



Automated API Security

LUBOŠ KLOKNER | **F5** | SR. SOLUTIONS ENGINEER

Applications are the most valuable asset

OF THE MODERN ENTERPRISE



Physical Capital

Ford

Carnegie

Rockefeller



Human Capital

IBM

McKinsey & Company



Application Capital

Waze

Moovit

Revolut

Nike

The image features a silhouette of an oil pumpjack against a vibrant sunset sky. The sun is a bright yellow circle positioned in the lower-left quadrant, partially obscured by a dark silhouette of a forest. The sky transitions from a deep orange near the horizon to a darker, almost black, at the top. The pumpjack is a large, dark silhouette on the right side of the frame, with its characteristic walking beam and counterweights. The text "DATA is the new OIL" is written in a bold, white, sans-serif font across the center of the image, overlapping the sunset and the pumpjack.

DATA is the new OIL

A person with dark hair is seen from behind, sitting at a table in a cafe. They are using a laptop. On the table next to the laptop is a smartphone displaying a video call. The background is a blurred cafe interior with other people and warm lighting. The text "APPs are the gateway to DATA" is overlaid in white, bold, sans-serif font across the center of the image.

APPs are the gateway to DATA

Learning APIs

HISTORY LESSON

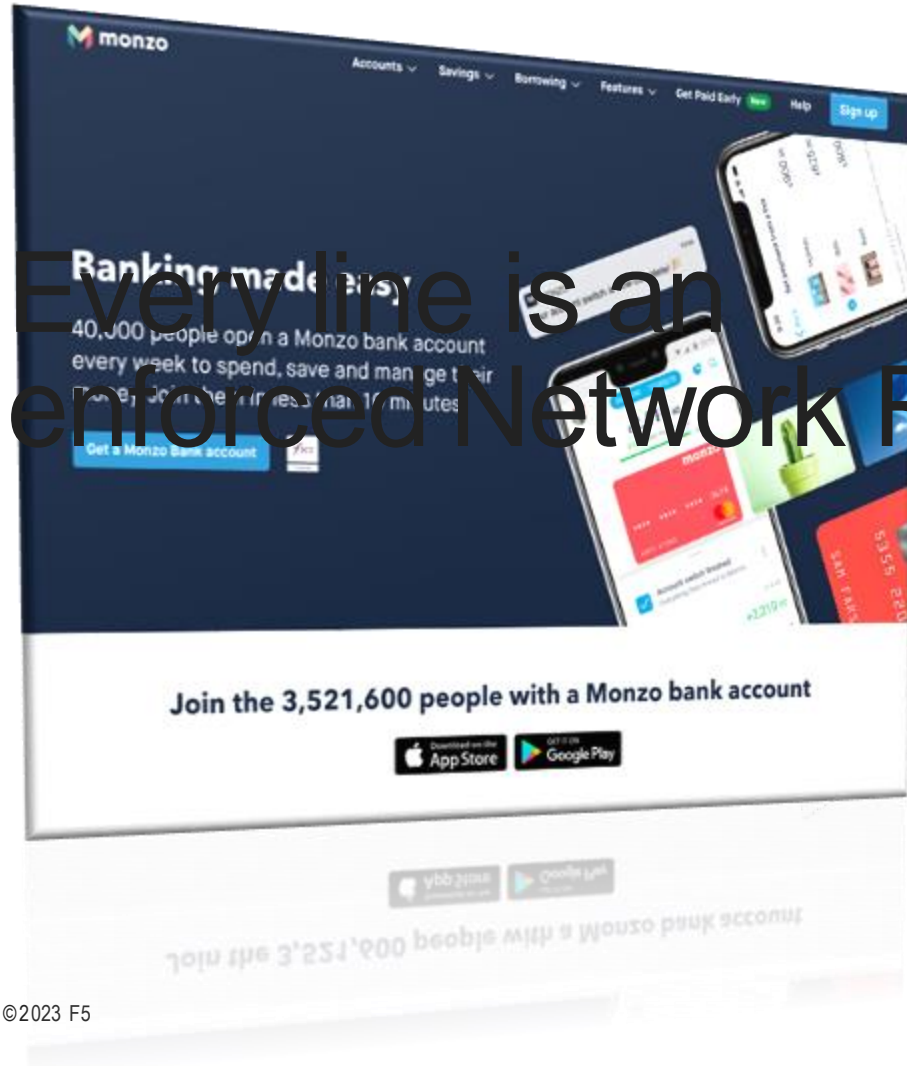
How we **USED** to build Apps



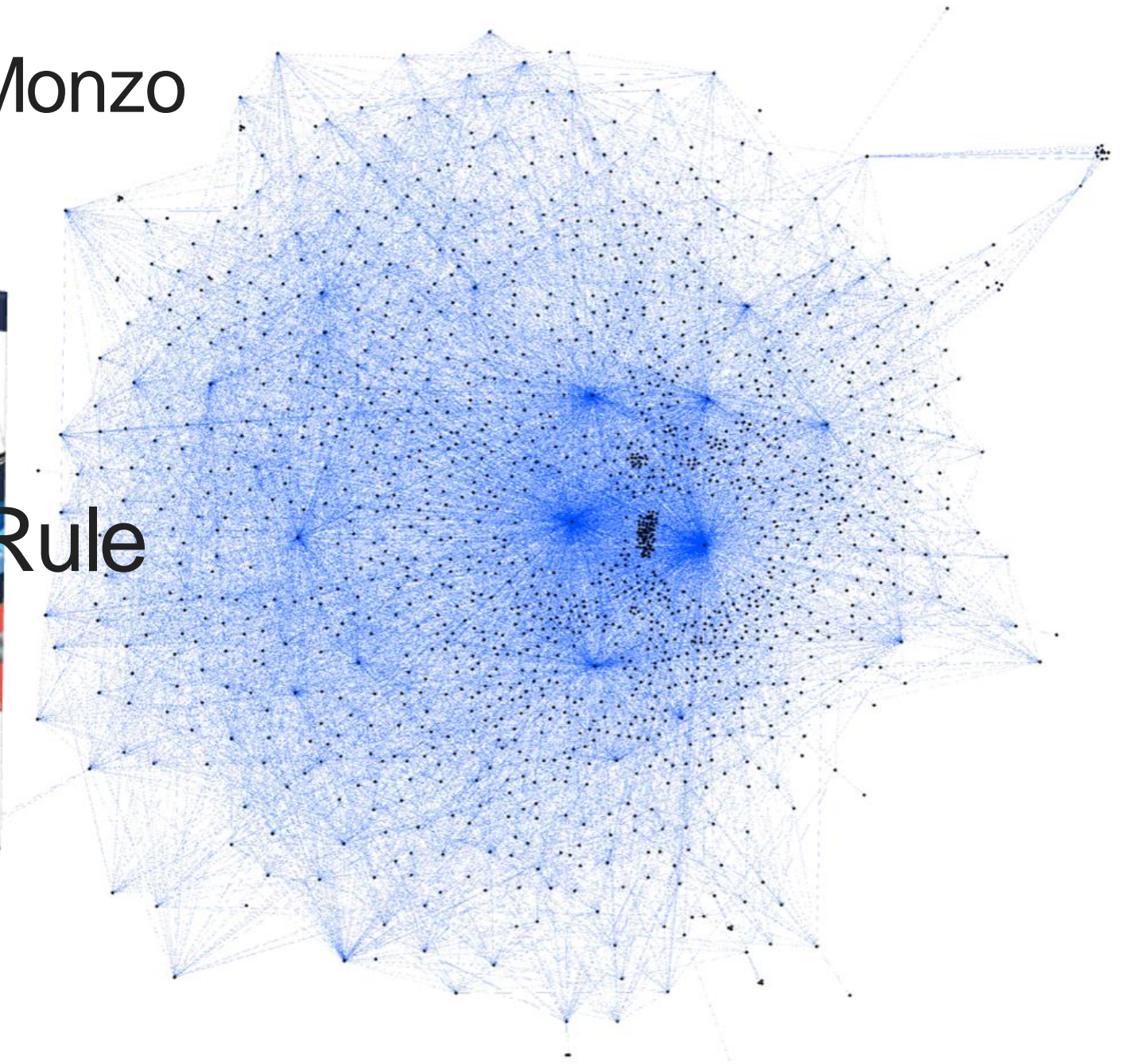
How we **NOW** build Apps



1500 Microservices at Monzo



Every line is an enforced Network Rule

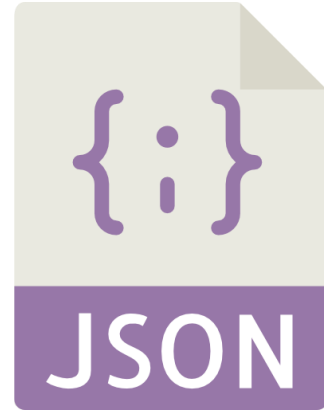


“...API attacks would be the most common attack vector in 2022, resulting in data breaches for enterprise web applications.

...by **2024, API abuses** and related data breaches **will double.**”

Gartner

A Modern App?



mongoDB®



nosql



OpenID

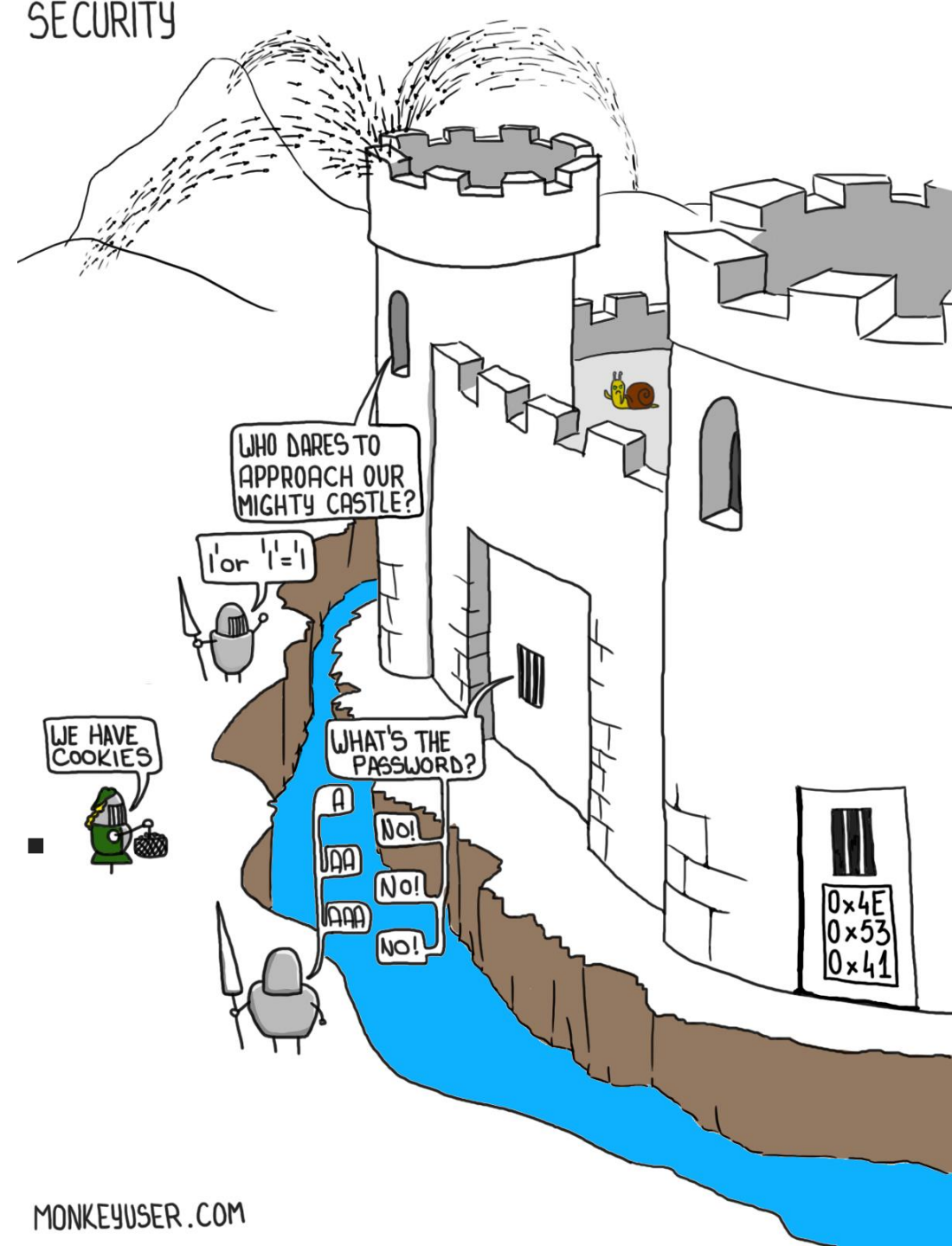


python™

<xml />



Security Castle of a Modern App....



Developers at the **beginning** of a project



Developers at the **end** of a project



petstore.swagger.io Swagger UI


Swagger Supported by SMARTBEAR

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

Swagger Petstore

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

store Access to Petstore orders

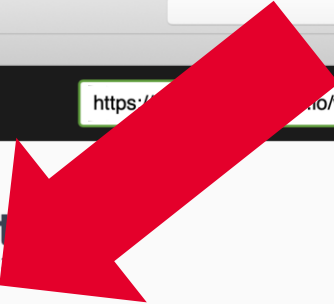
- POST** `/store/order` Place an order for a pet
- GET** `/store/order/{orderId}` Find purchase order by ID
- DELETE** `/store/order/{orderId}` Delete purchase order by ID
- GET** `/store/inventory` Returns pet inventories by status 

user Operations about user







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

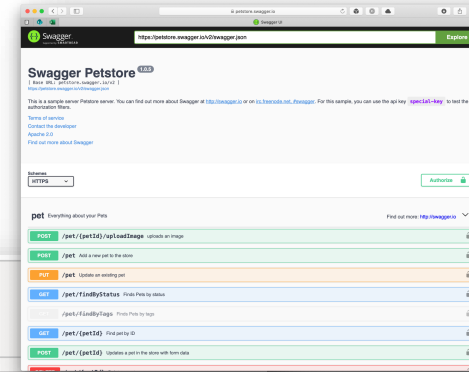
- POST** `/user/createWithArray` Creates list of users with given input array
- POST** `/user/createWithList` Creates list of users with given input array
- GET** `/user/{username}` Get user by user name
- PUT** `/user/{username}` Updated user
- DELETE** `/user/{username}` Delete user
- GET** `/user/login`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

Models



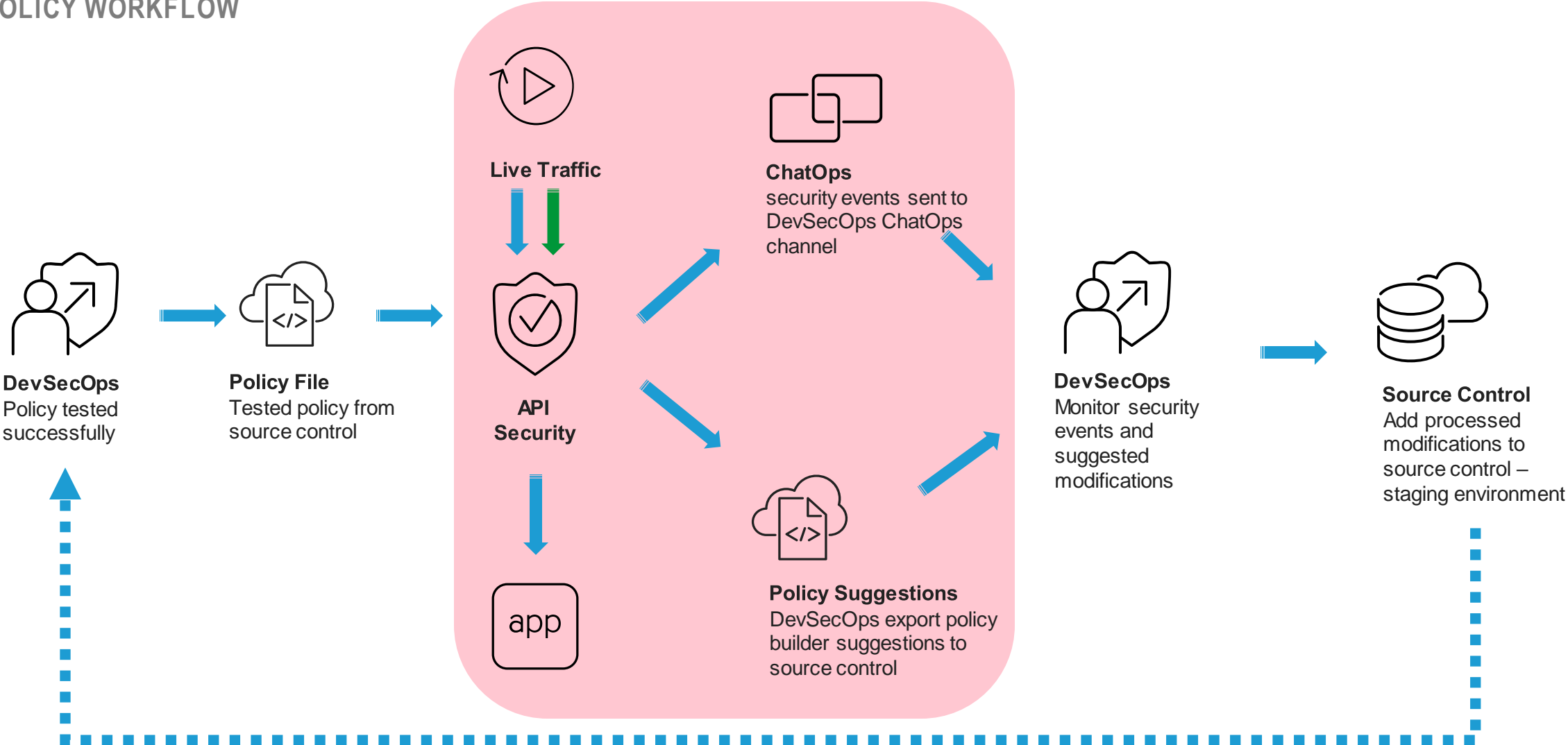
Modern App Security

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	<input type="radio"/> Transparent <input checked="" type="radio"/> Blocking View Learning and Blocking Settings 
Policy Building Learning Mode	<input type="radio"/> Automatic <input checked="" type="radio"/> Manual <input type="radio"/> Disabled 
Learning Speed	<input type="radio"/> Fast <input checked="" type="radio"/> Medium <input type="radio"/> Slow 



F5 API Security as part of your CI/CD

POLICY WORKFLOW



API Security Easy

- Single File (JSON, YAML):
 1. Swagger
 2. Security Policy
- **Positive Security**
- **No Learning = In Blocking from Day 1**
- Available as:
 - **Network Appliance**
 - **Container**
 - **...As A Service**

```
{
  "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"
          }
        ]
      }
    }
  }
}
```

```
{
  "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 WAF CI/CD Compliant

- JSON Declarative format for **F5 AWAFF** and **NGINX AppProtect**
- Ability to **PULL** the OpenAPI/Swagger files
- Policy **modifications**
- Webhooks for integration with **Slack/Teams**
- Send event logs in **JSON** format



F5 AWAF

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 <input type="radio"/> Blocking <input checked="" type="radio"/> View Learning and Blocking Settings
Policy Building Learning Mode	Automatic <input type="radio"/> Manual <input checked="" type="radio"/> Disabled <input type="radio"/>
Learning Speed	Fast <input type="radio"/> Medium <input checked="" type="radio"/> Slow <input type="radio"/>



NGINX AppProtect

```

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

```



Distributed Cloud Services

Form
Documentation
JSON

View

App Firewall
blocking-waf-api

- Metadata
- Enforcement Mode
- Detection Settings
- Advanced configuration

Metadata

Name: blocking-waf-api

Description: Blocking WAF created by Stephen Archer using API

Enforcement Mode: Blocking

Detection Settings

Security Policy: Custom

Attack Signatures

- Attack Types: Default
- Signature Selection By Accuracy: High and Medium

Automatic Attack Signatures Tuning: Enable

Threat Campaigns: Enable

Violations: Default

Signature-Based Bot Protection: Default

Advanced configuration

Allowed Response Status Codes: Default

Cancel and Exit



