Microsoft Security

Fortifying Your APIs

Best Practices for Securing APIs using Microsoft Technology

Ronny de Jong
Security Technology Specialist

Agenda

GET API security in practice 202 Accepted

What is an API & how do we use them?

The next underestimated attack surface?

How to approach & implement API Security practice.

Next steps

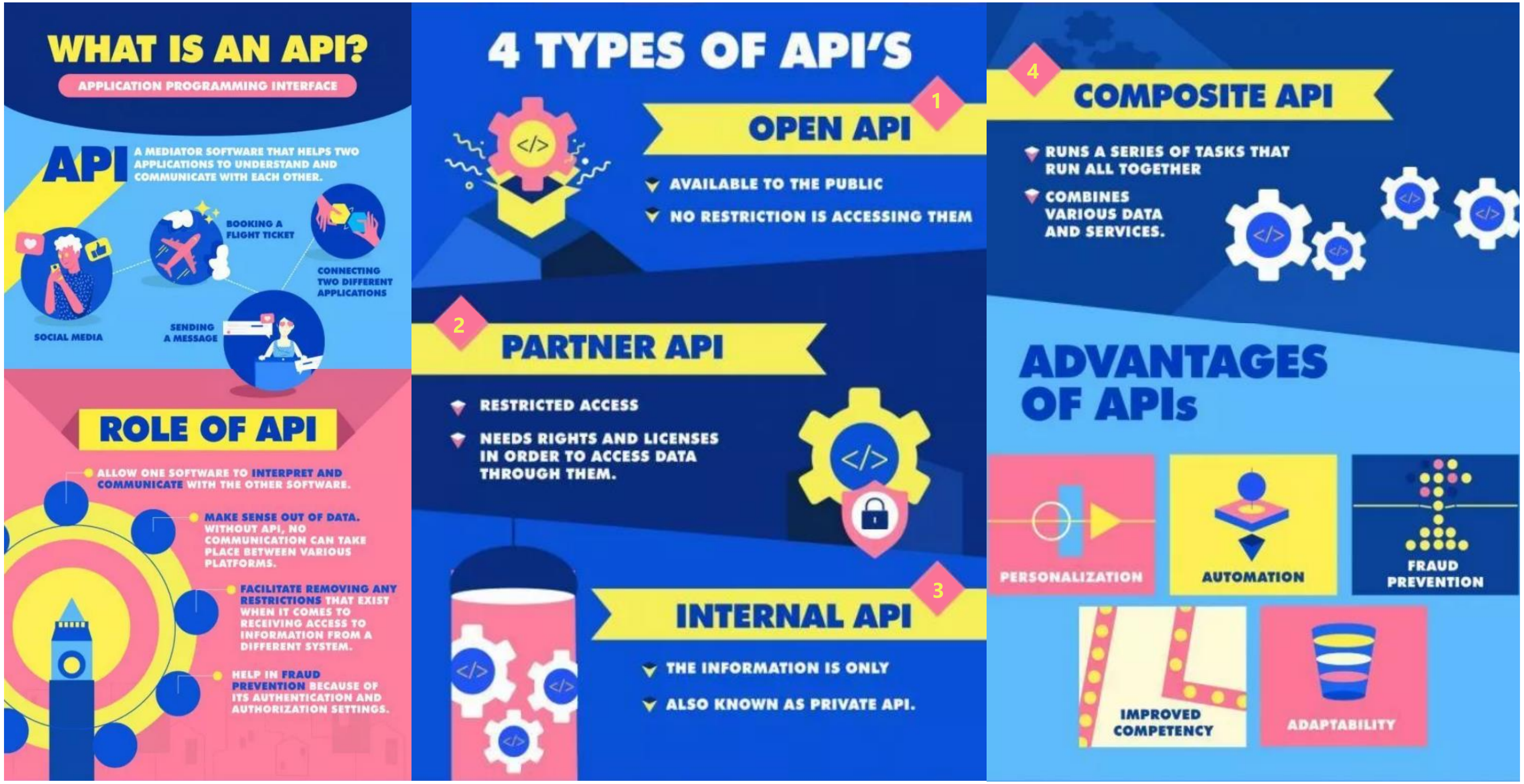
Microsoft Security

Introduction

- **What is an API & how do we use them?** »
- Why the next underestimated attack surface?
- How to approach & implement API Security practice.
- Next steps

API 101

All you must know about an API



WHAT IS AN API?

APPLICATION PROGRAMMING INTERFACE

API A MEDIATOR SOFTWARE THAT HELPS TWO APPLICATIONS TO UNDERSTAND AND COMMUNICATE WITH EACH OTHER.

ROLE OF API

- ALLOW ONE SOFTWARE TO INTERPRET AND COMMUNICATE WITH THE OTHER SOFTWARE.
- MAKE SENSE OUT OF DATA. WITHOUT API, NO COMMUNICATION CAN TAKE PLACE BETWEEN VARIOUS PLATFORMS.
- FACILITATE REMOVING ANY RESTRICTIONS THAT EXIST WHEN IT COMES TO RECEIVING ACCESS TO INFORMATION FROM A DIFFERENT SYSTEM.
- HELP IN FRAUD PREVENTION BECAUSE OF ITS AUTHENTICATION AND AUTHORIZATION SETTINGS.

4 TYPES OF API'S

1 OPEN API

- AVAILABLE TO THE PUBLIC
- NO RESTRICTION IS ACCESSING THEM

2 PARTNER API

- RESTRICTED ACCESS
- NEEDS RIGHTS AND LICENSES IN ORDER TO ACCESS DATA THROUGH THEM.

3 INTERNAL API

- THE INFORMATION IS ONLY
- ALSO KNOWN AS PRIVATE API.

4 COMPOSITE API

- RUNS A SERIES OF TASKS THAT RUN ALL TOGETHER
- COMBINES VARIOUS DATA AND SERVICES.

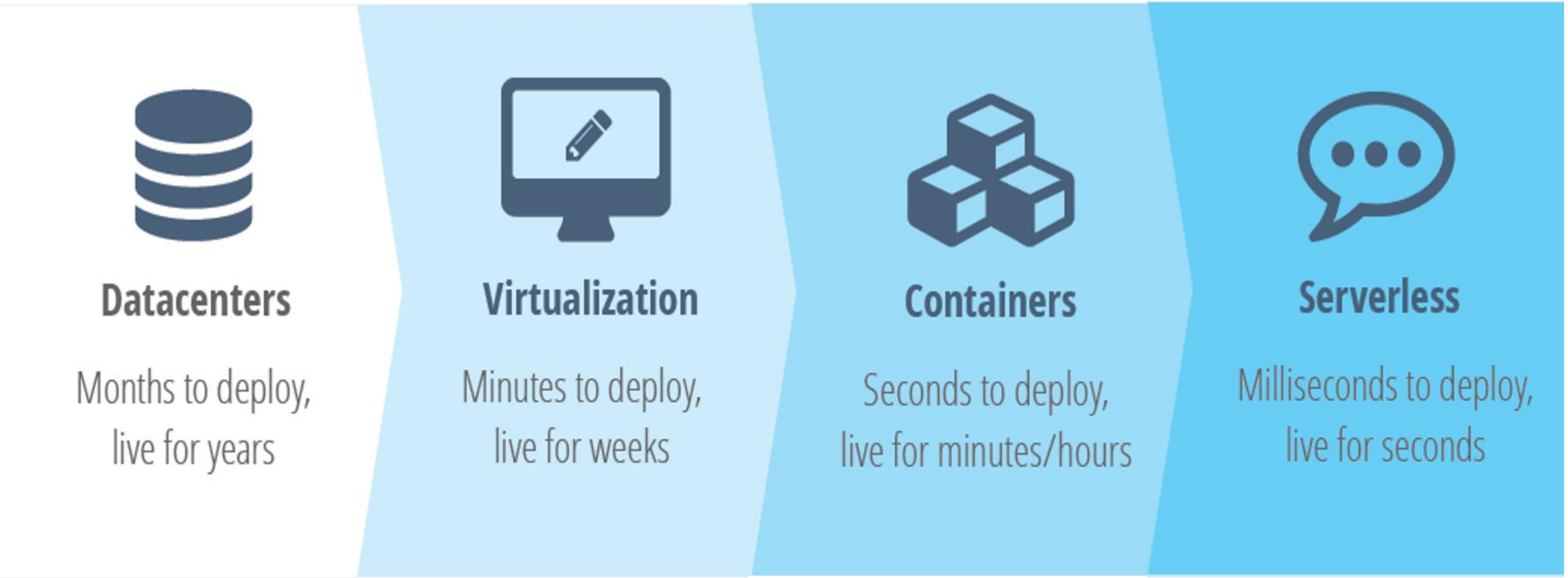
ADVANTAGES OF APIs

- PERSONALIZATION
- AUTOMATION
- FRAUD PREVENTION
- IMPROVED COMPETENCY
- ADAPTABILITY

Source: https://www.appseconnect.com/all-you-must-know-about-an-api-an-infographic/

The rise of APIs

It’s this speed that is most transforming. Speed enables and encourages new microservices architecture.


Datacenters
Months to deploy, live for years
Virtualization
Minutes to deploy, live for weeks
Containers
Seconds to deploy, live for minutes/hours
Serverless
Milliseconds to deploy, live for seconds

Source: https://www.slideshare.net/adriancockcroft/dockercon-state-of-the-art-in-microservices | thenewstack.io

Microsoft Security

Security risks related to APIs

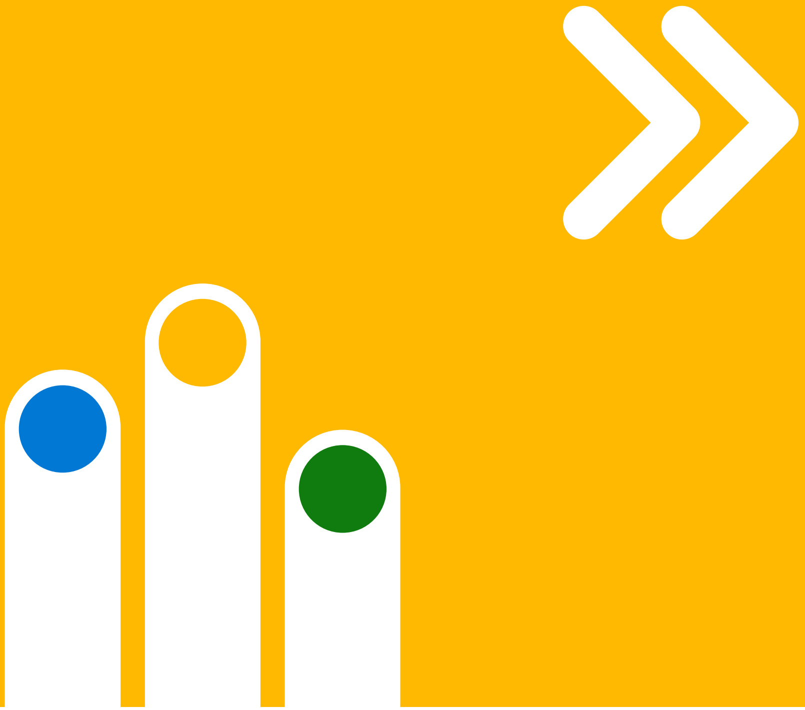
What is an API & how do we use them?

The next underestimated attack surface?

How to approach & implement API Security practice.

Next steps

Next underestimated attack surface?



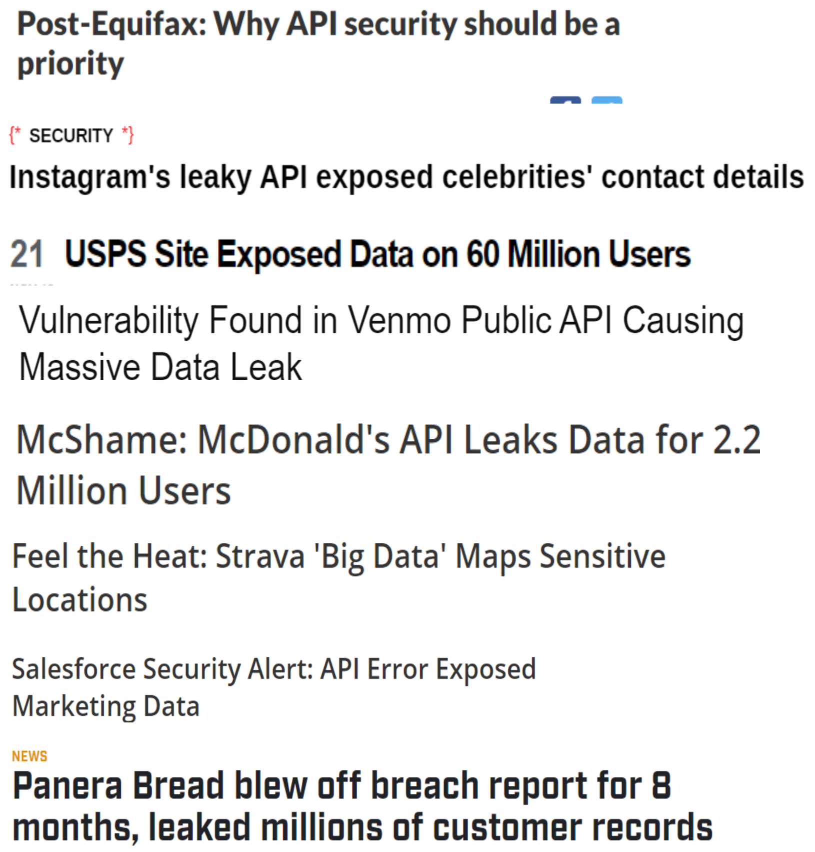
According to **Akamai**, **83%** of web traffic is **API** traffic.[1]

Gartner study points to **APIs** as the **Top Attack Vector** in 2022. [2]

1. Akamai State of the Internet Security Report
2. Gartner, Protect your APIs from attacks & data breaches

How can a lack of API security be harmful?

The current and feature reality



Post-Equifax: Why API security should be a priority

{* SECURITY *}

Instagram's leaky API exposed celebrities' contact details

21 **USPS Site Exposed Data on 60 Million Users**

Vulnerability Found in Venmo Public API Causing Massive Data Leak

McShame: McDonald's API Leaks Data for 2.2 Million Users

Feel the Heat: Strava 'Big Data' Maps Sensitive Locations

Salesforce Security Alert: API Error Exposed Marketing Data

NEWS

Panera Bread blew off breach report for 8 months, leaked millions of customer records

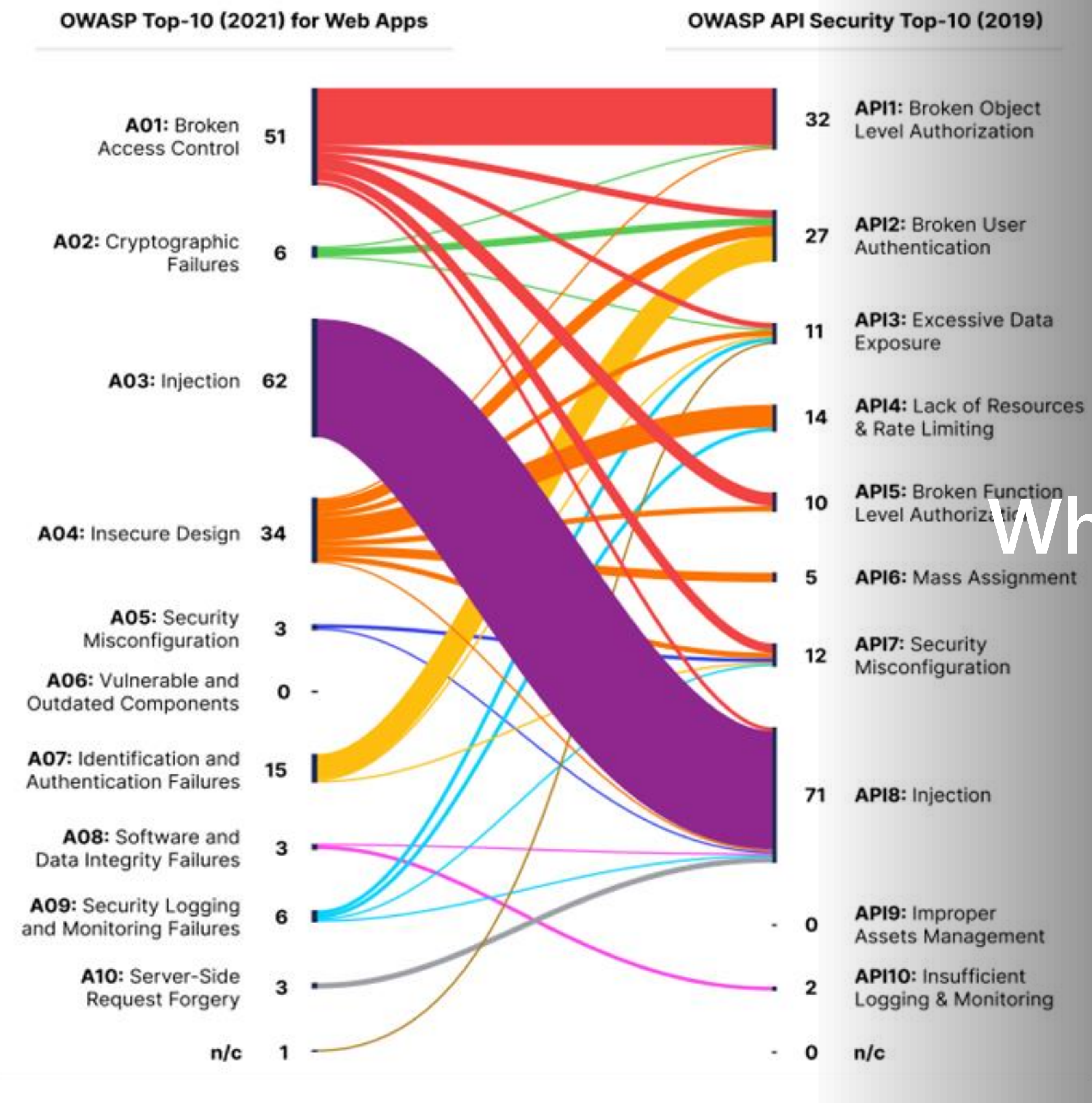
$3.92 Million: Average Cost Per Data Breach
$150: Average Cost Per Data Record
-According to 2019 IBM Research Study

OWASP Top-10 API Security Risk List

The Open Web Application Security Project (OWASP) focuses on strategies and solutions to understand and mitigate the unique vulnerabilities and security risks of APIs.

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

Which OWASP Top-10 matters most?



Source: Wallarm Q2-2022 API Vulnerability and Exploit infographic

Microsoft Security

Stages of protection

What is an API & how do we use them?

Why the next underestimated attack surface?

How to approach API Security practice >>

Next steps

Key components of API security

Discovery

Discovering all of the customers API assets (e.g., endpoints, serverless functions, gateways) and cataloging them

Understanding

Understanding API definition, API usage, API classification, and API interaction flows

Protection

Assessing APIs for best practices, for OWASP vulnerabilities both in CI/CD and in Runtime and for guided hardening

Detection

Analyzing API call contents and API sequence logic for suspicious behavior

Response

Integrating signals into SIEM systems and guiding automated and manual remediations

Microsoft’s approach to API security

Prevent, detect and respond to API security threats with integrated cloud security context

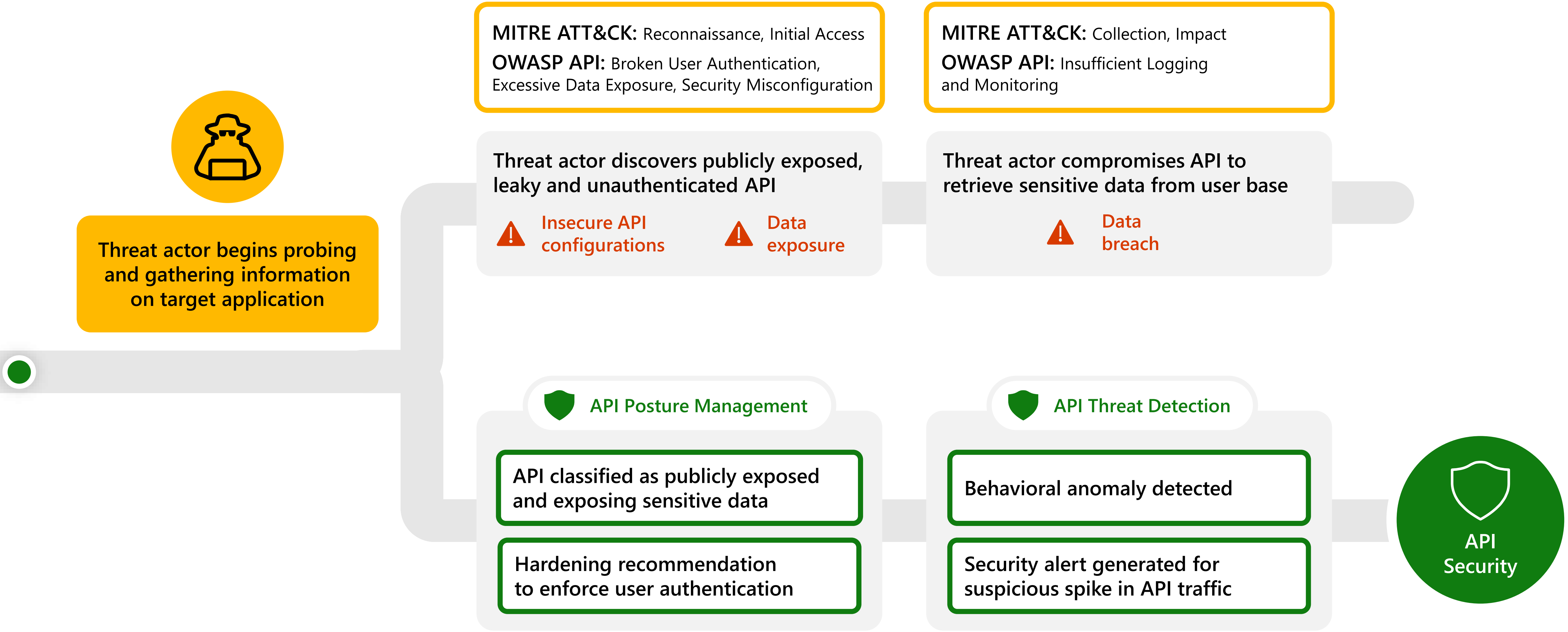
Classify and understand the security posture of your APIs

Harden API configurations and prioritize risk remediation

Monitor and protect APIs against attacks in runtime

Azure API Management integration available now

Protect against leaky APIs



Threat actor begins probing and gathering information on target application

MITRE ATT&CK: Reconnaissance, Initial Access
OWASP API: Broken User Authentication, Excessive Data Exposure, Security Misconfiguration

Threat actor discovers publicly exposed, leaky and unauthenticated API

⚠ Insecure API configurations

⚠ Data exposure

MITRE ATT&CK: Collection, Impact
OWASP API: Insufficient Logging and Monitoring

Threat actor compromises API to retrieve sensitive data from user base

⚠ Data breach

API Posture Management

API classified as publicly exposed and exposing sensitive data

Hardening recommendation to enforce user authentication

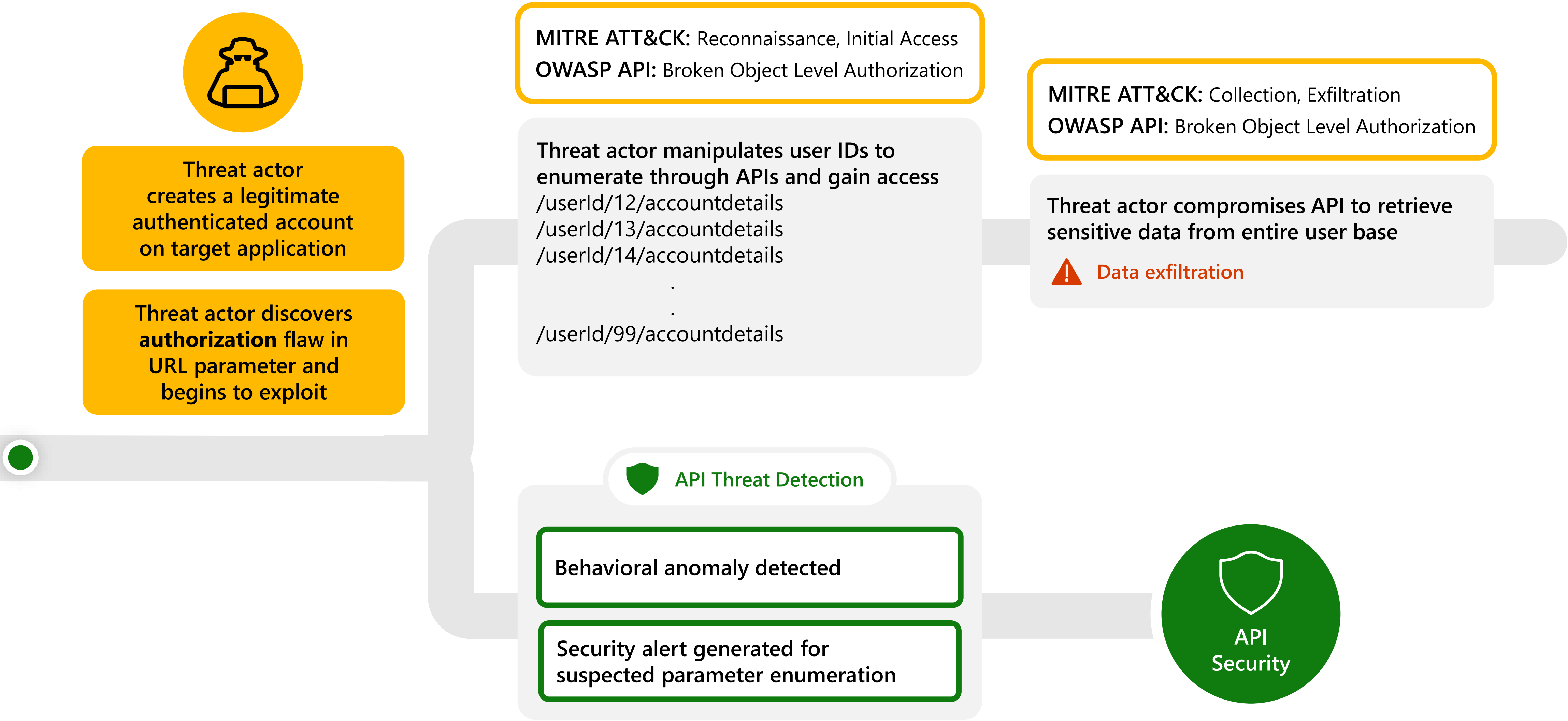
API Threat Detection

Behavioral anomaly detected

Security alert generated for suspicious spike in API traffic

API Security

Protect against broken authorization exploit



Threat actor creates a legitimate authenticated account on target application

Threat actor discovers **authorization** flaw in URL parameter and begins to exploit

MITRE ATT&CK: Reconnaissance, Initial Access
OWASP API: Broken Object Level Authorization

Threat actor manipulates user IDs to enumerate through APIs and gain access
/userId/12/accountdetails
/userId/13/accountdetails
/userId/14/accountdetails
.
.
/userId/99/accountdetails

MITRE ATT&CK: Collection, Exfiltration
OWASP API: Broken Object Level Authorization

Threat actor compromises API to retrieve sensitive data from entire user base

⚠ Data exfiltration

API Threat Detection

Behavioral anomaly detected

Security alert generated for suspected parameter enumeration

API Security

Microsoft Security

Stages of protection

What is an API & how do we use them?

Why the next underestimated attack surface?

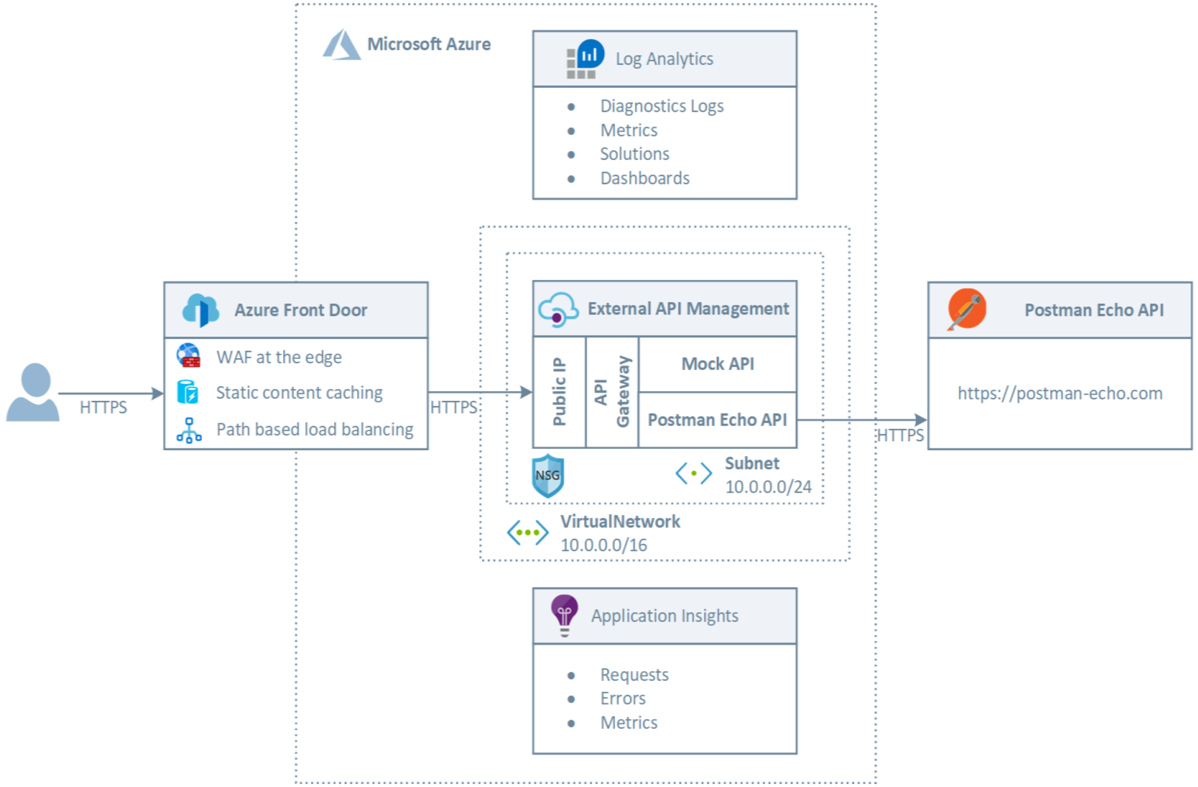
How to implement API Security practice »

Next steps

Build your API Security practice

Various controls to securely publish APIs to external, partner, and internal developers to unlock the potential of their data and services.

- Network security
- Access control
- Content validation
- Monitoring & analytics
- API Management (APIM)



Source: GitHub - paolosalvatori/front-door-apim

Azure API Management Security State

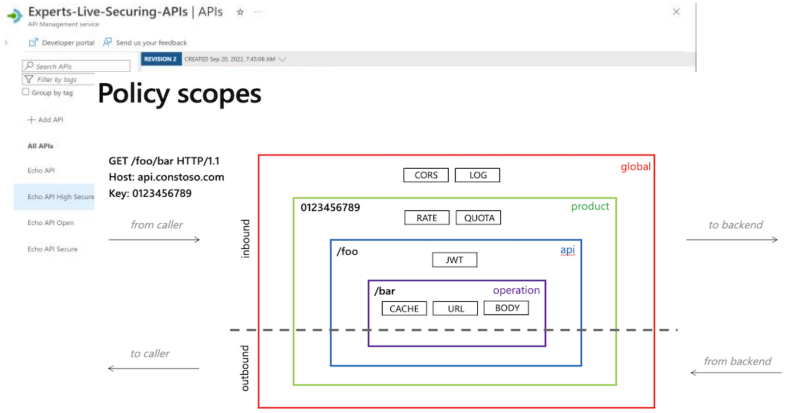
Various controls to securely publish APIs to external, partner, and internal developers to unlock the potential of their data and services.

Clients can set policies on APIs

- Limiting Call Rate
- Restricting Caller by IP Addresses
- Setting Usage Quotas
- Validating JWTs (JSON Web Tokens)

Client monitoring/logging

- Activity reports
  - Log any failed API calls
  - Log any changes to API
- Diagnostic reports/metrics
- Log all API calls
- Records



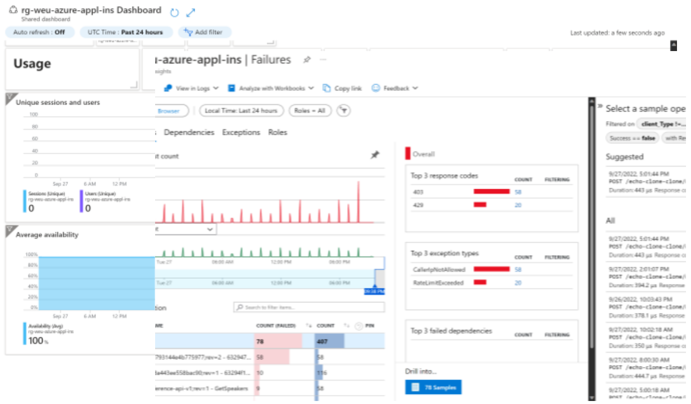
Experts-Live-Securing-APIs | APIs

API Management service

REVISION 2 CREATED Sep 20, 2022, 7:45:08 AM

Policy scopes

GET /foo/bar HTTP/1.1
Host: api.constoso.com
Key: 0123456789



rg-weu-azure-appl-ins Dashboard

Shared dashboard

Auto refresh : Off UTC Time : Past 24 hours Add filter

Last updated: a few seconds ago

Usage

ı-azure-appl-ins | Failures

Top 3 response codes

	COUNT	FILTERING
403	58	
429	20	

Top 3 exception types

	COUNT	FILTERING
CallerIpNotAllowed	58	
RateLimitExceeded	20	

Top 3 failed dependencies

ME	COUNT (FAILED)	COUNT	PIN
	78	407	
793144e4b775977;rev=2 - 632947...	58	58	
la443ee558bac90;rev=1 - 63294f1...	10	116	
erence-api-v1;rev=1 - GetSpeakers	9	58	

Select a sample ope

Filtered on client_Type !=... Success == false with Re

Suggested

9/27/2022, 5:01:44 PM
POST /echo-clone-clone/
Duration: 443 μs Response c

All

9/27/2022, 5:01:44 PM
POST /echo-clone-clone/
Duration: 443 μs Response c

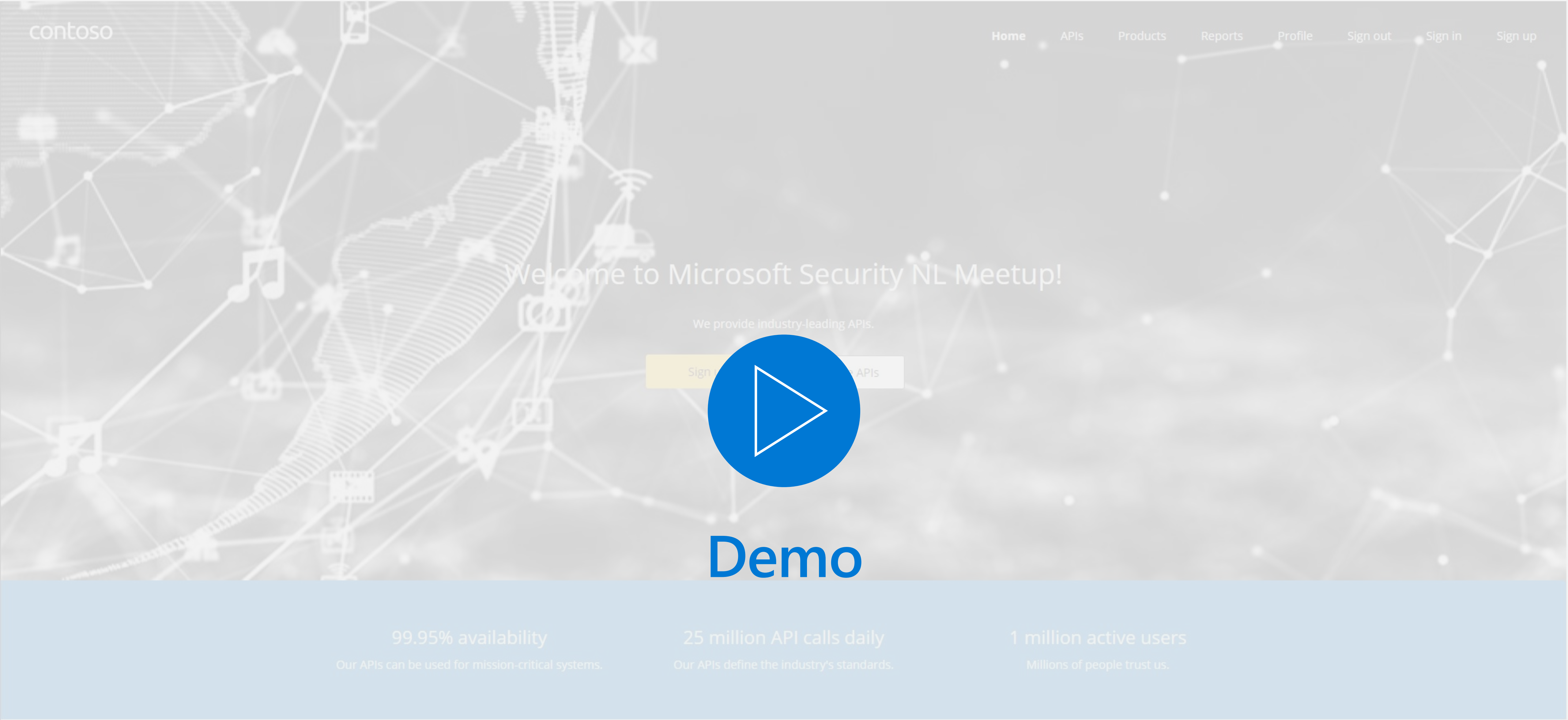
9/27/2022, 2:01:07 PM
POST /echo-clone-clone/
Duration: 394.2 μs Response

9/26/2022, 10:03:43 PM
POST /echo-clone-clone/
Duration: 378.1 μs Response

9/27/2022, 10:02:18 AM
POST /echo-clone-clone/
Duration: 350 μs Response c

9/27/2022, 8:00:30 AM
POST /echo-clone-clone/
Duration: 444.7 μs Response

9/27/2022, 5:00:18 AM



contoso

Home APIs Products Reports Profile Sign out Sign in Sign up

Welcome to Microsoft Security NL Meetup!

We provide industry-leading APIs.

Sign APIs

99.95% availability

Our APIs can be used for mission-critical systems.

25 million API calls daily

Our APIs define the industry's standards.

1 million active users

Millions of people trust us.

Demo

POST API security in practice 200 OK with Azure API Management & Defender for API

Microsoft Security

PUT API security in practice 200 OK

What is an API & how do we use them?

Why the next underestimated attack surface?

How to implement API Security practice

Next steps

Key Takeaways

To ensure secure use of APIs, below basic security measures, should be taken.

☑ APIs must be **managed** by **Azure API Management (APIM)**

☑ Register **Microsoft.ApiSecurity** resource provider

☑ Microsoft **Defender for API** plan should be **enabled**

☑ Onboarding via **Defender for Cloud Recommendations**

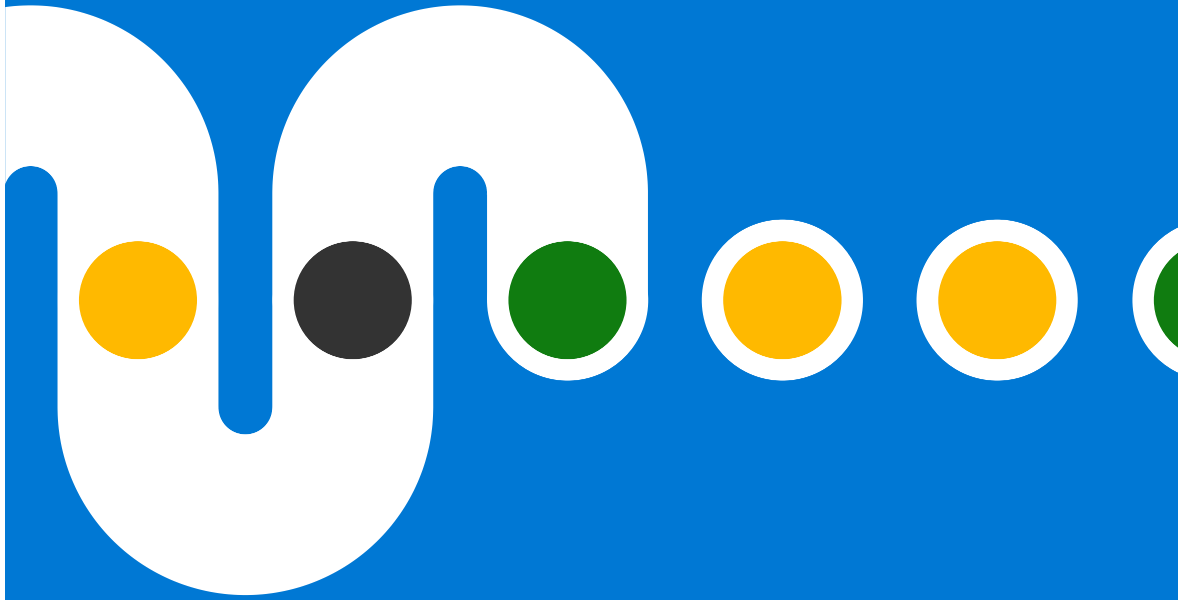
☑ Security insights refresh interval of **30 minutes**

Starting point of securing your APIs

☑ **Azure API Management (APIM)**
Classify and understand the security posture of your APIs (Discovery & Understanding)

☑ **Microsoft Defender for API**
Monitor and protect APIs against attacks in runtime (Detection & Response)

☑ **Azure Security Baseline 3.0** Harden API configurations and prioritize risk remediation (Protection)



Microsoft Security

Thank you!

Ronny de Jong
ronnydejong@microsoft.com