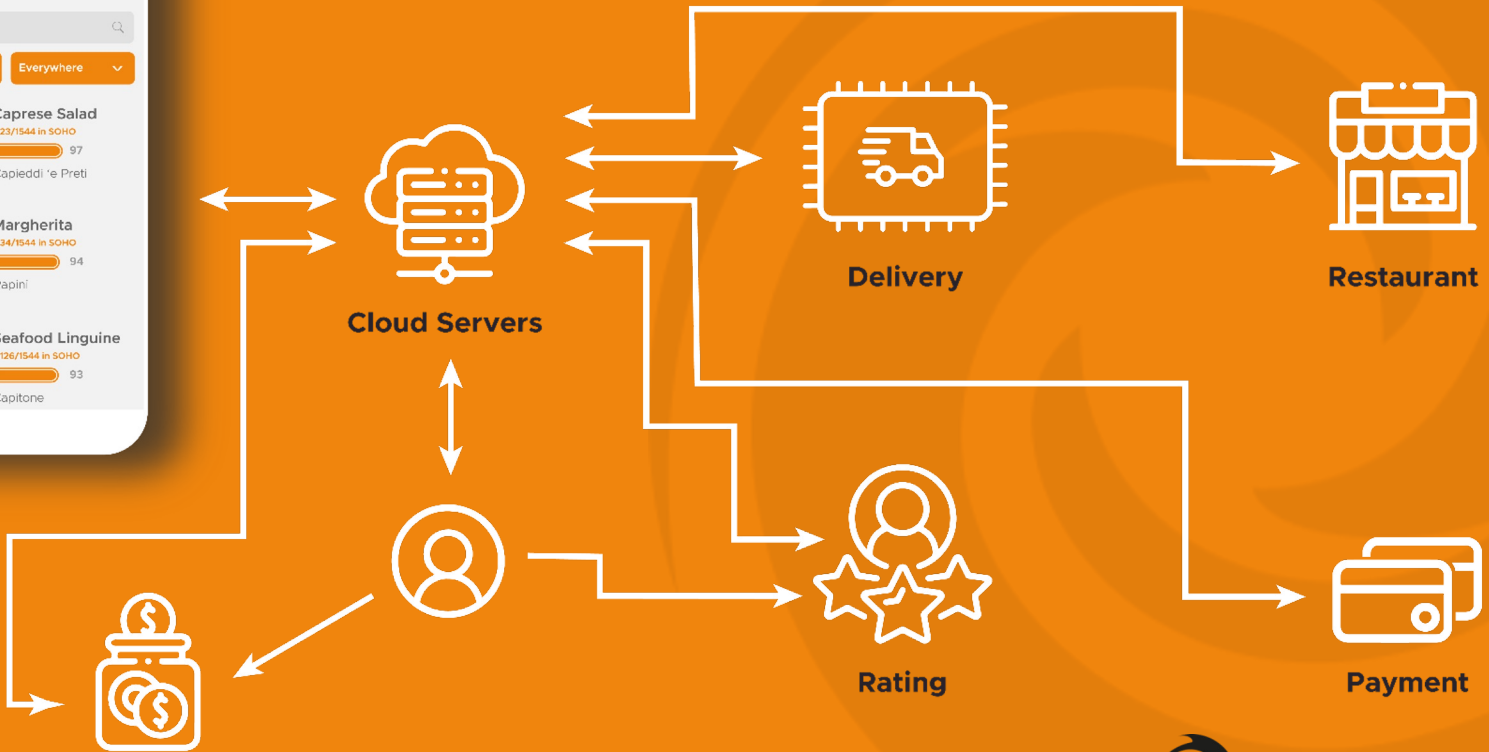
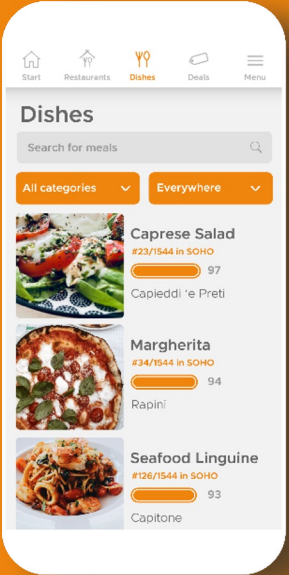
How?





83% of all web requests are API calls.

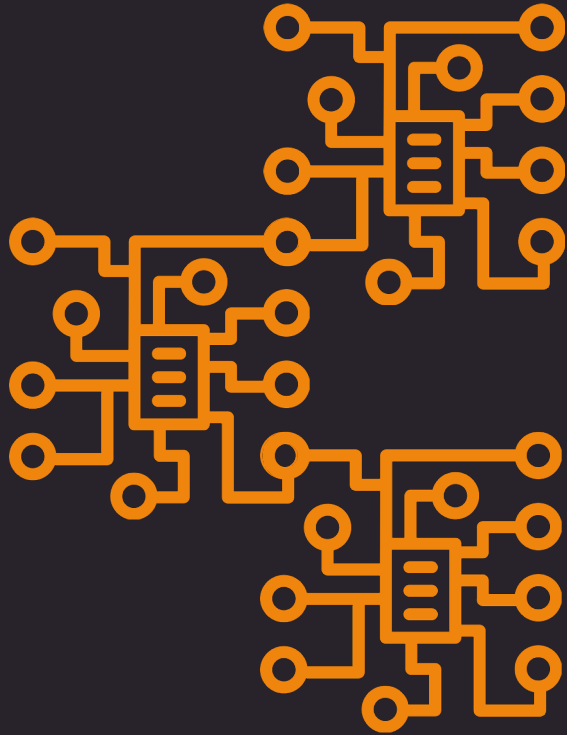
One order. Many API calls.



API Security

Urgent & Critical





Approaching
1 trillion
endpoints.

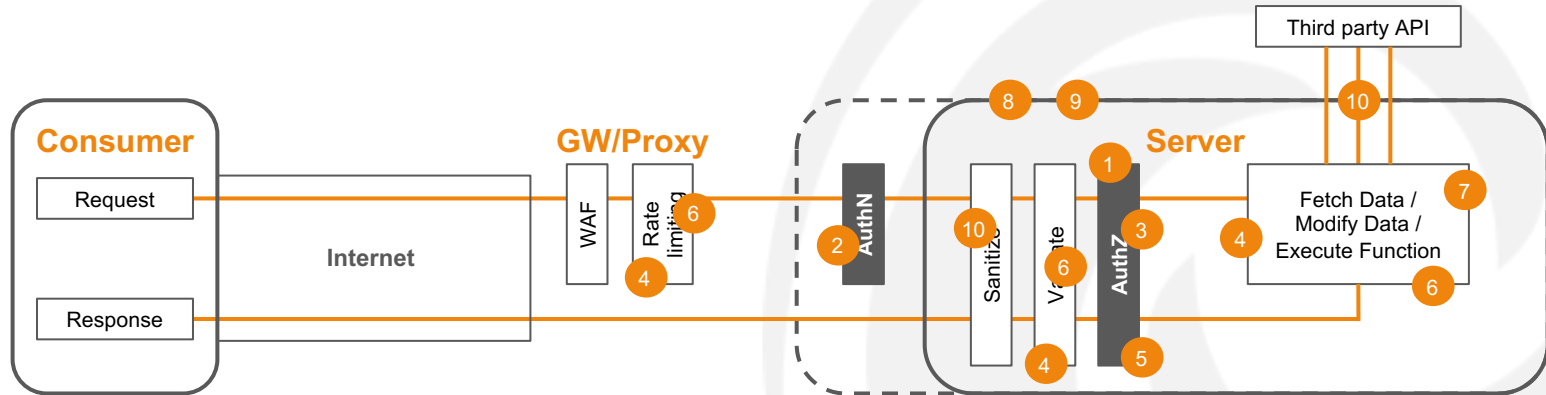
APIs are now
a leading
threat
vector.



**Traditional
security
doesn't work.**

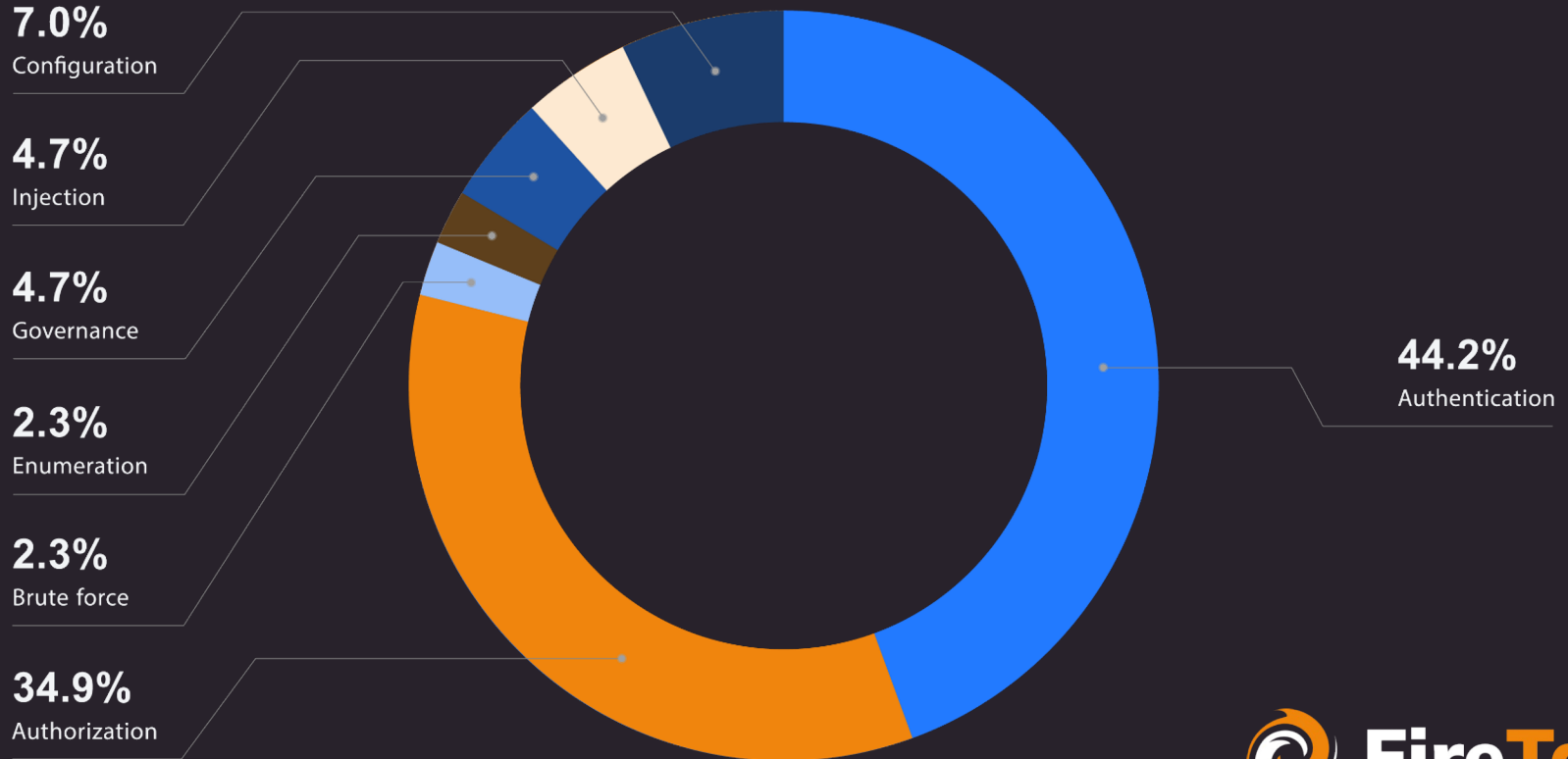


Breaches look like normal requests.



1. BOLA.
2. Broken AuthN.
3. BOPLA.
4. Unrestricted Resource Consumption.
5. BFLA.
6. Unrestricted Process Access.
7. SSRF.
8. Misconfiguration.
9. Improper Inventory Management.
10. Unsafe consumption of APIs.

Breach Events by Primary Attack Vector.





It's time
for a new
approach.





Bridging the
gap between
application &
security teams.





**Open source
code library**



**SaaS cloud
platform**

End-to-End API Security.



Discovery.

Finding APIs not running FireTail library via network traffic, code repos & cloud APIs



Visibility.

Get a complete view of your entire API landscape across your IT fleet.



Observability.

Commercial version sends configuration and success / failure events to cloud backend.



Policy.

APIs analyzed for configuration settings & security policy. API security posture management.



Enforcement.

Authentication, authorization, validation and sanitization directly in your code.



Audit.

Full & centralized audit trail of all APIs with FireTail library. Search & alert capabilities.

Overview.



Dashboard

1 Total Apps 12 Total APIs 11 API Endpoints 81 Detected PII 726K Requests

Requests + Add filter group

Polling interval: 30m Duration selector: Last 3 months

API requests grouped by apps



API requests grouped by location



API requests grouped by status code



Integrations

[Create integration](#)
[Existing integrations](#)
[All](#)
[Discovery](#)
[Code Libraries](#)
[Notification](#)
[Logging](#)

AWS API Inventory Scanning

This integration allows you to scan for API resources to populate them into FireTails SaaS platform.



AZURE API Inventory Scanning

This integration allows you to scan for API resources in Azure Cloud to populate them into FireTails SaaS platform.



Firetail Python Library

Get started with setting up the Python library.



Slack Webhook

Set up a Slack notification.



Lambda Function

Set up a Lambda integration.



Jira Issue

Set up a Jira integration.



HTTP Webhook (HMAC Signed)

Set up an HTTP notification.



Set up Firetail API Gateway logging in an AWS Region with AWS Lambda

This integration sets up logging resources in an AWS account region.



Set up Firetail API Gateway logging in an AWS Region with Kinesis

This integration sets up logging resources in an AWS account region.

Firetail Go Library

Get started with the Go library.



Firetail Node.js Library

Get started with the Node.js library.












Firetail Ruby Library

Get started with the Ruby Library.



Create API

Grid List

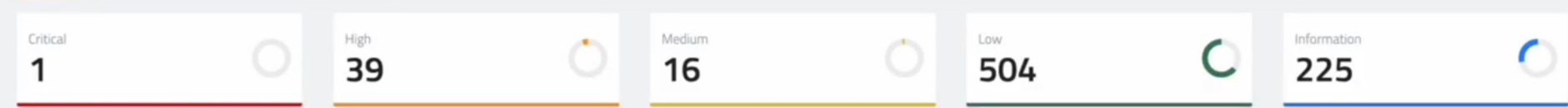
Source	Name	Created	Resources				
	acme-pre-prod-api	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	log ingest api	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	Sales-API-Gateway	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	saas-platform-api	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	Users API	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	dev-api-1	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	invoicing-api	22 minutes ago	Requests	Tokens	Logging	Collections	Settings
	collections	6 days ago	Requests	Tokens	Collections	Settings	
	bad-api	8 days ago	Requests	Tokens	Collections	Settings	

View the
discovered
APIs



Posture Management

- Findings Incidents Incidents Policy Events



Search findings Filters Grid List

Missing global security, Legacy integer limit, Missing rate limit headers, Unrestricted string

Undefined string limit, Legacy integer limit, Unrestricted string, Undefined integer format

Missing additional properties, Missing rate limit headers, Credentials in URL, Unrestricted string



Rule Severity: High

Ensure that security credentials are excluded from paths and query parameters.

This rule applies at the API Specification level (OAS/Swagger).

URL parameters should not include sensitive information such as API keys, passwords, or secrets.

1. How to Identify with Example Scenario

Find the text in bold to identify issues such as these in API specifications

```
paths:  
  /mypath/{id}/: # arbitrary path name  
  get:  
    description: 'get'  
    parameters:  
      - name: client_secret  
        in: query  
        required: true  
      - name: token  
      .
```



Collections

- + Demo Collection
 - VAmpI
 - GET Creates and populates the dat...
 - GET VAmpI home
 - GET Retrieves user by username
 - GET Retrieves all users
 - GET Retrieves all details for all user...
 - GET Retrieves all books
 - POST Register new user
 - Register new admin user (ex...
 - POST Login to VAmpI
 - Login to VAmpI (wrong pass ...
 - Login to VAmpI (wrong user ...
 - POST Add new book
 - GET Retrieves book by title along w...
 - PUT Update users email
 - PUT Update users password
 - DEL Deletes user by username (Onl...

VAmpI / Retrieves all users

GET `{{baseUrl}}/users/v1` Send

Params Authorization Headers (7) Body Pre-request Script Tests Settings Cookies

Query Params

Key	Value	Description
Key	Value	Description








Body Cookies Headers (5) Test Results (1/1)

Pretty Raw Preview Visualize JSON

```
1  [2024]
2  "users": [
3    {
4      "email": "mail1@mail.com",
5      "username": "name1"
6    },
7    {
8      "email": "mail2@mail.com",
9      "username": "name2"
10   },
11   {
12     "email": "admin@mail.com",
13     "username": "admin"
14   }
15 ]
16 [2024]
```

Checks, validates and enforces against API calls that lack proper authentication and authorization!

Logs

Status	Method	Date Created	Source	Domain	Path	Tags	Action
 200	GET	a few seconds ago		192.168.0.15:5009	/users/v1	Bot detected Request made from an internal IP address Missing referrer User agent is not a standard browser +3 tags	View details >
+ 200	GET	a few seconds ago		192.168.0.15:5009	/createdb	Bot detected Request made from an internal IP address Missing referrer User agent is not a standard browser +2 tags	View details >
+ 200	GET	6 minutes ago		192.168.0.15:5009	/createdb	Bot detected Request made from an internal IP address Missing referrer User agent is not a standard browser +2 tags	View details >
+ 400	POST	7 minutes ago		192.168.0.15:5009	/users/v1/register	Bad request Bad authentication request Bot detected Request made from an internal IP address +4 tags	View details >
+ 400	POST	4 days ago		192.168.0.15:5009	/users/v1/register	Bad request Bad authentication request Bot detected Request made from an internal IP address +4 tags	View details >
+ 200	POST	4 days ago		192.168.0.15:5009	/users/v1/register	Bot detected Request made from an internal IP address Missing referrer User agent is not a standard browser +3 tags	View details >



Come talk to us!

Startup City Area. Stand S51

- **Talk to us about the connection between identity and APIs!**
- **Get a demo.**
- **Ask us anything.**



Thanks

