Jak efektivně zabezpečit webové aplikace

Michal Zalewski
Sales Engineer, Barracuda
mzalewski@barracuda.com

Petr Konečný
Senior Account Manager, COMGUARD
petr.koneny@comguard.cz

Barracuda
Your journey, secured.

Agenda

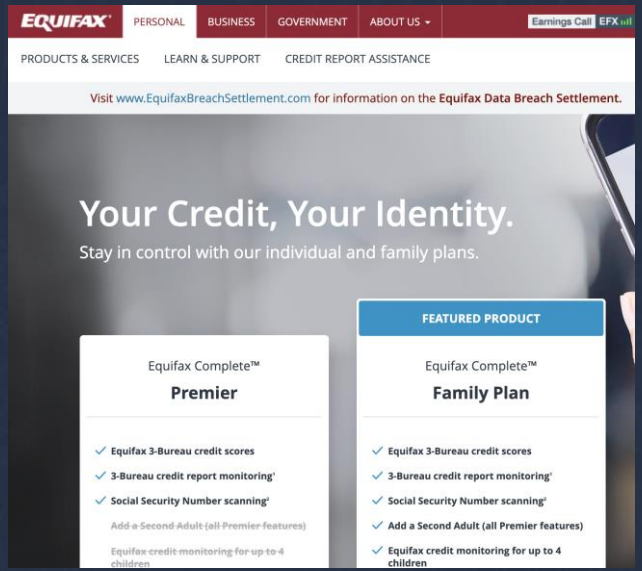
- Proč je ochrana webových aplikací tak důležitá
- Jaké jsou specifické požadavky na moderní zabezpečení
- Co by měla moderní WAF poskytovat

Počet webových aplikací neustále roste

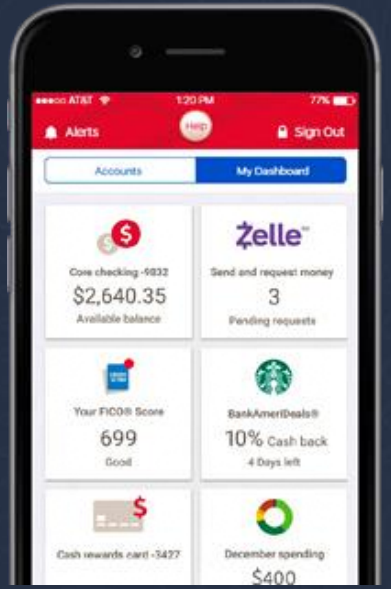
2017

2023

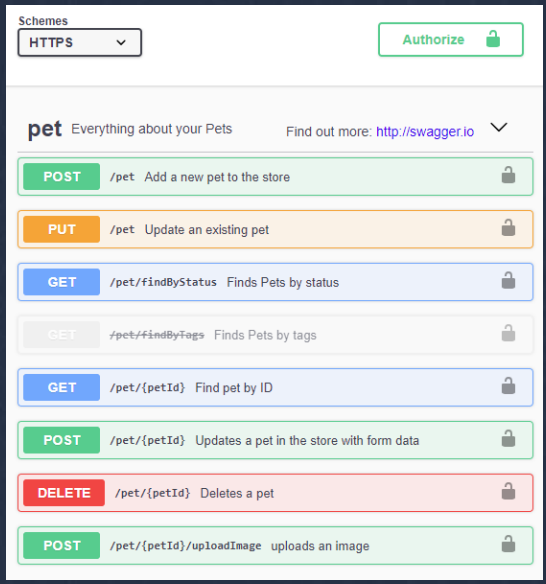
Téměř vše je webová aplikace



Webová stránka



Mobilní aplikace



App Interface (API)

Ztráta dat: nejčastěji ve spojitosti s web. aplikací

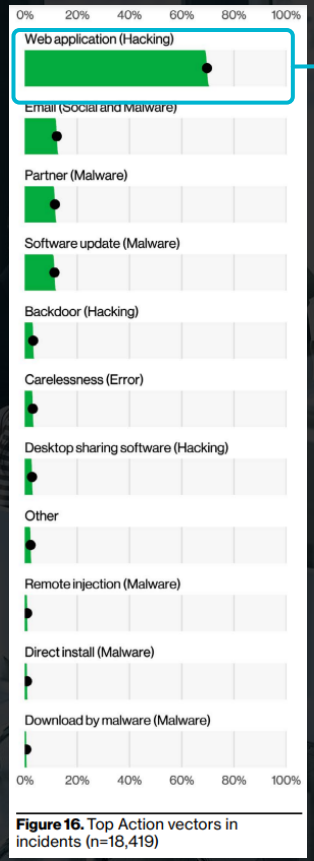


Figure 16. Top Action vectors in incidents (n=18,419)

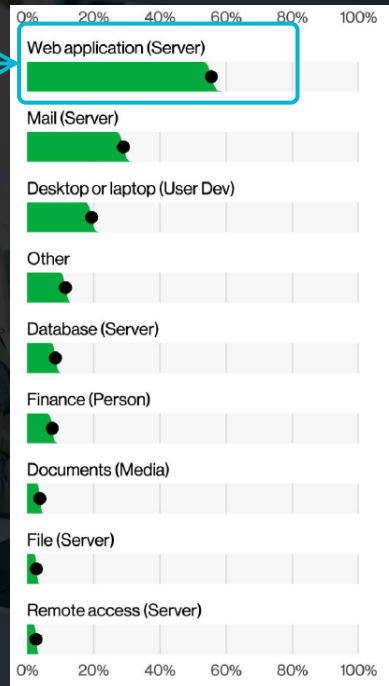
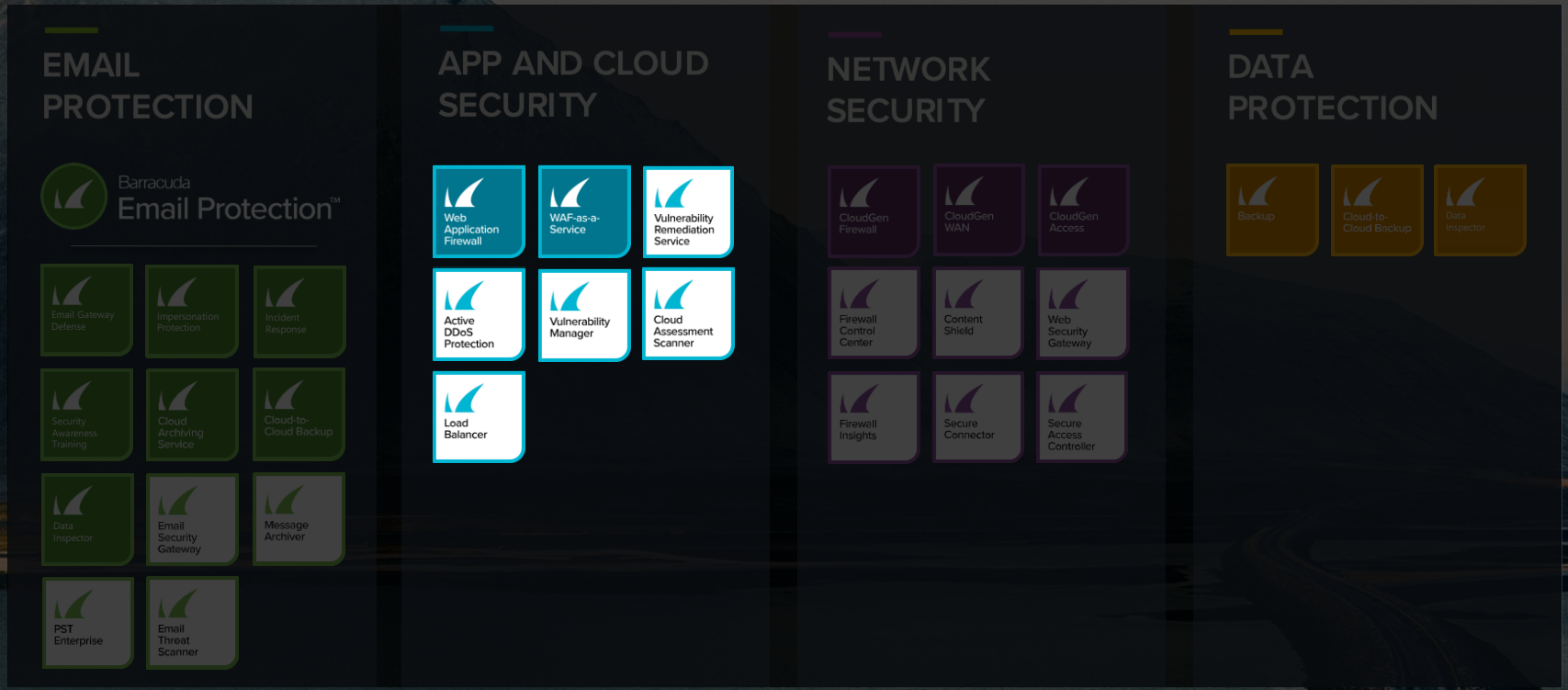


Figure 24. Top Asset varieties in breaches (n=2,796)

Source: Verizon, 2022 Data Breach Investigation Report

Web Application Protection – portfolio Barracuda



WAF: *hardwarová nebo virtuální appliance*

WAF-as-a-Service: *rychlé nasazení, jednoduchá správa*

Fyzické zařízení

Virtuální appliance

Podporuje:

- VMware
- Hyper-V
- KVM

Virtuální appliance

Podporuje:

- Azure
- AWS
- Google Cloud

WAF-as-a-Service

Why WAF-as-a-Service?

Existing Solutions are Ineffective…

WAF appliances are hard to deploy and manage

Customers lack sufficient AppSec skillsets / resources

SaaS solutions lack advanced functions

Add-on solutions (e.g. DDoS and bot protection are not integrated)

Barracuda WAF-as-a-Service

Enterprise-proven application security delivered in minutes

Built on the same proven technology

Simple **3-step** setup wizard adds protection in minutes

Intuitive component-based structure for fine-tuning policies

Fully featured REST API

Unmetered DDoS protection included

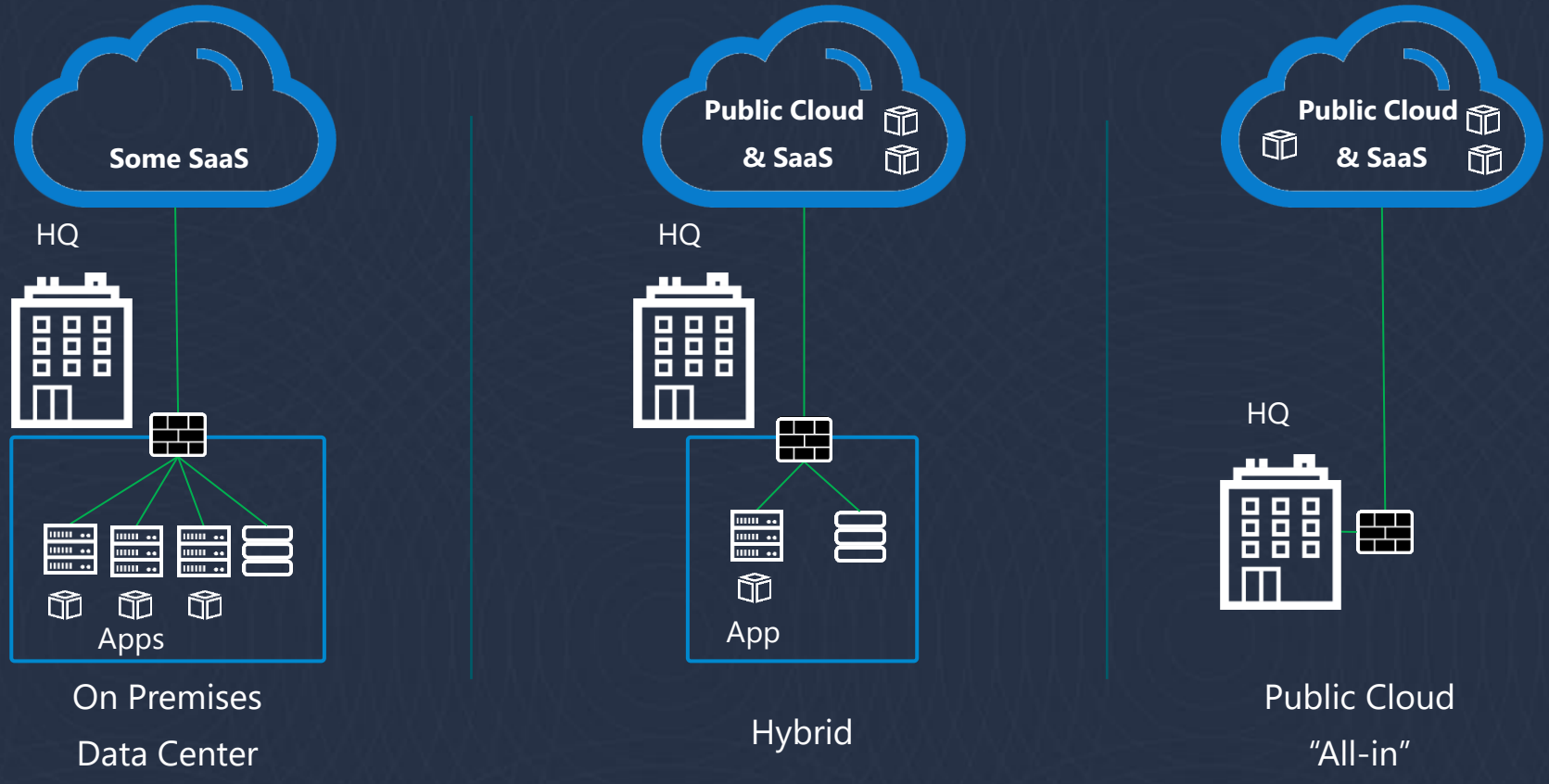
Automated vulnerability identification and remediation

WAF-as-a-Service Architecture

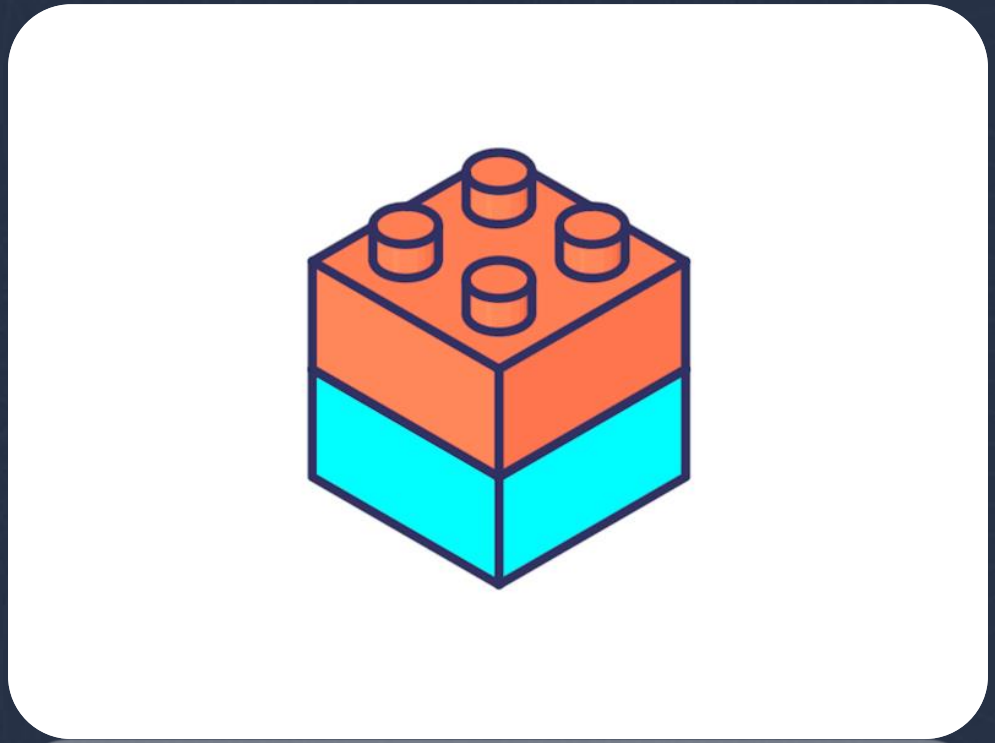
How it works


User
(Browser)
Perimeter
Firewall
App Servers
A: www.securedapp.com
CNAME: app123456.prod.cudawaas.com
WAF
Barracuda
WAF-as-a-Service
Barracuda Cloud Scrubbing Centers
(Multiple Global Locations)

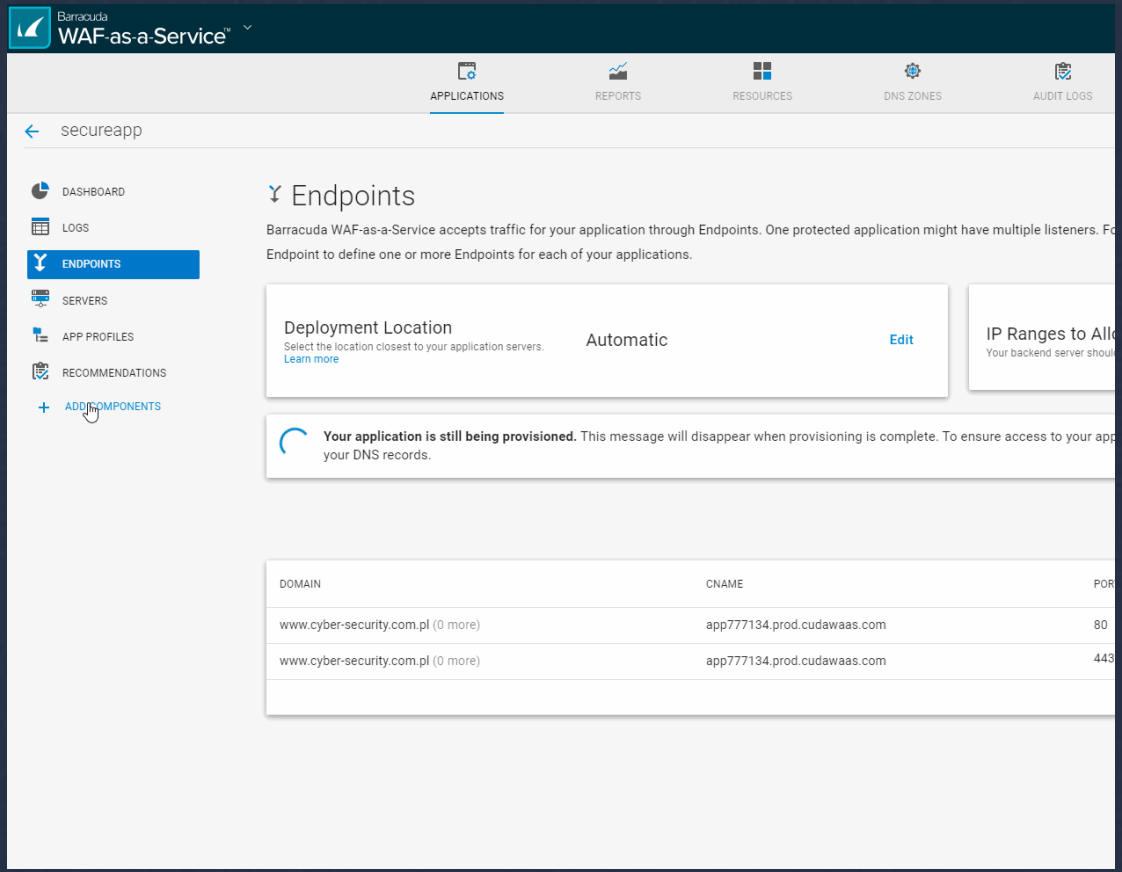
Protects your apps hosted everywhere



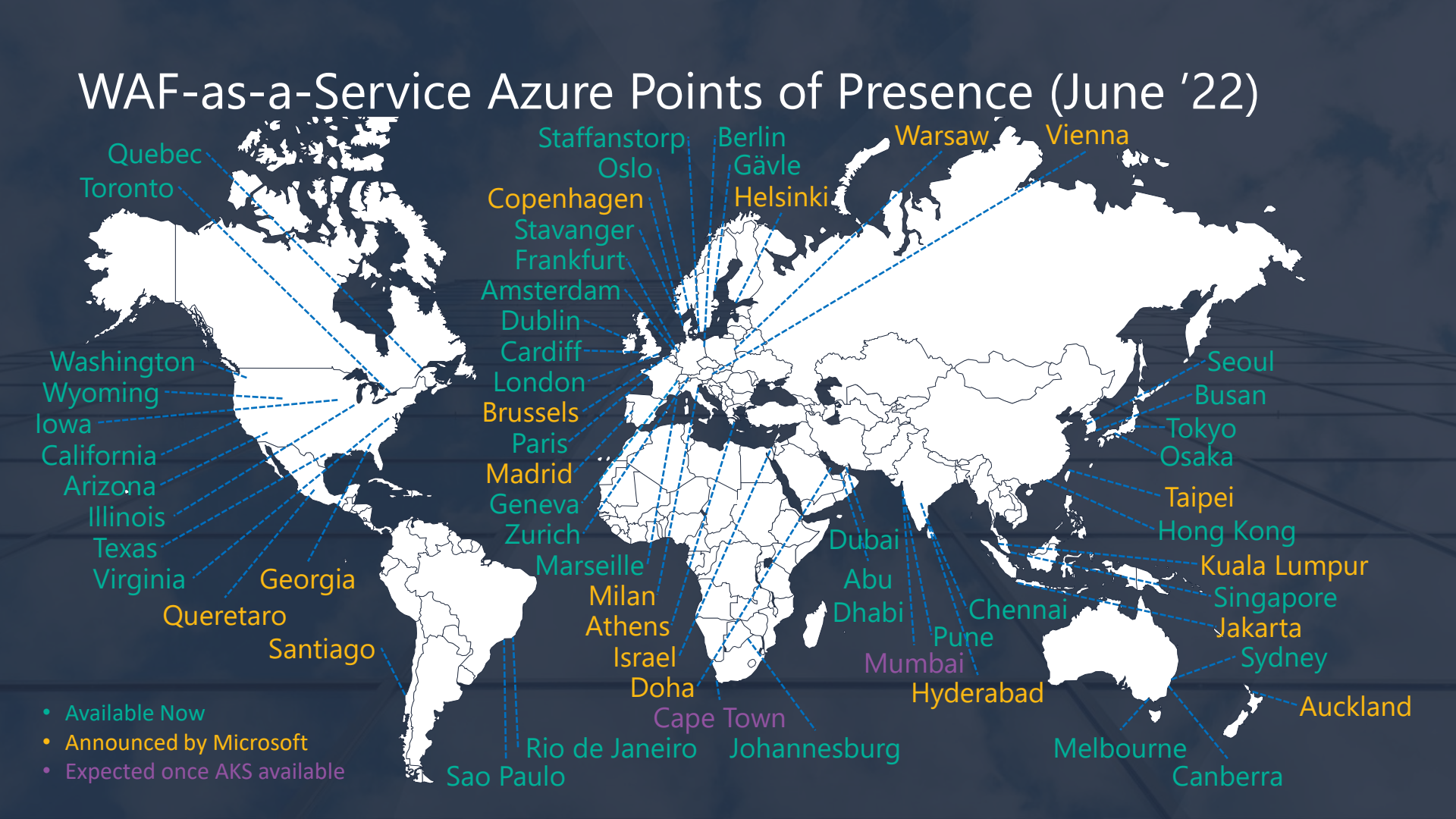
WAF-as-a-Service Components



WAF-as-a-Service Components



WAF-as-a-Service Azure Points of Presence (June ’22)



- Available Now
- Announced by Microsoft
- Expected once AKS available

API Protection

API Discovery

- Identifying and securing APIs is a massive problem
- Old API endpoints that are left unsecured can be very risky
- Configuring API Security can be complex
  - Most API Gateways offer limited security capabilities
  - Lack of knowledge and complexity in setting up security is a barrier
- First Steps to removing this complexity
  - API Discovery using configuration files
    - XML Schema validation / WS-I Security Validation
    - OpenAPI metadata file import for JSON Based API Validation

API Protection

1. DDoS Prevention
2. Bot Mitigation, IP Reputation, Rate Controlling
3. SSL/TLS Security
4. API Message Security
5. Protocol Security
6. Access Control

Inbound Inspection

Outbound Inspection

API Server

7. Cloaking
8. Data Theft Prevention

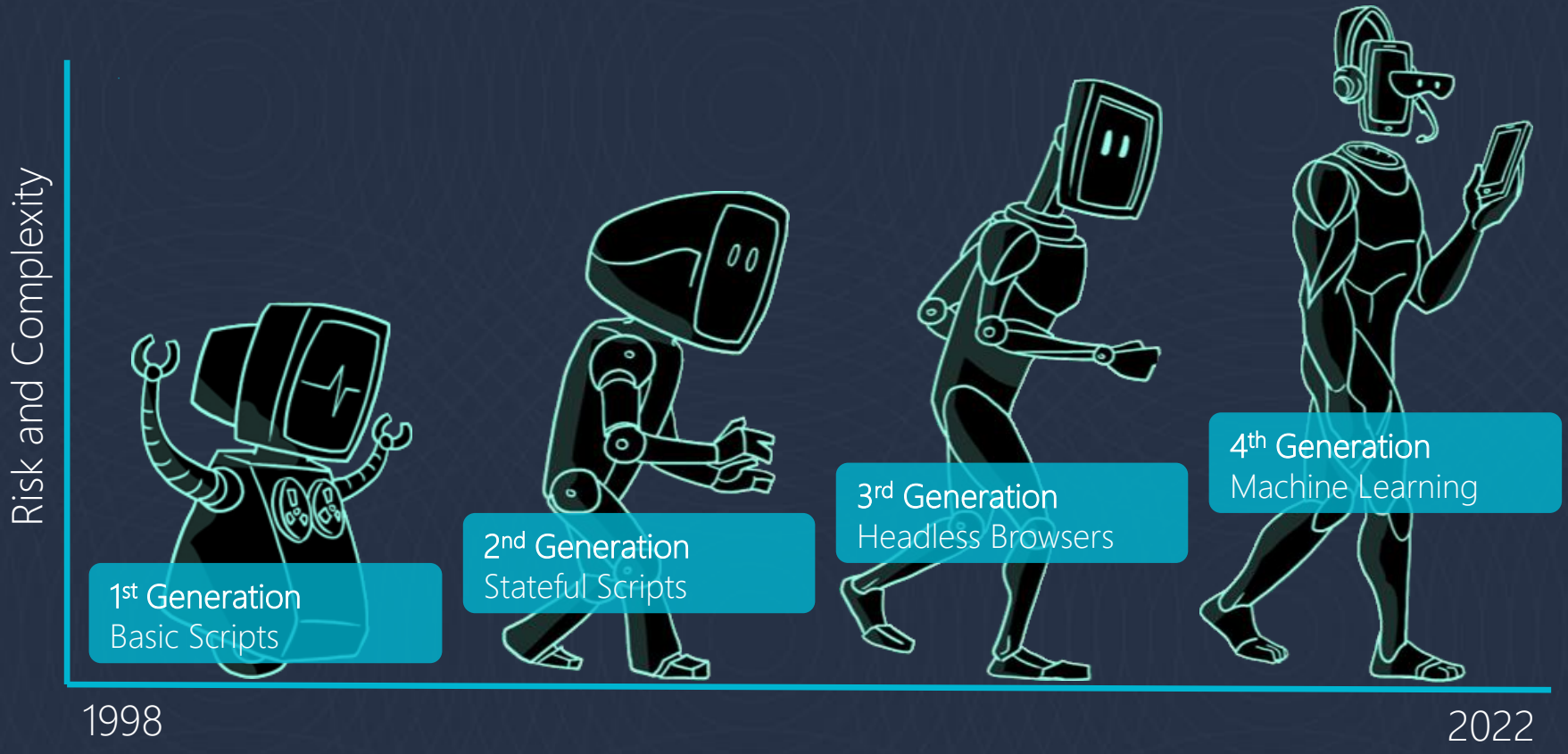
Advanced Bot Protection & Active DDoS Prevention

Bad bots – why?

Bad bots are the #1 contributing factor to application compromise

Source: "The state of application security in 2021", Barracuda Networks
https://www.barracuda.com/appsec-report-2021

Bots are becoming more sophisticated



Barracuda
Threat Intelligence Service™

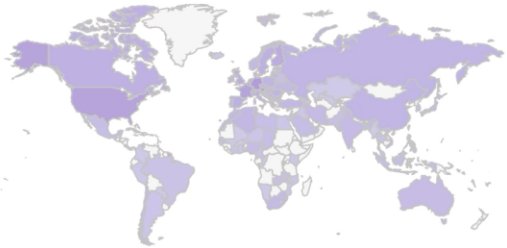
Web Application Firewall [1556467] | SIGN OUT

Adv Bot Protection | Client Side Protection

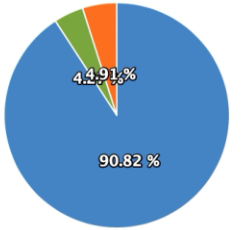
Last 24 Hours

Origins

ALL TRAFFIC | GOOD BOTS | BAD BOTS



Humans vs Bots



Human
Bad Bots
Good Bots

Requests

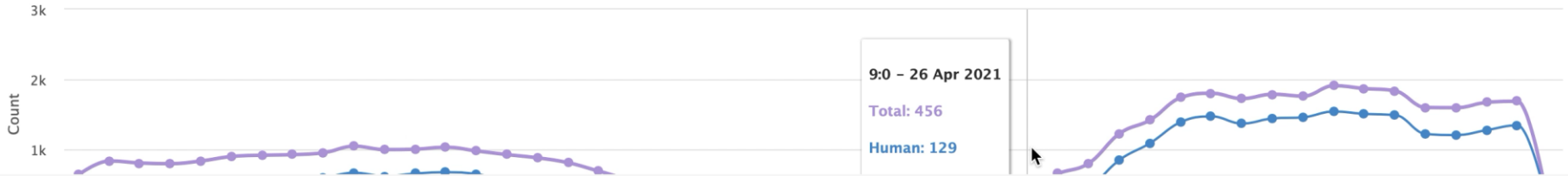
Requests

2,339,215

Attacks

114,876

Clients

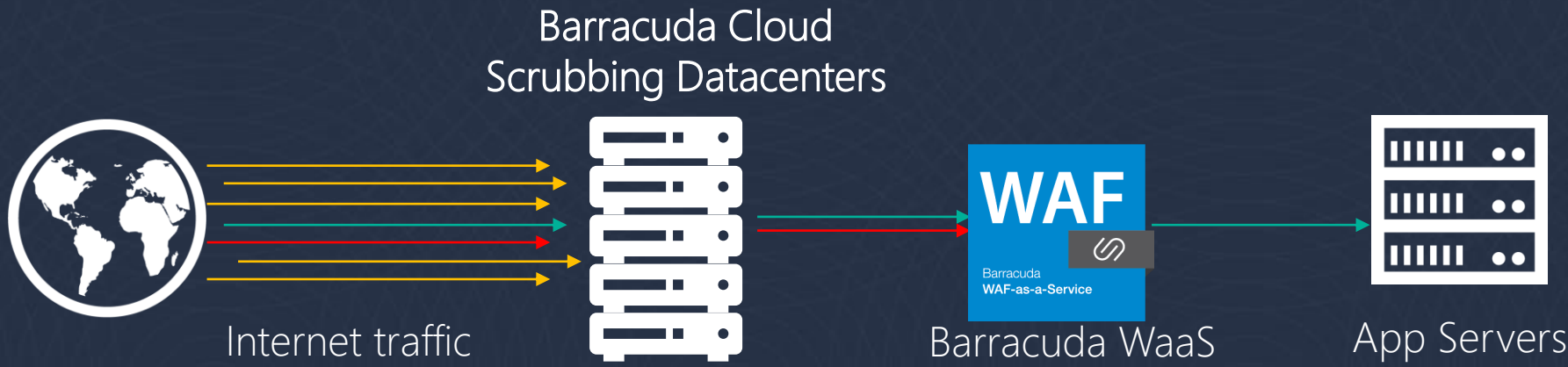


Barracuda

Why is DDoS protection important?

How ADP works

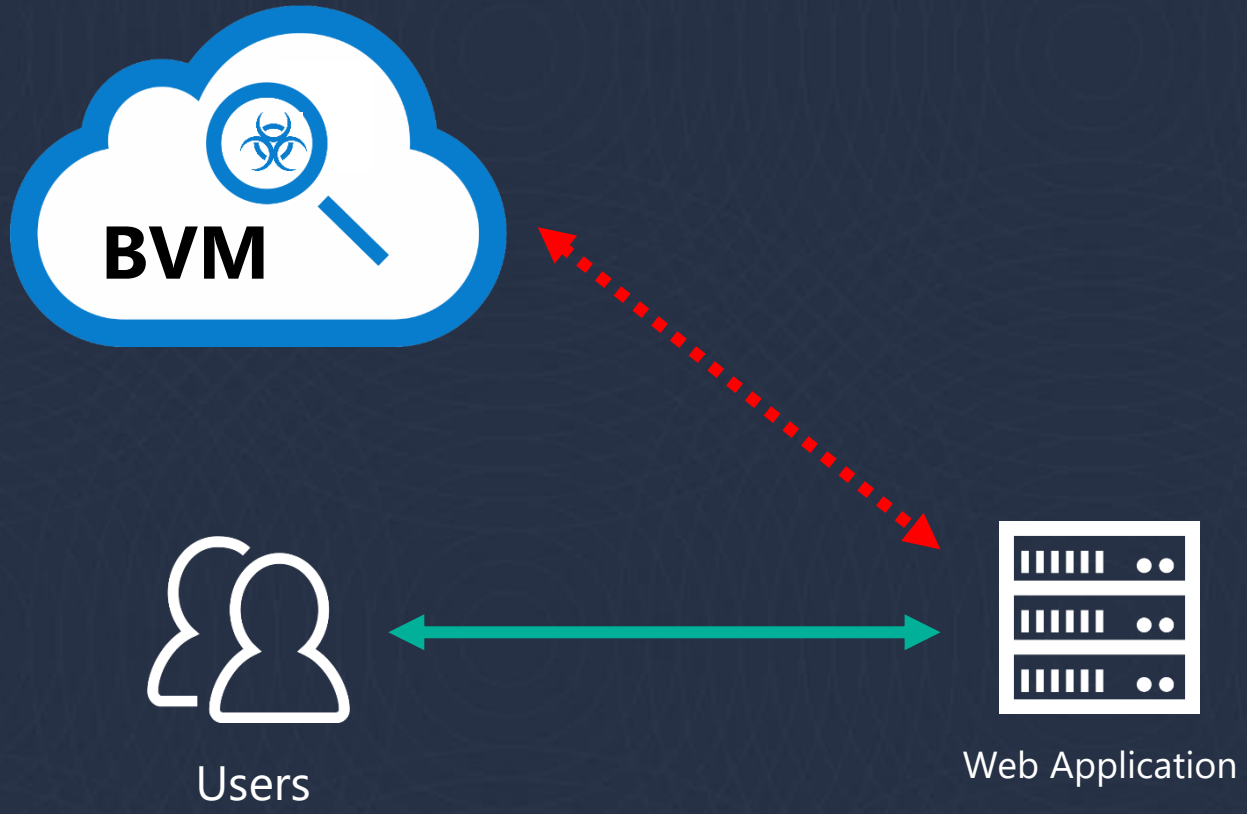
Always integrated with WaaS



Next steps…

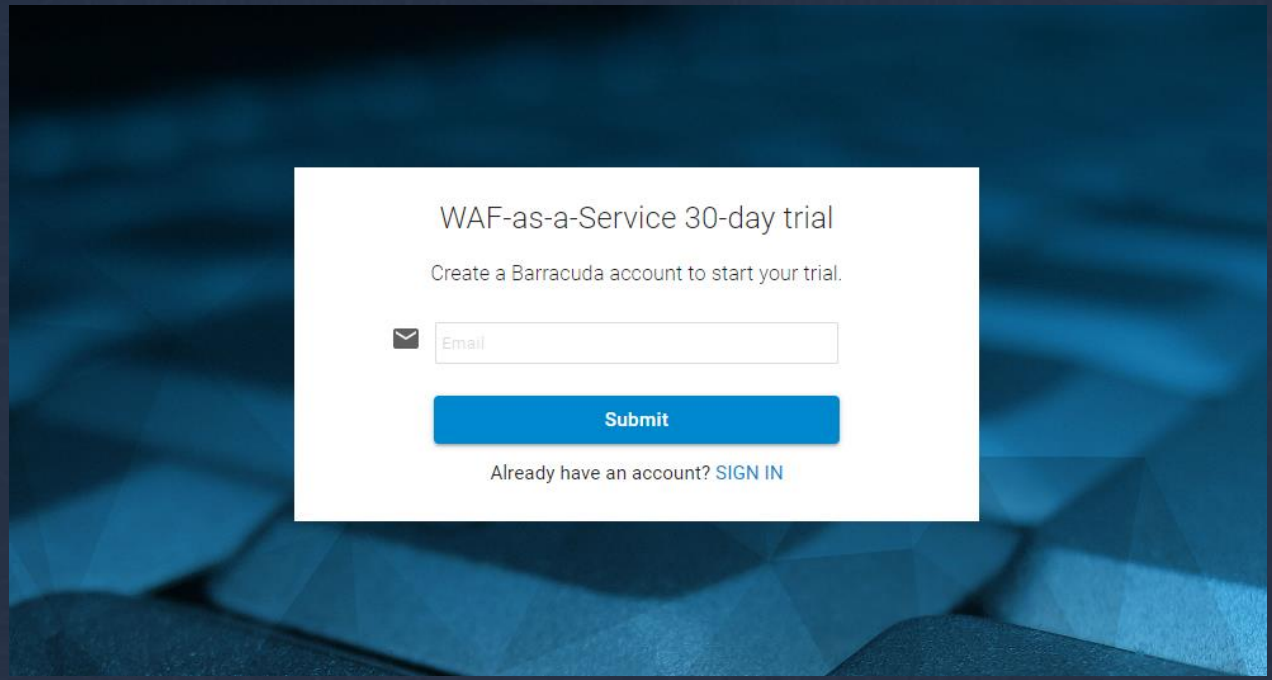
Run a free scan of your application:

https://bvm.barracuda.com/



Sign up for a free trial of WAF-as-a-Service:

https://waas.barracudanetworks.com/start-trial/




Thank you!
Barracuda
Your journey, secured.