

Jak efektivně zabezpečit webové aplikace

Michal Zalewski
Sales Engineer, Barracuda
mzalewski@barracuda.com

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



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

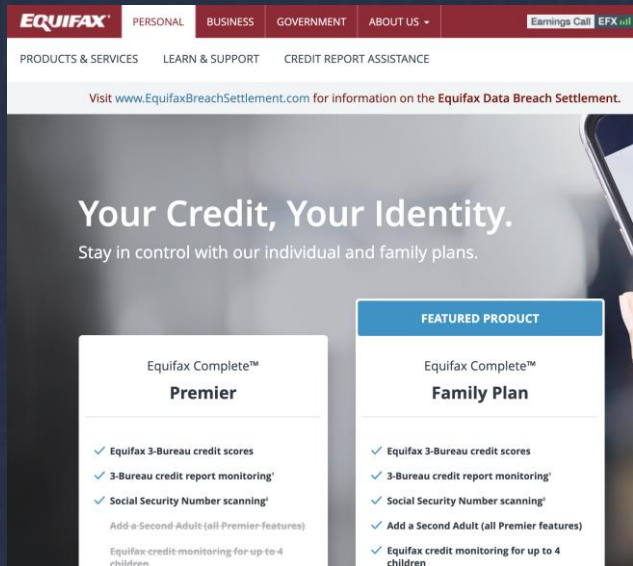


2017

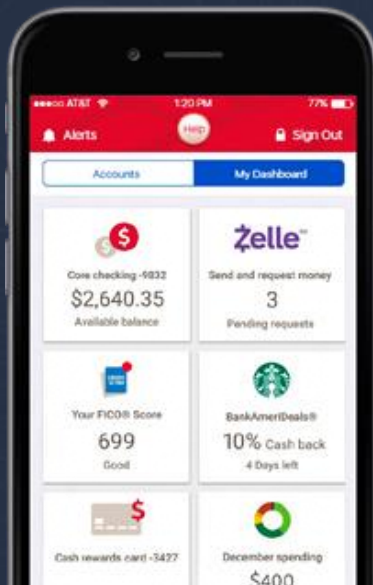


2023

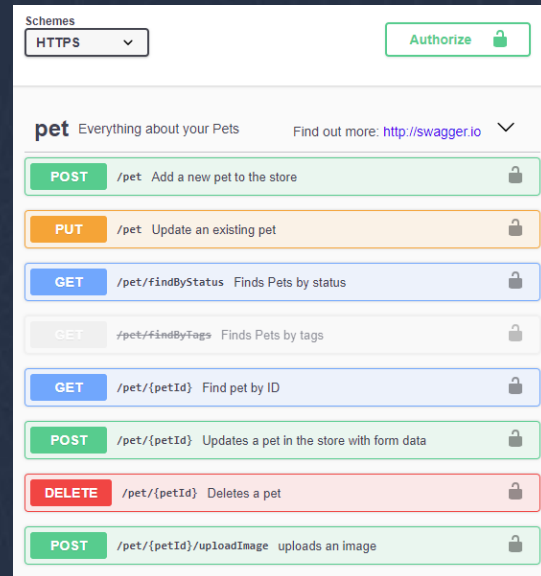
Téměř vše je webová aplikace



Webová stránka



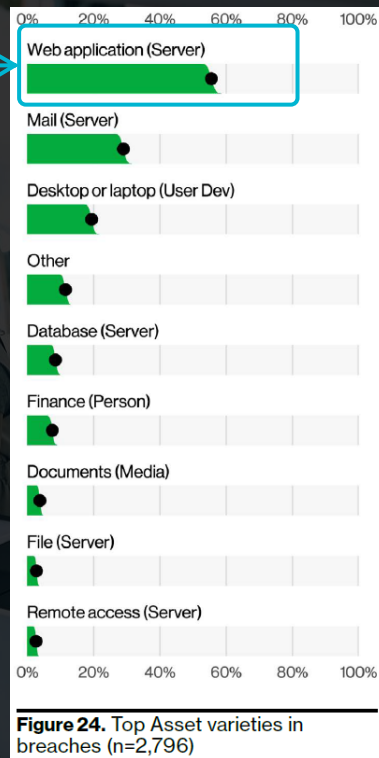
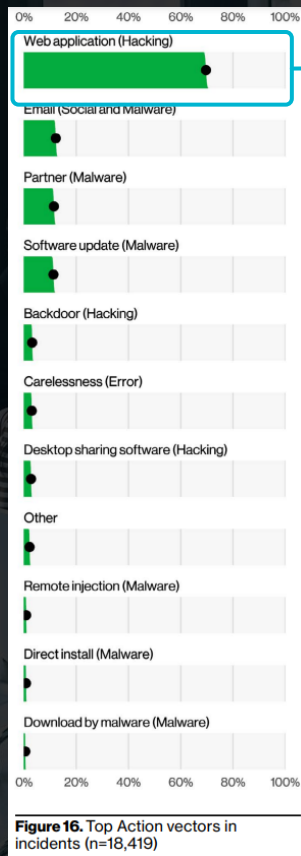
Mobilní aplikace



App Interface (API)

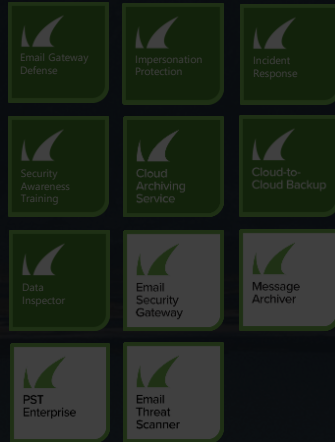


Ztráta dat: nejčastěji ve spojitosti s web. aplikací



Web Application Protection – portfolio Barracuda

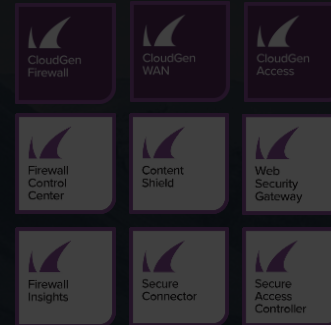
EMAIL PROTECTION



APP AND CLOUD SECURITY



NETWORK SECURITY



DATA PROTECTION



CENTRALIZED MANAGEMENT AND CONTROL

WAF: *hardwarová nebo virtuální appliance*

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

WAF

Barracuda
Web Application Firewall

Fyzické zařízení

WAF

Vx

Barracuda
Web Application Firewall

Virtuální appliance

Podporuje:

- VMware
- Hyper-V
- KVM

WAF



Barracuda
CloudGen WAF

Virtuální appliance

Podporuje:

- Azure
- AWS
- Google Cloud

WAF



Barracuda
WAF-as-a-Service

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

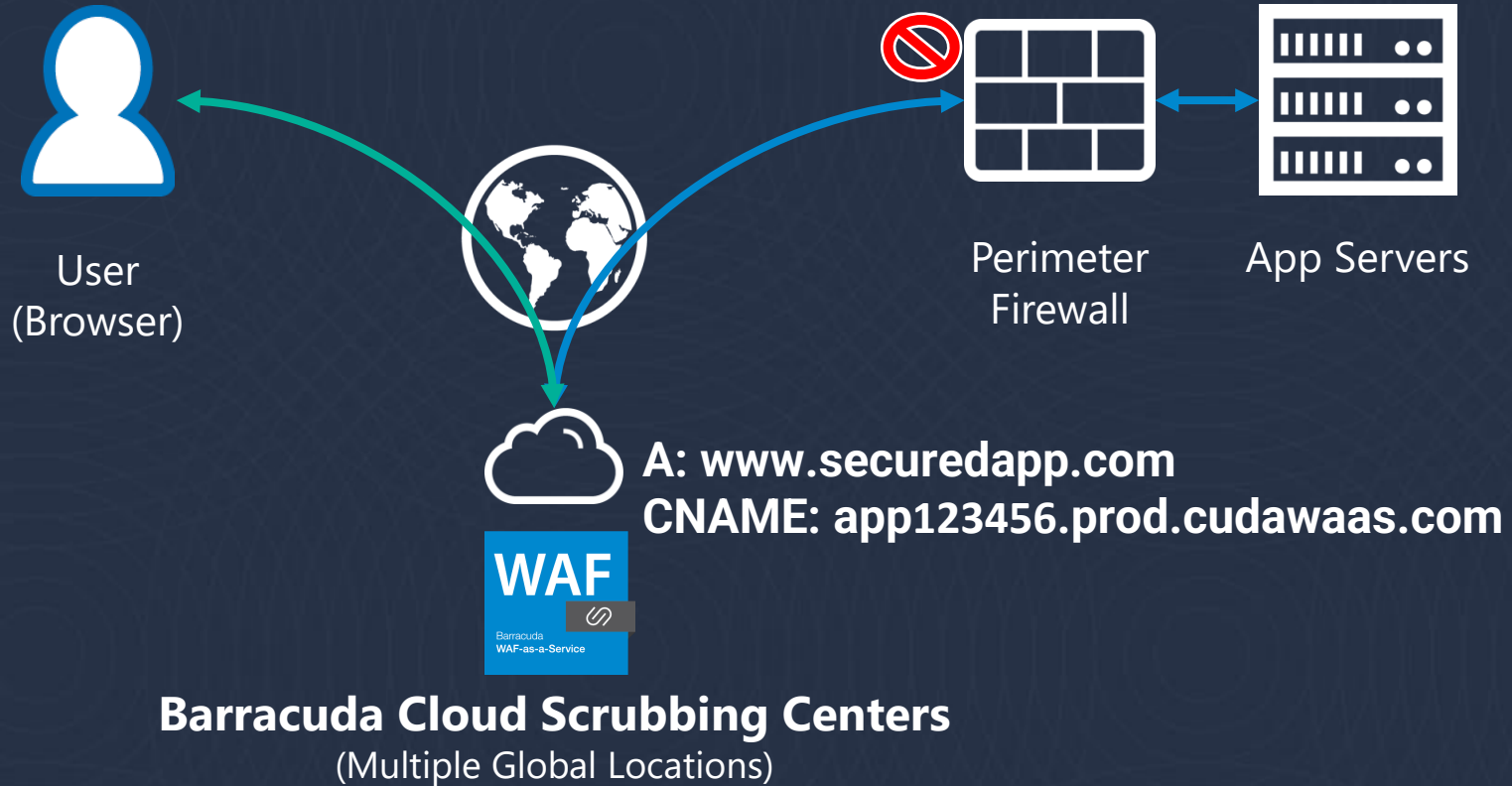
Fully **featured** REST API

Unmetered DDoS **protection** included

Automated vulnerability identification and remediation

WAF-as-a-Service Architecture

How it works



Protects your apps hosted everywhere



On Premises
Data Center

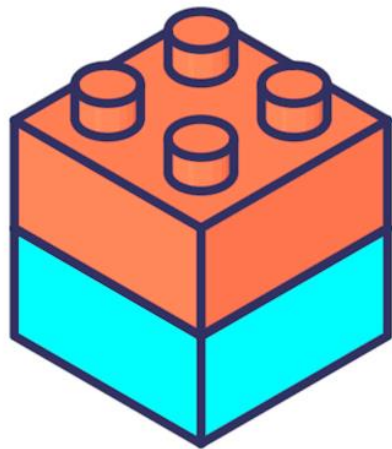


Hybrid



Public Cloud
"All-in"

WAF-as-a-Service Components



WAF-as-a-Service Components

The screenshot shows the Barracuda WAF-as-a-Service dashboard for an application named 'secureapp'. The interface includes a top navigation bar with icons for Applications, Reports, Resources, DNS Zones, and Audit Logs. A left sidebar contains a menu with options: Dashboard, Logs, Endpoints (highlighted), Servers, App Profiles, Recommendations, and a link to Add Components. The main content area is titled 'Endpoints' and contains a description of how endpoints work. Below this, there are configuration cards for 'Deployment Location' (set to Automatic) and 'IP Ranges to Allow'. A status message indicates the application is still being provisioned. At the bottom, a table lists DNS records for the domain 'www.cyber-security.com.pl'.

Endpoints

Barracuda WAF-as-a-Service accepts traffic for your application through Endpoints. One protected application might have multiple listeners. For each application, you can define one or more Endpoints for each of your applications.

Deployment Location
Select the location closest to your application servers. [Learn more](#) **Automatic** [Edit](#)

IP Ranges to Allow
Your backend server should be in one of the following IP ranges.

Your application is still being provisioned. This message will disappear when provisioning is complete. To ensure access to your application, you must update your DNS records.

DOMAIN	CNAME	PORT
www.cyber-security.com.pl (0 more)	app777134.prod.cudawaas.com	80
www.cyber-security.com.pl (0 more)	app777134.prod.cudawaas.com	443

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



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



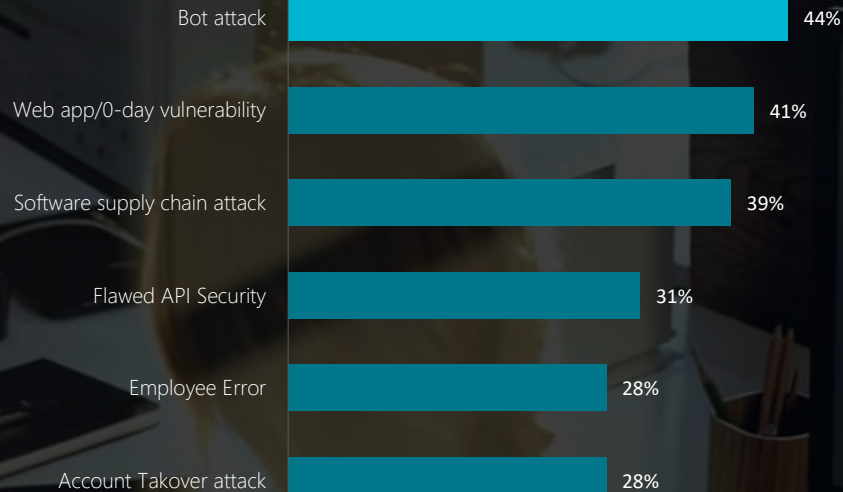
7. Cloaking
8. Data Theft Prevention

Advanced Bot Protection & Active DDoS Prevention

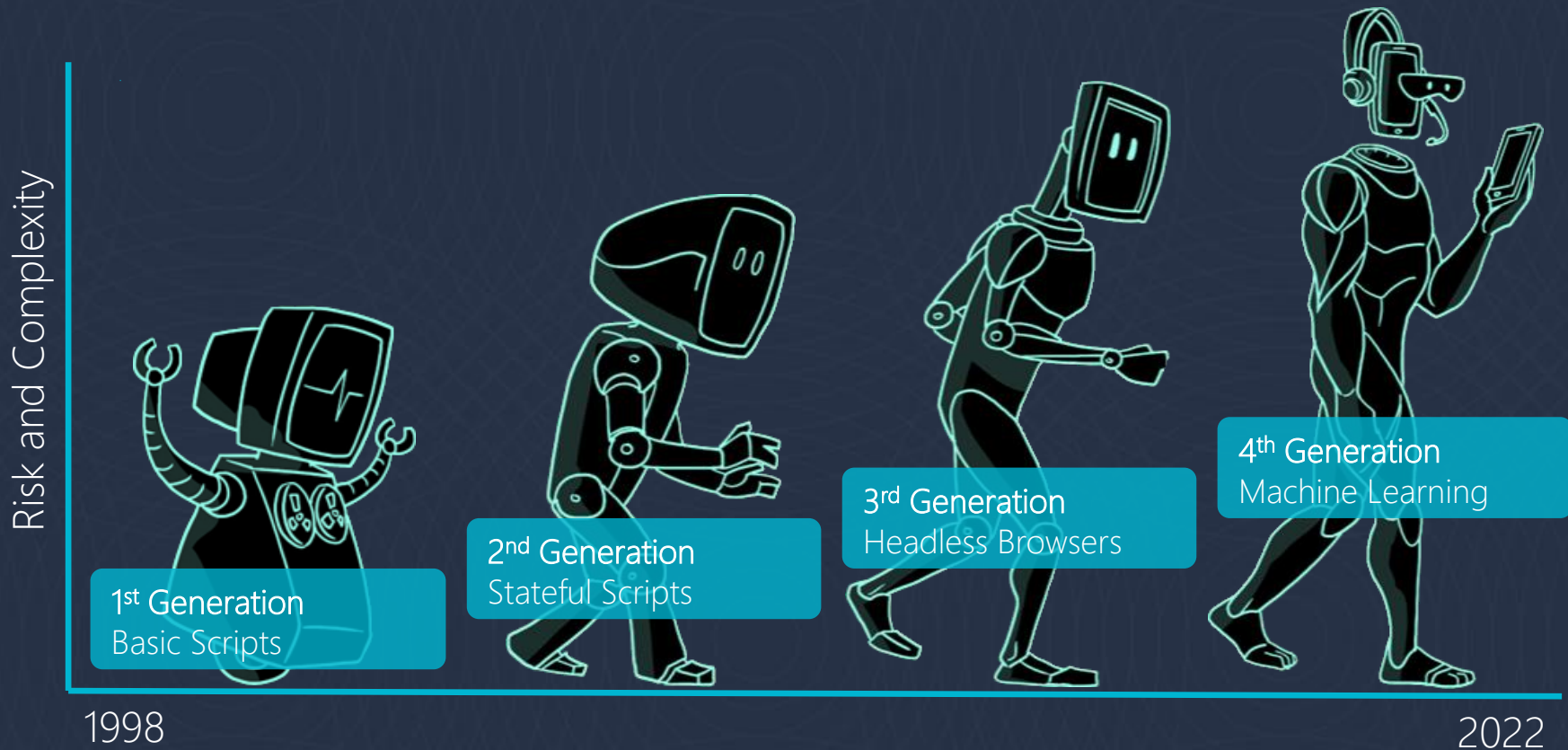
Bad bots – why?

Bad bots are the **#1 contributing factor** to application compromise

Which of the following contributed to the successful security breach that exploited a vulnerability in one of your organization's applications in the last 12 months?



Bots are becoming more sophisticated



Adv Bot Protection

Client Side Protection

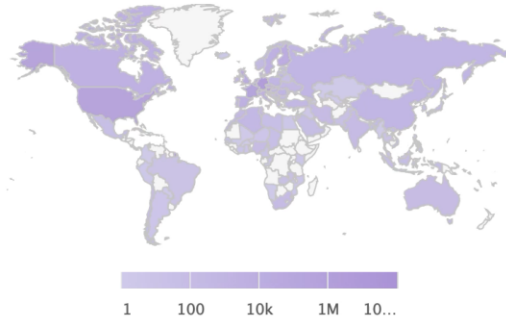
Last 24 Hours

Origins ⓘ

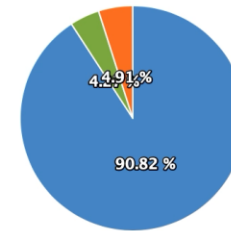
ALL TRAFFIC

GOOD BOTS

BAD BOTS



Humans vs Bots ⓘ



Human
Bad Bots
Good Bots

Requests ⓘ

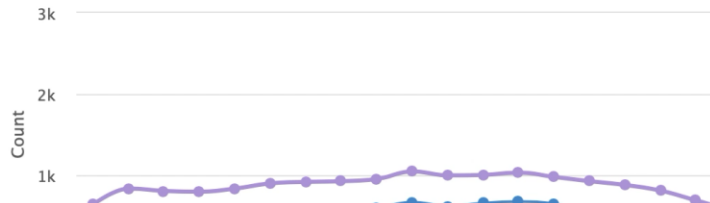
Requests

2,339,215

Attacks

114,876

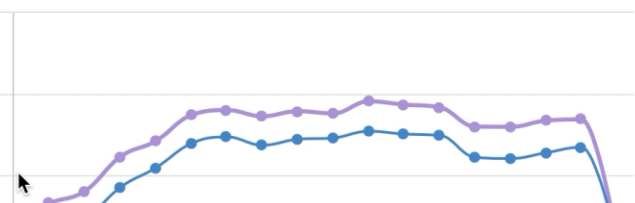
Clients ⓘ



9:0 - 26 Apr 2021

Total: 456

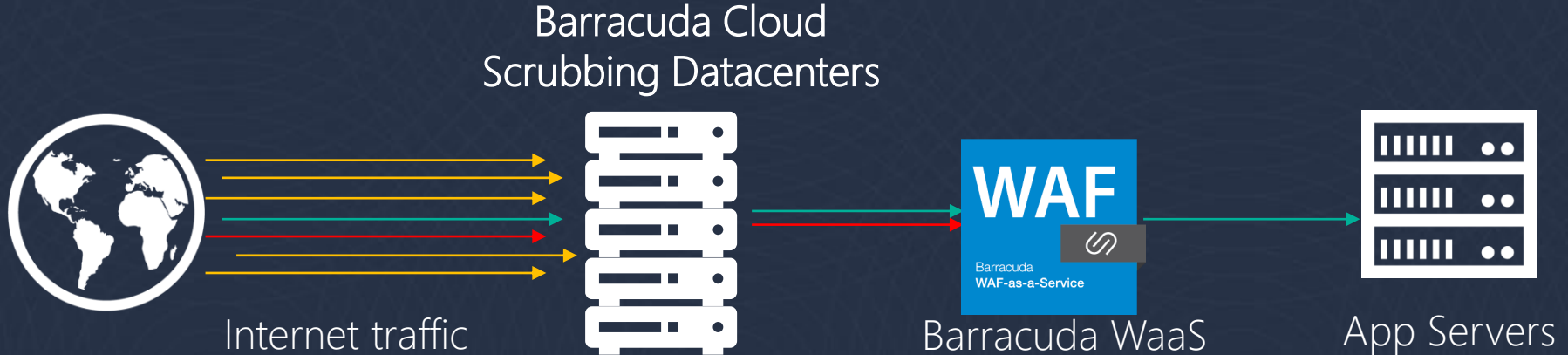
Human: 129



Why is DDoS protection important?

How ADP works

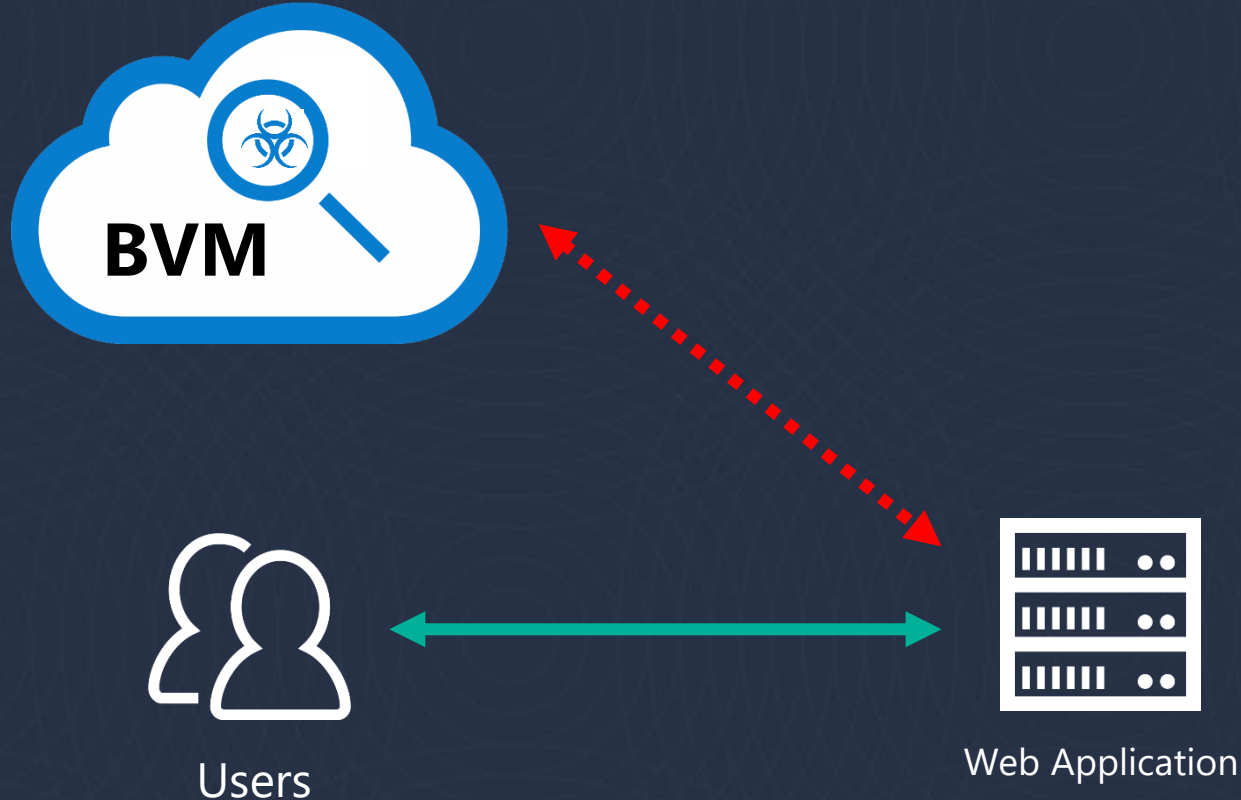
Always integrated with WaaS



Next steps...

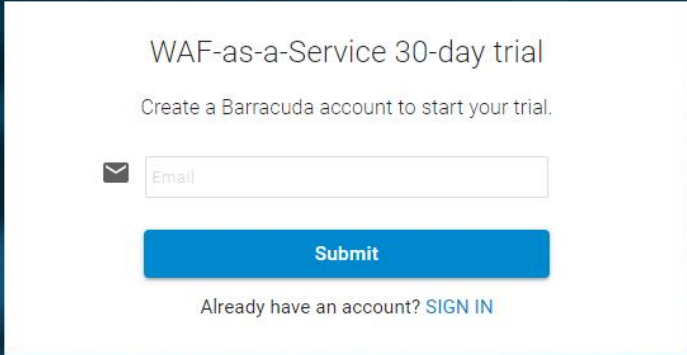
Run a free scan of your application:

<https://bvm.barracuda.com/>



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

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



WAF-as-a-Service 30-day trial

Create a Barracuda account to start your trial.



Submit

Already have an account? [SIGN IN](#)



Thank you!

