BIG COMPASS

WHAT HACKERS DON'T WANT YOU TO KNOW: HOW TO MAXIMIZE YOUR API SECURITY

Azure User Group – September 2020

BIG COMPASS

Overview

1. API Lifecycle
2. API Management
3. Securing an API
4. API Landscape
5. Maximizing API Security

BIG COMPASS

About Big Compass

- Boutique consulting firm
- Specializing in integration and related technologies
- We build connections
  - Systems
  - Apps
  - People
  - Corporations

MuleSoft Boomi webMethods

aws Azure snowflake

CONFLUENT PingIdentity

BIG COMPASS

Attack!

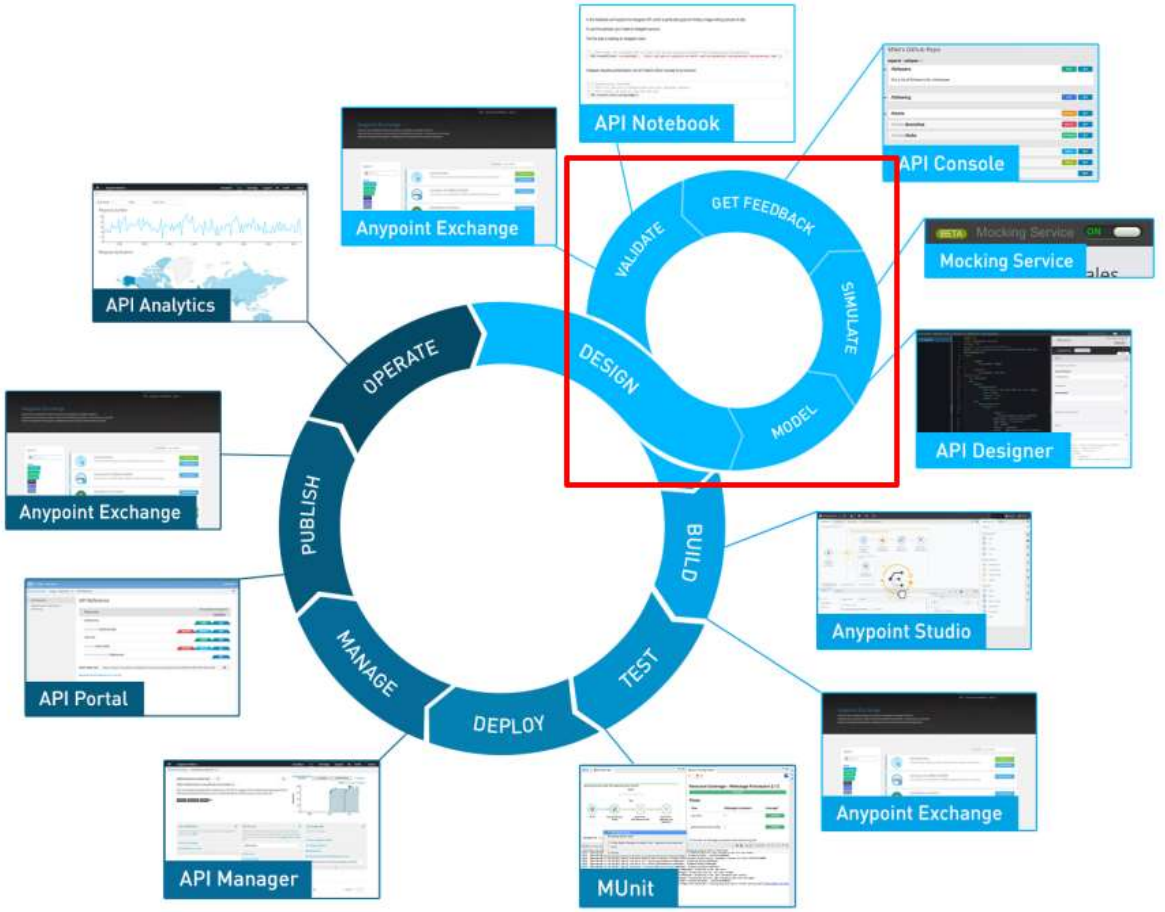
BIG COMPASS

API Lifecycle and Management

BIG COMPASS

API Lifecycle

- Design
- Build
- Test
- Deploy
- Manage



API Management

- Create API
- Connect the API
- Secure
- Manage/Monitor

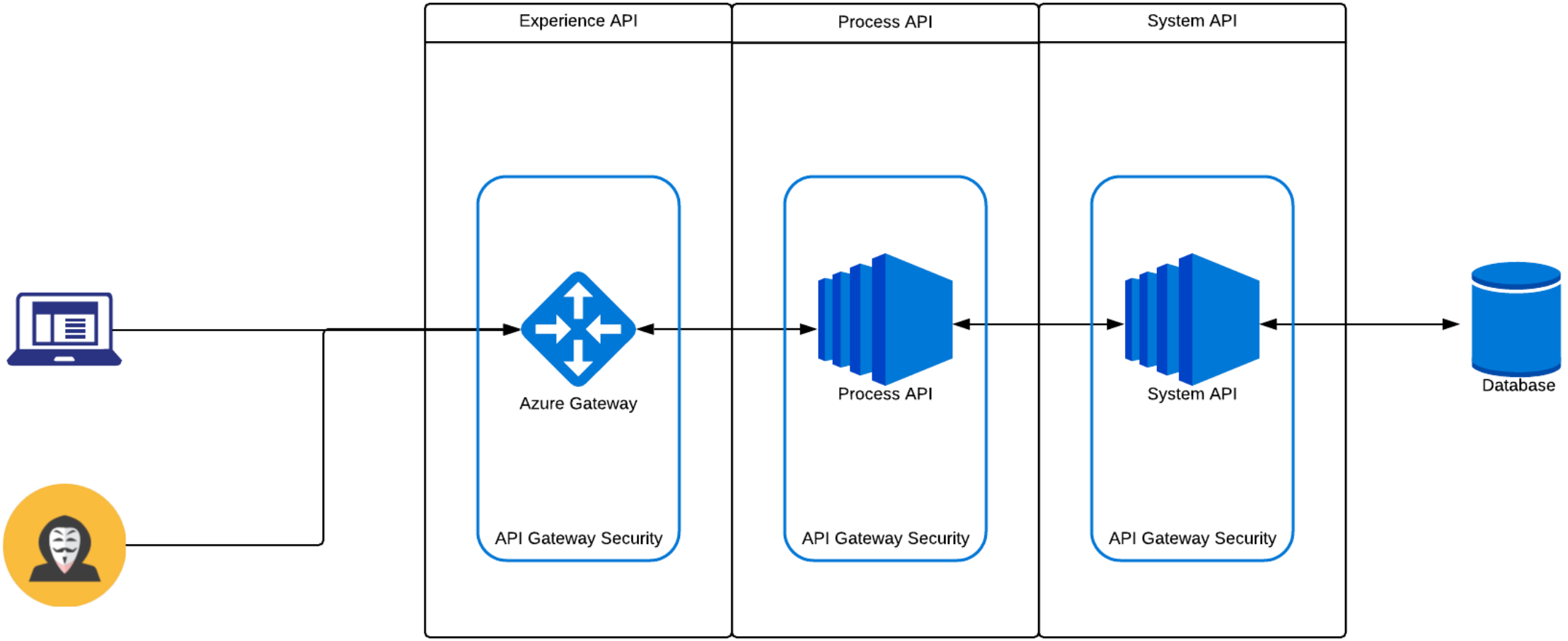
BIG COMPASS

First Line of Defense - Gateway Security

- Basic authentication
- IP whitelisting
- Client ID enforcement
- SLA based rate limiting and throttling
- OAuth 2.0
- JWT
- TLS

BIG COMPASS

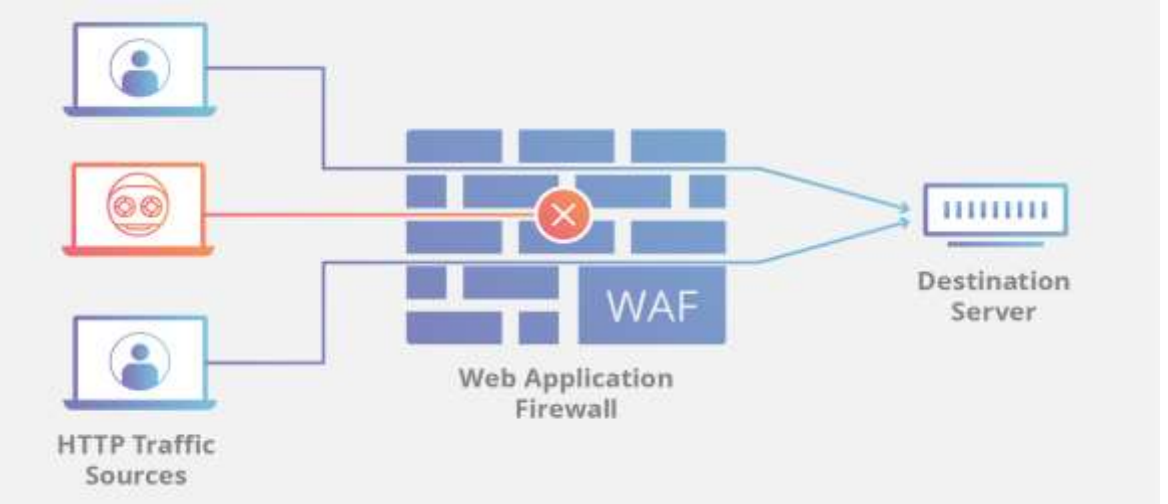
API Gateway Security



BIG COMPASS

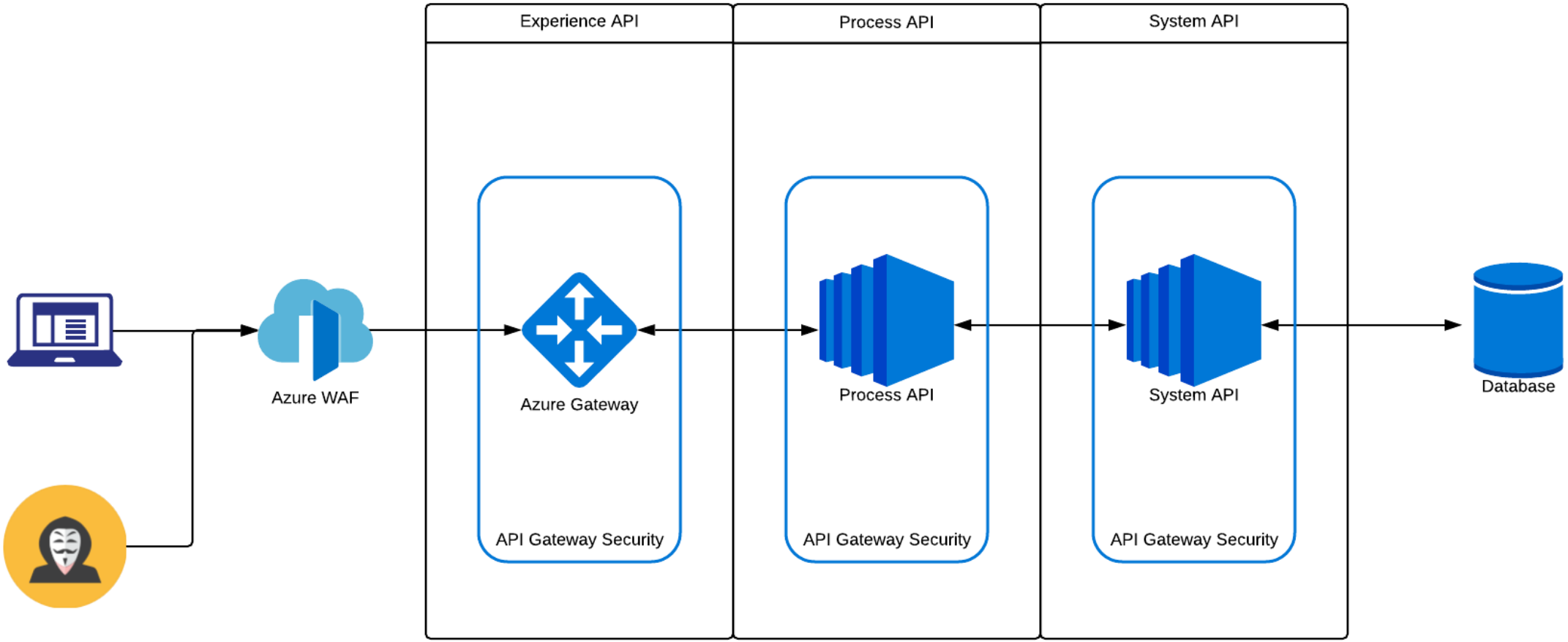
Second Line of Defense - API Security + WAF

- Protects against many common attacks - OWASP Top 10 attacks
  - SQL injection
  - Cross Site Scripting
  - Body scanning
  - DDoS
- What are the vulnerabilities?
  - Advanced API attacks from authenticated hackers
    - Detecting authenticated attacks is difficult!



BIG COMPASS

API Security + WAF

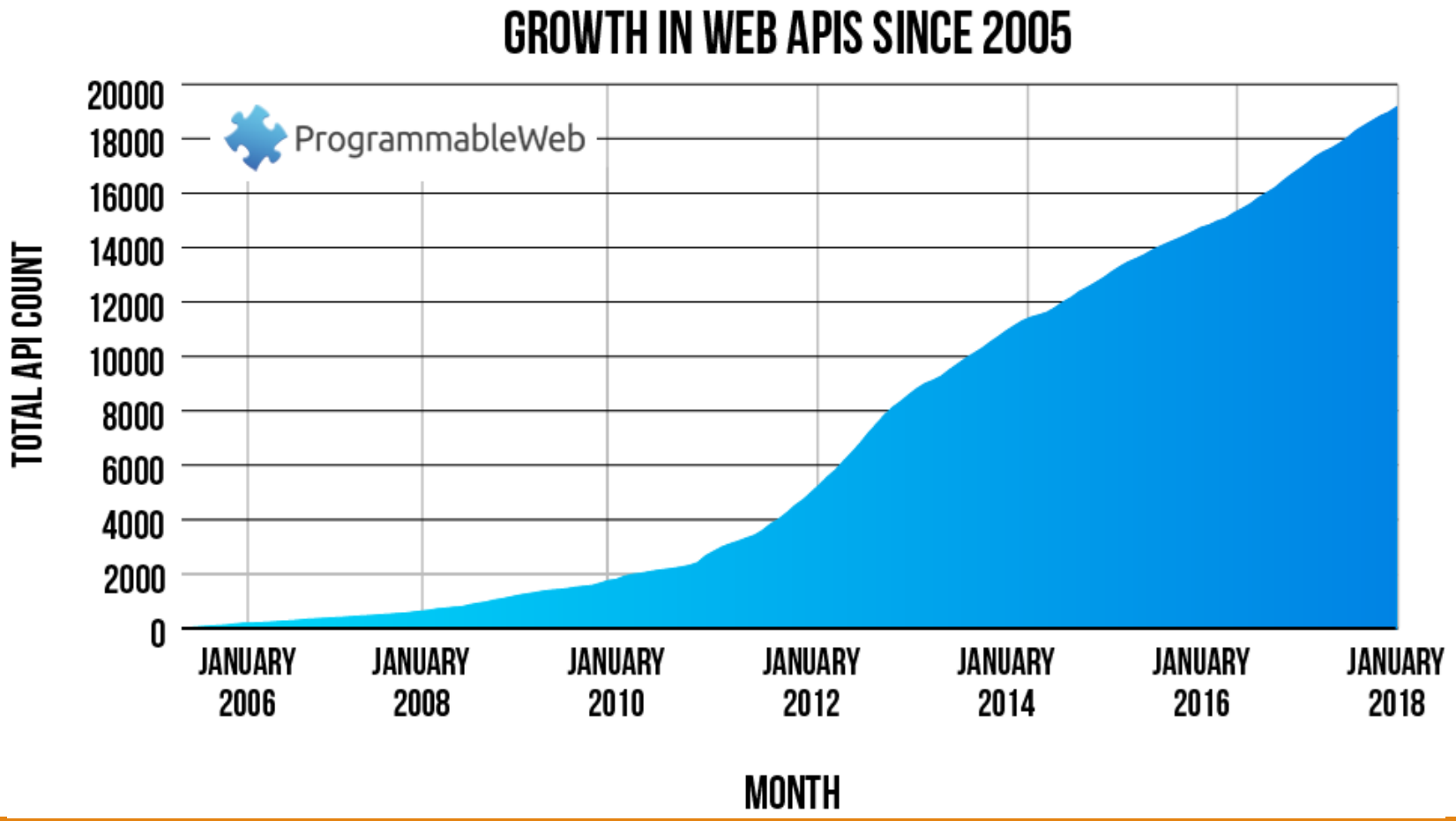


BIG COMPASS

API Landscape

BIG COMPASS

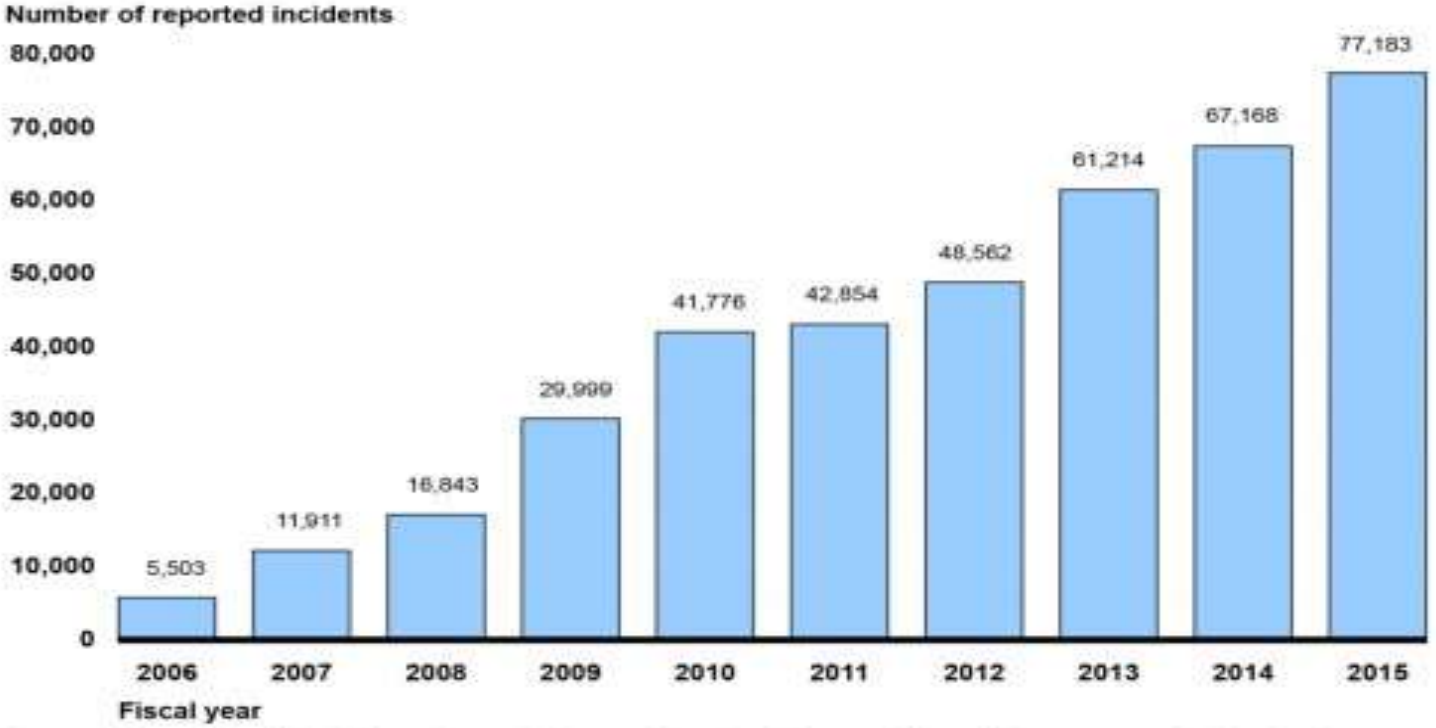
Current API Landscape



BIG COMPASS

Current API Security Landscape

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-501

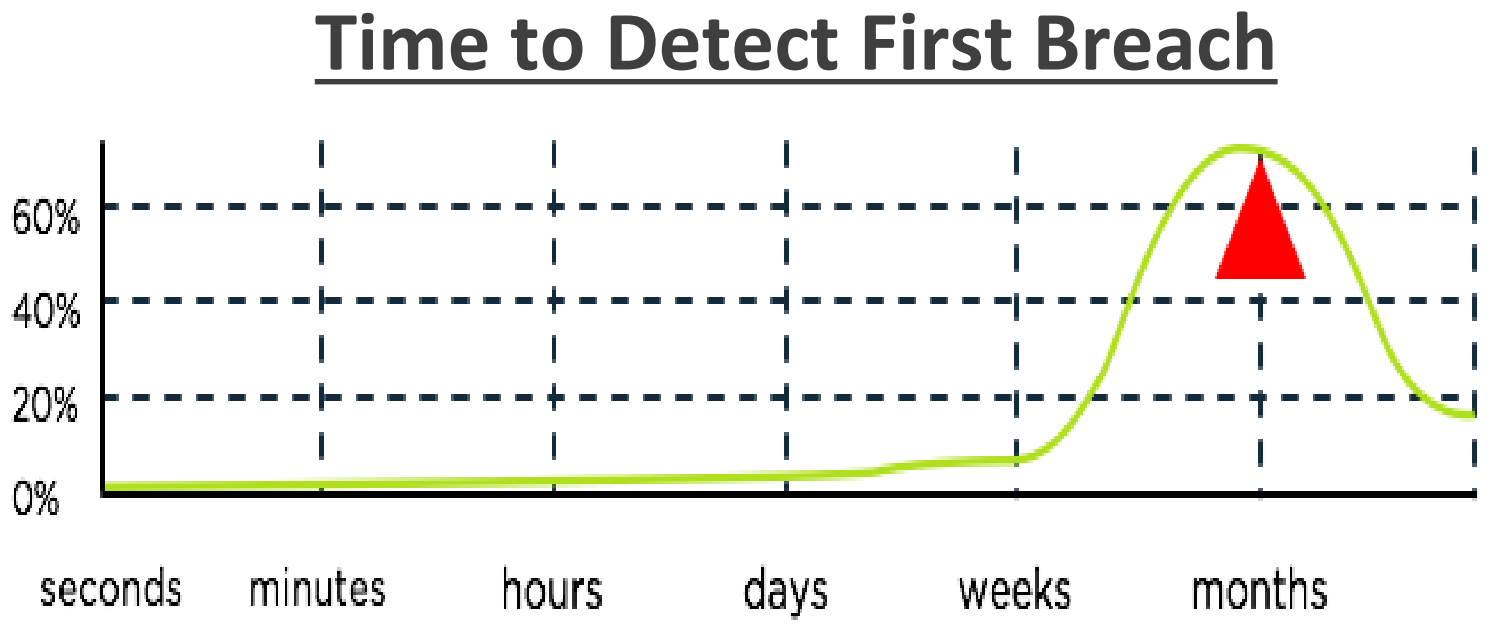
BIG COMPASS

Current API Security Landscape

- API Security Survey
  - 45% not confident in ability to detect malicious API access
  - 51% not confident in security team's awareness of all API's
- Lesson learned: reactivity to proactivity

BIG COMPASS

API Attack Detection



The Difficult Problem of Securing APIs

- High volume of traffic across many APIs
- High velocity connections across many APIs
- Variety of client types and activity
- Who is responsible for APIs?

How Vulnerable are APIs?

API login and DDoS attacks	Stolen account	Hackers using Machine Learning
Attacks from valid identities	Account takeover	Every attacks looks different
Stolen identifiers	Data theft	Every blocked attack leads to a new attack
Under-the-radar API DDoS attacks	App control	Always getting smarter

Answer: Leverage Machine Learning and AI

Model

- Behavioral learning
- Continuously build security model

Detect

- Look for deviations from the learned behavior

Block

- Block compromised tokens/access
- Notify/alert

PingIntelligence for APIs

Deep API visibility

- Dynamically discover APIs across all environments
- Monitor APIs across all environments

Automated threat detection and blocking

- Detect and block attacks on your APIs
- API honeypots to instantly detect probing hackers

Self learning

- Use AI to build behavioral model
- No need to author and manage policies and update API security

BIG COMPASS

Zero Trust

- You can’t trust your own tokens!
- Bearer tokens are vulnerable (but necessary)
- Vulnerabilities at other vectors are exploited at API level
  - Client app, user, 3rd party identities

GitHub leaking client secrets

Phishing

Stolen token

User data

<api>

API Security + PingIntelligence

Azure APIM

Content Injection

JSON, XML, SQL, XSS

Flow Control

Throttling, metering, quota management

Access Control

AuthN, AuthZ, Tokens

AI-Powered Threat Protection For APIs

PingIntelligence for APIs

Automated Cyber-Attack Blocking

Blocks stolen tokens/cookies, Bad IPs, and API keys

API Deception and Honeypots

Instant hacking detection and blocking

Deep Visibility and Reporting

Monitor and report on all API activity

PingIntelligence Augments API Security

API Gateways

- API management
- Security policies

Web Application Firewalls

- OWASP top 10 protection

PingIntelligence for APIs

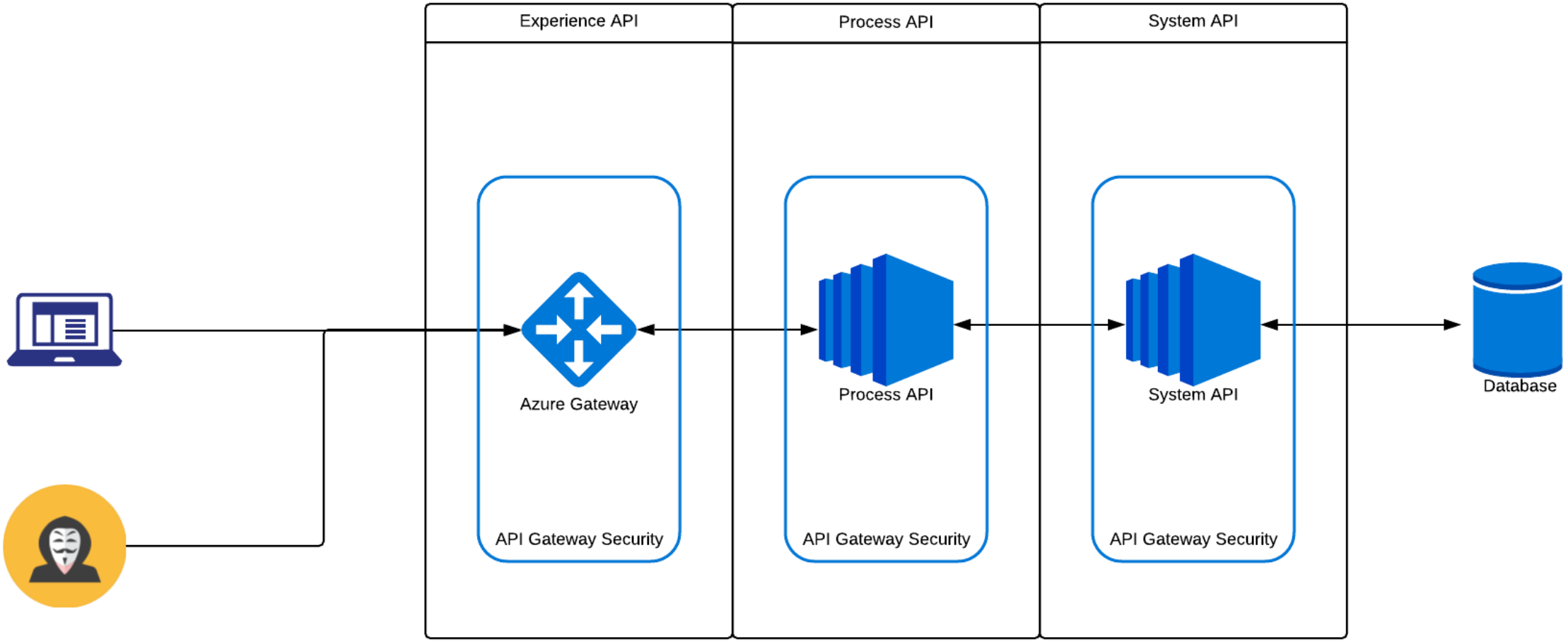
- Authenticated users
- Advanced attacks

Attack Landscape Summary

- API breaches go undetected for months or years
- Zero trust strategy for securing APIs is crucial
- Gartner: "by 2022, API abuses will be the most frequent attack vector that result in breaches"
- Many attacks can't be detected with traditional API security
- Help is here from PingIntelligence + API Gateways

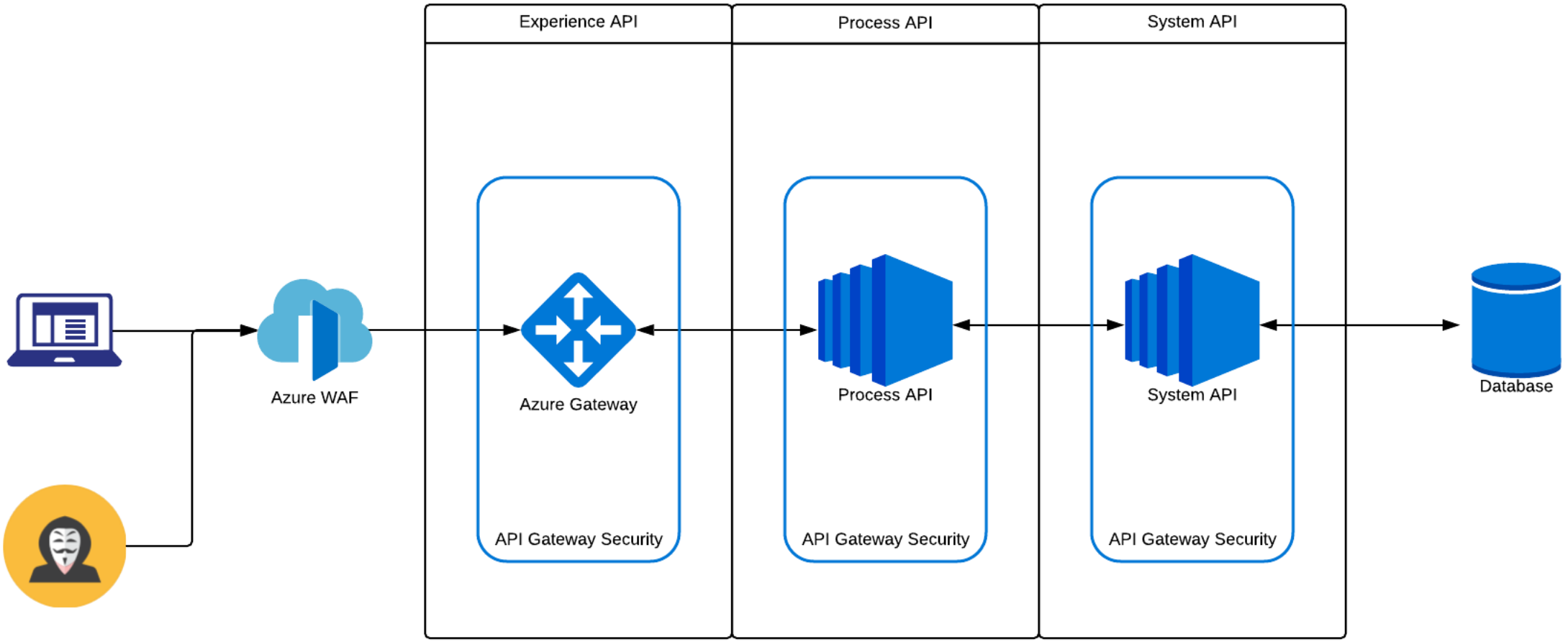
BIG COMPASS

API Gateway Security



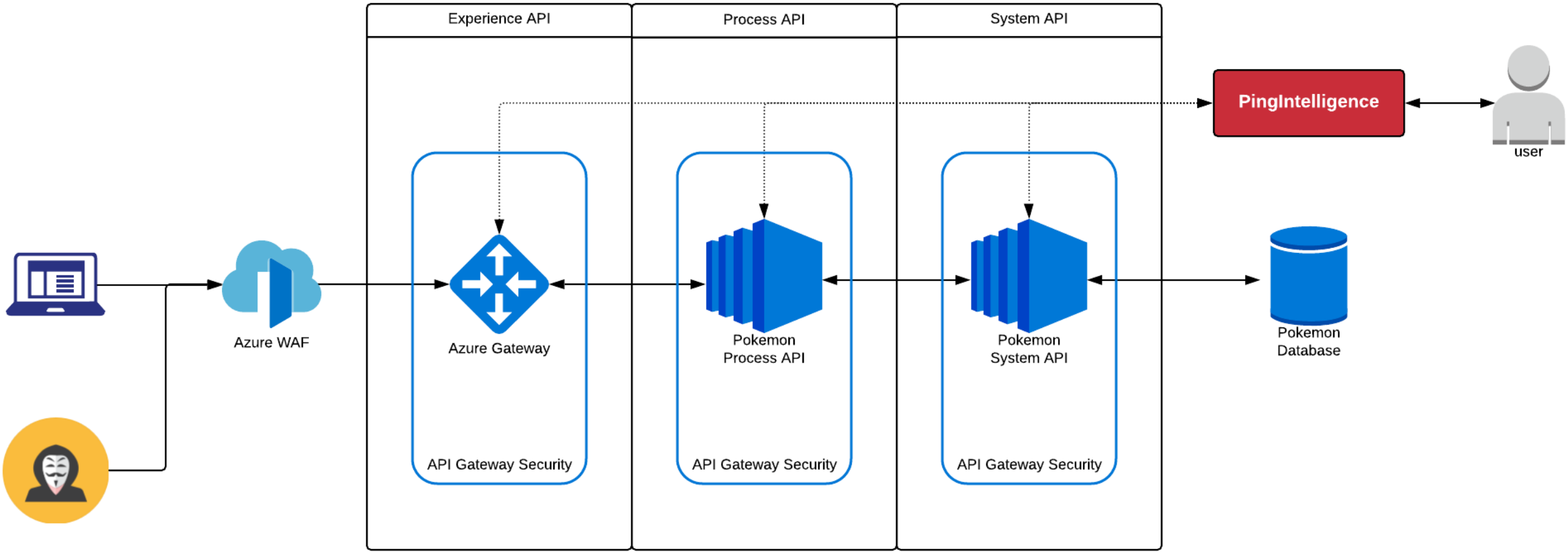
BIG COMPASS

API Security + WAF



BIG COMPASS

API Security + WAF + PingIntelligence



BIG COMPASS

Demo

ATTACKING AN AZURE GATEWAY SECURITY + WAF + PINGINTELLIGENCE PROTECTED API

BIG COMPASS

References and Documentation

- OWASP
  - https://www.owasp.org/index.php/Main_Page
- PingIntelligence for APIs
  - https://docs.pingidentity.com/bundle/pingintelligence-41/page/dvy1564008964001.html
- Undisturbed REST
  - https://www.mulesoft.com/lp/ebook/api/restbook
- API Security
  - Kin Lane, API Evangelist, Evolving API Security Landscape Whitepaper
    - https://www.pingidentity.com/en/resources/client-library/white-papers/2018/evolving-api-security-landscape.html

BIG COMPASS

References and Documentation

- Azure
  - API Manager
    - https://azure.microsoft.com/en-us/services/api-management/
  - Azure API Security
    - https://docs.microsoft.com/en-us/azure/api-management/api-management-security-controls
- MuleSoft Documentation
  - API Manager
    - https://docs.mulesoft.com/api-manager/2.x/
  - Anypoint Security
    - https://docs.mulesoft.com/anypoint-security/

Connect With Us

- Big Compass
  - Website - https://www.bigcompass.com
  - LinkedIn - https://www.linkedin.com/company/big-compass/
  - Twitter - https://twitter.com/big_compass
  - Facebook - https://www.facebook.com/bigcompass/
  - YouTube - https://www.youtube.com/channel/UCe789BLAsirAsl7w0skJlJQ?view_as=subscriber

Questions?