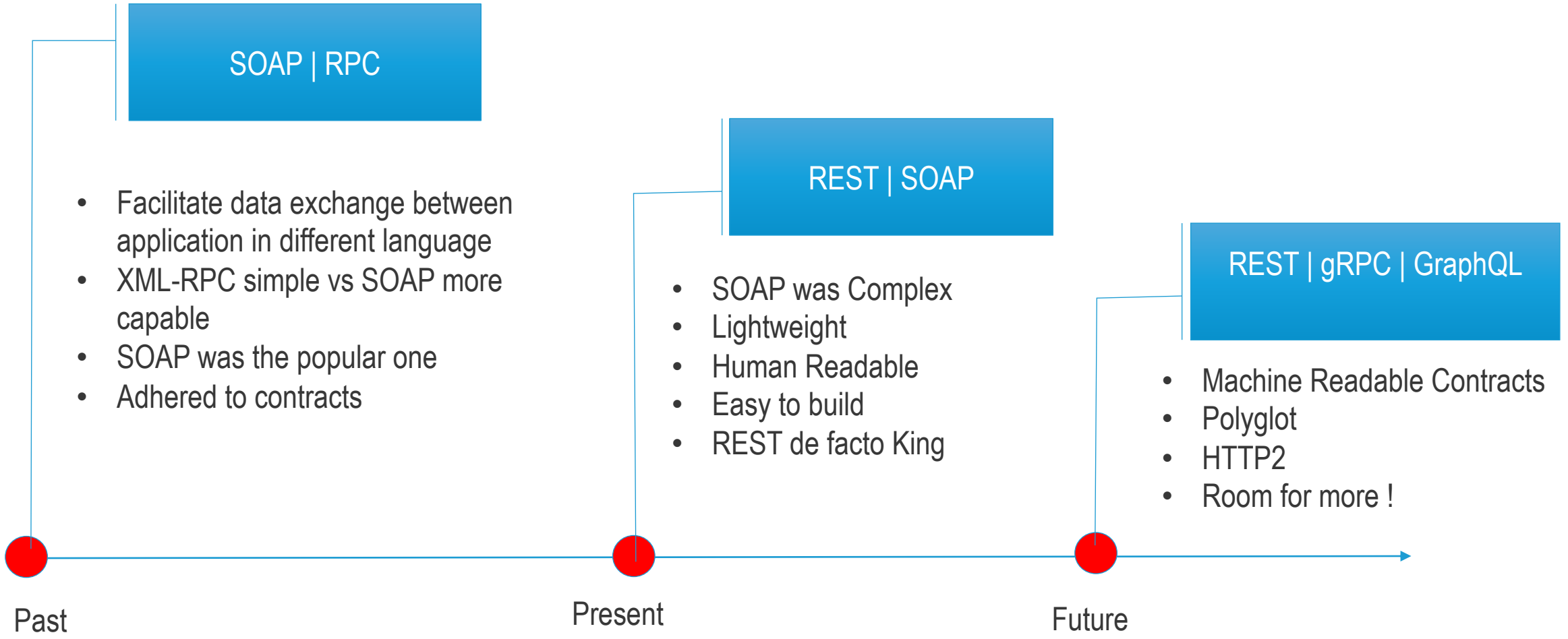
2021 Application Protection Report: Art of Securing Modern APIs

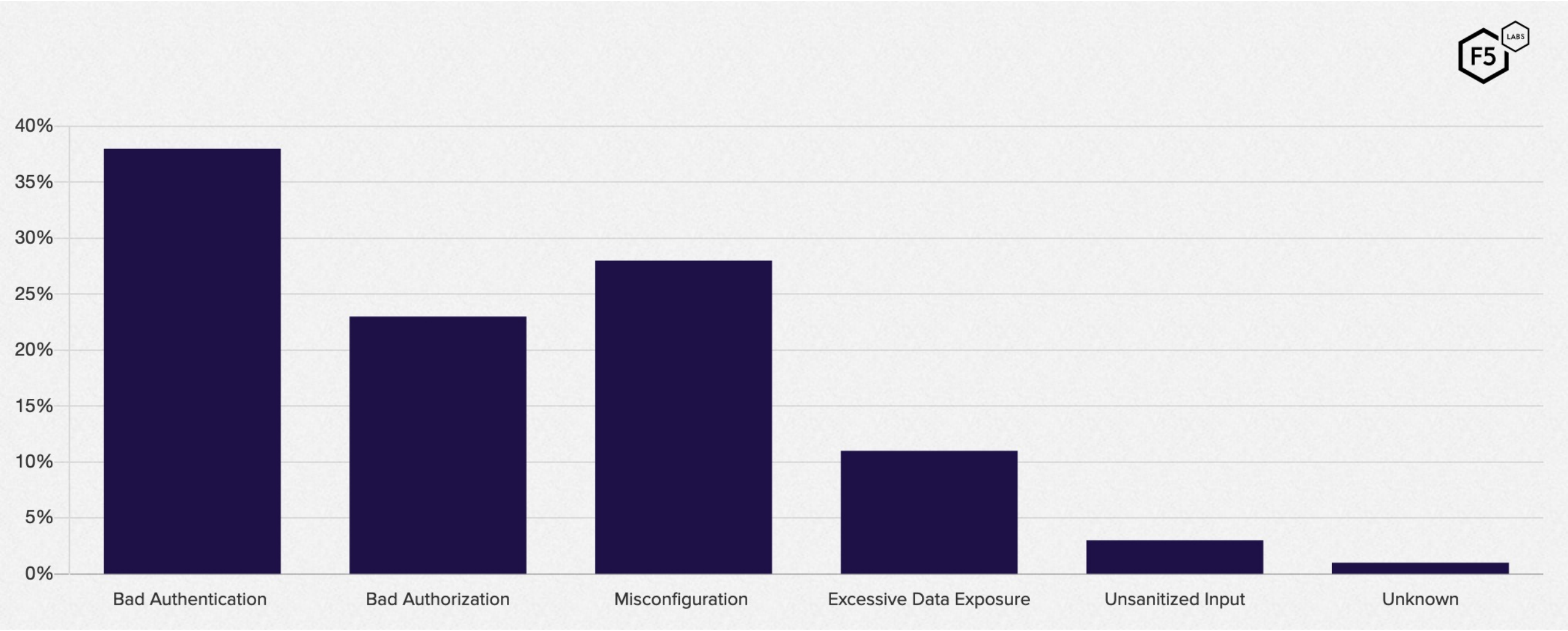
Shain Singh | Cloud/5G Security Architect | @shainsingh

Shahn Backer | Principal Security Advisor | @sbacker27

Brief History of API



Challenges With APIs – Breach Analysis 2020



Authentication & Authorization Challenges

- Unauthenticated Access
- API Keys Without Rotation
- Usage of Weak Tokens
- OAuth Implementation Challenges
- Guess Endpoints
- Exposing Internal APIs
- Brute Force and Credential Stuffing


How do you enumerate user login details?

API Request

Request

Pretty | Raw | \n | Actions

```
POST /graphql HTTP/1.1
Host: gql-graphql-gateway.prod.k8s.onepeloton.com
Content-Type: application/json
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Peloton-Platform: iOS_app
Content-Length: 222
X-APOLLO-OPERATION-TYPE: query
Peloton-Feature-Include-Tread: true
Connection: close
Cookie: peloton_session_id=x; path=/; domain=.pelotoncycle.com;

{"query":
"query SharedTags($currentUserID: ID!) {\n  User: user(id: $currentUserID) {\r\n
  __typename\n    id\r\n    username\r\n    location\r\n  }\r\n}","variables":{
"currentUserID":"REDACTED"}}
```

API Response (Sample)

```
{
  "data":{
    "User":{
      "__typename":"User",
      "id":"1[redacted]",
      "username":"No[redacted]",
      "location":"UK - Test"
    }
  }
}
```

Try an API endpoint and ASK!

REST Data Access

With REST we access ‘items’ with individual calls

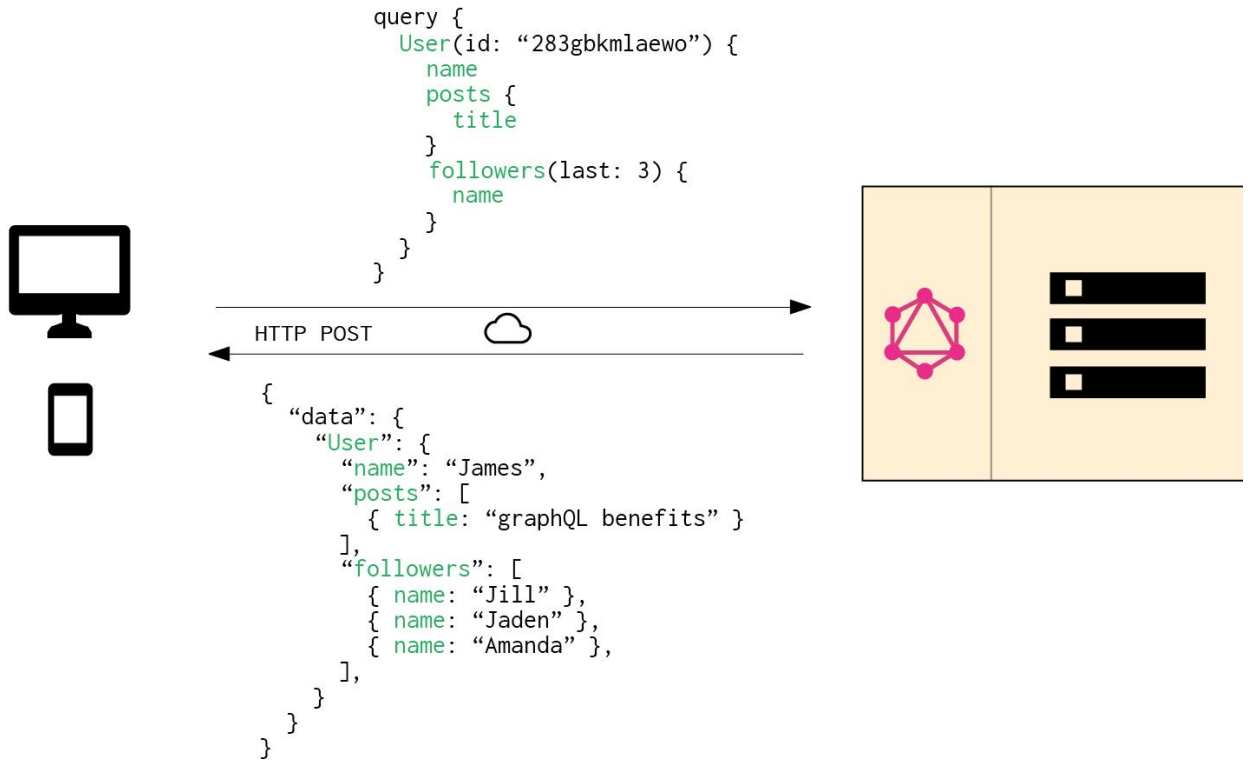
If we need to access ‘composite’ items, that needs to be built into a query or view

GraphQL Data Access

All elements are available to be called in a single query

Pagination is built into the query request

Introspection allows devs to probe the data model



Some challenges with APIs

JWT validations attacks

GraphQL

API Vulnerabilities Were Found in All Sectors

- Government
- Finance
- Technology Service Providers
- Entertainment
- Manufacturing
- Health
- Social Media

The Story of Fraud in API Ecosystem

WHEN SOMEONE IN THE ECOSYSTEM FALTERS

Attacker

```
{
    "action": "topup",
    "noAkun": "6281284147433",
    "date": "31-01-2019",
    "amount": "100.000",
    "point":"120.000"
}
```

API REQ/RESP

```
{
  "response":"TOP OK",
  "responsecode":"00"
}
```

```
{
    "action": "topup",
    "noAkun": "6281284147433",
    "date": "31-01-2019",
    "amount": "100.000",
    "point":"0"
}
```

Merchant

API REQ/RESP

API

API

Industry Trends push for more APIs

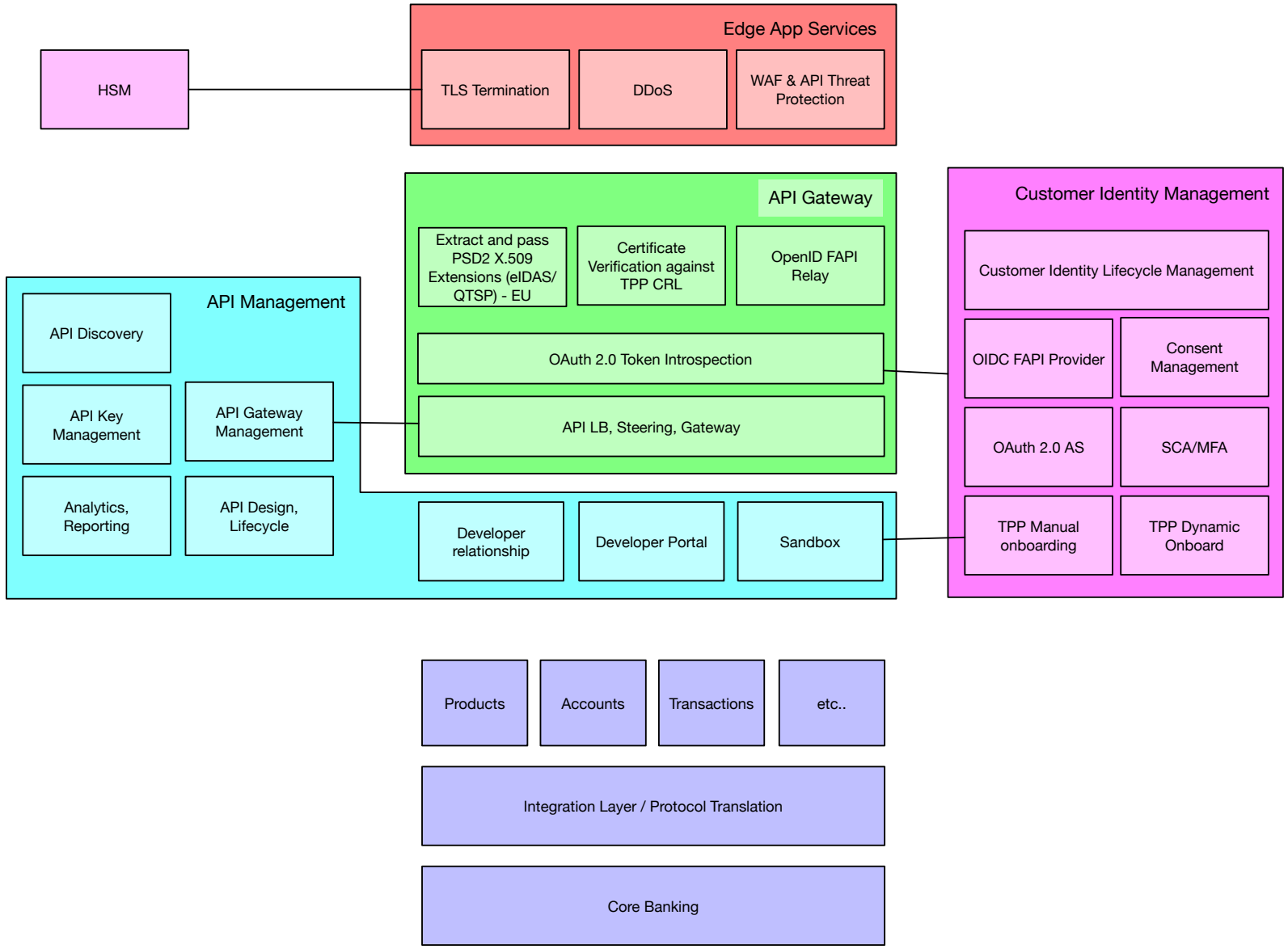
ORGANISATIONS NEED INTEROPERABILITY

Standards continue to form for information sharing

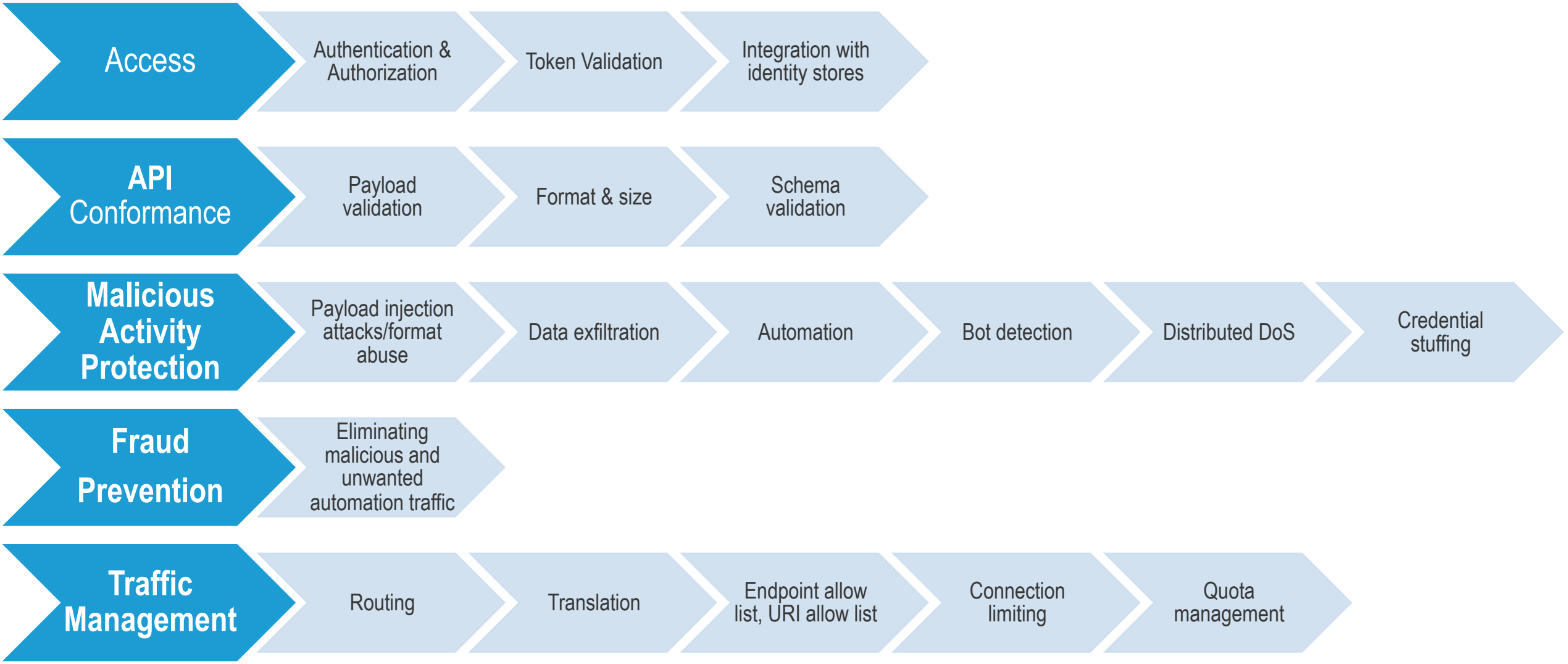
Major Industries are pushing new standards

- Open Banking
- Open Government
- Digital Health
- Consumer Retail (Utilities, Telecommunications)

Open Banking Application Services Reference



Critical Controls for APIs



APIs need tailored security controls

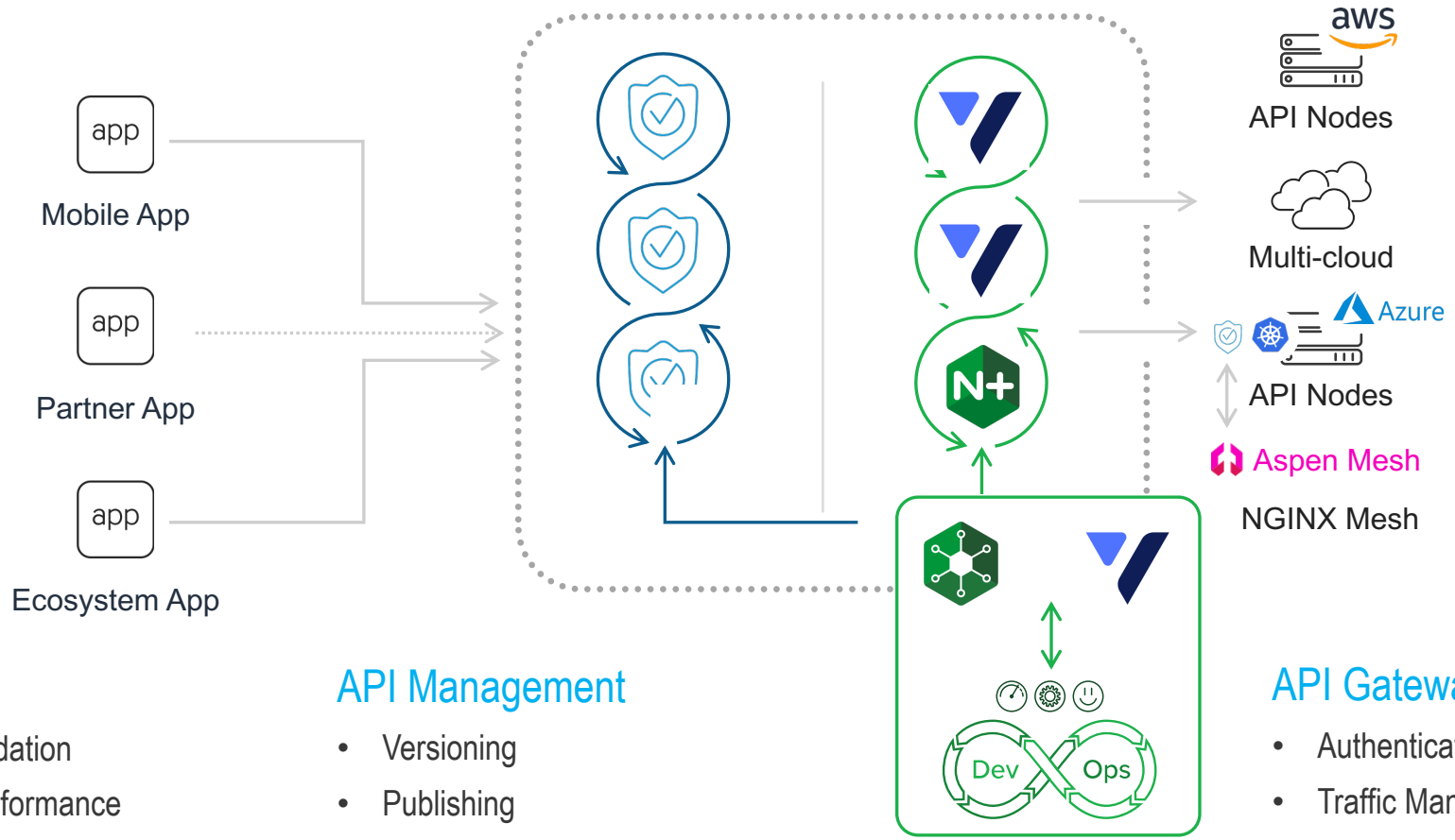
PROTECT APIs LIKE WEB APPS

APIs NEED DEDICATED SECURITY CONTROLS THAT CAN ONLY BE DELIVERED USING WEB APPLICATION AND API PROTECTION (WAAP)

OWASP **API SECURITY TOP 10**

API1:	Broken object level authorization
API2:	Broken user authentication
API3:	Excessive data exposure
API4:	Lack of resources & rate limiting
API5:	Broken function level authorization
API6:	Mass assignment
API7:	Security misconfiguration
API8:	Injection
API9:	Improper assets management
API10:	Insufficient logging & monitoring

API Management & Security



API Security

- Schema Validation
- Protocol Conformance
- Vulnerability Mitigation
- Fraud Prevention
- Bot and DoS Defense

API Management

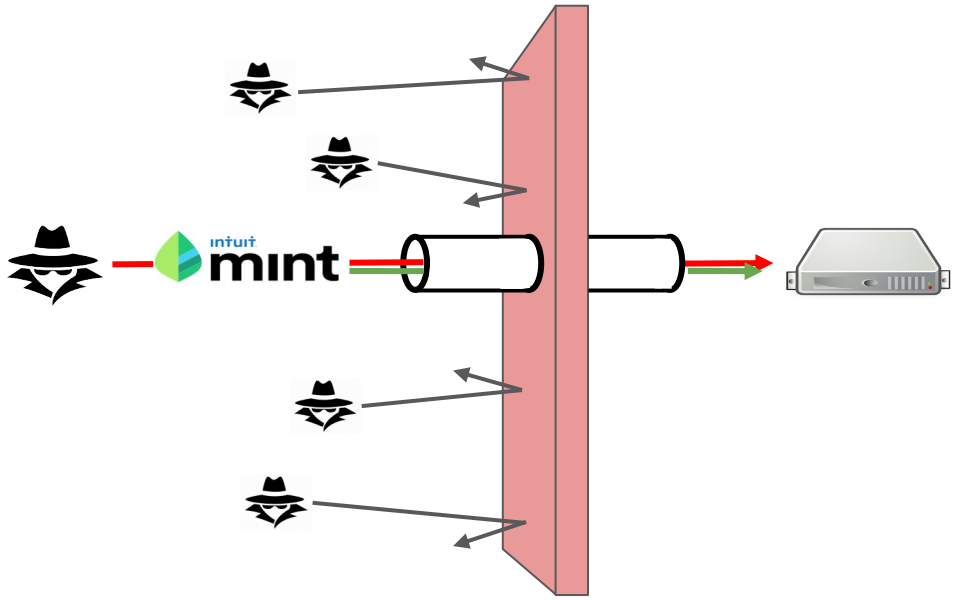
- Versioning
- Publishing
- Schema/definition
- Monitoring & Dashboard
- Onboarding - Documenting

API Gateway

- Authentication & Authorization
- Traffic Management
- Rate-limiting/Thresholding
- Allow/Deny List
- Routing

We identify and protect financial aggregators

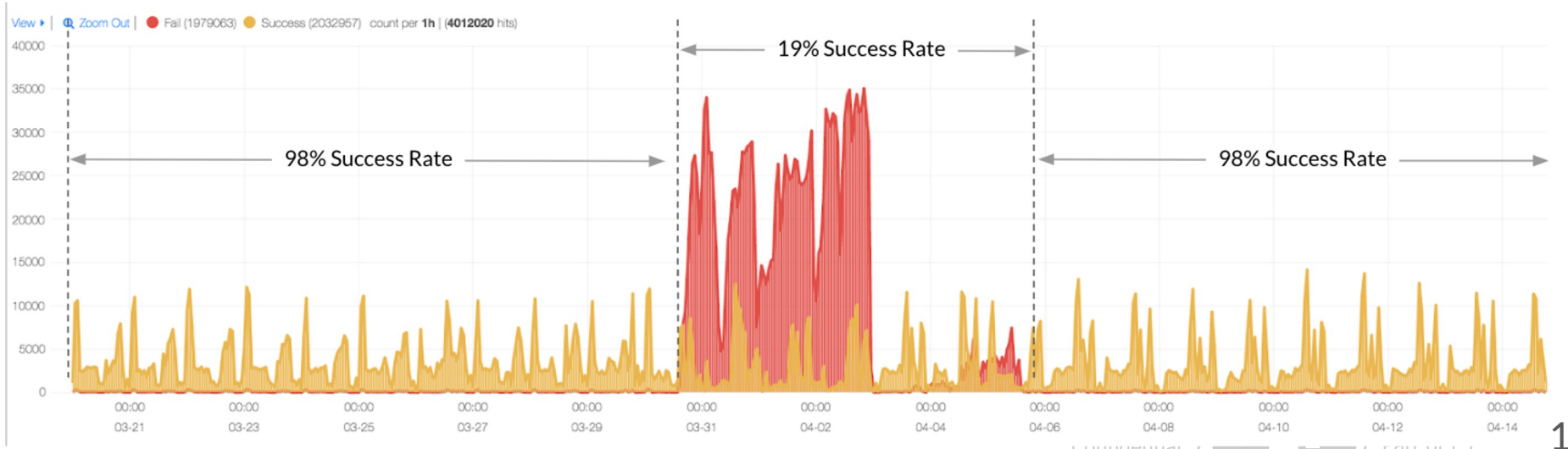
SOME BANKS HAVE 40% AGGREGATOR/WEB SCRAPER TRAFFIC



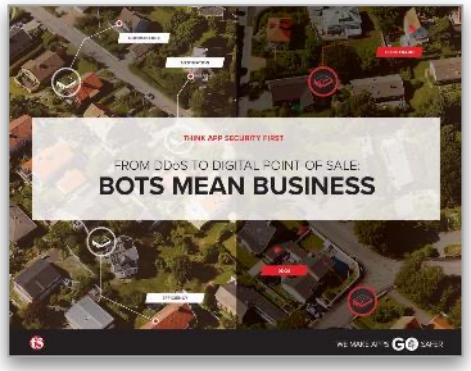
Dark Web Forum

Open a **mint.com** account and add the bank account using the username/password. This will

1) Check if the account is still live,
2) Let you see the balance of the accounts, and
3) If needed, let you check for deposits from PayPal, as well as to keep an eye on it. Research the background of account holder and get their SSN from ssnvalidator.com

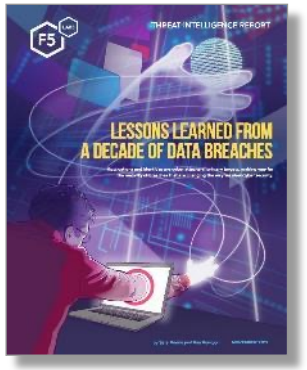


Read more about these and other threats



https://interact.f5.com/AppProtectLibrary

Stay up-to-date Sign up for F5 Labs



F5labs.com