
AWS
re:Invent

SEC211-S

Five-step plan for securing your APIs

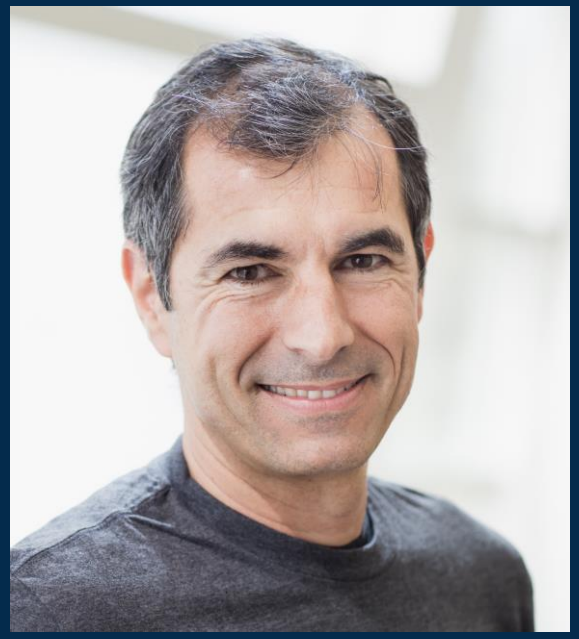
Javier Garza
Sr. Developer Evangelist
Akamai Technologies

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Speaker



@jjaviergarza

Javier Garza

Developer Evangelist @Akamai (San Francisco, CA)

- 15+ years at Akamai helping large enterprises run fast and secure apps at the edge
- Co-author of O'Reilly's "Learning HTTP/2" book, blogger, speaker, one-liner king
- Motto: Share what you know, and learn what you don't
- Hobbies: Challenging workouts, non-profit volunteering

Agenda

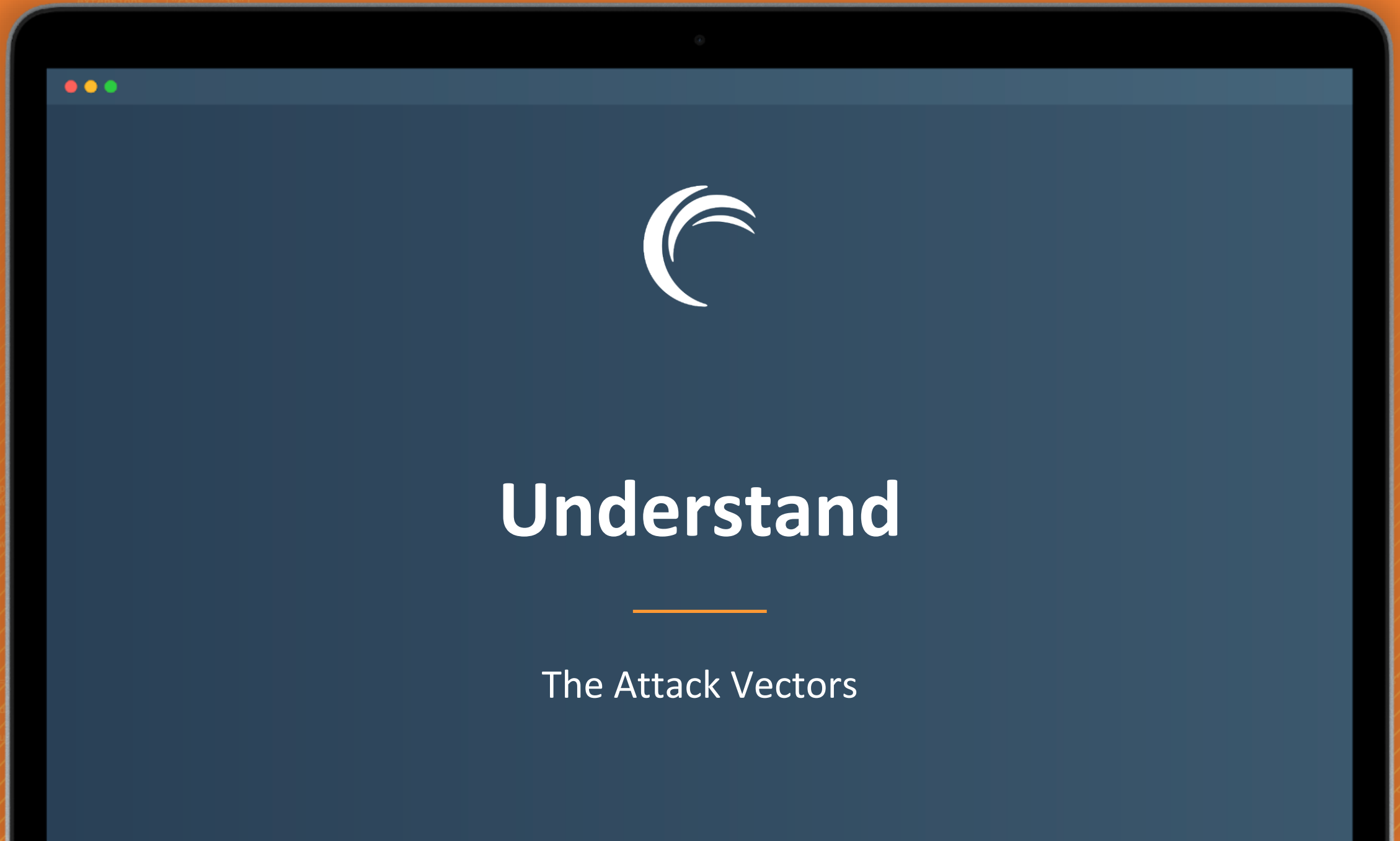
Introduction

Part 1 Understand the Attack Vectors

Part 2 Mitigate the Attacks with a Five-Step Plan

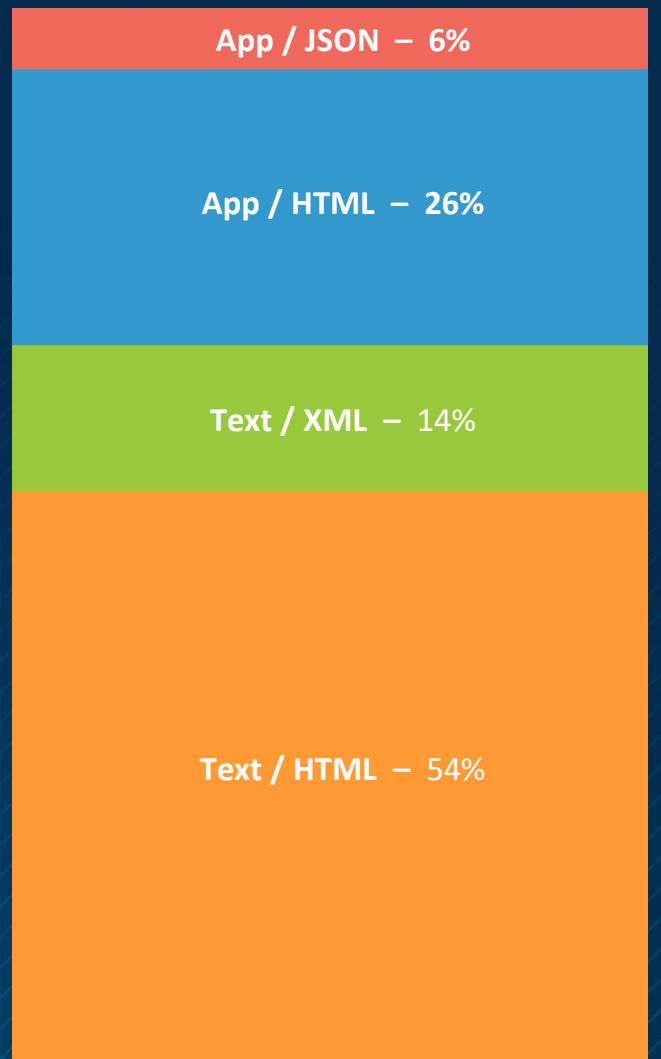
Part 3 Leverage the Edge

Wrap-Up


Understand
The Attack Vectors

Growth of API Use

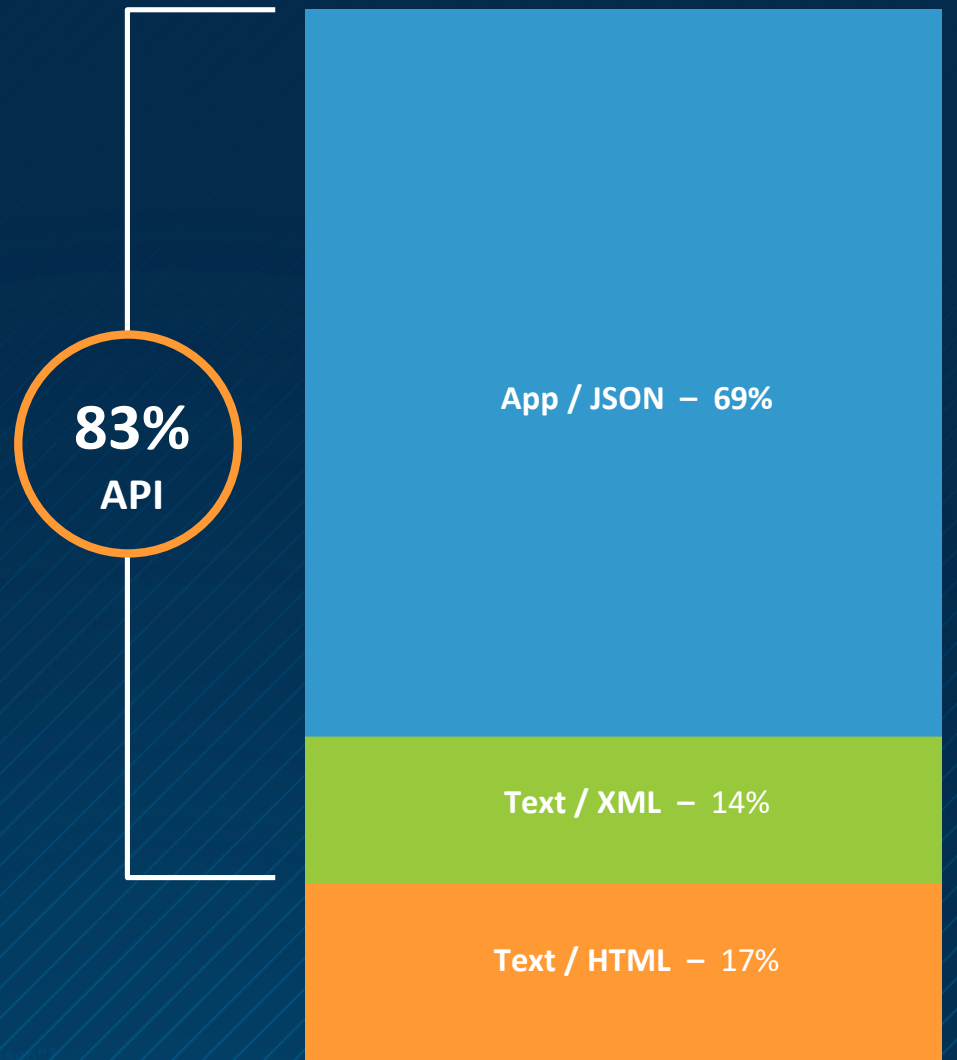
2014 through 2018



Source: Akamai ESSL Network, SOTI Q1 2019

Growth of API Use

2014 through 2018

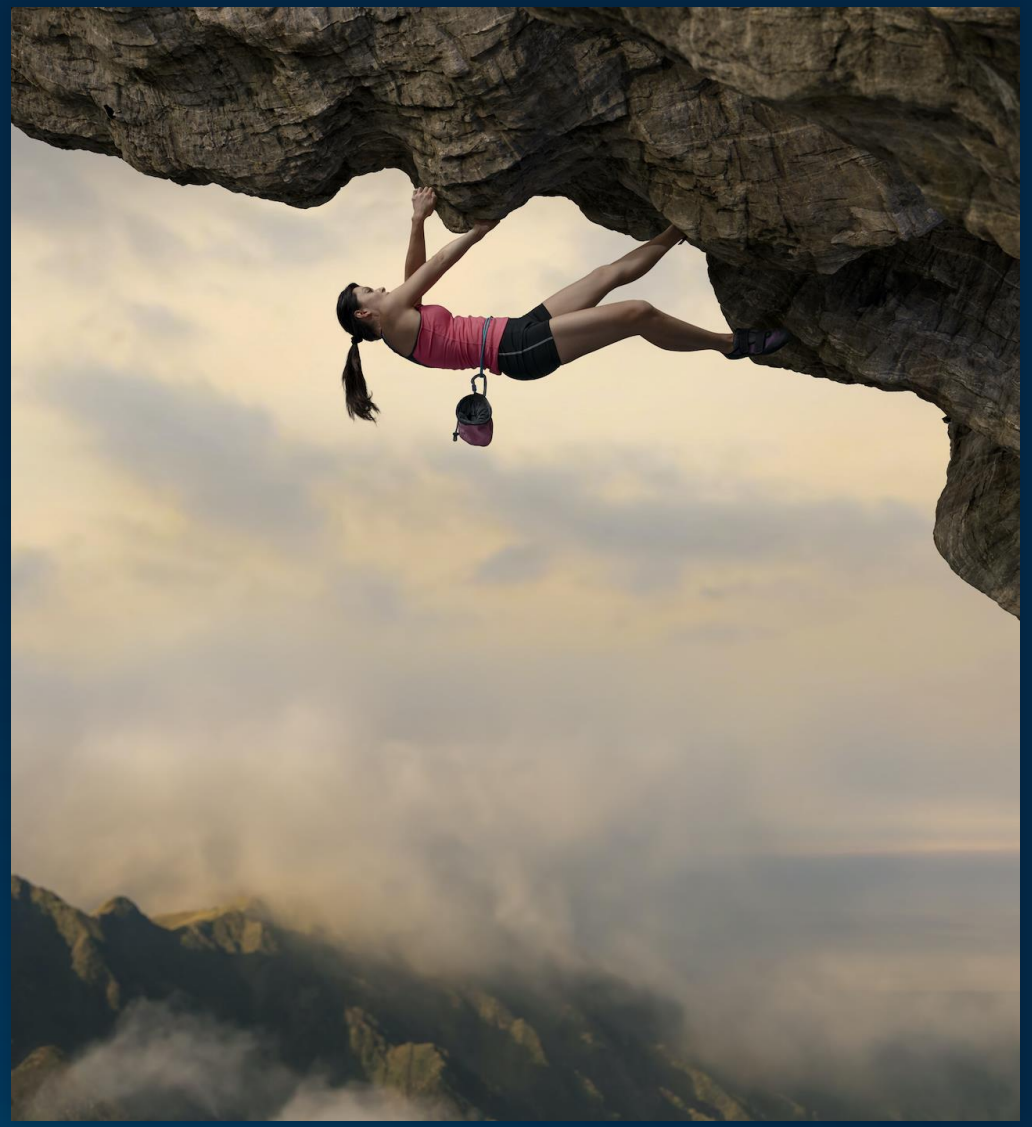


API calls now dominate overall web hits

Source: Akamai ESSL Network, SOTI Q1 2019

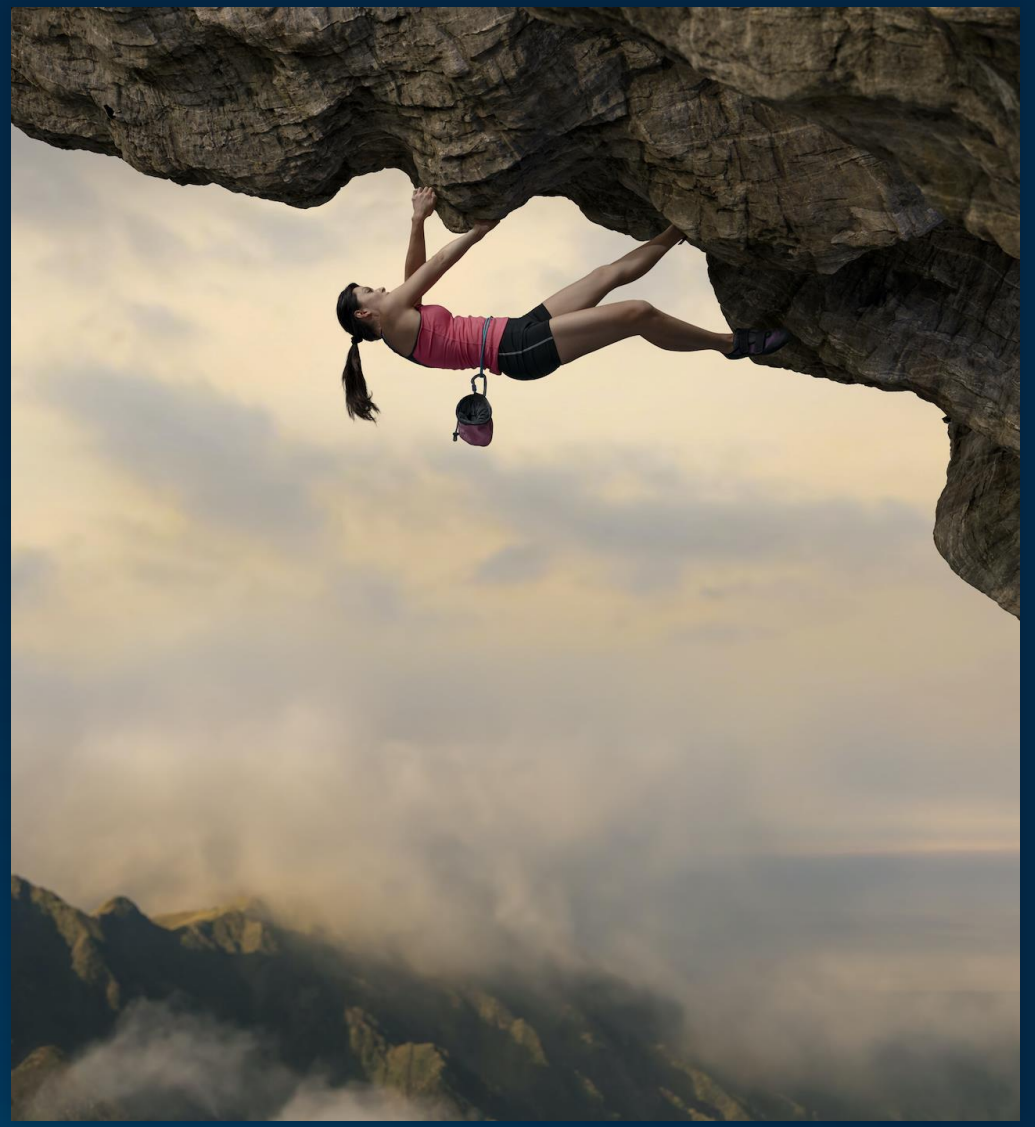
Challenges in API Security

- Often InfoSec/DevSecOps is looped too late in the development process



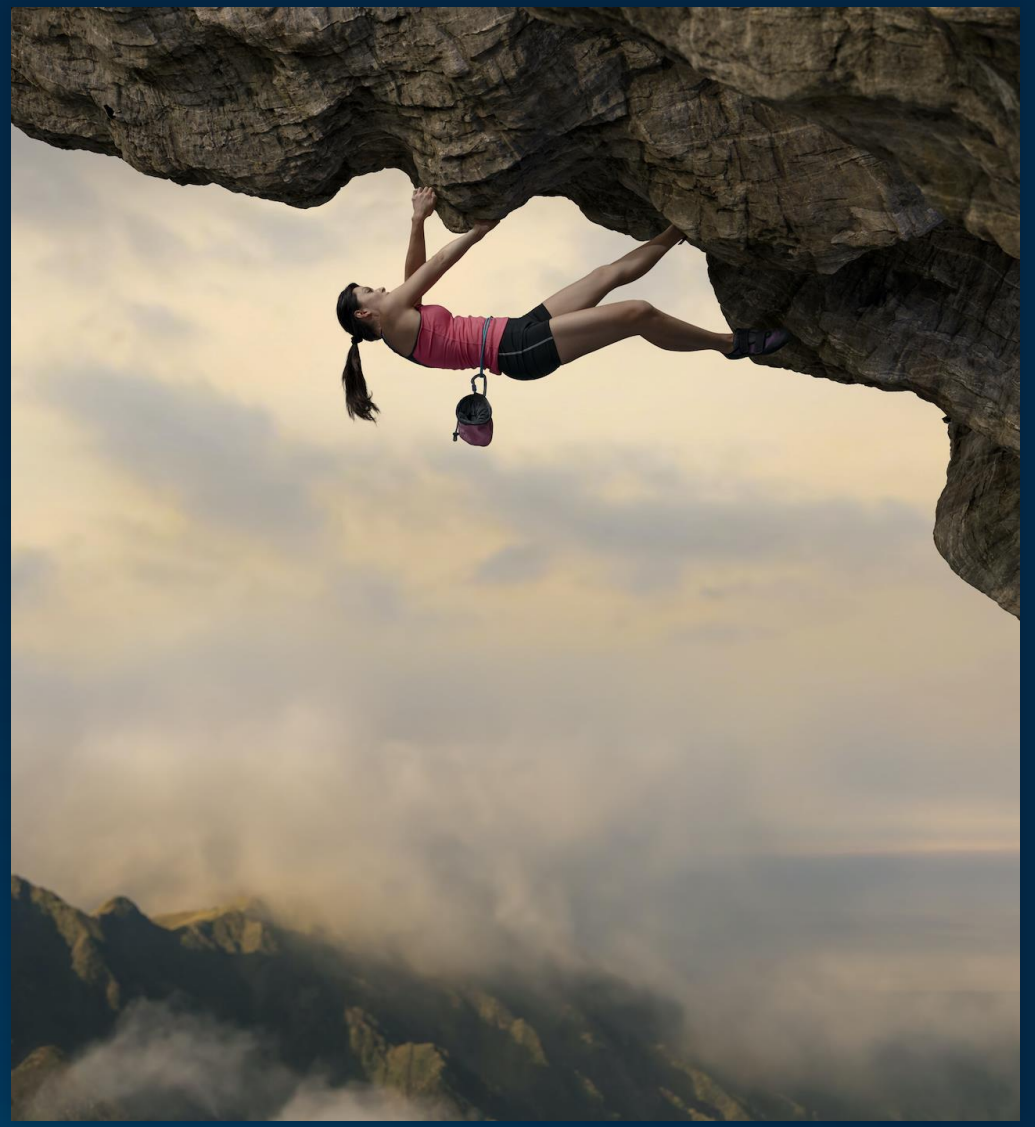
Challenges in API Security

- Often InfoSec/DevSecOps is looped too late in the development process
- API security is often complex (multiple standards, limited number of tools, lack of expertise)



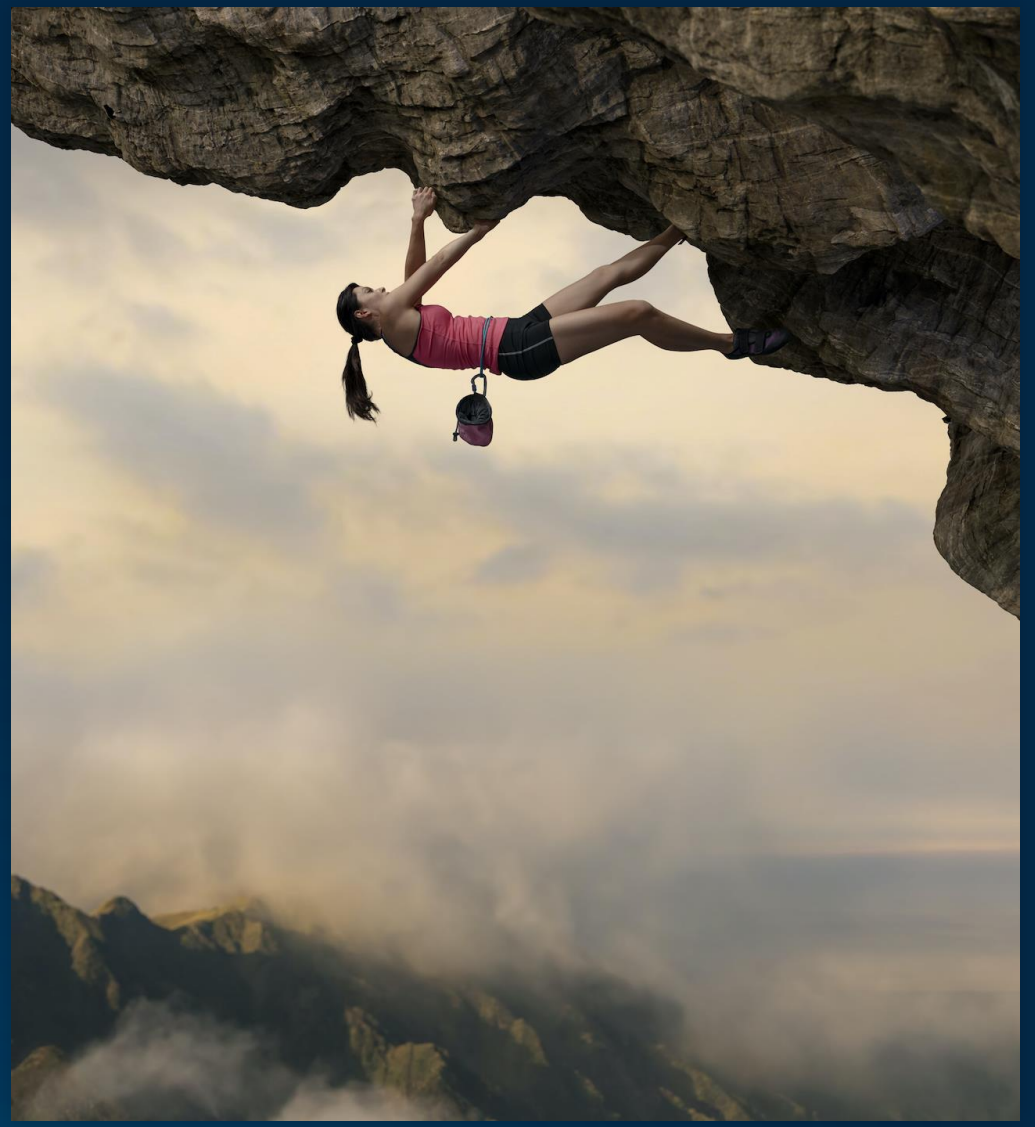
Challenges in API Security

- Often InfoSec/DevSecOps is looped too late in the development process
- API security is often complex (multiple standards, limited number of tools, lack of expertise)
- Great level of effort to apply API security at scale, specially across diverse cloud infrastructure

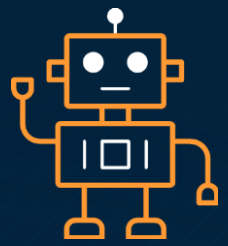


Challenges in API Security

- Often InfoSec/DevSecOps is looped too late in the development process
- API security is often complex (multiple standards, limited number of tools, lack of expertise)
- Great level of effort to apply API security at scale, specially across diverse cloud infrastructure
- Hard to stay up to date with new vulnerabilities



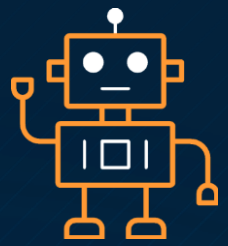
APIs are a Primary Target for Attackers Today



4X more

credential stuffing attacks on APIs

APIs are a Primary Target for Attackers Today

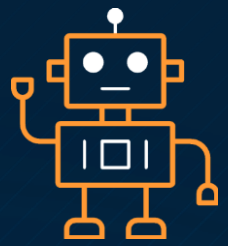


4X more

credential stuffing attacks on APIs

#heartbleed

APIs are a Primary Target for Attackers Today



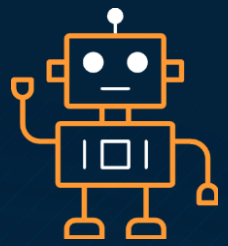
4X more

credential stuffing attacks on APIs

#heartbleed

#DROWN

APIs are a Primary Target for Attackers Today



4X more

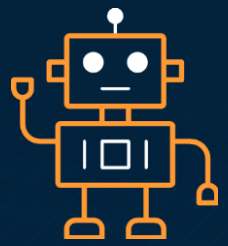
credential stuffing attacks on APIs

#heartbleed

#DROWN

#shellshock

APIs are a Primary Target for Attackers Today



4X more

credential stuffing attacks on APIs

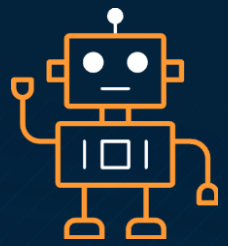
#heartbleed

#DROWN

#shellshock

#poodle

APIs are a Primary Target for Attackers Today



4X more

credential stuffing attacks on APIs

#heartbleed

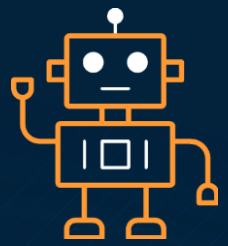
#DROWN

#shellshock

#fappening

#poodle

APIs are a Primary Target for Attackers Today



4X more

credential stuffing attacks on APIs

#heartbleed

#DROWN

#shellshock

#fappening

#poodle

#snappening

API Security Top 10

A1: Broken Object Level Authorization

A2: Broken Authentication

A3: Excessive Data Exposure

A4: Lack of Resources & Rate Limiting

A5: Broken Function Level Authorization

A6: Mass Assignment

A7: Security Misconfiguration

A8: Injection

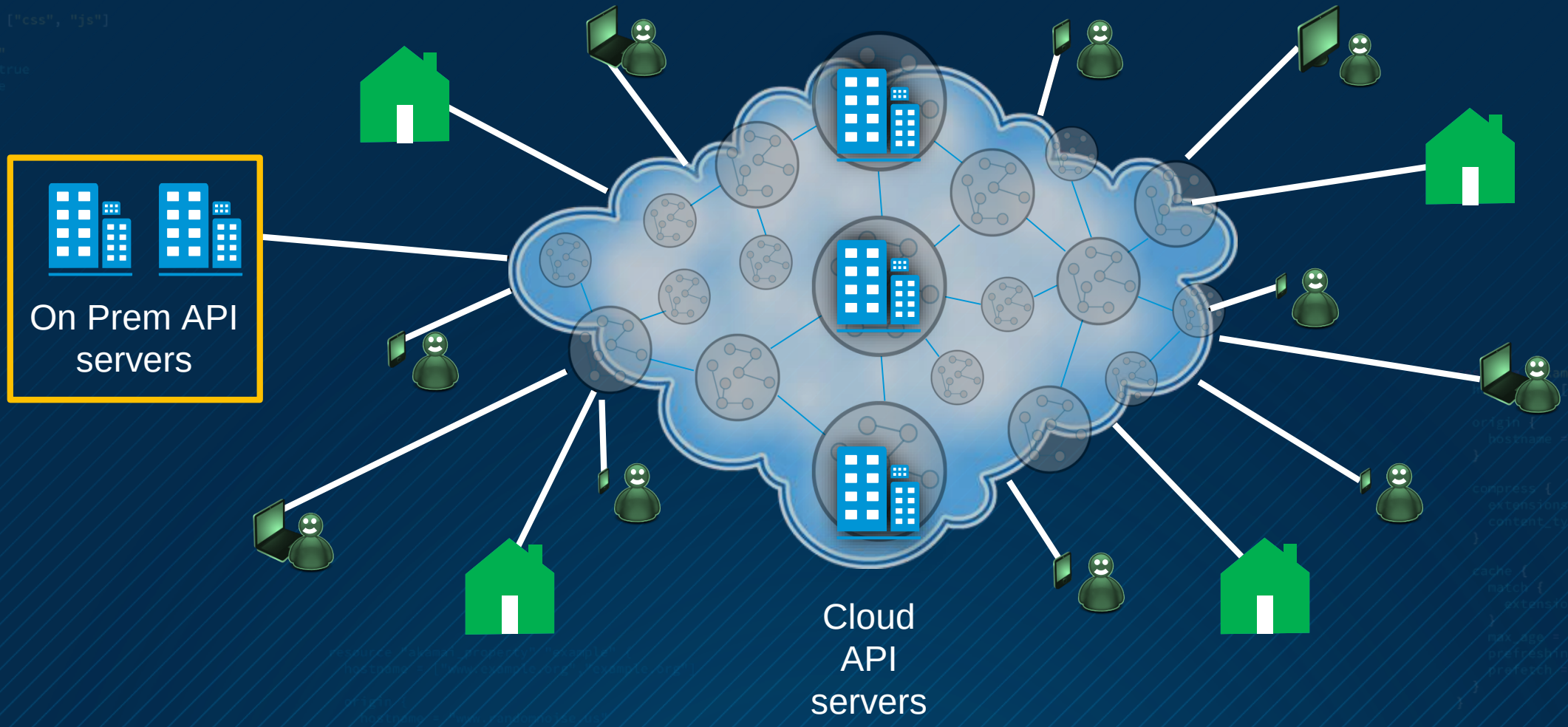
A9: Improper Assets Management

A10: Insufficient Logging & Monitoring



Source: https://www.owasp.org/images/5/59/API_Security_Top_10_RC.pdf

API Security: client > network > server



The 4 Areas Where Your APIs are the Most Vulnerable

1. DDoS Attacks
2. Parameter Attacks
3. SQL Injection Attacks
4. Credential Stuffing Attacks

Distributed Denial of Service (DDoS) Attacks



Targeted attack

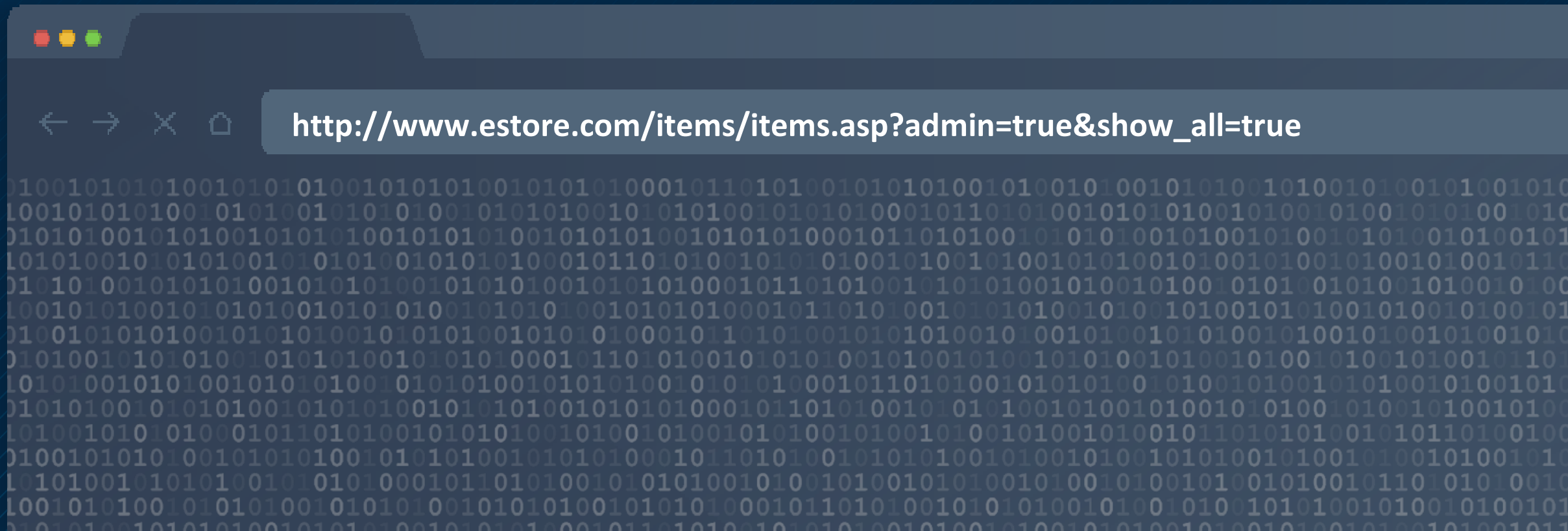


Misconfigured automation scripts

Source: API & Security Trends for 2018

Parameter Attacks

An important step for any resilient API implementation is to sanitize all incoming data to confirm that it is valid and will not cause harm



SQL Injection Attacks

76%

of attacks are SQL injections

SQL query:

```
sql_query= "
SELECT ItemName, ItemDescription
FROM Item
WHERE ItemNumber = "& Request.QueryString("ItemID")
```

Normal request:

http://www.estore.com/items/items.asp?itemid=999

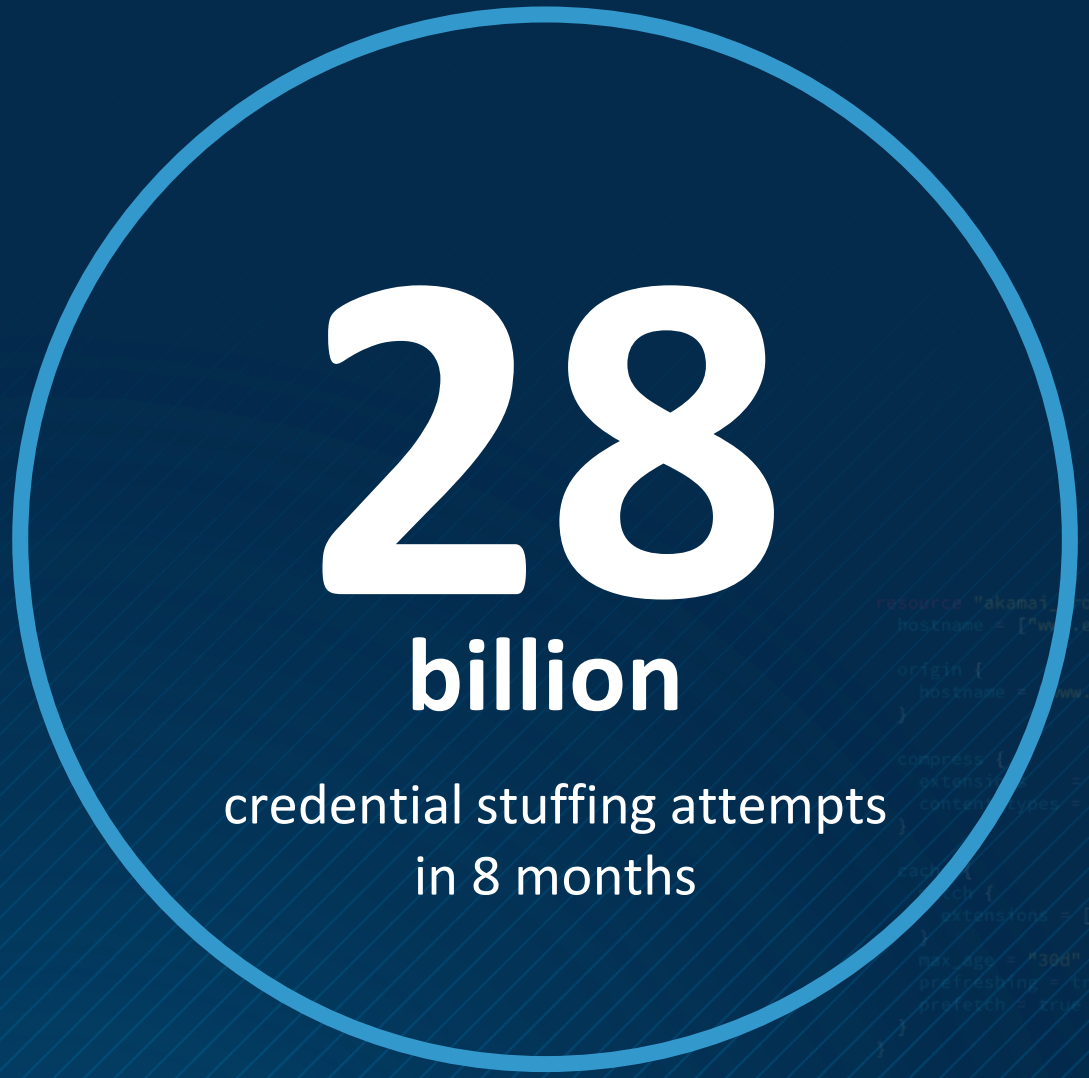
SQL injection:

http://www.estore.com/items/items.asp?itemid=999;DROP TABLE Users

4 Credential Stuffing Attacks

With clients that don’t render JavaScript, a lot of the typical credential stuffing defenses just don’t work

Aggressive botnets will overwhelm origin with login requests



Source: Akamai SOTI 1Q 2019
(Observed on Akamai Intelligent Edge Platform, 2018

Akamai DEVELOPER

Recap:

The 4 Areas Where Your APIs Are the Most Vulnerable

1. DDoS Attacks
2. Parameter Attacks
3. SQL Injection Attacks
4. Credential Stuffing Attacks



Mitigation

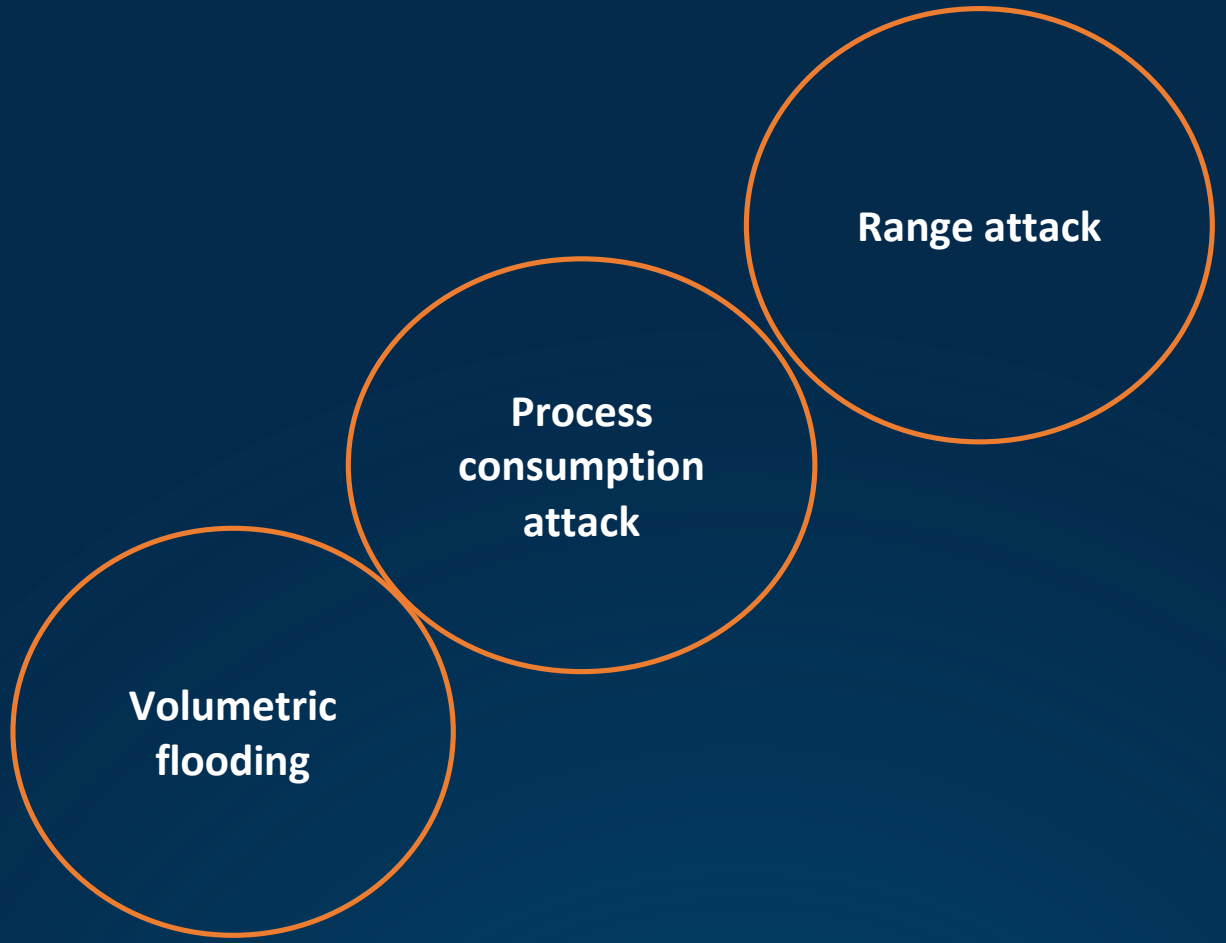
Know How to Stop the Attack



Step 1: DDoS Mitigation

DDoS Attacks

The Types



Volumetric Flooding

Overwhelm APIs with a flood of HTTP/HTTPS requests

Attacks can leverage IoT devices (Mirai Botnet)

One way to do this is by purchasing access to a booter service, which is a marketing term for “DDoS for hire”

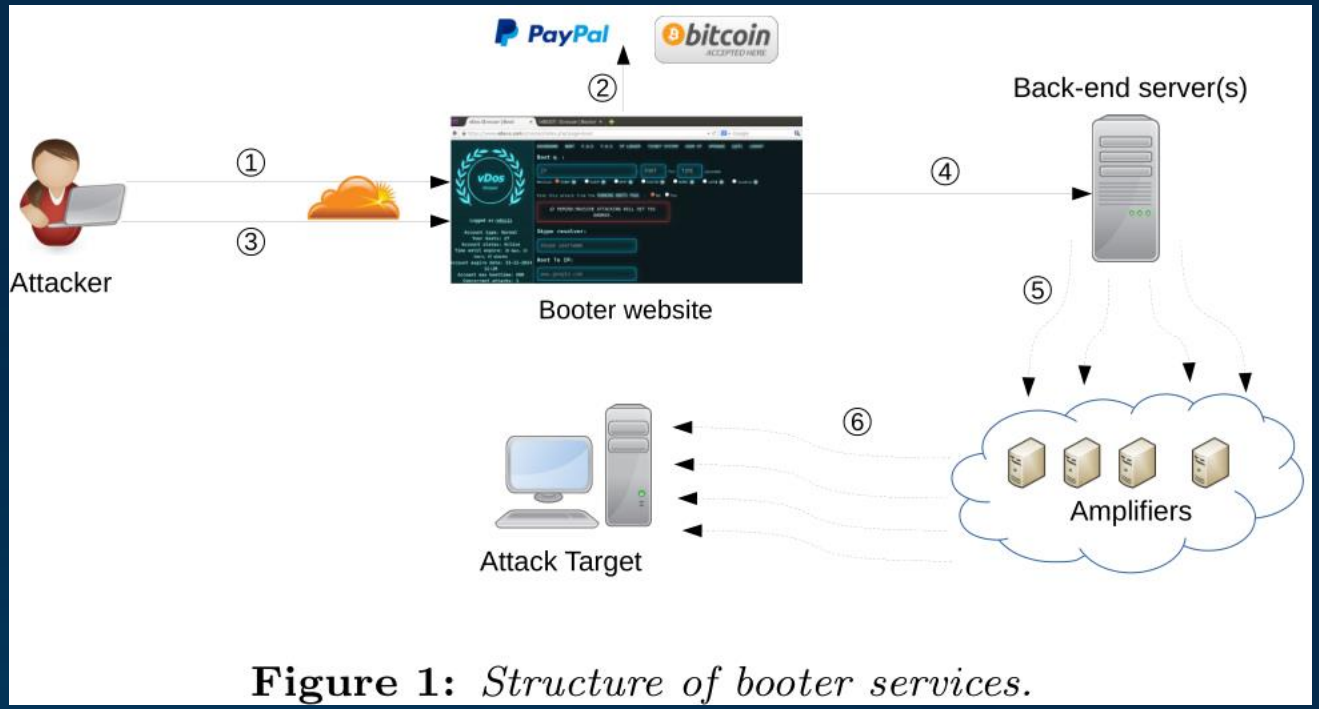


Figure 1: *Structure of booter services.*

Mitigation

Network controls

- Blacklisting IPs and CIDR range
- IP reputation lists

Rate limits

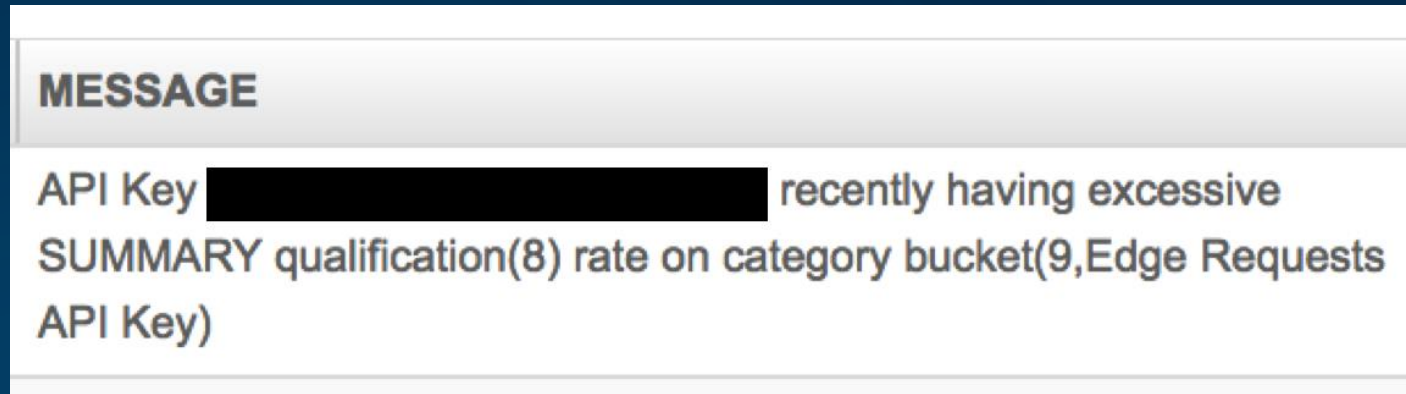
- Defining thresholds

Slow posts

- Protect against attacks that try to consume application resources by opening an HTTP connection and then sending data very slowly

Authentication

- Mutual authentication (client certs)





Step 2: Protect Processes

Process Consumption Attacks

Akamai DEVELOPER

Target CPU/RAM

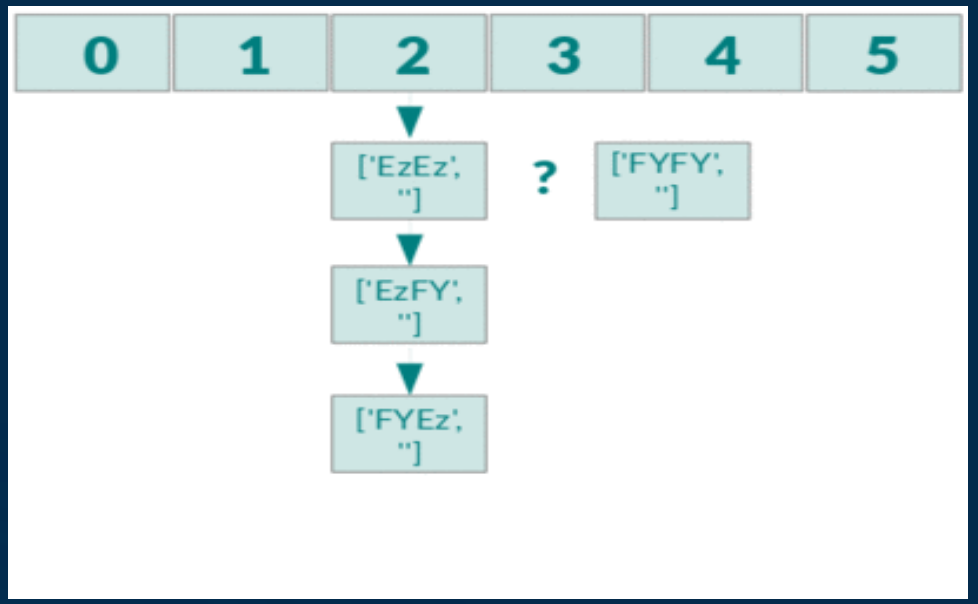
Focus on allocations rather than network bandwidth

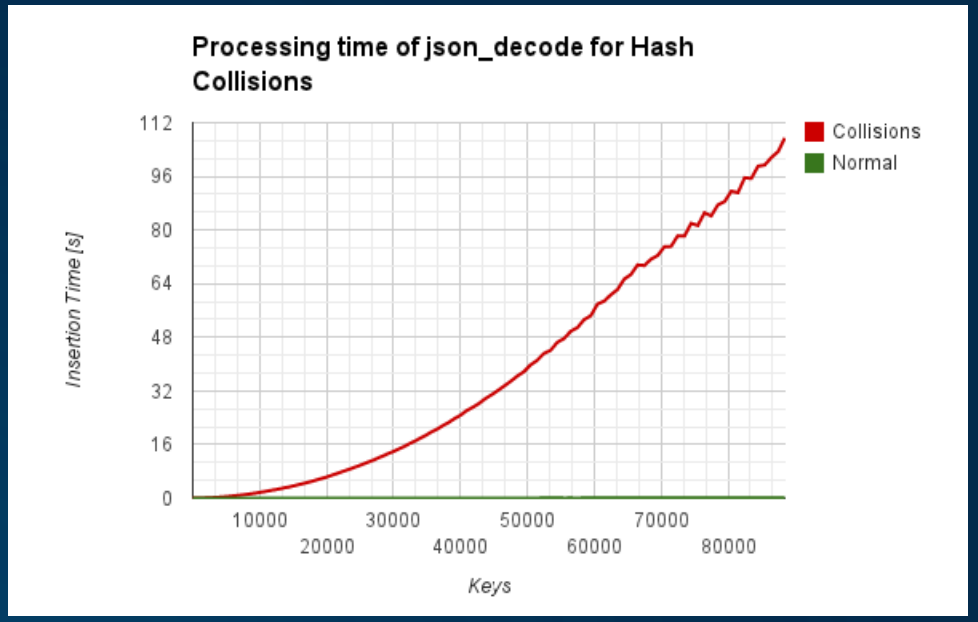
Hash collision

Commonly knows consumption attack

Malicious JSON

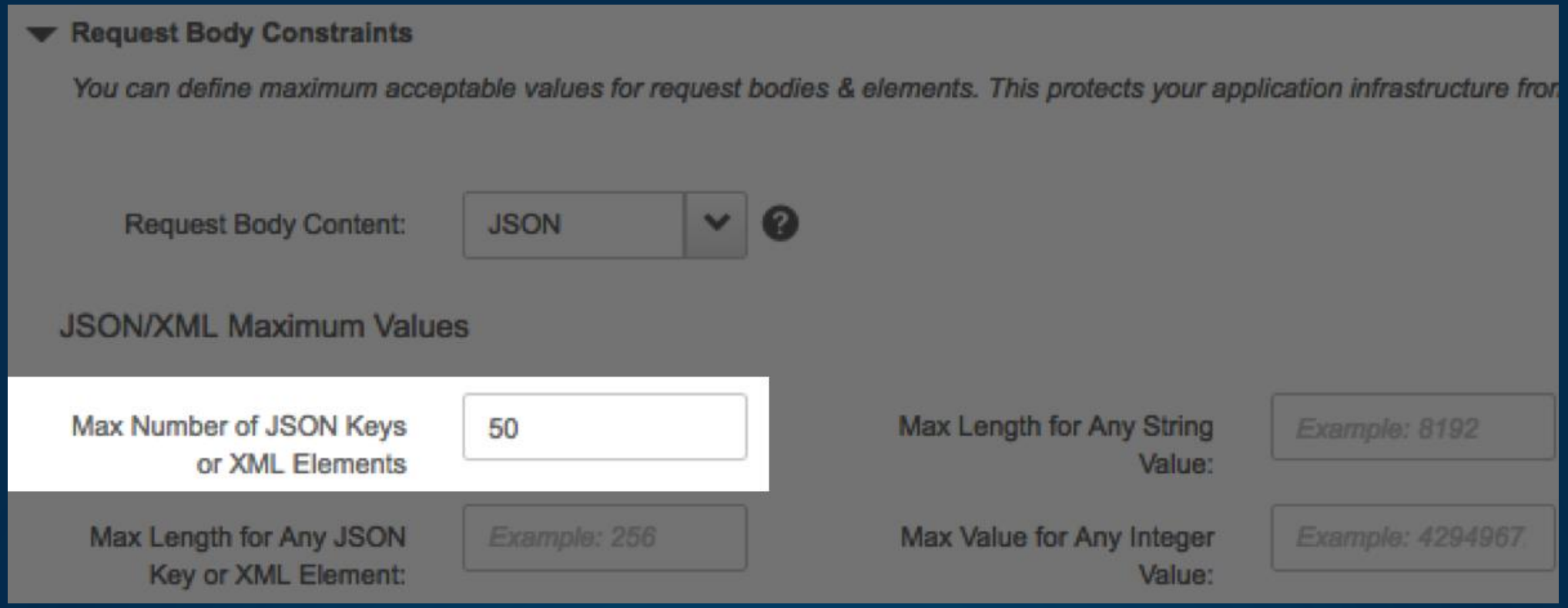
Overwhelm the CPU by sending bulk of malicious JSON





Mitigation

Setting a limit on the number of the keys
Set maximum nesting depth





Step 3: Range Attacks/Scraping

Scraping/Range Attack

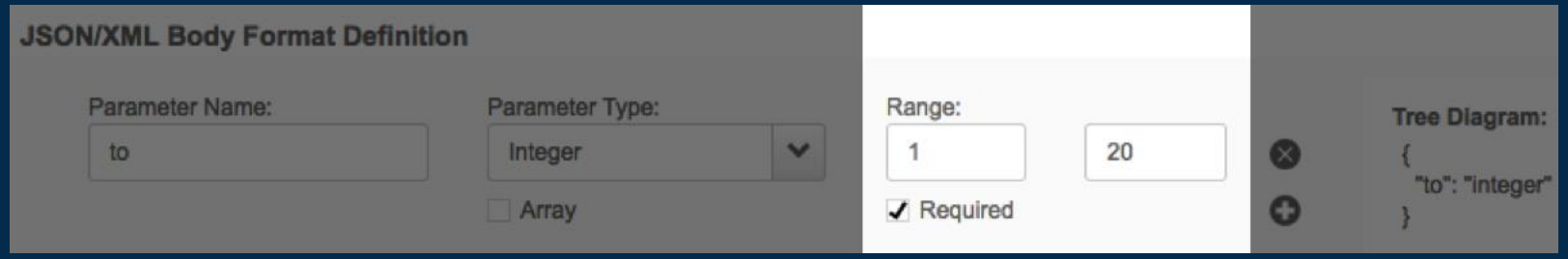
Trying retrieval of large volume of data leading to DDoS-like conditions

```
{
  "items": [
    ["recommendation", "english", "spanish", {
        "from": 1,
        "to": 2
      },
      ["description", "title", "artwork"]
    ],
    ["recommendation", "english", "spanish", {
      "from": 1,
      "to": 2
    }, "art_size", "_342x192", "jpg"]
  ],
  "csrf": "some_token_here_possibly"
}
```

```
{
  "items": [
    ["recommendation", "english", "spanish", {
        "from": 1,
        "to": 200000
      },
      ["description", "title", "artwork"]
    ],
    ["recommendation", "english", "spanish", {
      "from": 1,
      "to": 2
    }, "art_size", "_342x192", "jpg"]
  ],
  "csrf": "some_token_here_possibly"
}
```

Mitigation

Setting a limit on the allowed range



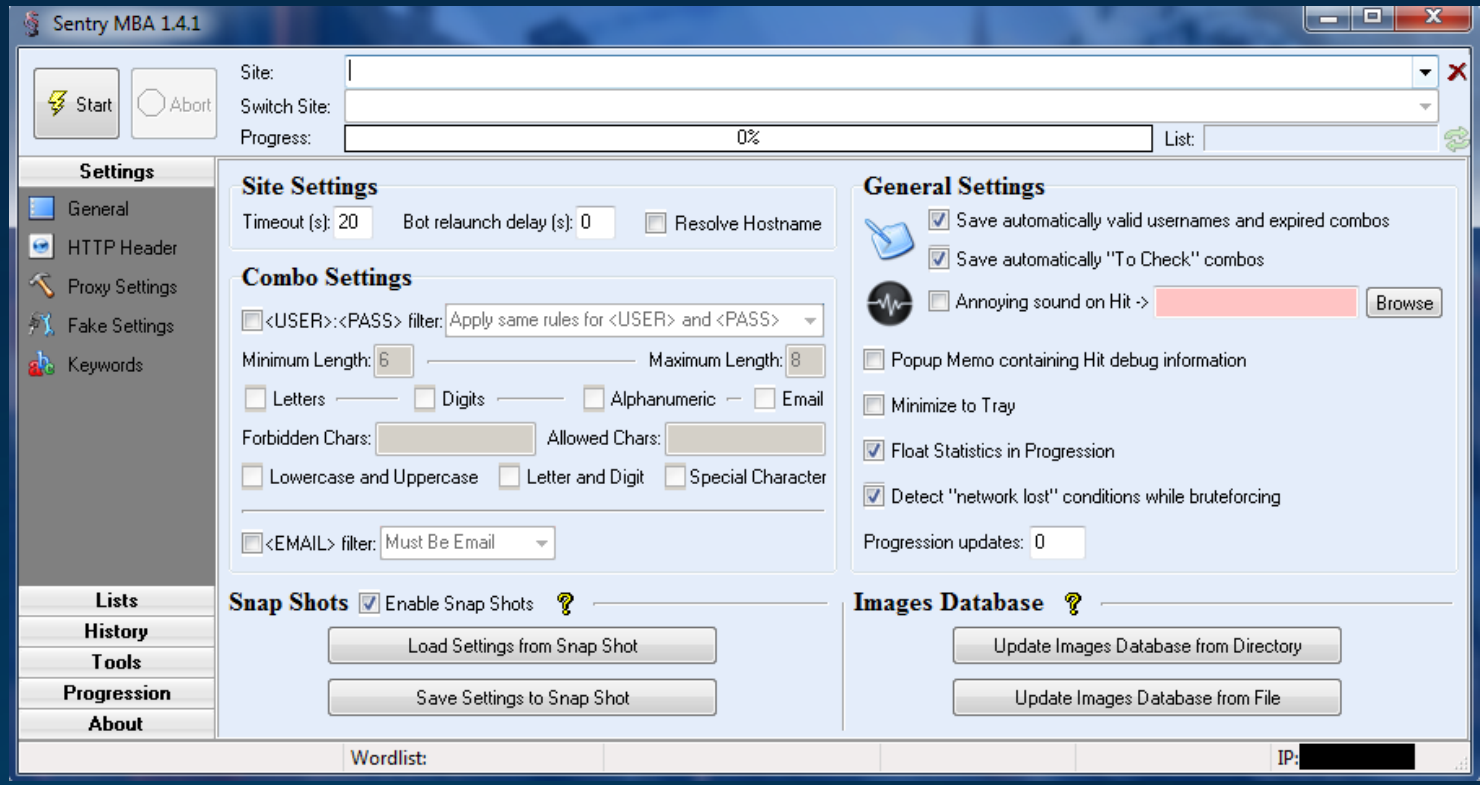


Step 4: Protect Credentials

Credentials Abuse

Bots Stealing Your Credentials

- 30% of all API authentication attempts are fraudulent
- Credential abuse campaigns vs. normal form-based authentication applications = 4 times
- Credential abuse campaigns launched at API authentication endpoints may employ 4.75% more botnet clients



Mitigation

- Good practices; i.e., don’t give them hints regarding valid users and passwords, password recovery, etc.
- Rate controls on login, password recovery, etc.
- Strong authentication (two-factor authentication, biometric/security keys)
- Human behavior detection (automatically distinguish if the user is a human or not)



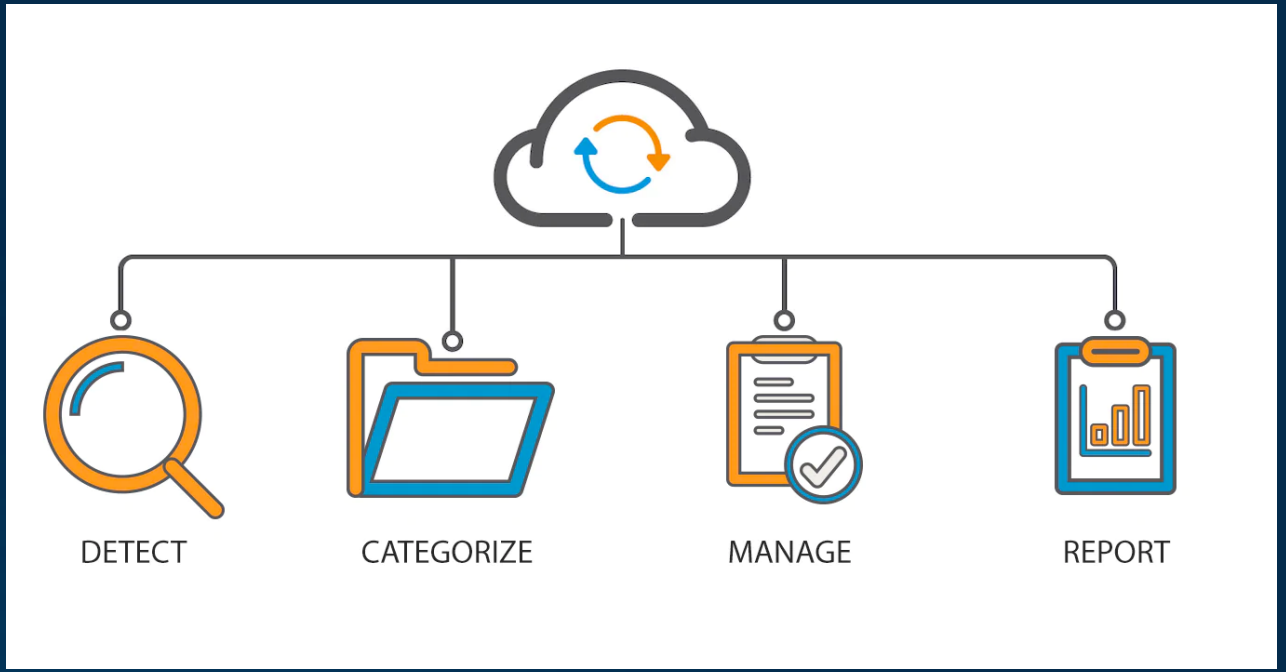


Step 5: Manage Bots

Bot Management

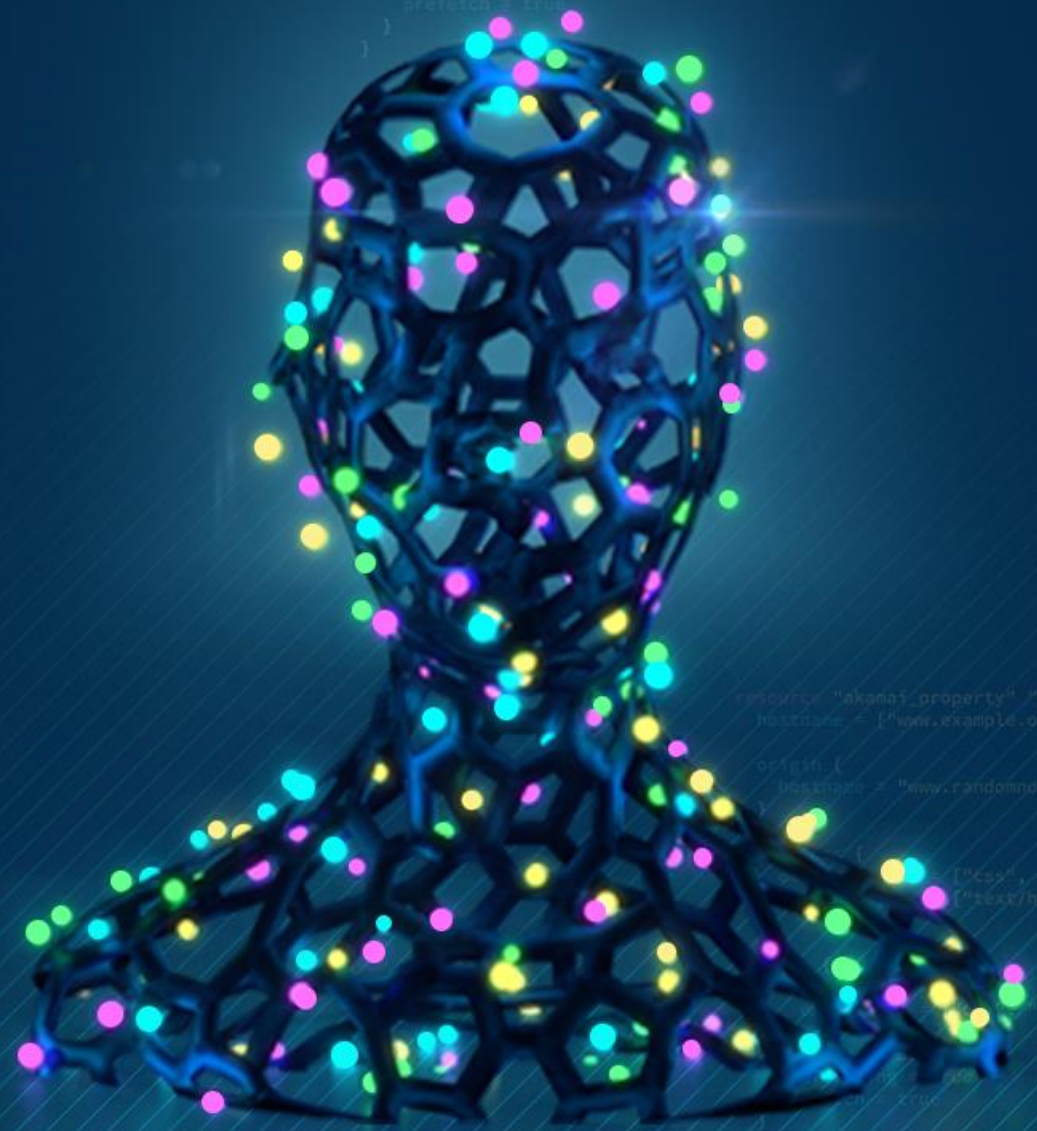
Understand Bots

- Bots represent up to 50% or more of the overall website traffic
- All bots are not equal and can only be managed
- Good bots vs. bad bots
- Identify, categorize, manage, and report bot traffic



Mitigation

- Enforce quotas
- Analyze traffic and try to categorize known bot traffic
- Use a bot detection tool





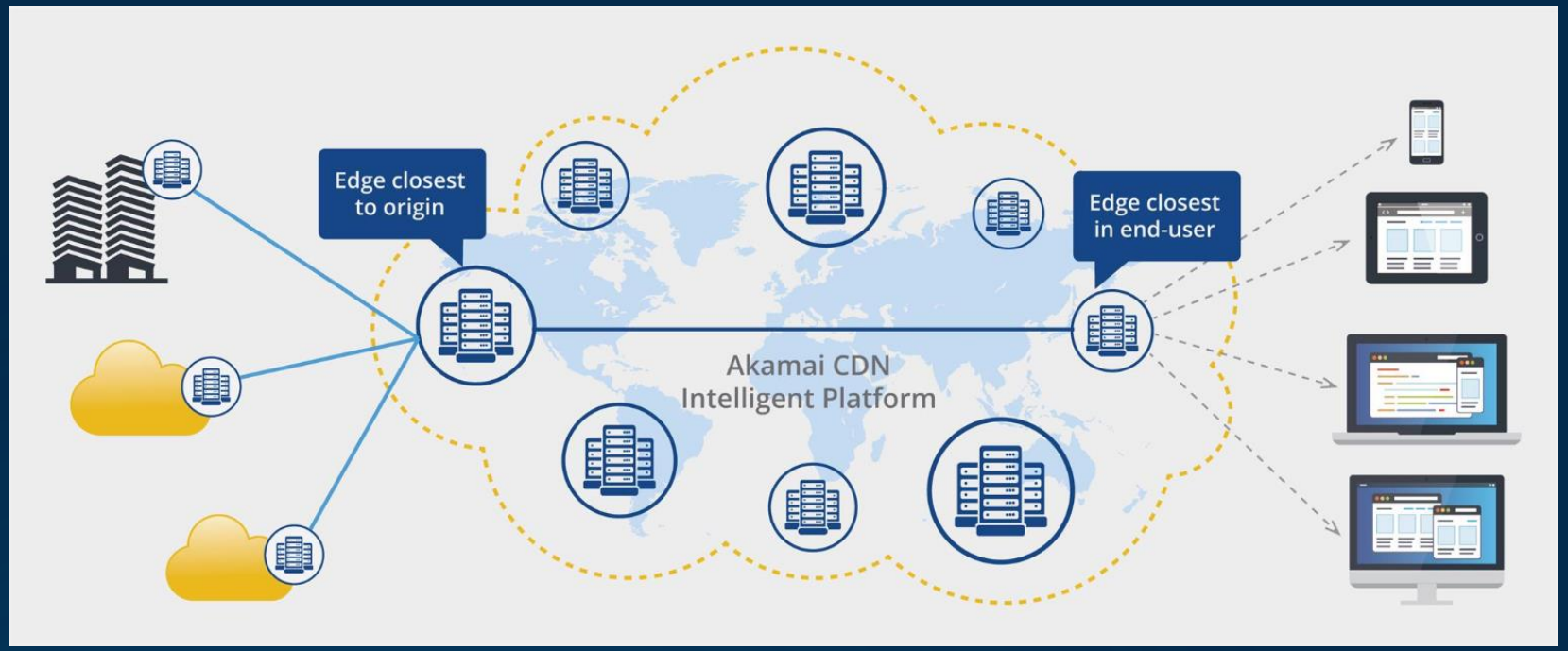
Leverage the Edge

Thwart Attacks Closer to Your Origin

The Edge of the Internet

CDN Evolving into Secured Edge Platform

- A decade-old cloud dominance is reaching saturation
- Migration from central processing to distributed edge processing
- CDN technologies have evolved to thwart attack closer to origin of attacks



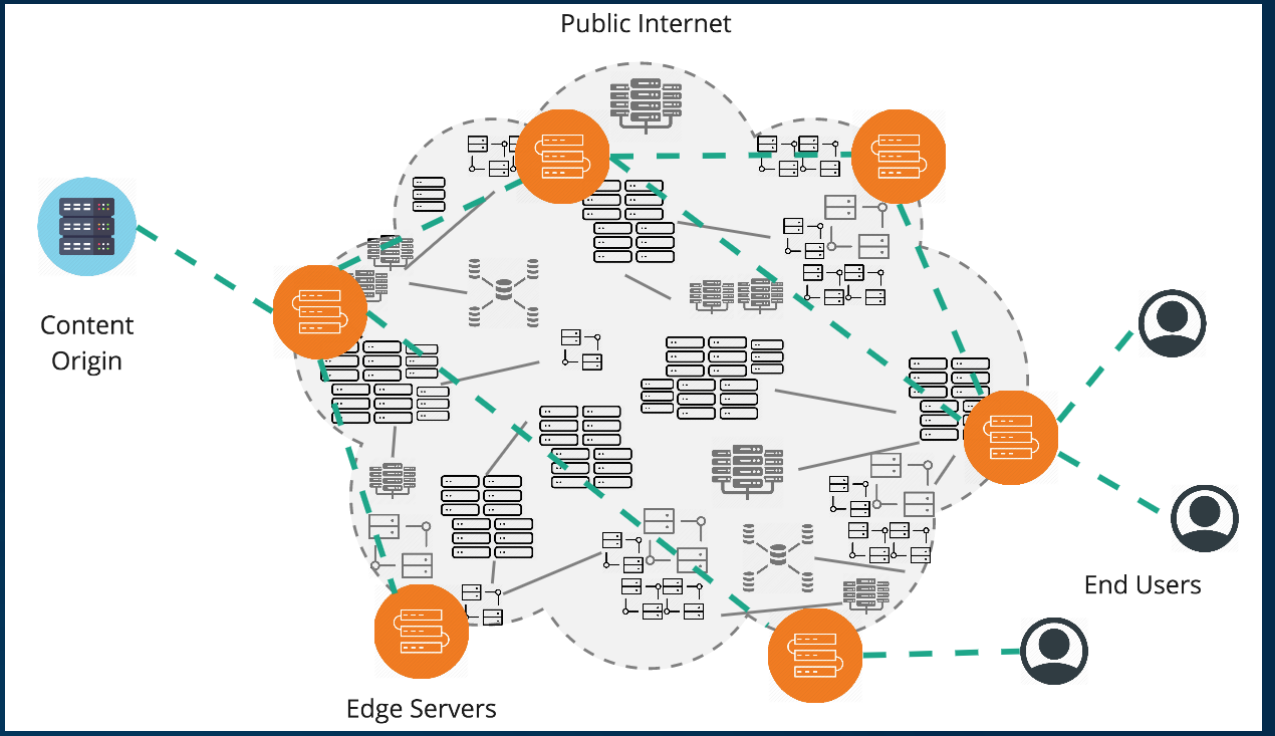
Source: The Future Is Moving to the Edge, Nasdaq, 2018

Why Fight Attacks at the Edge?

Thwart Attacks Closer to the Source

Fight attacks far away from your origin servers, and keep your infrastructure safe

- Defend your attacks closer to the source
- Integrated protection for your APIs without compromising on your performance
- Apply machine learning to outsmart your attackers



Secure APIs = Security + Management

API Management

With API Gateway

Manage and govern all your API operations at the edge

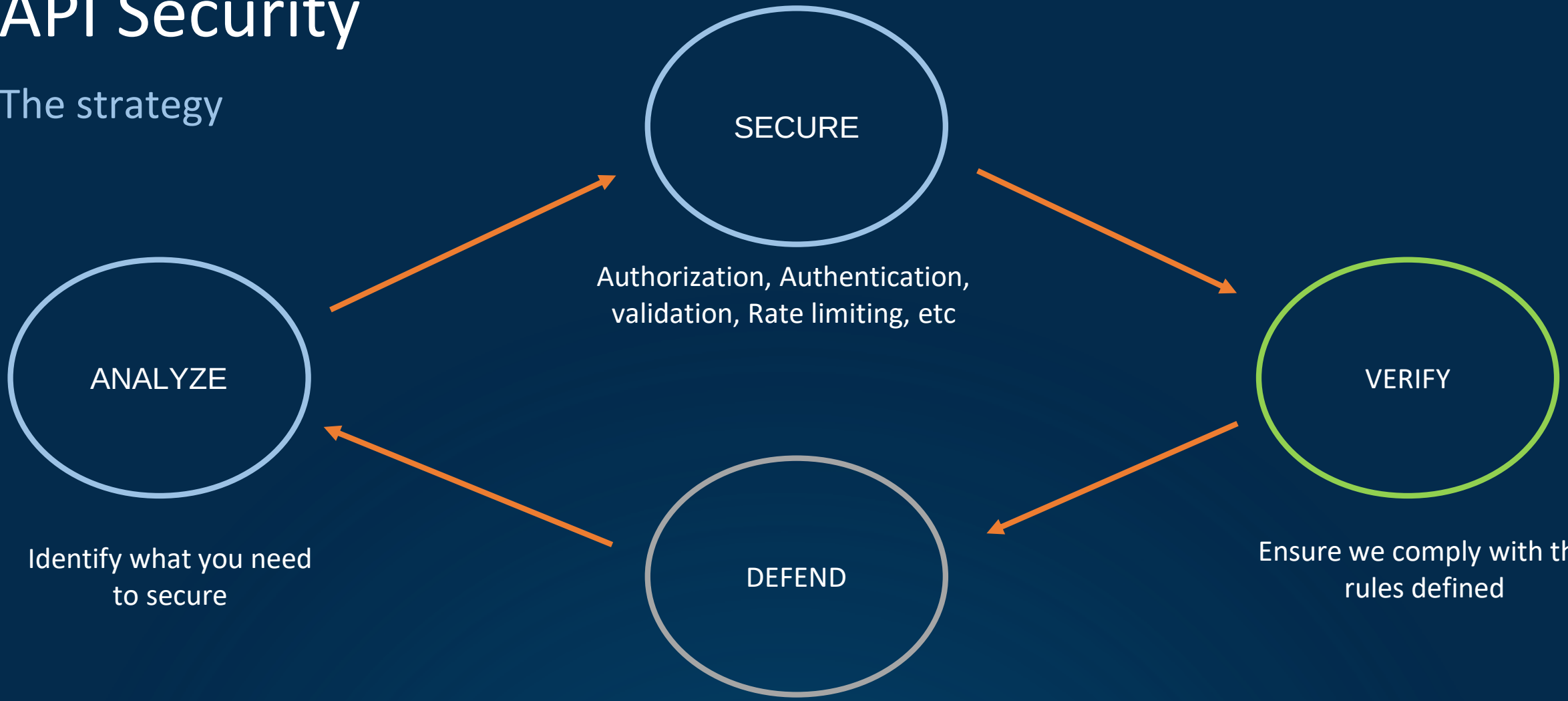
- Prevention of intentional and unintentional abuses
- Rate limiting
- Quotas
- Authentication
- Rule-based defense shield on the edge



Demo

API Security

The strategy



Develop an API Protection Plan Today

Within 7 days you should

- Assess your APIs, and identify potential security risks

Within 1 month you should

- Understand who is accessing your APIs from where and how
- Define appropriate API security measures

Within 3 months you should

- Select a security solution that allows for customizable and automated API protection that is tailored to your organization's needs
- Drive an implementation project to protect all public and private APIs

Thank you!

Javier Garza

@jjaviergarza
Slides: https://www.slideshare.net/JavierGarza18

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws



Please complete the session survey in the mobile app.

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws