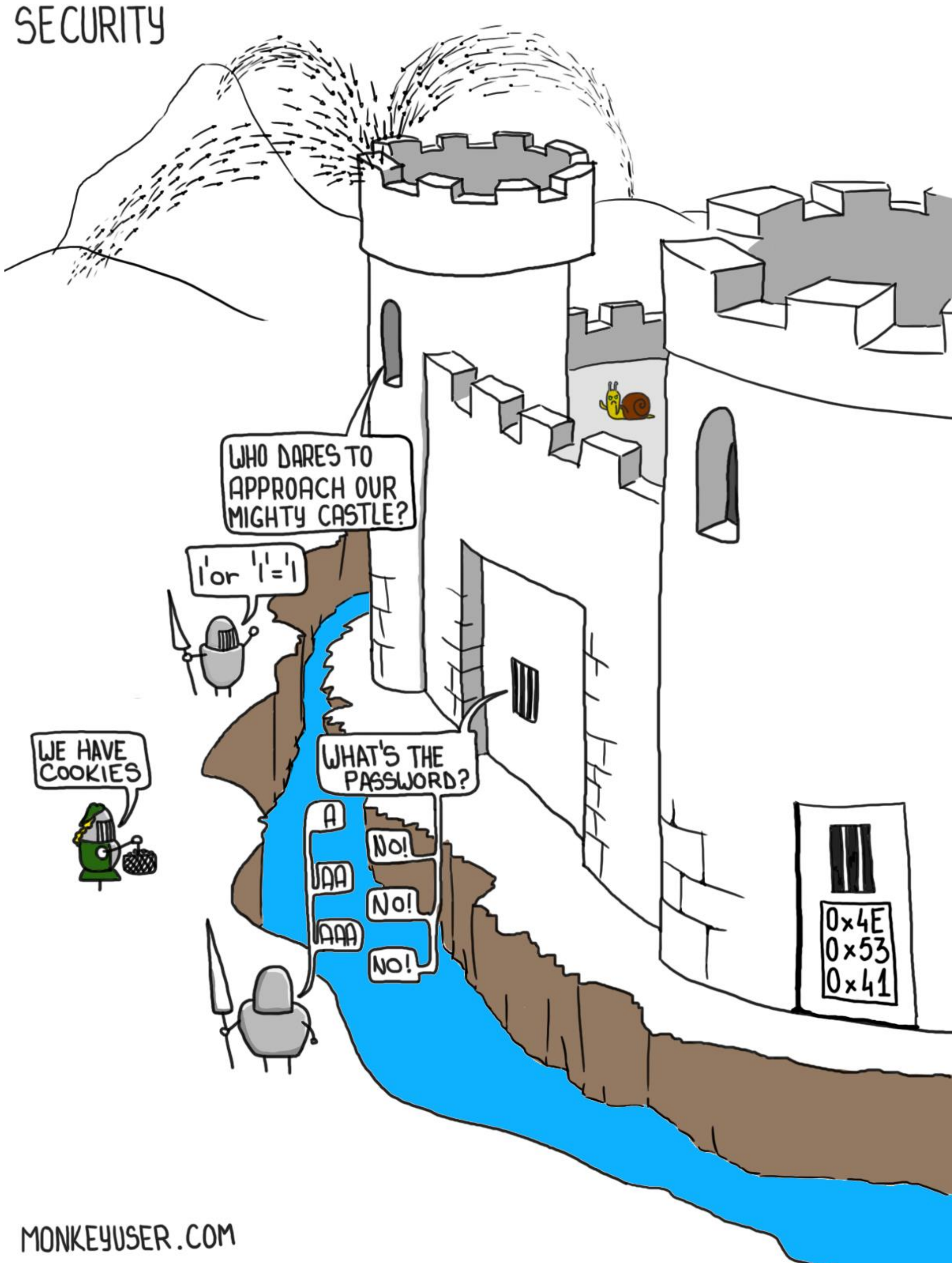
Sú legacy aplikácie bezpečnejšie ako microservices?

LUBOŠ KLOKNER | F5 | SENIOR SOLUTIONS ENGINEER

Security Castle



DATA is the new OIL

APPs are the gateways to DATA

APPs are Moving to an API Based Architecture

API = The Gateway to Digital Transformation

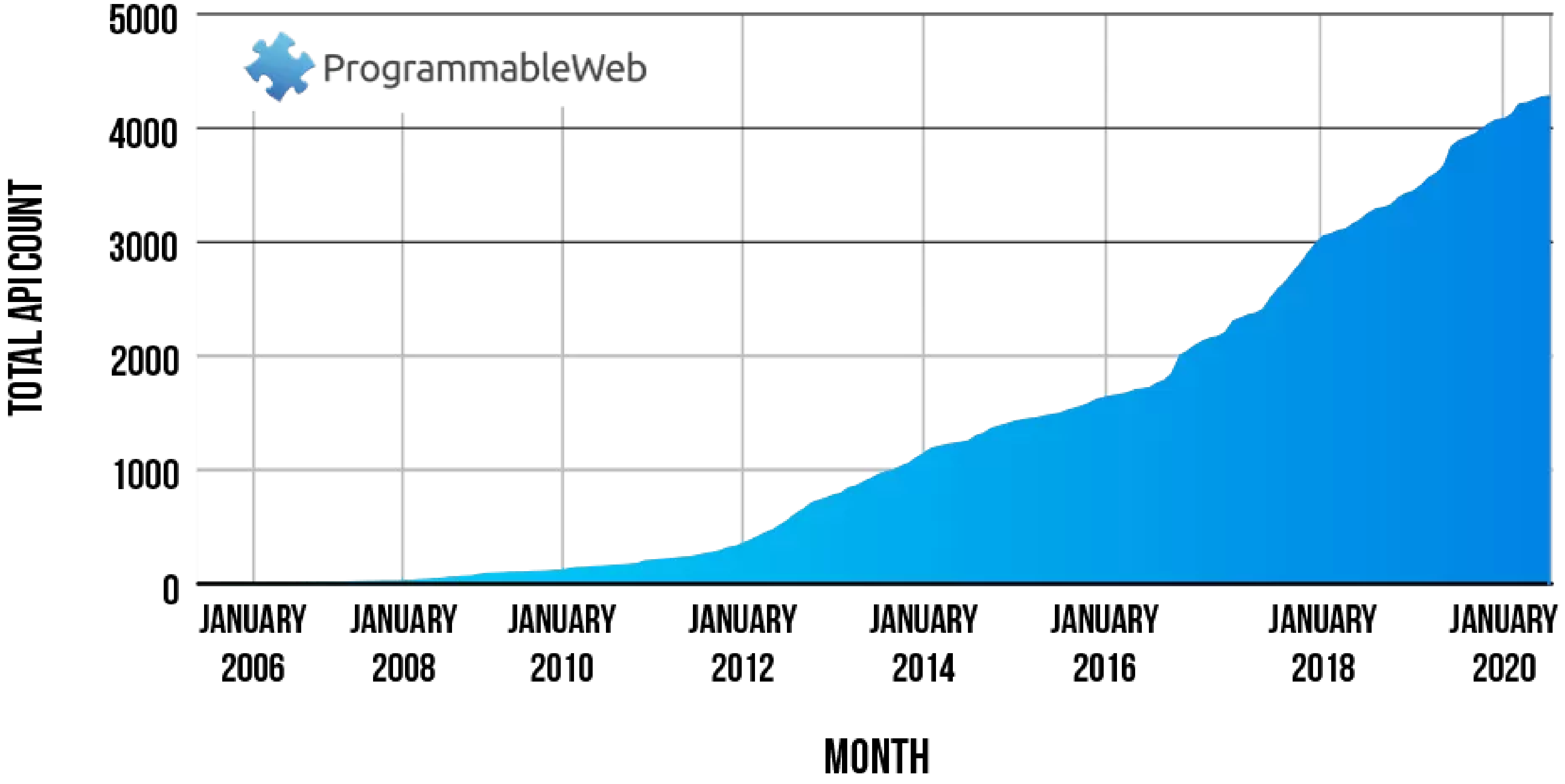
Learning APIs

HISTORY LESSON

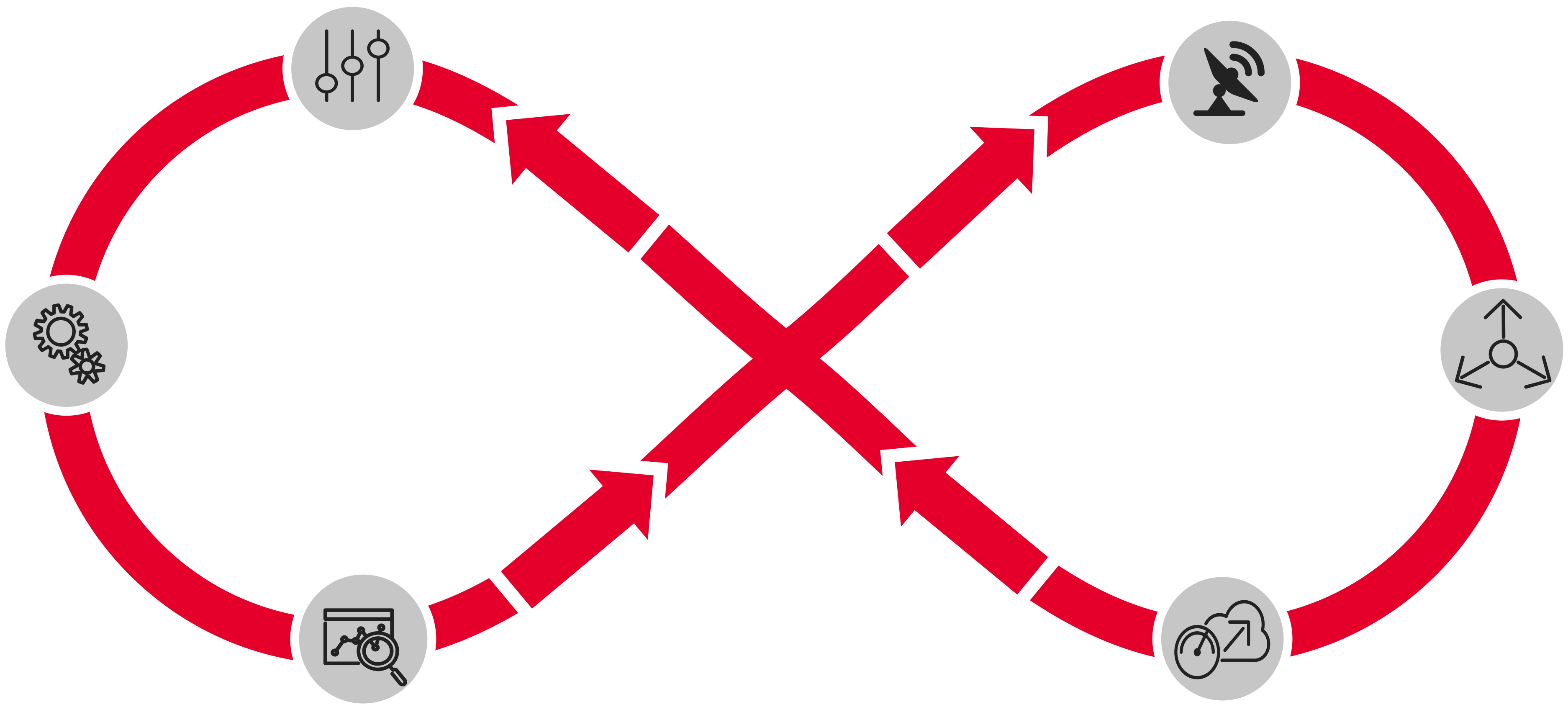
How we USED to build Apps

How we NOW build Apps

GROWTH IN FINANCIAL RELATED (FINANCIAL, BANKING, PAYMENTS, MONETIZATION) APIS SINCE 2005



Rapid Feedback & Innovation Cycle



Configure / Deploy
Self Service

Feedback
Customer Interaction

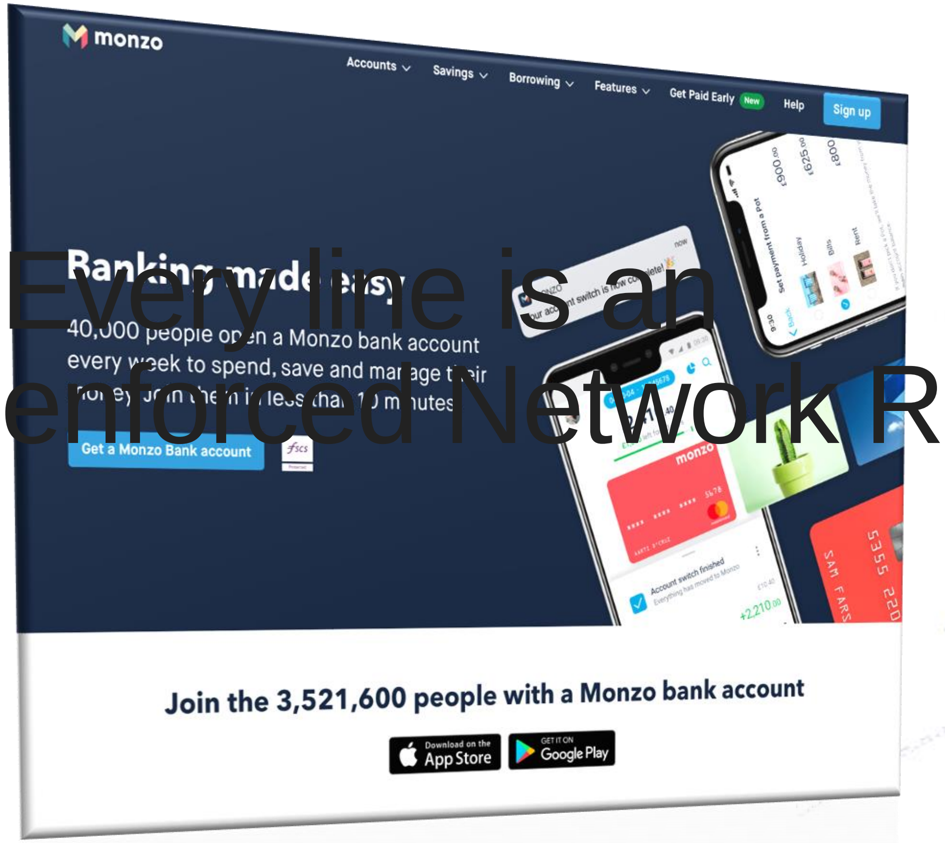
Use
Flexible Consumption

Improve
Agile Driven Development

Understand
Real Time Analytics and Insights

Release
Continuous Rapid Releases

1500 Microservices at Monzo



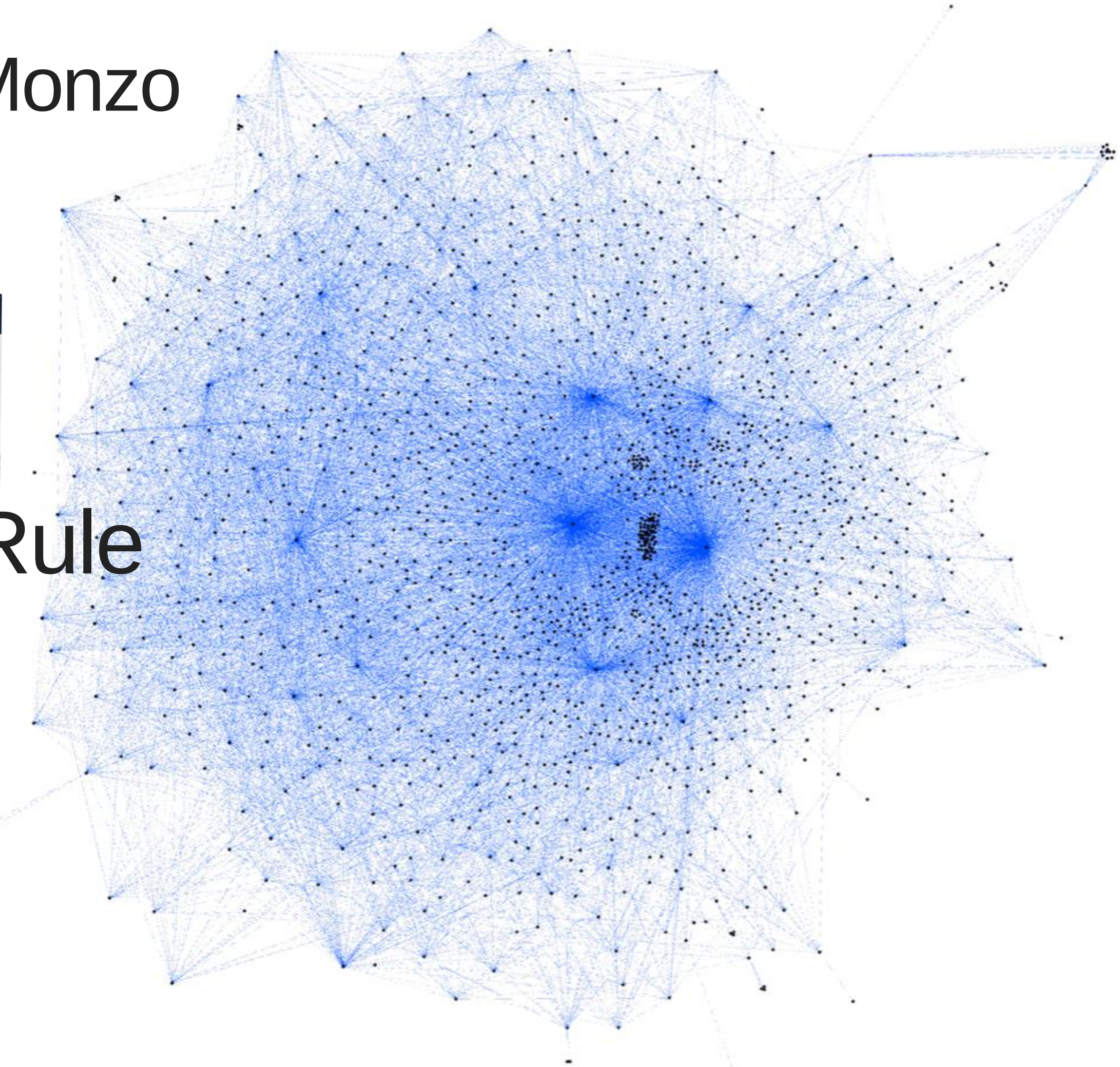
Banking made easy

40,000 people open a Monzo bank account every week to spend, save and manage their money. Join them in less than 10 minutes.

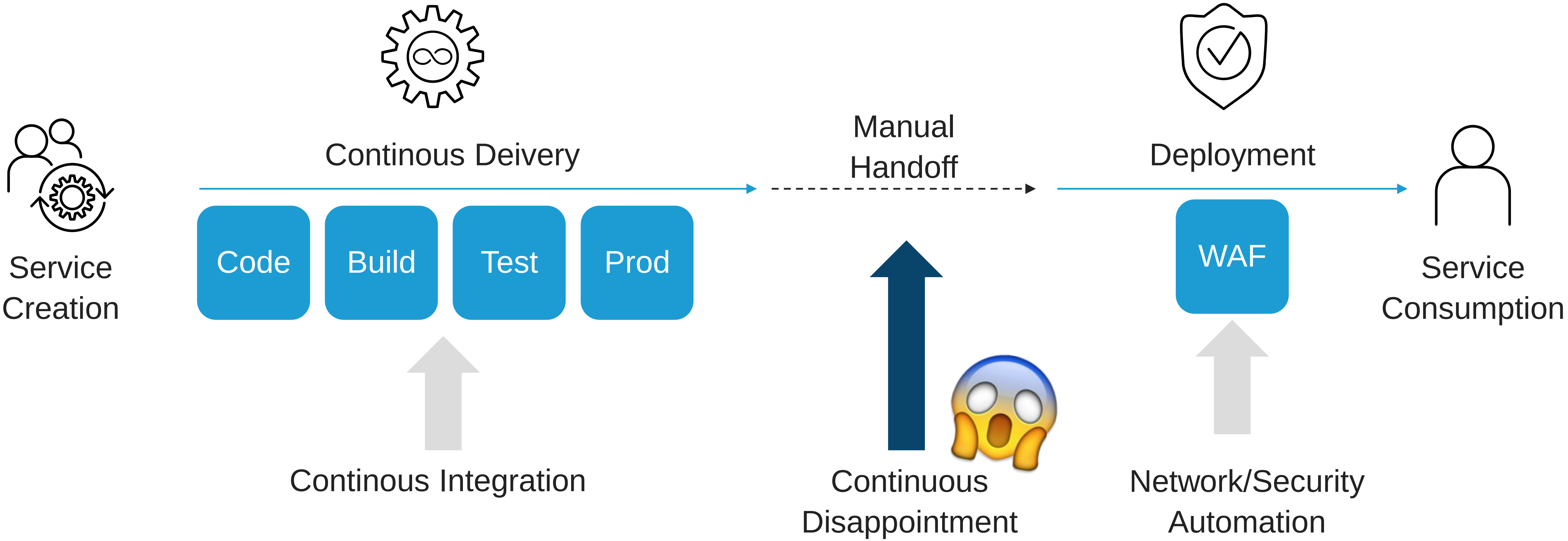
Get a Monzo Bank account

Join the 3,521,600 people with a Monzo bank account

Every line is an enforced Network Rule



CI/CD Pipeline



Service Creation

Continous Deivery

Code

Build

Test

Prod

Continous Integration

Manual Handoff

Continuous Disappointment

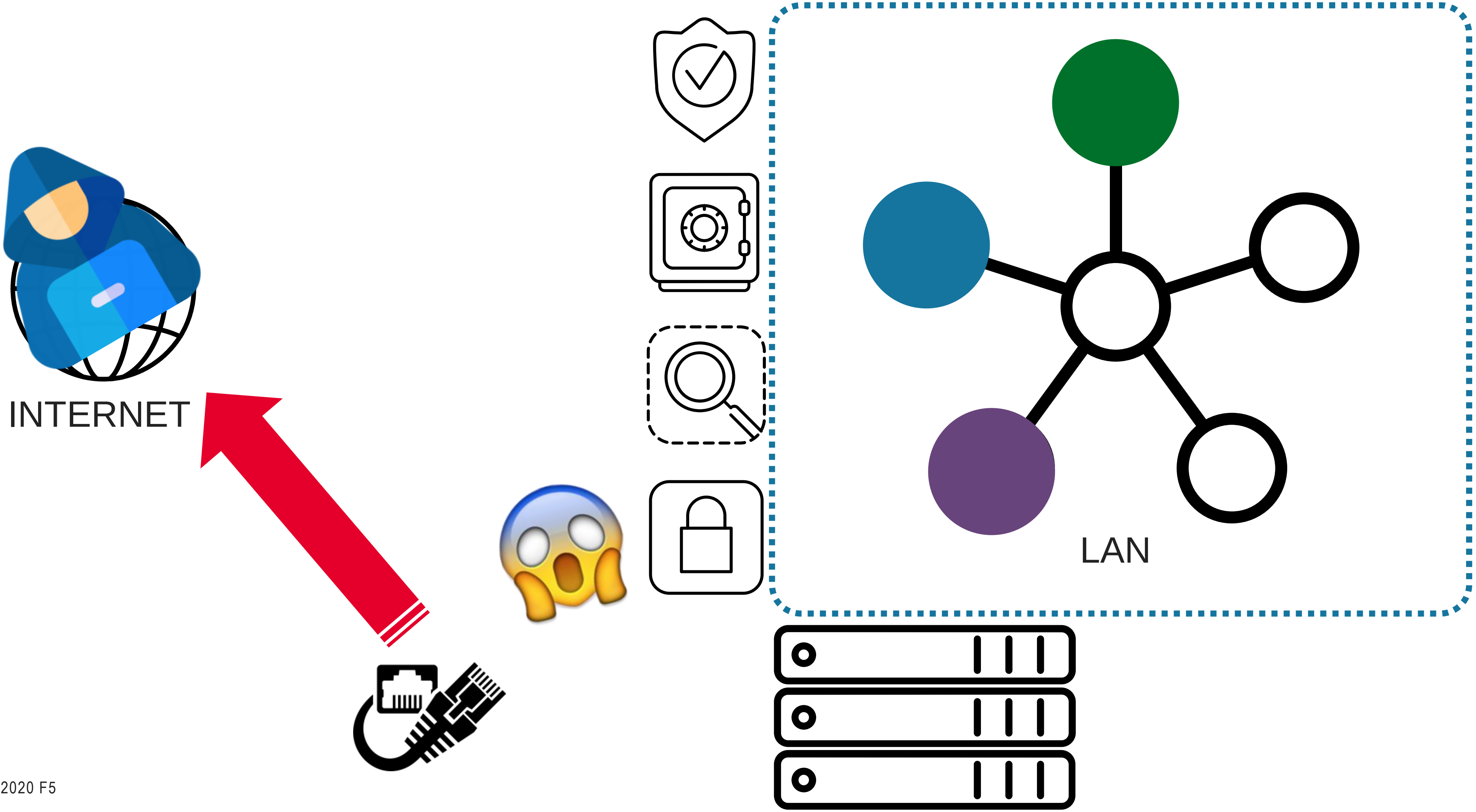
Deployment

WAF

Network/Security Automation

Service Consumption

Agile way…



> “By 2022, API abuses will be the most-frequent attack vector resulting in data breaches…”

Gartner

A Modern App?

node JS®

JSON

mongoDB®

GraphQL

php

OpenID

nosql

ASP.NET™

python™

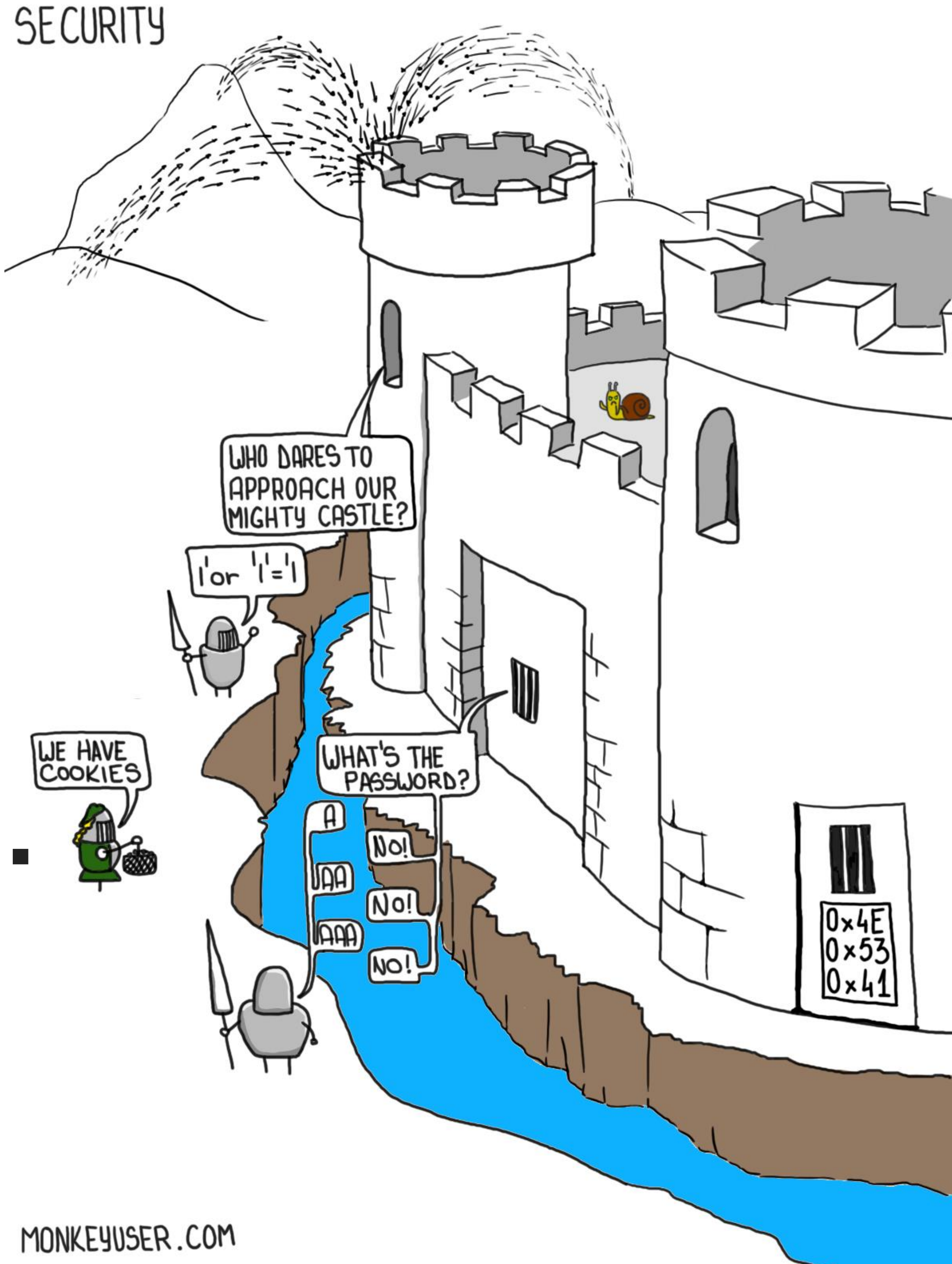
gRPC

JavaScript

JSP

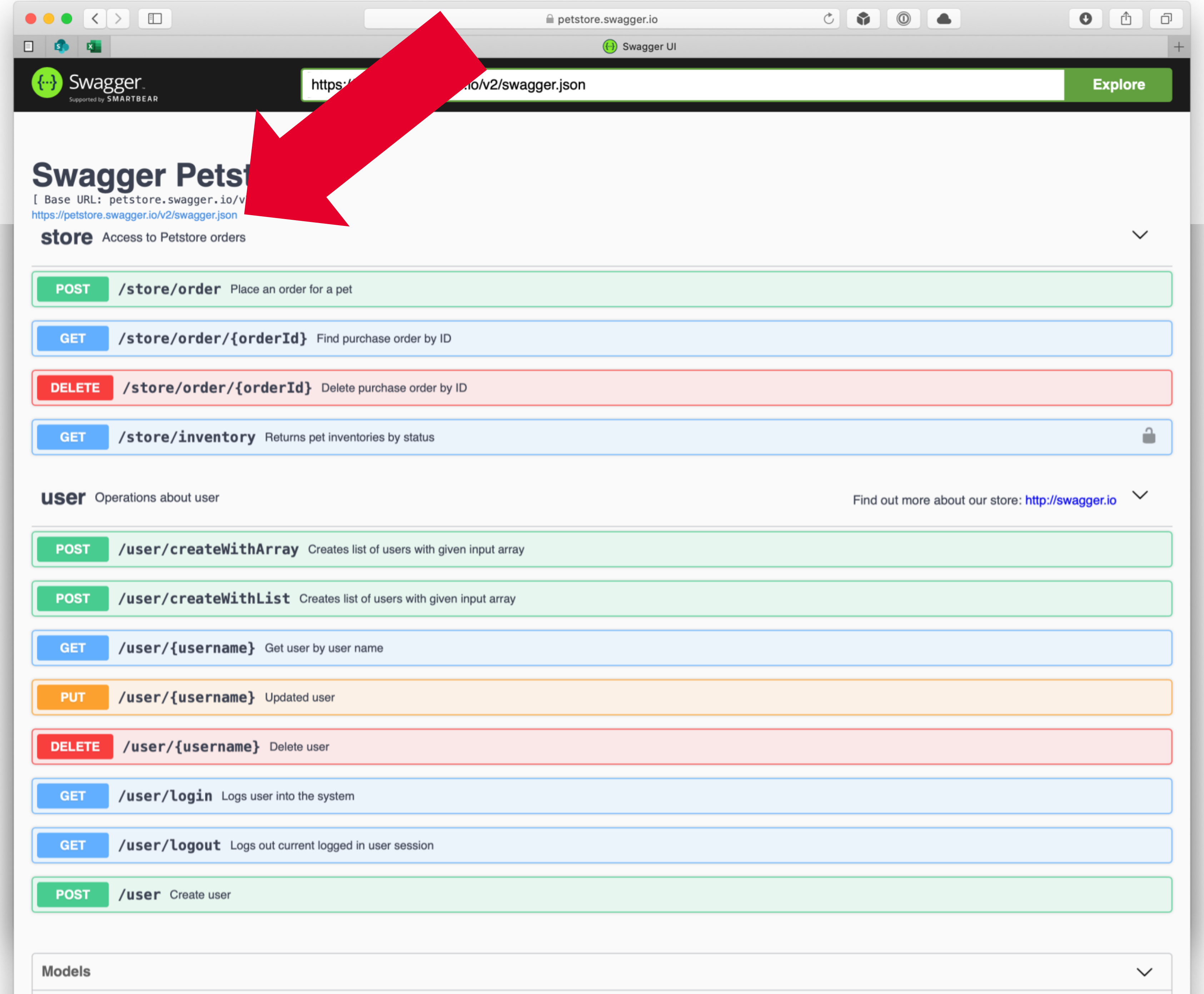
<xml />

Security Castle of a Modern App…



Developers at the beginning of a project

Developers at the end of a project



https:/ .io/v2/swagger.json

Swagger Petst

[Base URL: petstore.swagger.io/v

https://petstore.swagger.io/v2/swagger.json

store Access to Petstore orders

- 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

user Operations about user

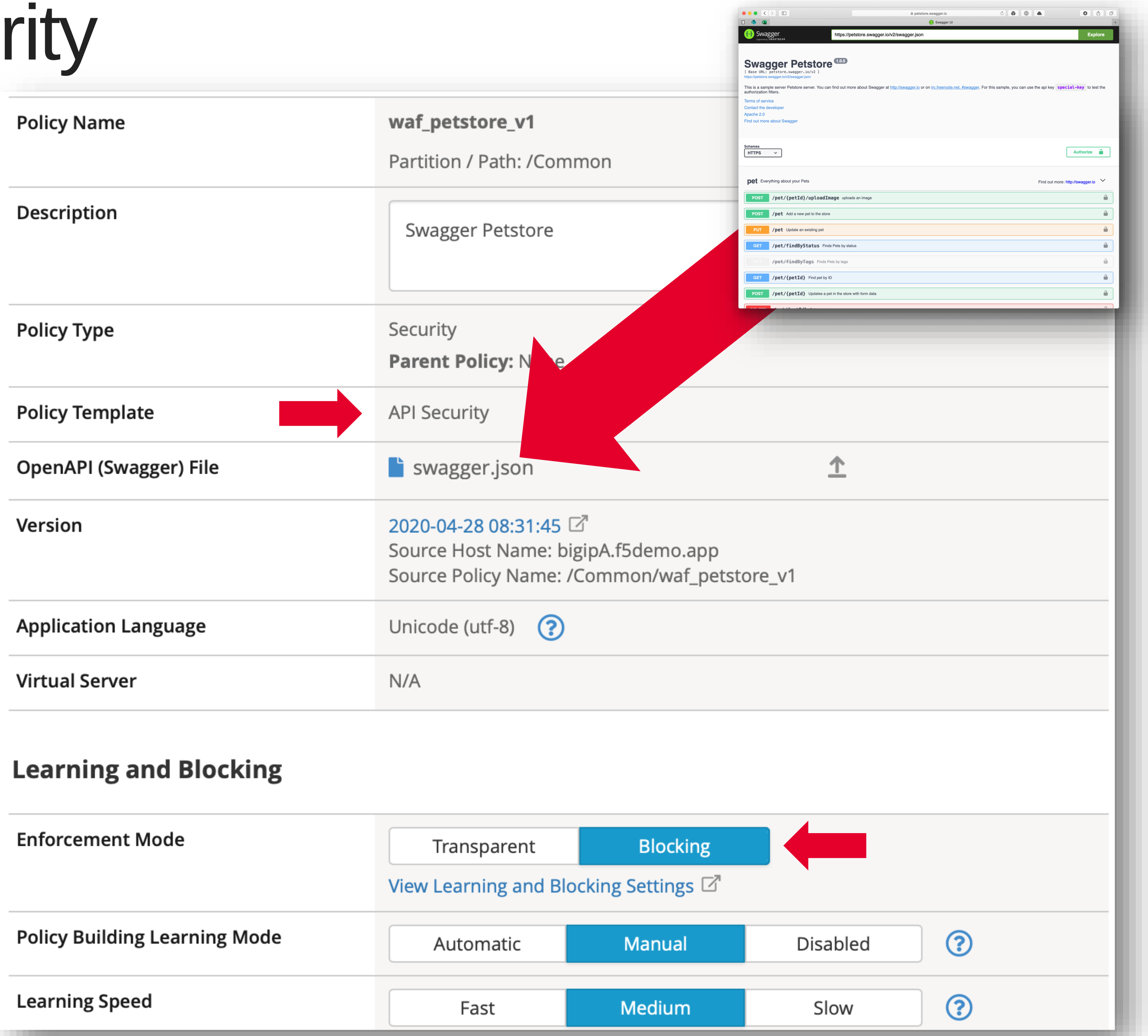
Find out more about our store: http://swagger.io

- 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
- GET `/user/logout` Logs out current logged in user session
- POST `/user` Create user

Models

Modern App Security

ADVANCED WAF POLICY



petstore.swagger.io

Swagger UI

Swagger

https://petstore.swagger.io/v2/swagger.json

Explore

Swagger Petstore 1.0.5

[Base URL: petstore.swagger.io/v2]

https://petstore.swagger.io/v2/swagger.json

This is a sample server Petstore server. You can find out more about Swagger at http://swagger.io or on irc.freenode.net, #swagger. For this sample, you can use the api key `special-key` to test the authorization filters.

Terms of service

Contact the developer

Apache 2.0

Find out more about Swagger

Schemes: HTTPS

Authorize

pet Everything about your Pets — Find out more: http://swagger.io

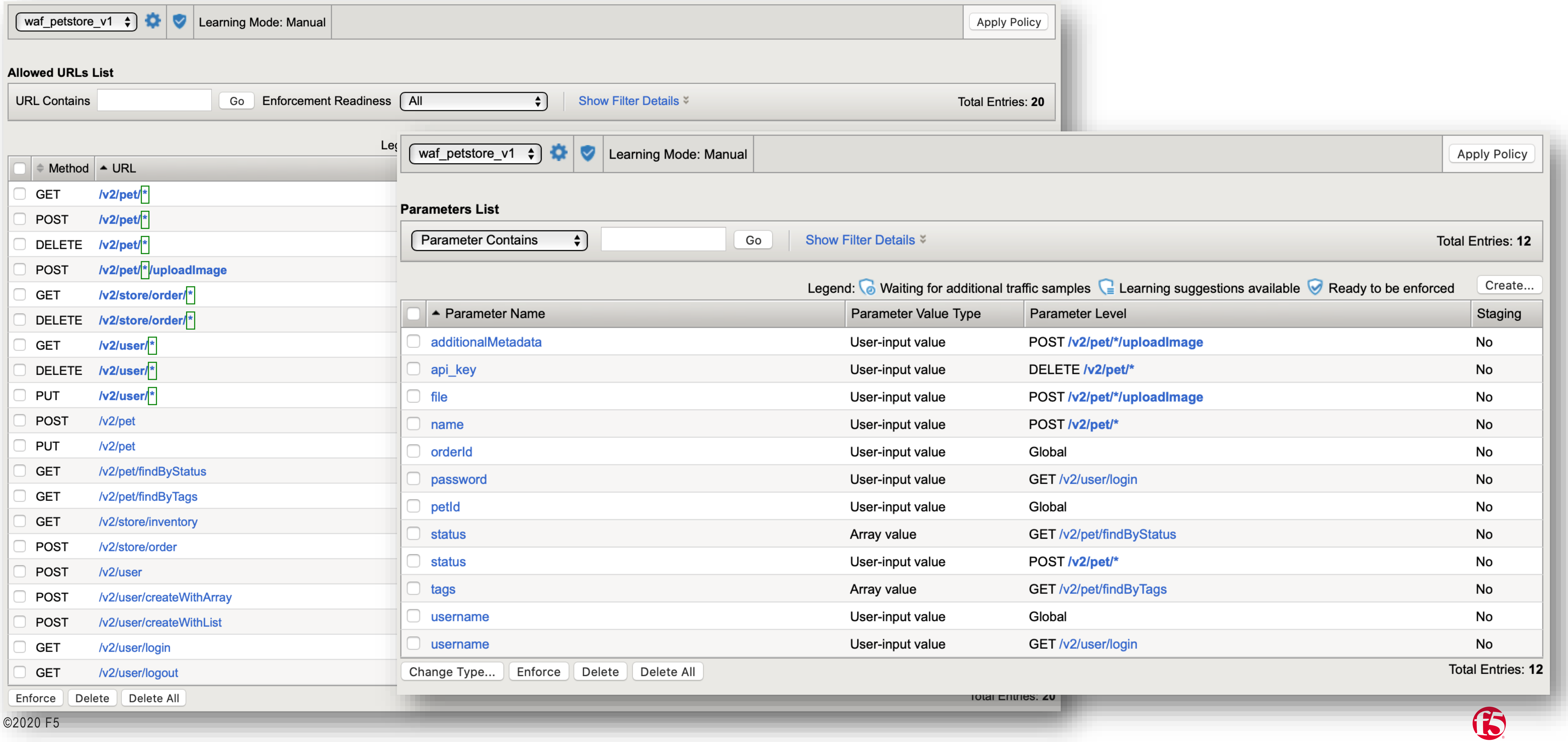
POST	`/pet/{petId}/uploadImage`	uploads an image
POST	`/pet`	Add a new pet to the store
PUT	`/pet`	Update an existing pet
GET	`/pet/findByStatus`	Finds Pets by status
GET	~~`/pet/findByTags`~~	Finds Pets by tags
GET	`/pet/{petId}`	Find pet by ID
POST	`/pet/{petId}`	Updates a pet in the store with form data

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

Modern App Security



Allowed URLs List

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

□	Method	URL
□	GET	/v2/pet/*
□	POST	/v2/pet/*
□	DELETE	/v2/pet/*
□	POST	/v2/pet/*/uploadImage
□	GET	/v2/store/order/*
□	DELETE	/v2/store/order/*
□	GET	/v2/user/*
□	DELETE	/v2/user/*
□	PUT	/v2/user/*
□	POST	/v2/pet
□	PUT	/v2/pet
□	GET	/v2/pet/findByStatus
□	GET	/v2/pet/findByTags
□	GET	/v2/store/inventory
□	POST	/v2/store/order
□	POST	/v2/user
□	POST	/v2/user/createWithArray
□	POST	/v2/user/createWithList
□	GET	/v2/user/login
□	GET	/v2/user/logout

Parameters List

Parameter Contains Go Show Filter Details Total Entries: **12**

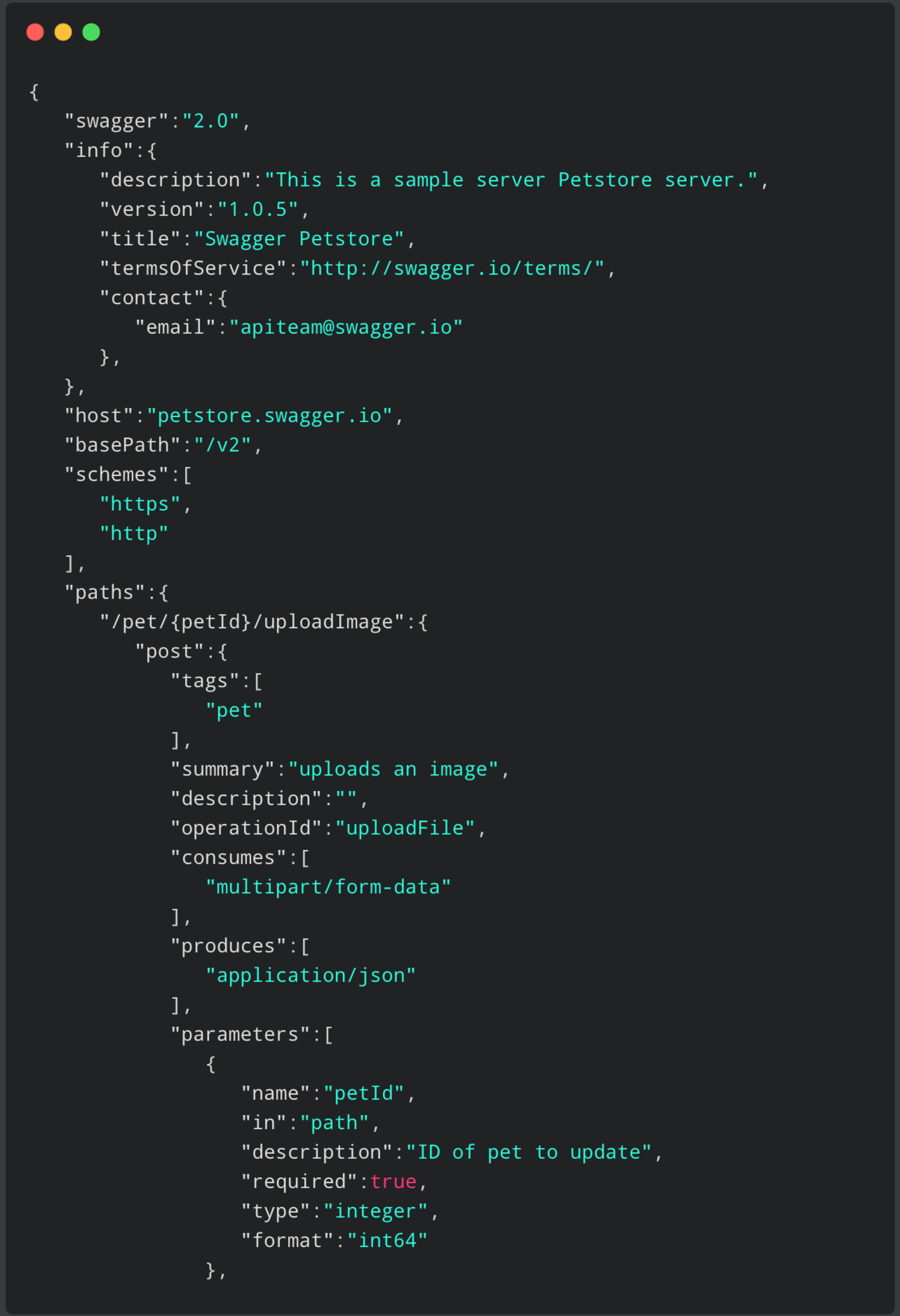
Legend: Waiting for additional traffic samples Learning suggestions available Ready to be enforced

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

Total Entries: **12**

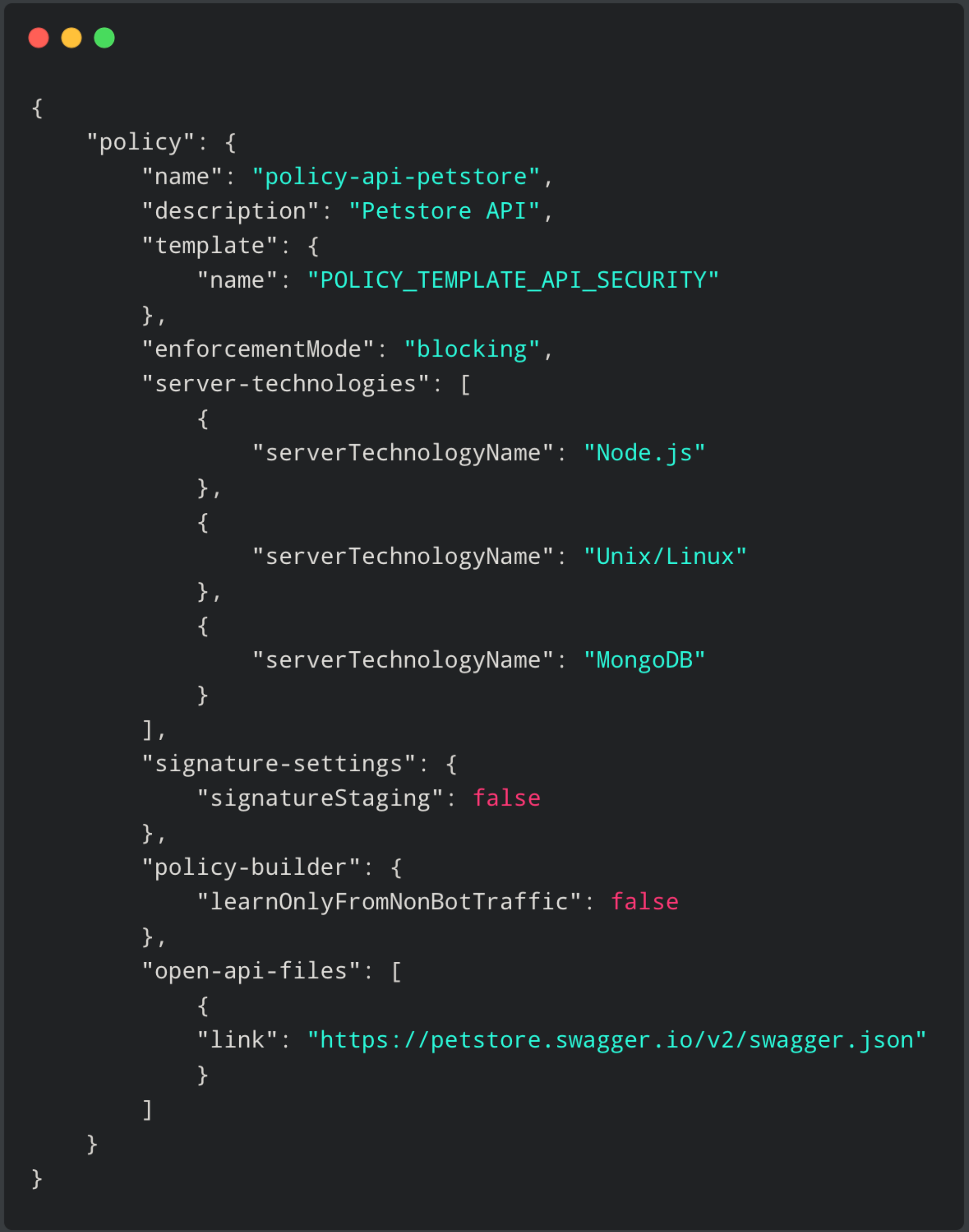
WAF Easy

- Single File (JSON, YAML)
- Can Share Settings from **Parent Policy**
- **Positive** Security
- **No Learning**
- In **Blocking** from **Day 1**



```
{
   "swagger":"2.0",
   "info":{
      "description":"This is a sample server Petstore server.",
      "version":"1.0.5",
      "title":"Swagger Petstore",
      "termsOfService":"http://swagger.io/terms/",
      "contact":{
         "email":"apiteam@swagger.io"
      },
   },
   "host":"petstore.swagger.io",
   "basePath":"/v2",
   "schemes":[
      "https",
      "http"
   ],
   "paths":{
      "/pet/{petId}/uploadImage":{
         "post":{
            "tags":[
               "pet"
            ],
            "summary":"uploads an image",
            "description":"",
            "operationId":"uploadFile",
            "consumes":[
               "multipart/form-data"
            ],
            "produces":[
               "application/json"
            ],
            "parameters":[
               {
                  "name":"petId",
                  "in":"path",
                  "description":"ID of pet to update",
                  "required":true,
                  "type":"integer",
                  "format":"int64"
               },
```

WAF CI/CD Compliant

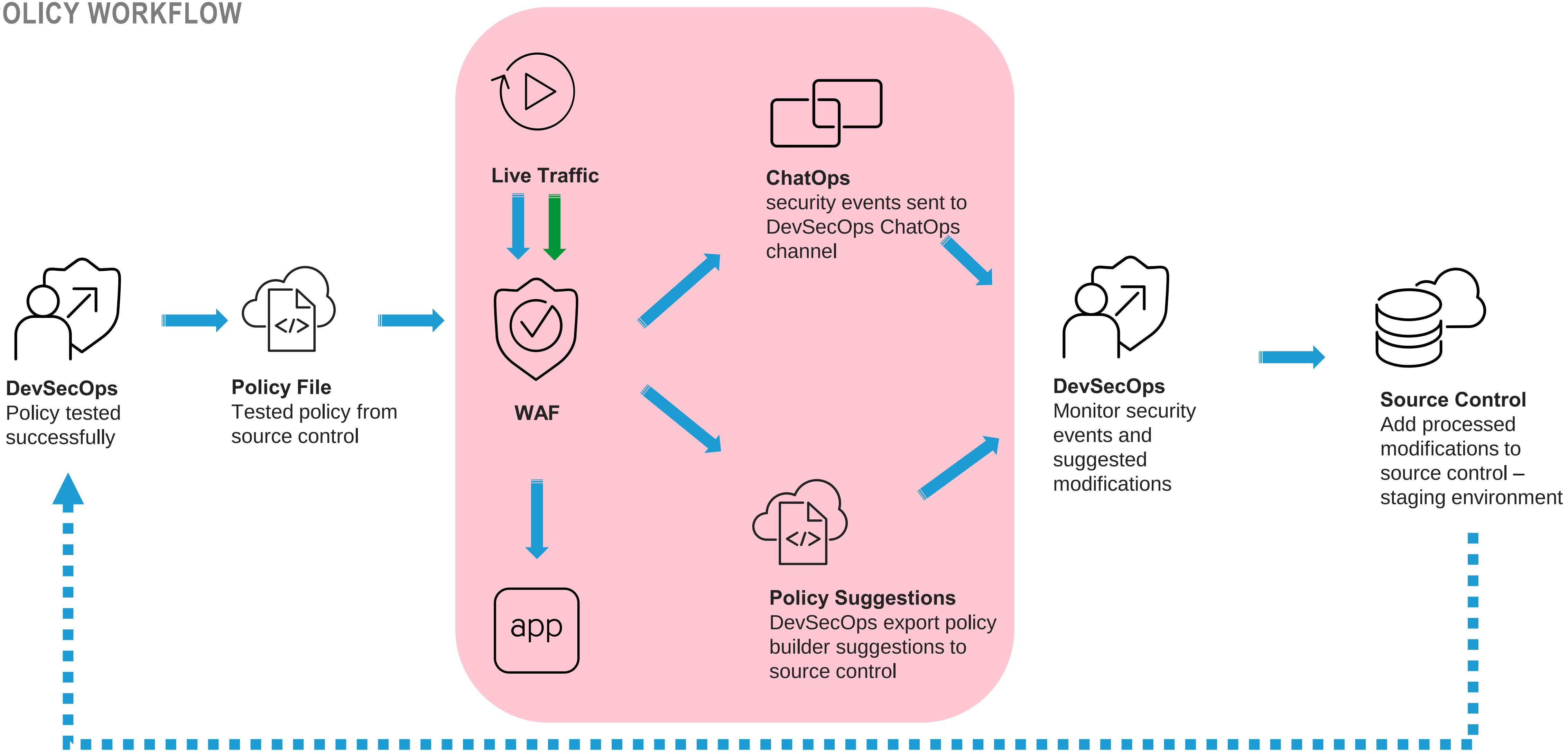


```
{
    "policy": {
        "name": "policy-api-petstore",
        "description": "Petstore API",
        "template": {
            "name": "POLICY_TEMPLATE_API_SECURITY"
        },
        "enforcementMode": "blocking",
        "server-technologies": [
            {
                "serverTechnologyName": "Node.js"
            },
            {
                "serverTechnologyName": "Unix/Linux"
            },
            {
                "serverTechnologyName": "MongoDB"
            }
        ],
        "signature-settings": {
            "signatureStaging": false
        },
        "policy-builder": {
            "learnOnlyFromNonBotTraffic": false
        },
        "open-api-files": [
            {
            "link": "https://petstore.swagger.io/v2/swagger.json"
            }
        ]
    }
}
```

- Ability to consume **JSON Declarative** format
- Ability to **PULL** the **OpenAPI**/Swagger files
- Policy **Modifications / Patching**
- Webhooks for integration with **Slack/Teams**
- Send event logs in **JSON** format

F5 AWAF as part of your CI/CD

POLICY WORKFLOW



DevSecOps
Policy tested successfully

Policy File
Tested policy from source control

Live Traffic

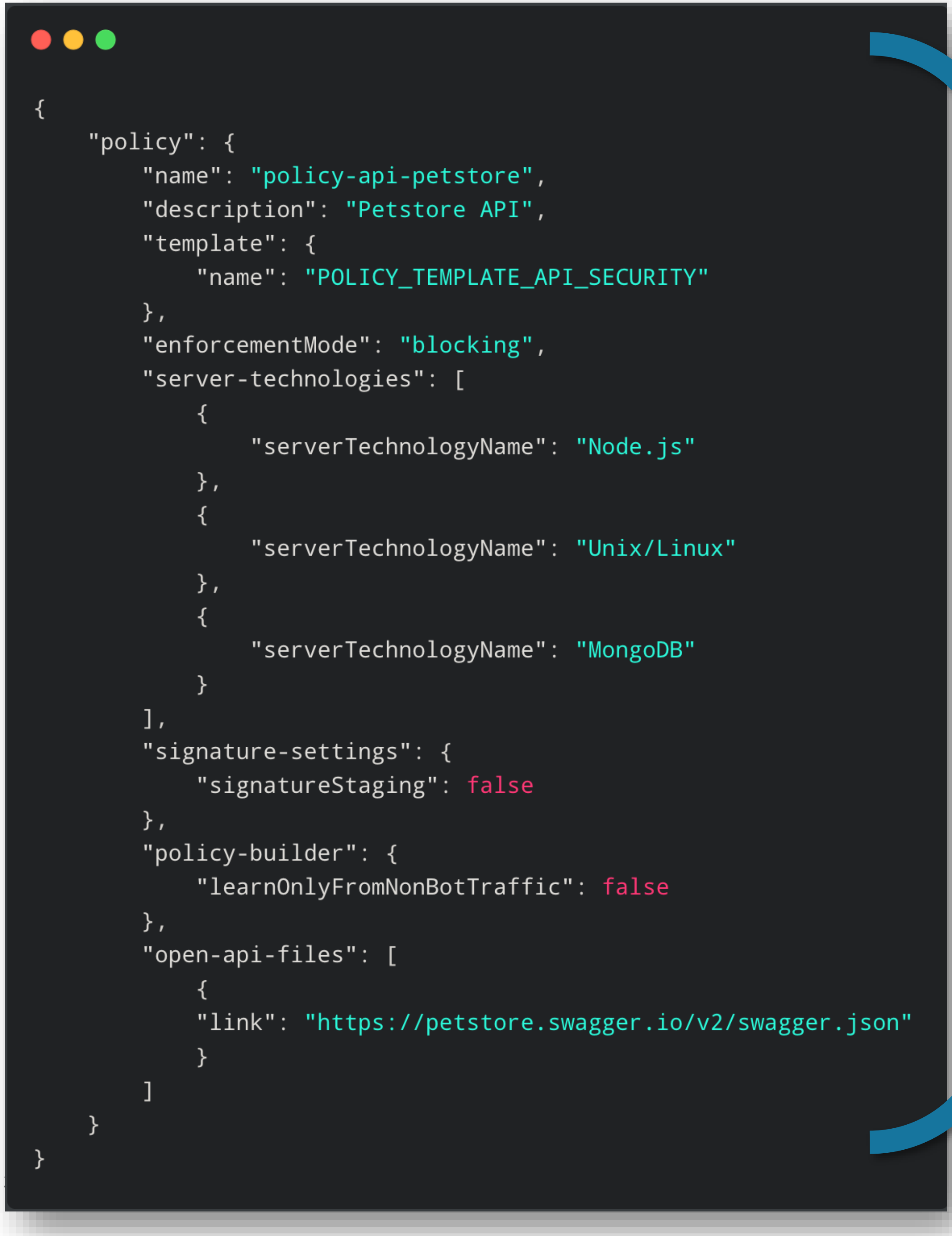
WAF

ChatOps
security events sent to DevSecOps ChatOps channel

Policy Suggestions
DevSecOps export policy builder suggestions to source control

DevSecOps
Monitor security events and suggested modifications

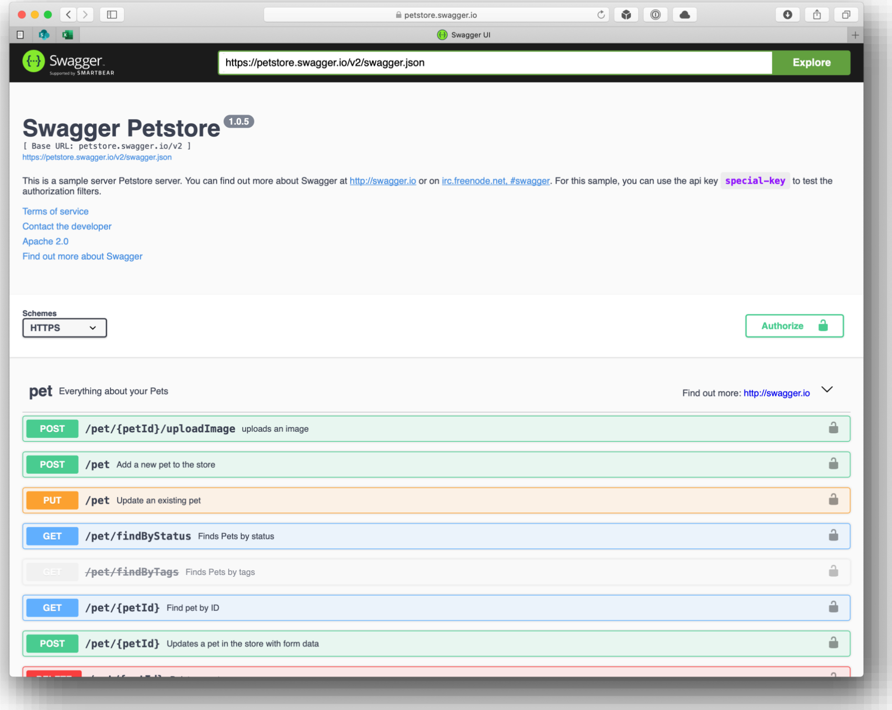
Source Control
Add processed modifications to source control – staging environment



```
{
    "policy": {
        "name": "policy-api-petstore",
        "description": "Petstore API",
        "template": {
            "name": "POLICY_TEMPLATE_API_SECURITY"
        },
        "enforcementMode": "blocking",
        "server-technologies": [
            {
                "serverTechnologyName": "Node.js"
            },
            {
                "serverTechnologyName": "Unix/Linux"
            },
            {
                "serverTechnologyName": "MongoDB"
            }
        ],
        "signature-settings": {
            "signatureStaging": false
        },
        "policy-builder": {
            "learnOnlyFromNonBotTraffic": false
        },
        "open-api-files": [
            {
            "link": "https://petstore.swagger.io/v2/swagger.json"
            }
        ]
    }
}
```

F5 AWAF

NGINX App Protect



petstore.swagger.io

Swagger UI

Swagger Supported by SMARTBEAR

https://petstore.swagger.io/v2/swagger.json Explore

Swagger Petstore 1.0.5

[Base URL: petstore.swagger.io/v2]
https://petstore.swagger.io/v2/swagger.json

This is a sample server Petstore server. You can find out more about Swagger at http://swagger.io or on irc.freenode.net, #swagger. For this sample, you can use the api key `special-key` to test the authorization filters.

Terms of service
Contact the developer
Apache 2.0
Find out more about Swagger

Schemes
HTTPS

Authorize

pet Everything about your Pets — Find out more: http://swagger.io

- POST `/pet/{petId}/uploadImage` uploads an image
- POST `/pet` Add a new pet to the store
- PUT `/pet` Update an existing pet
- GET `/pet/findByStatus` Finds Pets by status
- GET ~~`/pet/findByTags`~~ Finds Pets by tags
- GET `/pet/{petId}` Find pet by ID
- POST `/pet/{petId}` Updates a pet in the store with form data

Any Deployment & Any Tool

elastic
GitLab
CHEF
Prometheus
N+
SHAPE
Part of F5
f5
Jenkins
ANSIBLE
GitHub
Terraform
Google Cloud Platform
Azure
aws