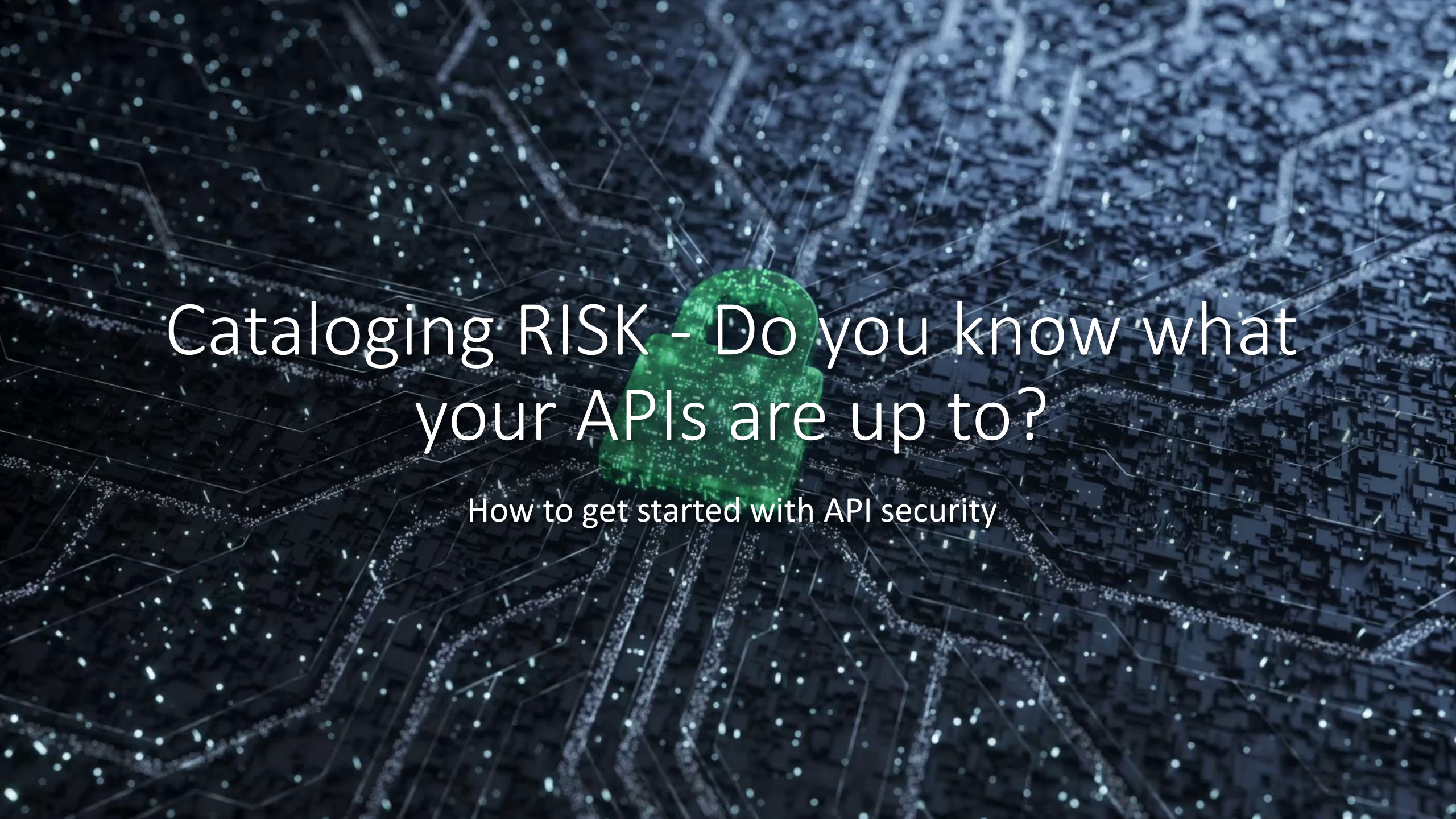


Cataloging RISK - Do you know what your APIs are up to?

How to get started with API security

Speakers

Chris Dale

- Principal SANS Instructor
- Co-Founder and Principal Consultant at River Security
  - Penetration Testing
  - Incident Response

Amod Gupta

- Product Manager at Traceable
- Previously software engineering

API Terminology 101

API – Application Programming Interface

OpenAPI – describe API's so they can be parsed and understood

REST – Common lightweight way to represent API's

SOAP – XML based type and definition language for API's

JSON-RPC – JSON based Remote Procedure Calls

XML-RPC – XML based Remote Procedure Calls

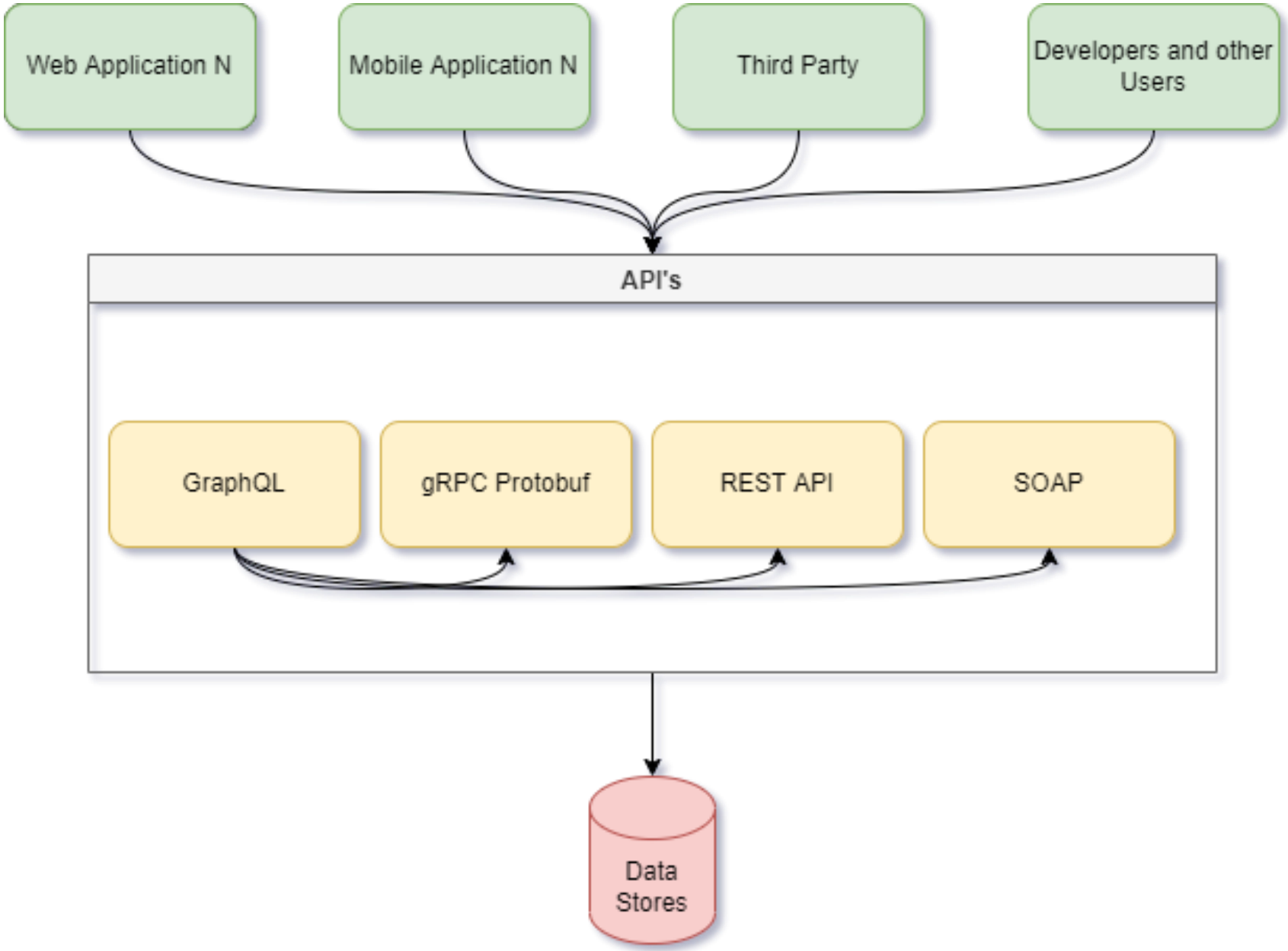
gRPC – open-source RPC from Google using protobuf

GraphQL – API stitching, query language for your other API's

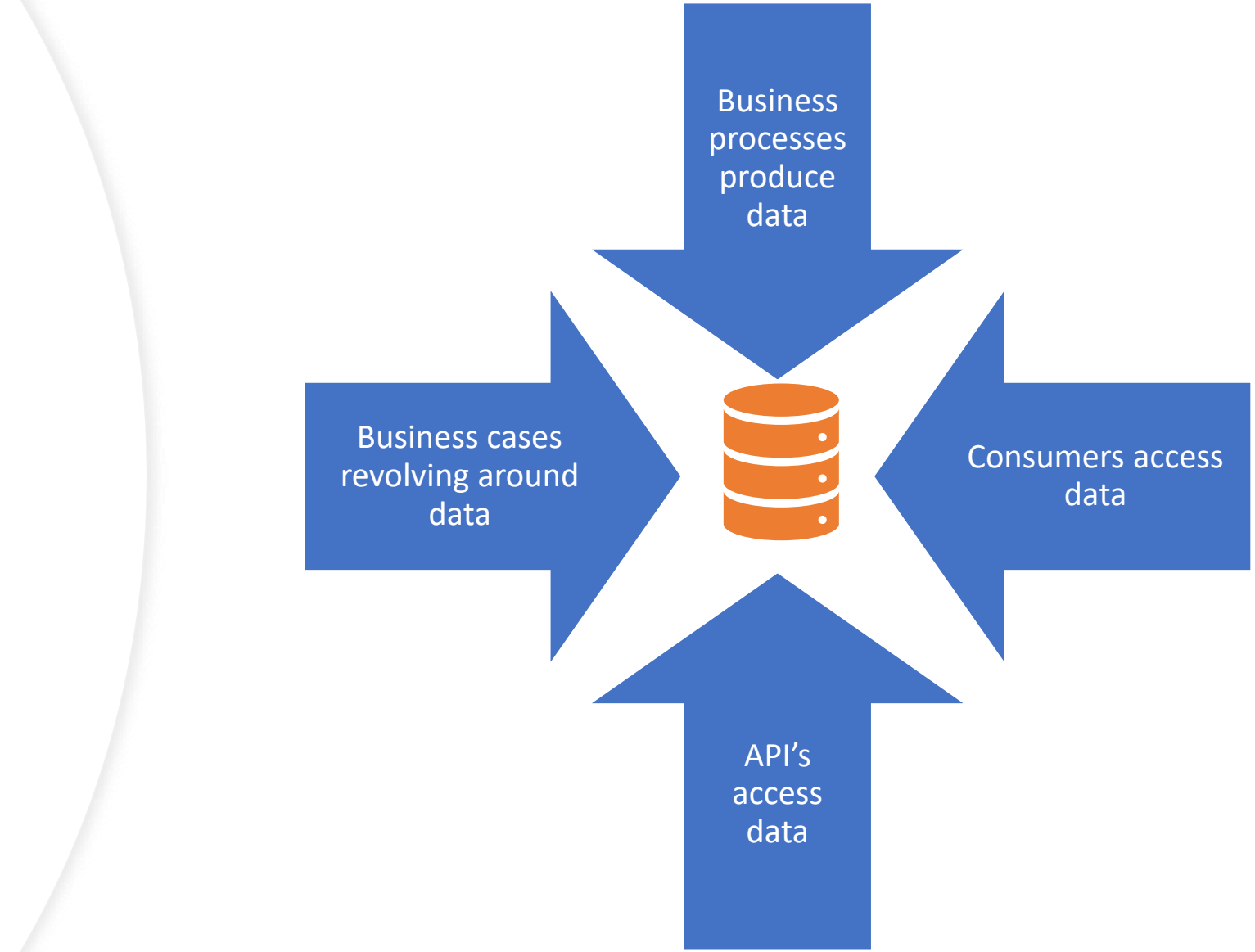
Most Likely You Are Building API's

- You don't normally build a single application
  - First, you build an API which interacts with data
  - Second, you build a client which uses the API
- The client, often a web- or mobile-application, is what your users' access
- By having the API, you can design more clients rather easily
  - Instead of building monolith applications, you can diversify applications
- Customers might be using and building their own client applications
  - As such, connecting to an API is essential

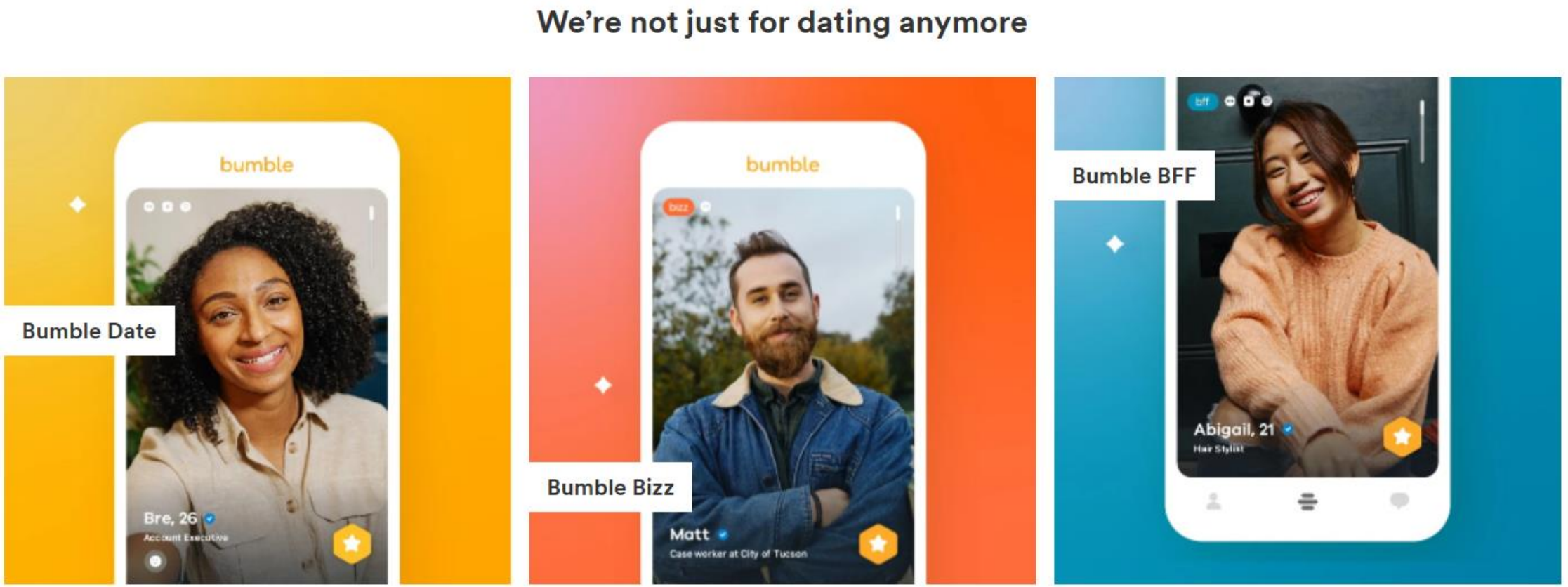
An Example Typical Architecture



Many Companies are Data Driven

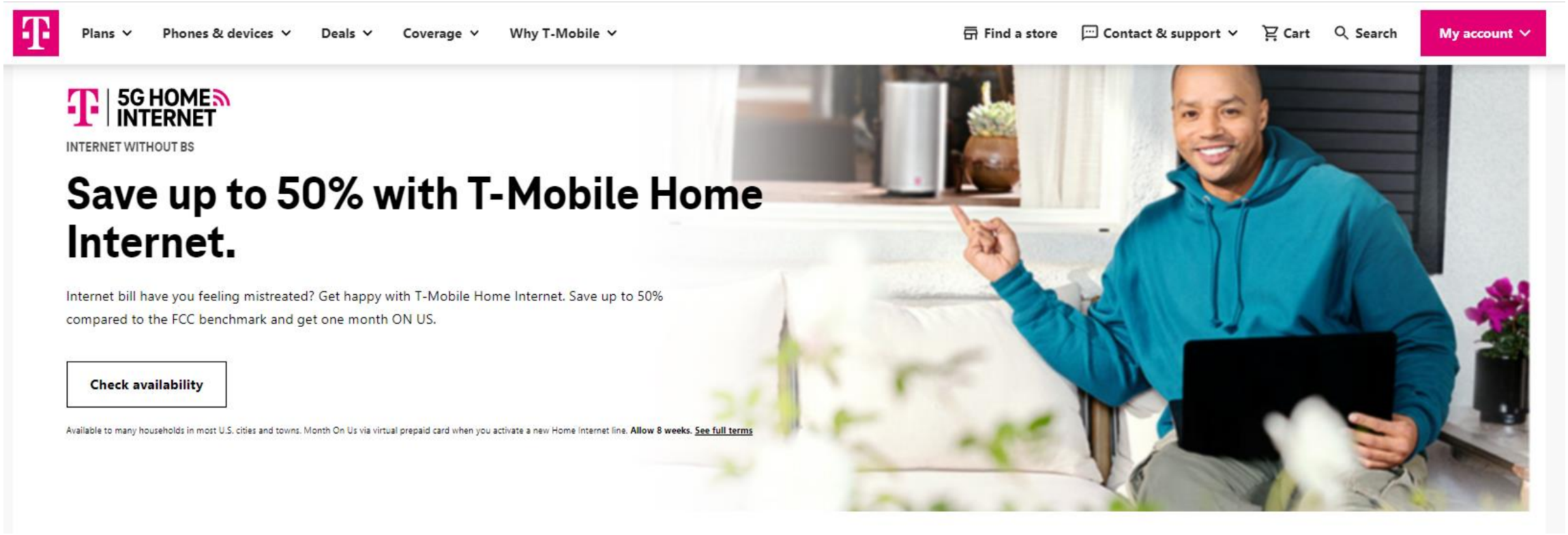


Bumble: Finding Honey in the API



Source: https://blog.securityevaluators.com/reverse-engineering-bumbles-api-a2a0d39b3a87

T-Mobile: 2021 – Yet Another Data Breach



Current Status Quo

- Checklists exists for developers to follow
  - But are they being verified ?
- Anyone could code and deploy today
  - But there is a tremendous skill gap
  - Reliance on frameworks and libraries to “add security”.
- Privacy regulations exists which could cause huge fines
- DevOps pressured to deliver faster
  - Do less with more.
- It takes time to keep DevOps up to date with current practices and DevSecOps
- OWASP API Security Top 10

OWAPS API Security Top 10 - 2019

- Broken Object Level Authorization
- Broken User Authentication
- Excessive Data Exposure
- Lack of Resources & Rate Limiting
- Broken Function Level Authorization
- Mass Assignment
- Security Misconfiguration
- Injection
- Improper Assets Management
- Insufficient Logging & Monitoring

Experience from Penetration Testing

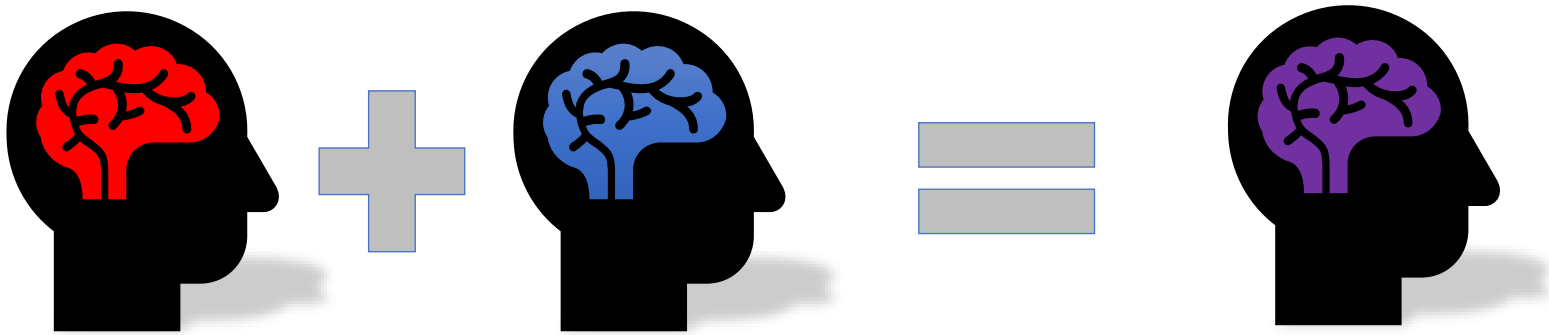
- API's are often a gold mine
- Mobile applications often turn into API testing
- A lot of Broken Access Control issues
- Lack of tenant segregation
- Undocumented features
- API's often behind authentication, but applications allow self-registration
  - Or credential stuffing provides access
- Lack of monitoring (blind spot)
- Excessive Data Exposure

Testing API Security

- Most web-application scanners will be able to process OpenAPI definitions and scan based on it
  - OWASP ZAP, free open-source
- Consider implementing scanning as part of CI/CD pipelines
- Which API endpoints are accessible without authentication?
  - What about differences in access levels on authentication tokens?
- Segregation between data/tenants
- Vulnerabilities like XSS are less interesting
- Use the OWASP API Security Top 10 to guide

Old Fashioned Security Measures Are Too Slow

- A penetration test “once a year” just doesn’t cut it anymore
- Blue and Red must strive to merge to Purple
  - Red Team should be informed by Blue Team when there is changes
  - Blue Team should be informed by Red Team when there is risk
- Releases could/should happen continuously
- Innovation should not be hindered



Target Goals for Organizations

- CI/CD processes which allows Red to test API's as they change
- CI/CD processes which allows Blue to automatically monitor API's for abuse
- Rapid Development Workflows which helps Compliance and Security
- Faster remediation of problems, before Threat Actors can exploit
- Asset inventory – What API's do we have and what data do they expose?

GOAL

- Define API Discovery in the context of API Security
- Minimum set of discovery features that make API Security tools actionable

What makes **API discovery** challenging

Deployment Options

- Public cloud
- On-premises
- Hybrid

Distributed

Microservices architecture has made applications massively distributed

Agile releases

Dev teams are releasing multiple times a week

API discovery tool should…

- **Automatically discover all API endpoints (by inspecting traffic)**
- **Group APIs by apps, services, domains etc. so security teams can digest the information**
- **Classify APIs as external (public), internal or 3rd party**
- **Automatically catalog new APIs and updates to existing APIs**

Now, that we have an API Catalog, how do we *make it actionable*

Open
API Specification

Without

Are APIs being consumed securely?

Are APIs being consumed as the developer intended?

Are APIs exposing unknown parameters, responses, content-types etc. ?

With

Common source of truth between different teams and partners

Portability between different security tools

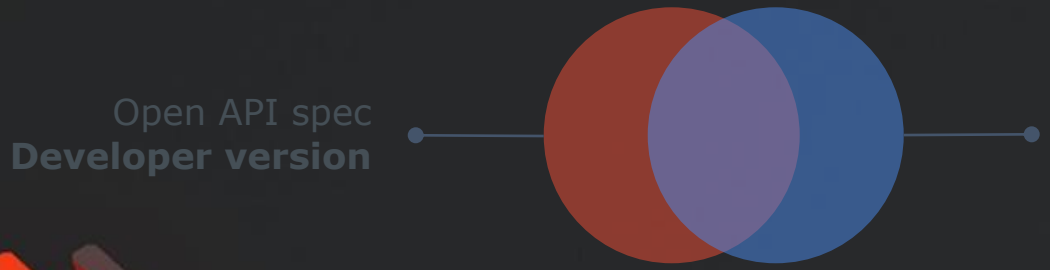
Easy to identify which APIs expose sensitive data and where

TRACEABLE.

Doing this at scale…

- We've cataloged all the API endpoints
- We have Open API specifications for them
- ? But how do we consume this when there are 1000s of endpoints?

CONFORMANCE ANALYSIS



- Missing APIs (Shadow APIs)
- Issues with parameters
- Issues with request/response bodies

TRACEABLE.

Sensitive data exposure

Catalog of Sensitive Data

SSN | email | age | aws_api_key

ip_address | gcp_api_key | TIN

credit_card_no | address | SIN

Integrated workflows

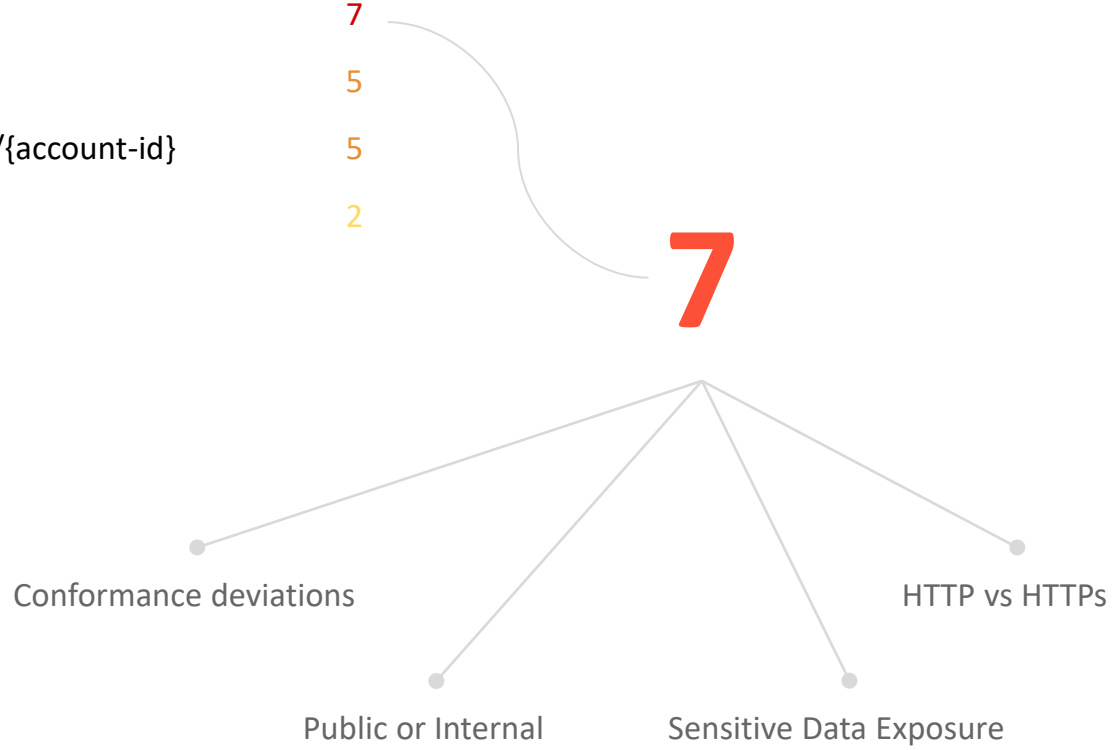
Detect
- New data exposure
- Policy violations

Log
- Create tickets
- Integrations

Track & Verify
- Pre-prod environments

Risk Score brings it together

API Endpoints	Risk Score
/juiceshop/getorder/{order-id}	8
/juiceshop/create-account	7
/juiceshop/order/checkout/	5
/juiceshop/account/getaccount/{account-id}	5
/juiceshop/order/notification/	2



Summary

API Catalog

Automatically create and keep up to date

Open API Spec

Automatically create and keep up to date

Conformance

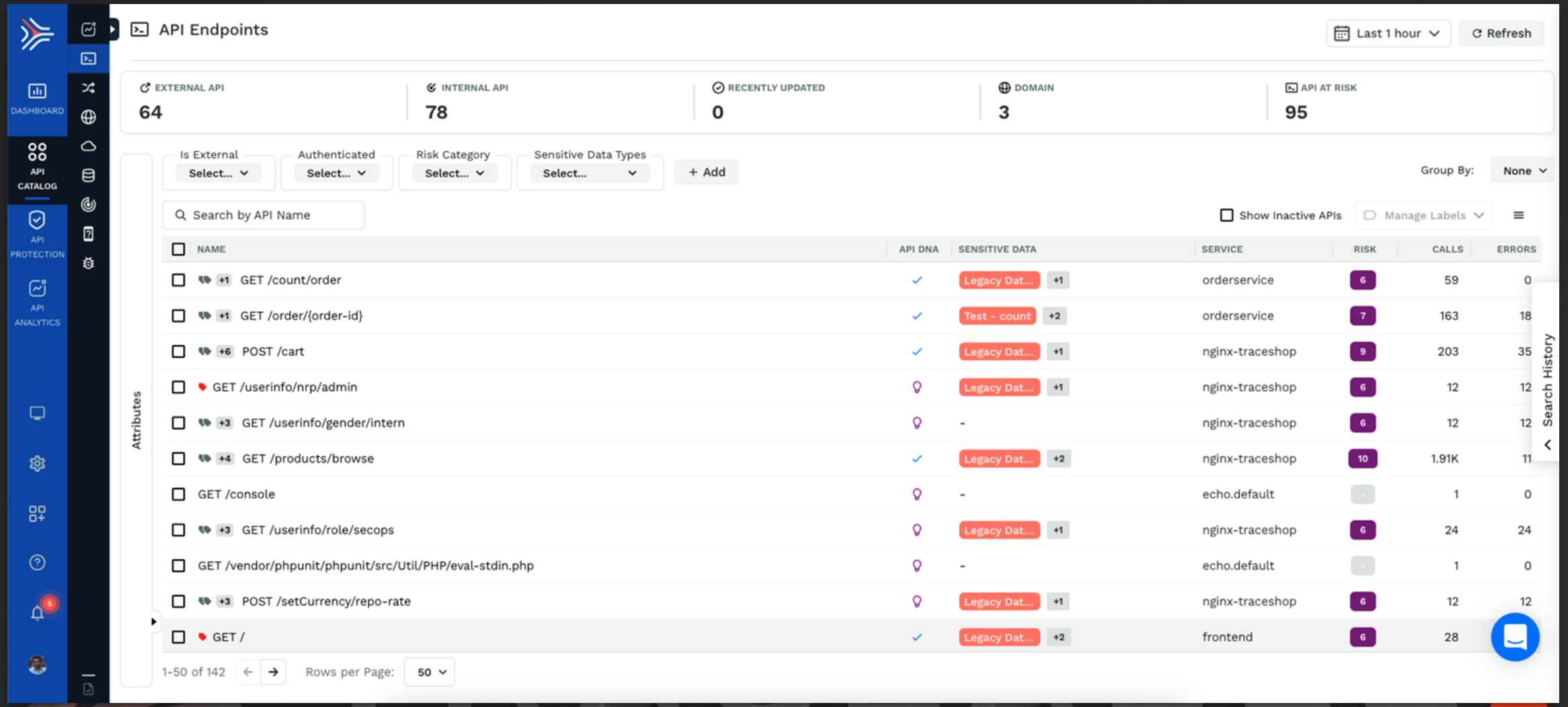
Identify the drift from expected behavior

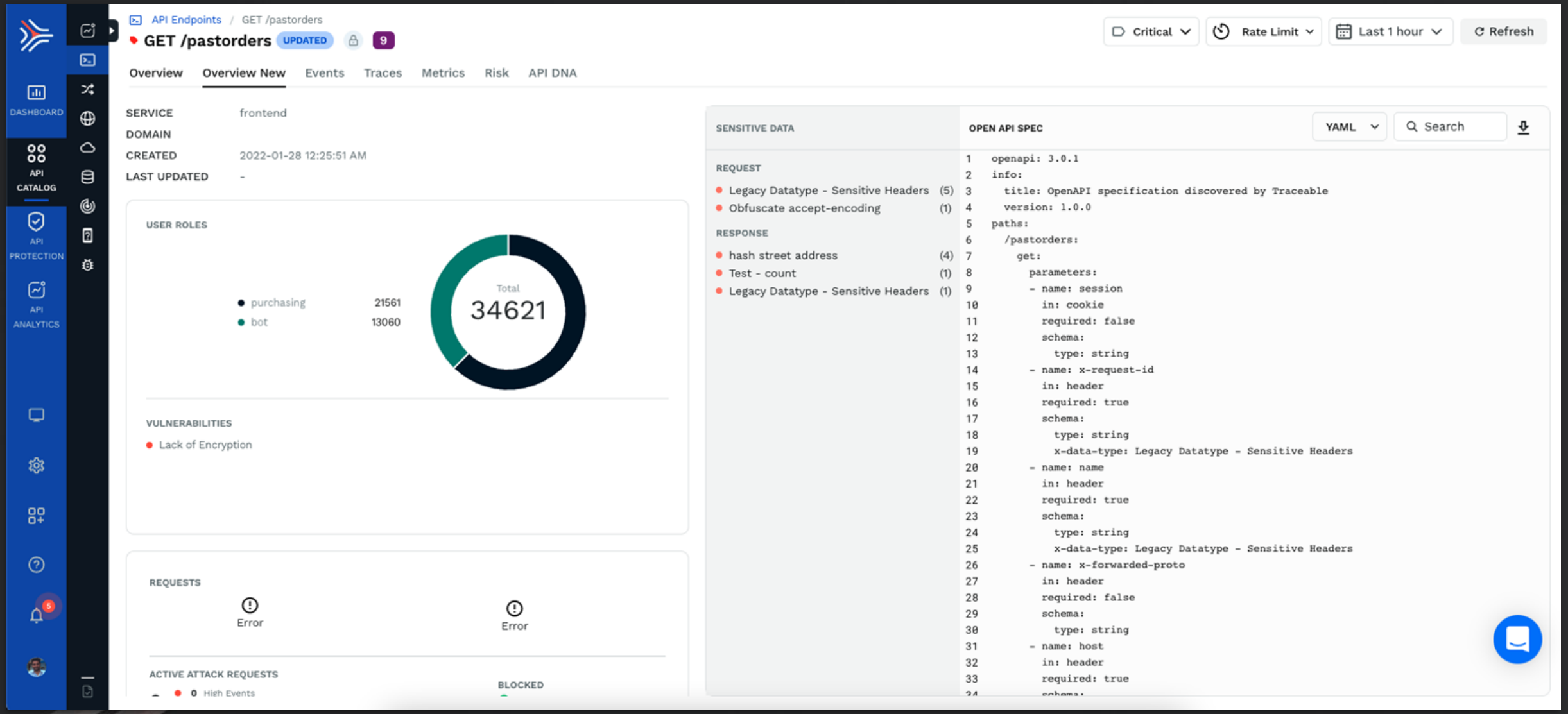
Sensitive Data

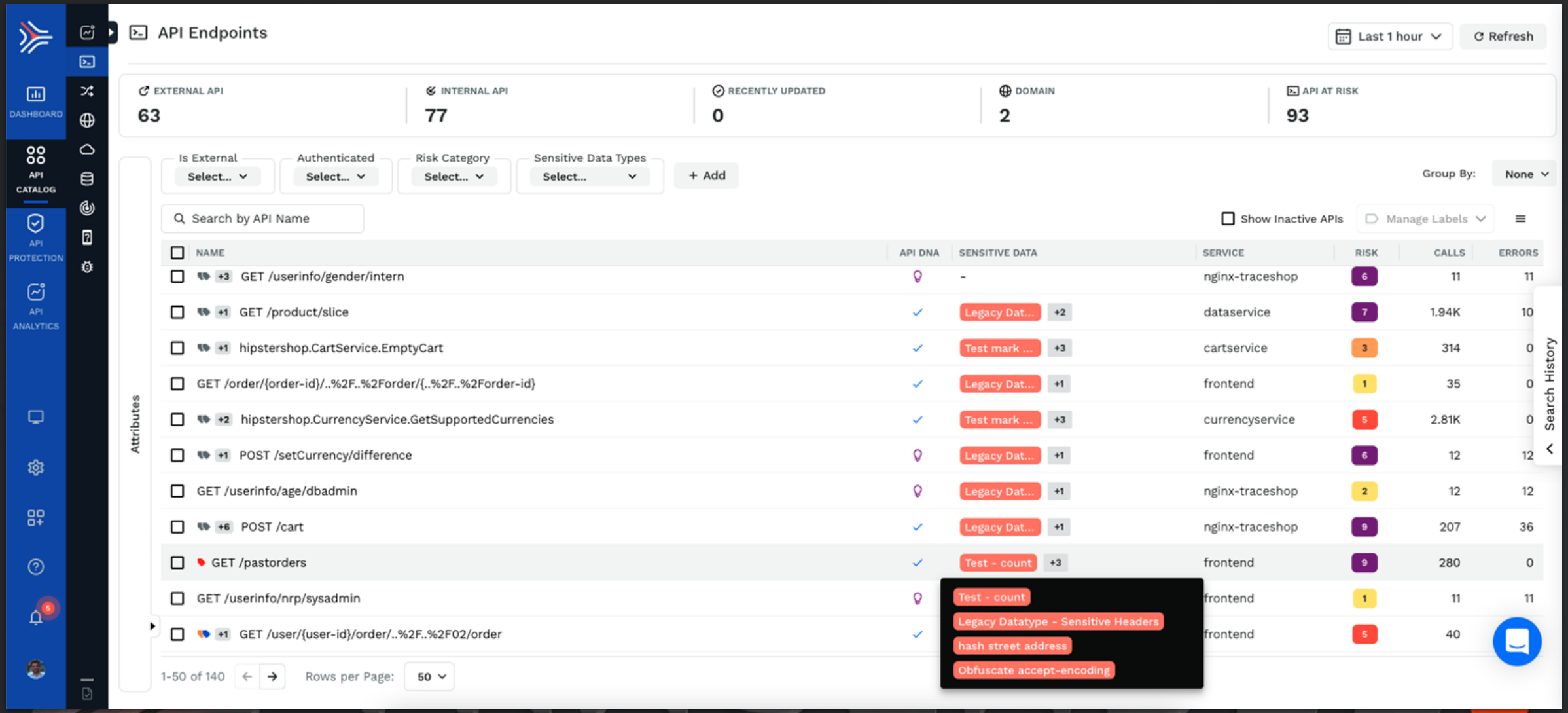
Integrated score to identify APIs that need attention

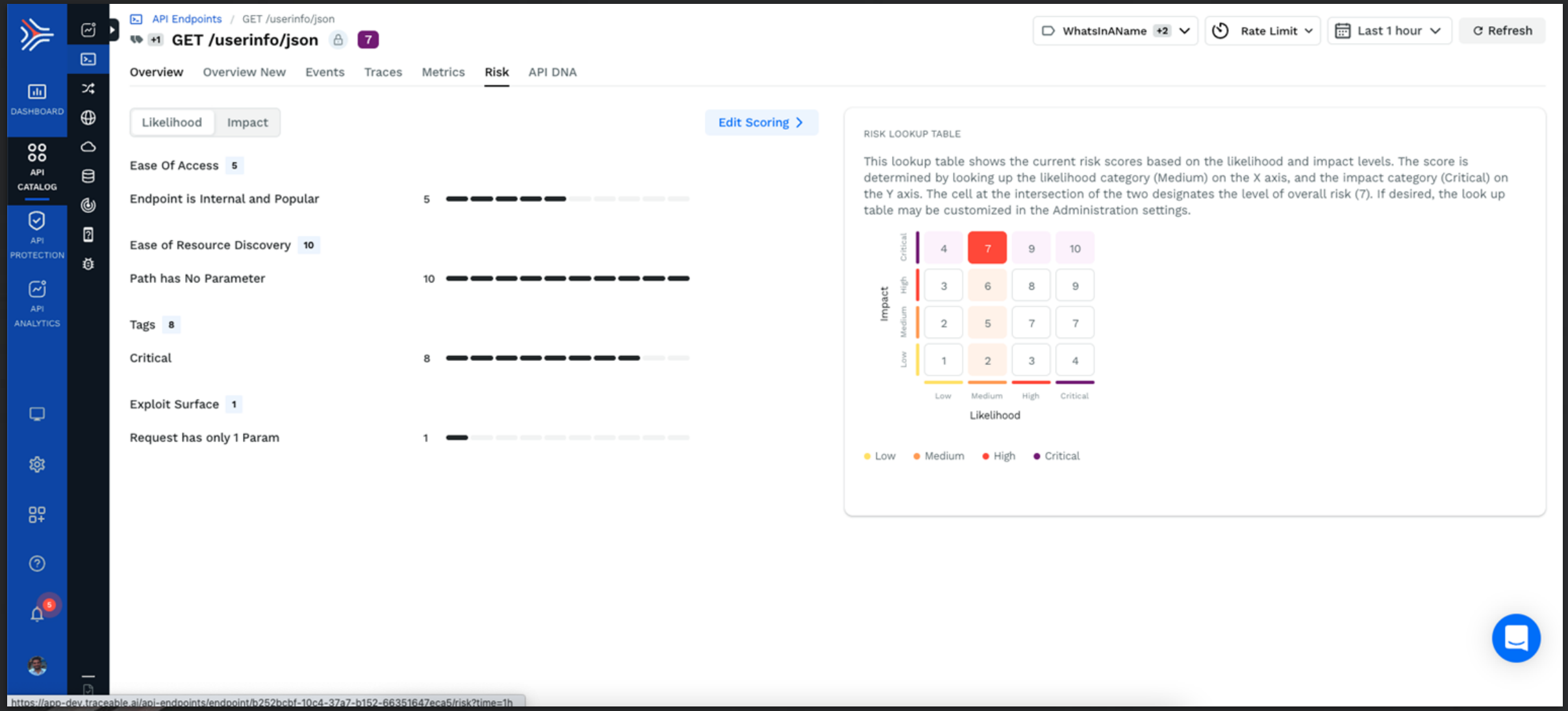
Risk Score

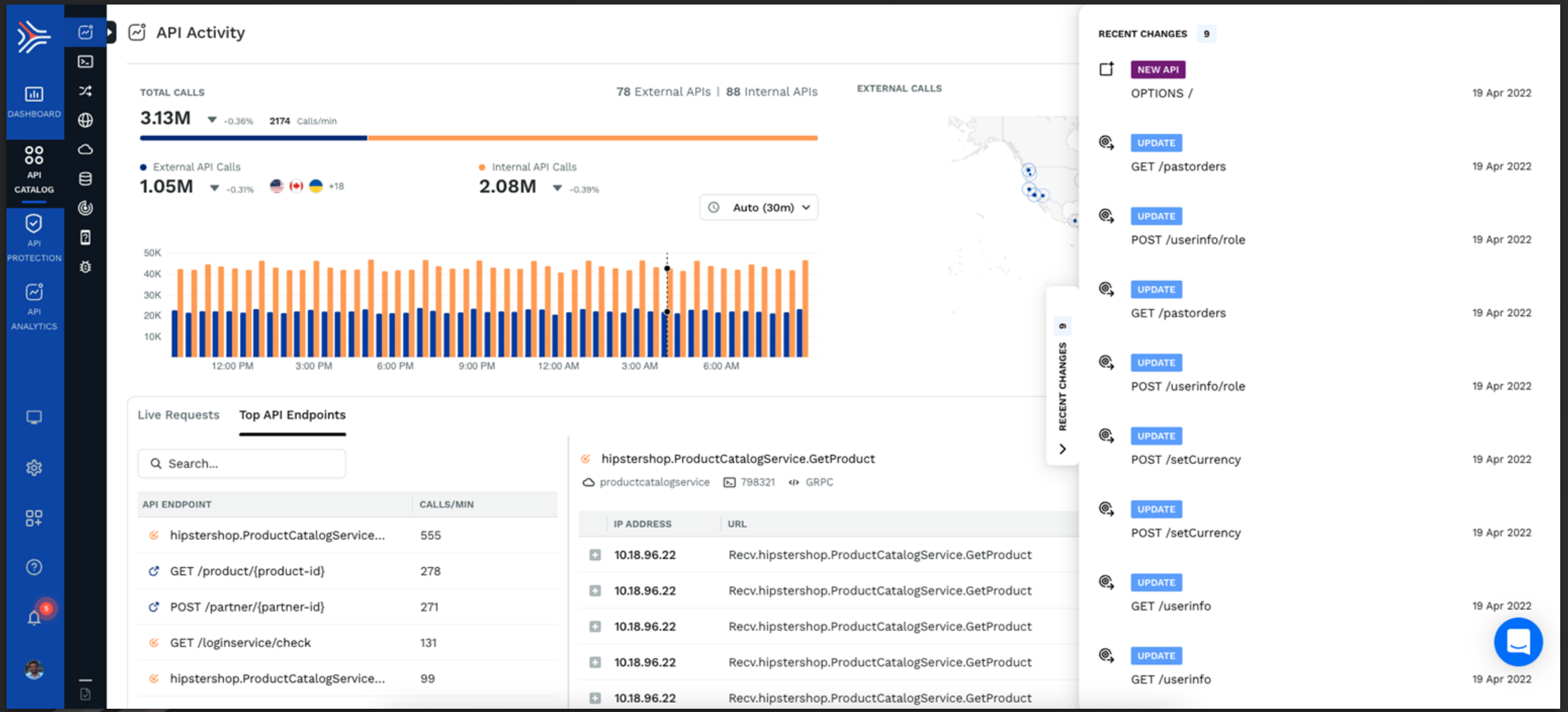
Integrated score to identify APIs that need attention


DASHBOARD
API CATALOG
API PROTECTION
API ANALYTICS
API Endpoints
Last 1 hour
Refresh
EXTERNAL API
64
INTERNAL API
78
RECENTLY UPDATED
0
DOMAIN
3
API AT RISK
95
Is External
Select...
Authenticated
Select...
Risk Category
Select...
Sensitive Data Types
Select...
+ Add
Group By:
None
Search by API Name
Show Inactive APIs
Manage Labels
Attributes
Search History
NAME
API DNA
SENSITIVE DATA
SERVICE
RISK
CALLS
ERRORS
+1 GET /count/order
Legacy Dat... +1
orderservice
6
59
0
+1 GET /order/{order-id}
Test - count +2
orderservice
7
163
18
+6 POST /cart
Legacy Dat... +1
nginx-traceshop
9
203
35
GET /userinfo/nrp/admin
Legacy Dat... +1
nginx-traceshop
6
12
12
+3 GET /userinfo/gender/intern
-
nginx-traceshop
6
12
12
+4 GET /products/browse
Legacy Dat... +2
nginx-traceshop
10
1.91K
11
GET /console
-
echo.default
1
0
+3 GET /userinfo/role/secops
Legacy Dat... +1
nginx-traceshop
6
24
24
GET /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
-
echo.default
1
0
+3 POST /setCurrency/repo-rate
Legacy Dat... +1
nginx-traceshop
6
12
12
GET /
Legacy Dat... +2
frontend
6
28
1-50 of 142
Rows per Page:
50


DASHBOARD
API CATALOG
API PROTECTION
API ANALYTICS
API Endpoints / GET /pastorders
GET /pastorders
UPDATED
9
Critical
Rate Limit
Last 1 hour
Refresh
Overview
Overview New
Events
Traces
Metrics
Risk
API DNA
SERVICE frontend
DOMAIN
CREATED 2022-01-28 12:25:51 AM
LAST UPDATED -
USER ROLES
purchasing 21561
bot 13060
Total
34621
VULNERABILITIES
Lack of Encryption
REQUESTS
Error
Error
ACTIVE ATTACK REQUESTS
0 High Events
BLOCKED
SENSITIVE DATA
REQUEST
Legacy Datatype - Sensitive Headers (5)
Obfuscate accept-encoding (1)
RESPONSE
hash street address (4)
Test - count (1)
Legacy Datatype - Sensitive Headers (1)
OPEN API SPEC
YAML
Search
1 openapi: 3.0.1
2 info:
3 title: OpenAPI specification discovered by Traceable
4 version: 1.0.0
5 paths:
6 /pastorders:
7 get:
8 parameters:
9 - name: session
10 in: cookie
11 required: false
12 schema:
13 type: string
14 - name: x-request-id
15 in: header
16 required: true
17 schema:
18 type: string
19 x-data-type: Legacy Datatype - Sensitive Headers
20 - name: name
21 in: header
22 required: true
23 schema:
24 type: string
25 x-data-type: Legacy Datatype - Sensitive Headers
26 - name: x-forwarded-proto
27 in: header
28 required: false
29 schema:
30 type: string
31 - name: host
32 in: header
33 required: true


DASHBOARD
API CATALOG
API PROTECTION
API ANALYTICS
API Endpoints
Last 1 hour
Refresh
EXTERNAL API
63
INTERNAL API
77
RECENTLY UPDATED
0
DOMAIN
2
API AT RISK
93
Is External
Select...
Authenticated
Select...
Risk Category
Select...
Sensitive Data Types
Select...
+ Add
Group By:
None
Search by API Name
Show Inactive APIs
Manage Labels
Attributes
Search History
NAME
API DNA
SENSITIVE DATA
SERVICE
RISK
CALLS
ERRORS
+3 GET /userinfo/gender/intern - nginx-traceshop 6 11 11
+1 GET /product/slice Legacy Dat... +2 dataservice 7 1.94K 10
+1 hipstershop.CartService.EmptyCart Test mark ... +3 cartservice 3 314 0
GET /order/{order-id}/..%2F..%2Forder/{..%2F..%2Forder-id} Legacy Dat... +1 frontend 1 35 0
+2 hipstershop.CurrencyService.GetSupportedCurrencies Test mark ... +3 currencyservice 5 2.81K 0
+1 POST /setCurrency/difference Legacy Dat... +1 frontend 6 12 12
GET /userinfo/age/dbadmin Legacy Dat... +1 nginx-traceshop 2 12 12
+6 POST /cart Legacy Dat... +1 nginx-traceshop 9 207 36
GET /pastorders Test - count +3 frontend 9 280 0
GET /userinfo/nrp/sysadmin frontend 1 11 11
+1 GET /user/{user-id}/order/..%2F..%2F02/order frontend 5 40
Test - count
Legacy Datatype - Sensitive Headers
hash street address
Obfuscate accept-encoding
1-50 of 140
Rows per Page:
50


API Endpoints / GET /userinfo/json
+1 GET /userinfo/json 7
WhatsInAName +2
Rate Limit
Last 1 hour
Refresh
Overview
Overview New
Events
Traces
Metrics
Risk
API DNA
DASHBOARD
API CATALOG
API PROTECTION
API ANALYTICS
Likelihood
Impact
Edit Scoring
Ease Of Access 5
Endpoint is Internal and Popular 5
Ease of Resource Discovery 10
Path has No Parameter 10
Tags 8
Critical 8
Exploit Surface 1
Request has only 1 Param 1
RISK LOOKUP TABLE
This lookup table shows the current risk scores based on the likelihood and impact levels. The score is determined by looking up the likelihood category (Medium) on the X axis, and the impact category (Critical) on the Y axis. The cell at the intersection of the two designates the level of overall risk (7). If desired, the look up table may be customized in the Administration settings.
Impact
Critical 4 7 9 10
High 3 6 8 9
Medium 2 5 7 7
Low 1 2 3 4
Low Medium High Critical
Likelihood
Low Medium High Critical


API Activity
DASHBOARD
API CATALOG
API PROTECTION
API ANALYTICS
TOTAL CALLS
3.13M -0.36% 2174 Calls/min
78 External APIs | 88 Internal APIs
External API Calls
1.05M -0.31% +18
Internal API Calls
2.08M -0.39%
Auto (30m)
50K
40K
30K
20K
10K
12:00 PM
3:00 PM
6:00 PM
9:00 PM
12:00 AM
3:00 AM
6:00 AM
EXTERNAL CALLS
RECENT CHANGES 9
NEW API OPTIONS / 19 Apr 2022
UPDATE GET /pastorders 19 Apr 2022
UPDATE POST /userinfo/role 19 Apr 2022
UPDATE GET /pastorders 19 Apr 2022
UPDATE POST /userinfo/role 19 Apr 2022
UPDATE POST /setCurrency 19 Apr 2022
UPDATE POST /setCurrency 19 Apr 2022
UPDATE GET /userinfo 19 Apr 2022
UPDATE GET /userinfo 19 Apr 2022
Live Requests
Top API Endpoints
Search...
API ENDPOINT
CALLS/MIN
hipstershop.ProductCatalogService... 555
GET /product/{product-id} 278
POST /partner/{partner-id} 271
GET /loginservice/check 131
hipstershop.ProductCatalogService... 99
hipstershop.ProductCatalogService.GetProduct
productcatalogservice 798321 GRPC
IP ADDRESS
URL
10.18.96.22 Recv.hipstershop.ProductCatalogService.GetProduct
10.18.96.22 Recv.hipstershop.ProductCatalogService.GetProduct
10.18.96.22 Recv.hipstershop.ProductCatalogService.GetProduct
10.18.96.22 Recv.hipstershop.ProductCatalogService.GetProduct
10.18.96.22 Recv.hipstershop.ProductCatalogService.GetProduct

Questions

THANK YOU