

Web Application Firewall

Security for Web Applications



Web apps are at the center of your business

1.1B

apps worldwide vs ~20k in 1995

508

average number of apps per enterprise

“Websites are now the primary window through which businesses conduct business”



Evolving Web:

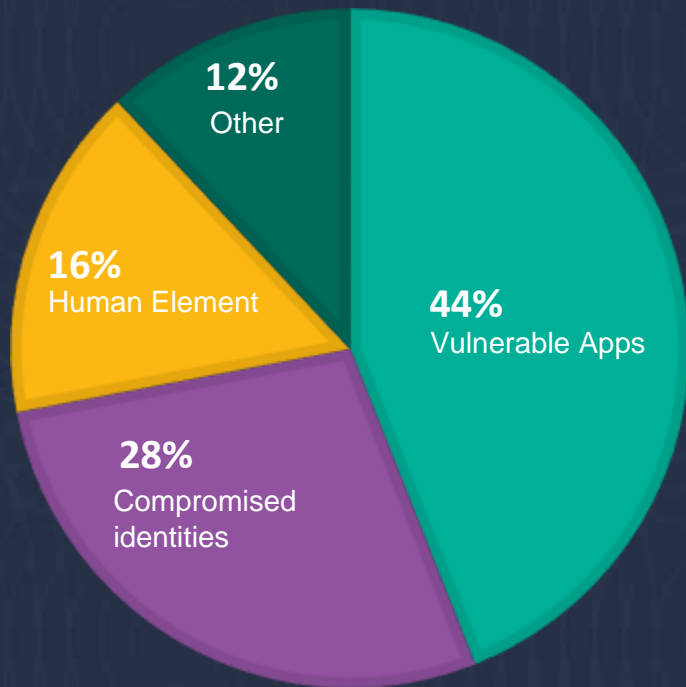
- E-commerce
- Social Networking
- Online Banking
- Office Applications
- Intranet Applications
- CRM
- Content Management Systems



Explosive mobile/SaaS growth



Web Apps are the most Vulnerable Targets



Verizon Data Breach Report 2017

Every 27 minutes a website is hit by a critical exploit

Cisco Annual Security Report 2017

3.1M bots actively attacking

Symantec Internet Security Report 2016

129+ days average time to fix a critical vulnerability

WhiteHat Security Statistics Report 2017

51 vulnerabilities exist on average per website

WhiteHat Security Statistics Report 2017



Yet remain less secured

Perimeter Security

25%

attacks target the perimeter

90%

of security investment

Application Security

75%

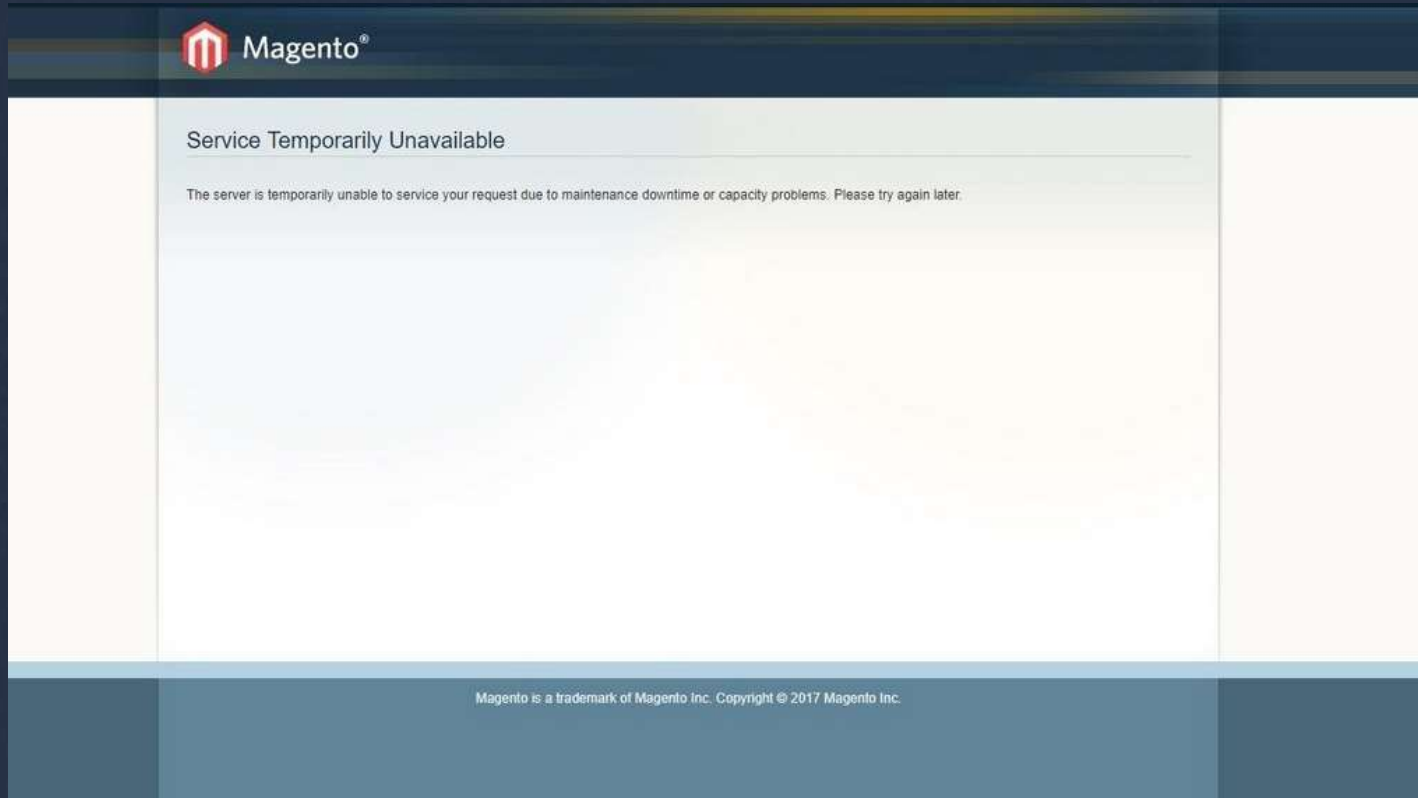
attacks target applications

10%

of security investment



Web App attacks are very disruptive



Risk & Recent Incidents



Allianz-Studie: Cybervorfälle gehören zu größten Unternehmensrisiken

Unternehmensschäden durch Cybervorfälle summieren sich auf 500 Milliarden Euro weltweit, in Deutschland sind es pro Fall durchschnittlich zwei Millionen.

Betriebsstillstand und Cybervorfälle bleiben nach einer Umfrage der Allianz in 80 Ländern die größten Sorgen für Unternehmen rund um den Globus.

Hackerangriffe und sonstige IT-Unfälle belegen in dem neuen "Risikobarometer" des größten europäischen Versicherers sogar erstmals gemeinsam mit Betriebsunterbrechungen den Spitzenplatz, gefolgt von Naturkatastrophen.

Magento: Webserver über Schwachstelle im MySQL-Protokoll gehackt

Eine lange bekannte Funktion im Datenbank-Protokoll MySQL führt aktuell dazu, dass Kriminelle Schadcode in E-Commerce-Shops einbauen.



```
0...
5.1.73.....7!68Hjs.....e8gh!9jG4.=.....
.....root...mysql_native_password.....SET NAMES
utf8,.../home/aapasom/public_html/app/etc/local.xml6 ..<?xml version="1.0"?>
<!--
/**
 * Magento
 *
 * NOTICE OF LICENSE
 *
 * This source file is subject to the Academic Free License (AFL 3.0)
 * that is bundled with this package in the file LICENSE_AFL.txt.
 * It is also available through the world-wide-web at this URL:
 * http://opensource.org/licenses/afl-3.0.php
 * If you did not receive a copy of the license and are unable to
 * obtain it through the world-wide-web, please send an email
 * to license@magentocommerce.com so we can send you a copy immediately.
 *
 */

```

11 client pkts/1. 8 server pkts/1. 75 turns/1.

Entire conversation (7,495 bytes) Show and save data as: ASCII Stream 0

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

Source: <https://www.heise.de/security/>

PHP-Code-Bibliothek: PEAR-Website nach Hack offline

Der Grund ist eine Hacker-Attacke auf die PEAR-Website. Den Verantwortlichen zufolge stand dort rund ein halbes Jahr eine wahrscheinliche mit Schadcode manipulierte Version der Installationsdatei zum Download.



Dreimal so viele Sicherheitslücken in WordPress wie im Vorjahr

WordPress bot 2018 so viel Angriffsfläche, wie noch nie. Daran ist aber nicht das CMS direkt Schuld. 98 Prozent gehen auf das Konto von Plug-ins für das CMS. Derzeit sind in der offiziellen Quelle von WordPress mehr als 54.000 Plug-ins verfügbar.



Source: <https://www.heise.de/security/>

Datendiebstahl mittels Web Scraping



23 JUN 2015 **NEWS**

Data Theft Watch: Web Scraping Attacks Almost Double

Tara Seals US/North America News Reporter, Infosecurity Magazine
[Email Tara](#)

Online businesses' risk from data theft due to web scraping—harvesting website info—has almost doubled, especially for sectors like travel sites.

Save S\$200 when you register before 18 June. #RSAC

... Very recently we've seen airlines announce increases in booking fees to tickets booked through third parties, because scraping and the loss of revenue that causes is a very real threat to their businesses ...

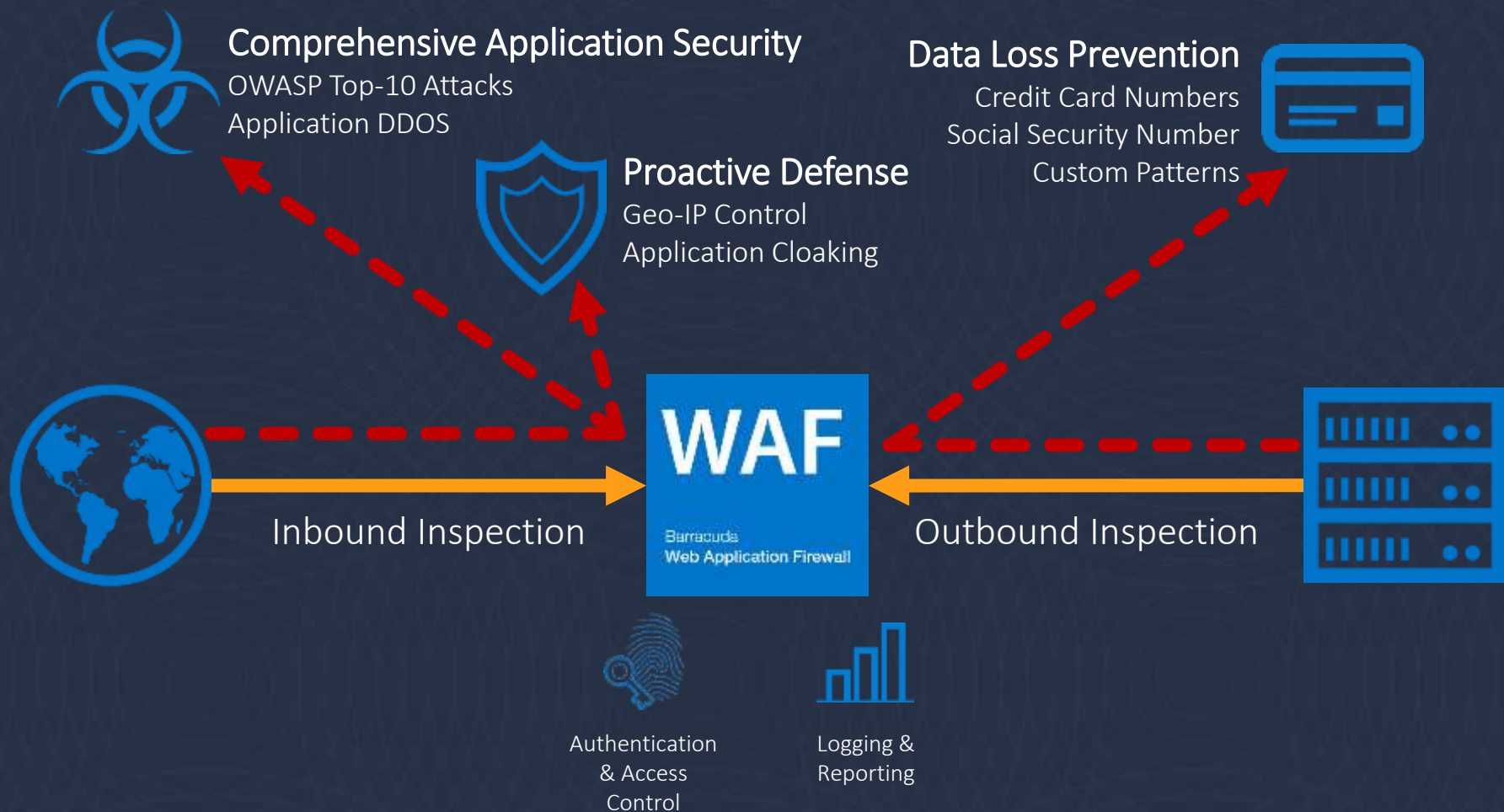
Cloud Generation Application Security



Challenges with traditional Application Security

- Too expensive
- Too complex
- Does not provide enough controls
- Does not work for apps deployed on cloud platforms





All-in-One Application Security Platform

WAF
AZURE
Barrauda
Web Application Firewall



Security &
DDoS Protection



Load Balancing &
Server Health Monitoring



Logging & Reporting



Authentication & Access
Control



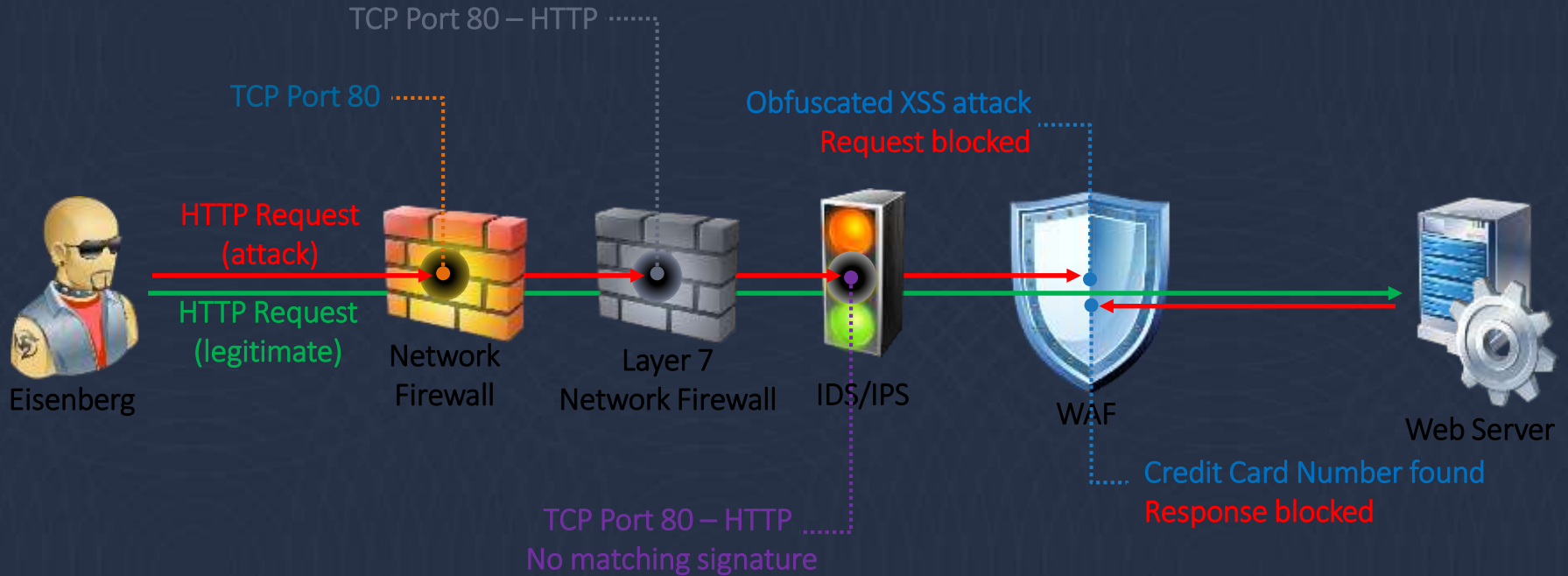
Session Persistence



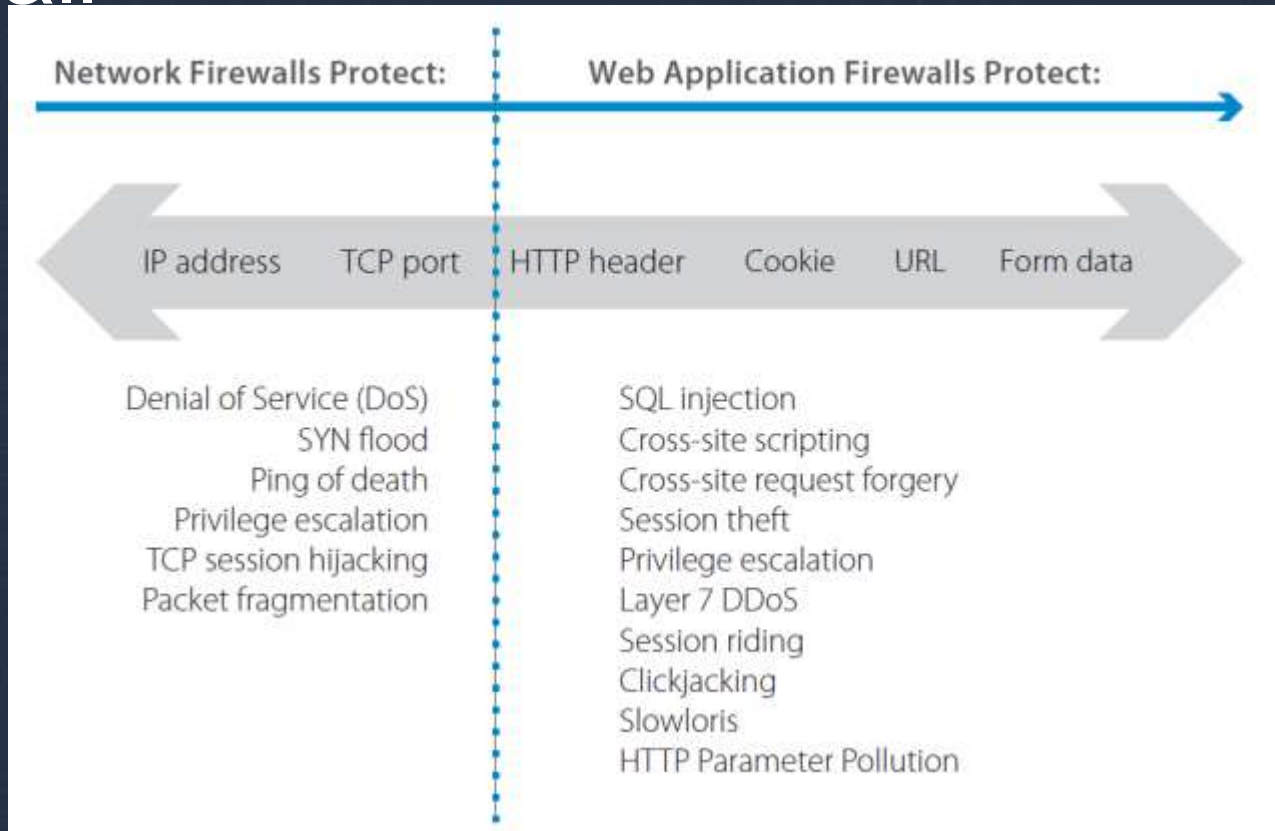
SSL & Performance
Acceleration



The WAF reverse proxy paradigm



Network Firewall vs. Web Application Firewall



WAF Deployment Options



Barracuda Web Application Security



Enterprise proven security

Application acceleration and access control

Complete control and visibility

Fully automated vulnerability scanning and remediation

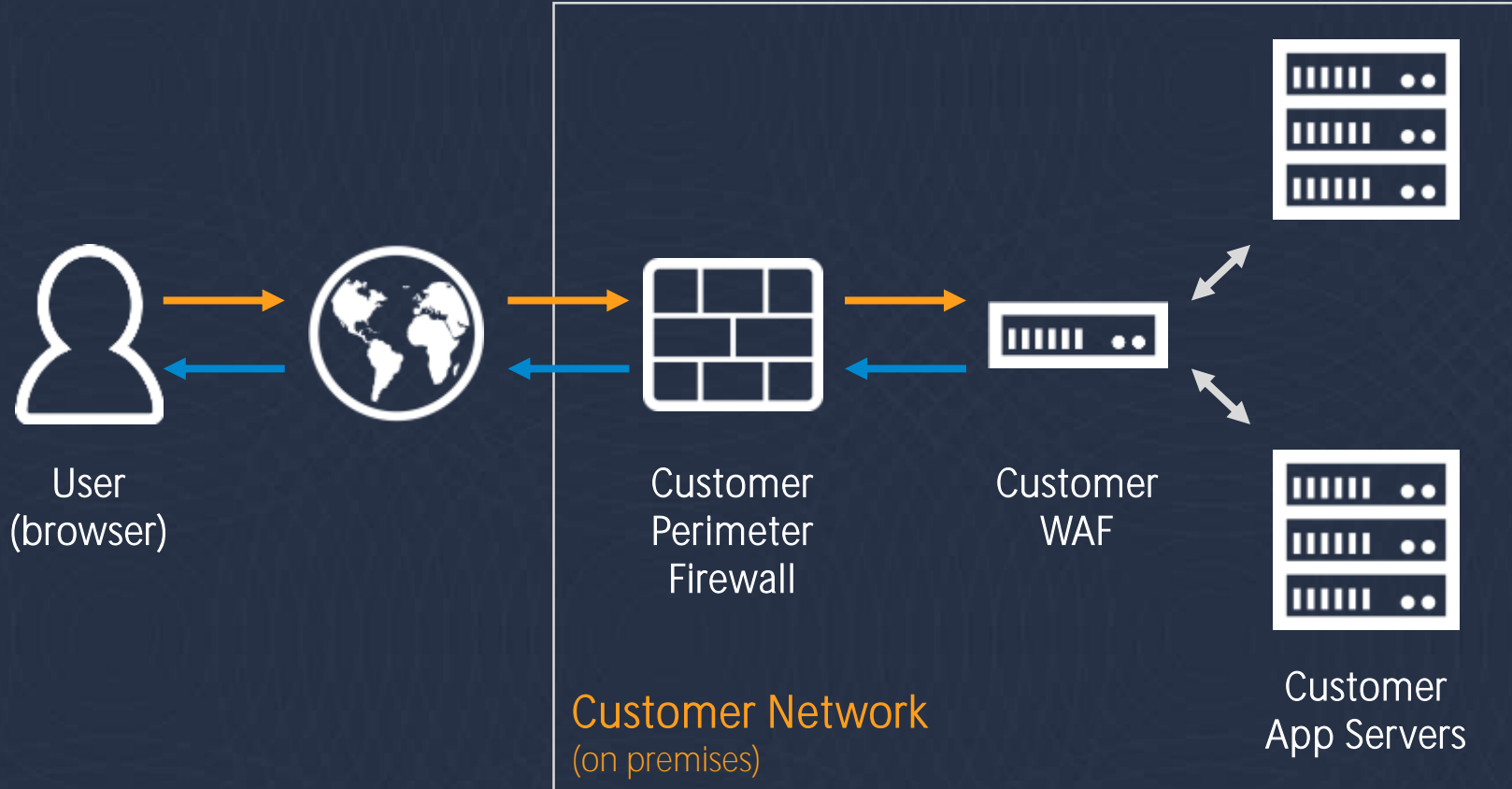
Deploy in any way you want (on-prem, SaaS, public cloud)

Automation and orchestration

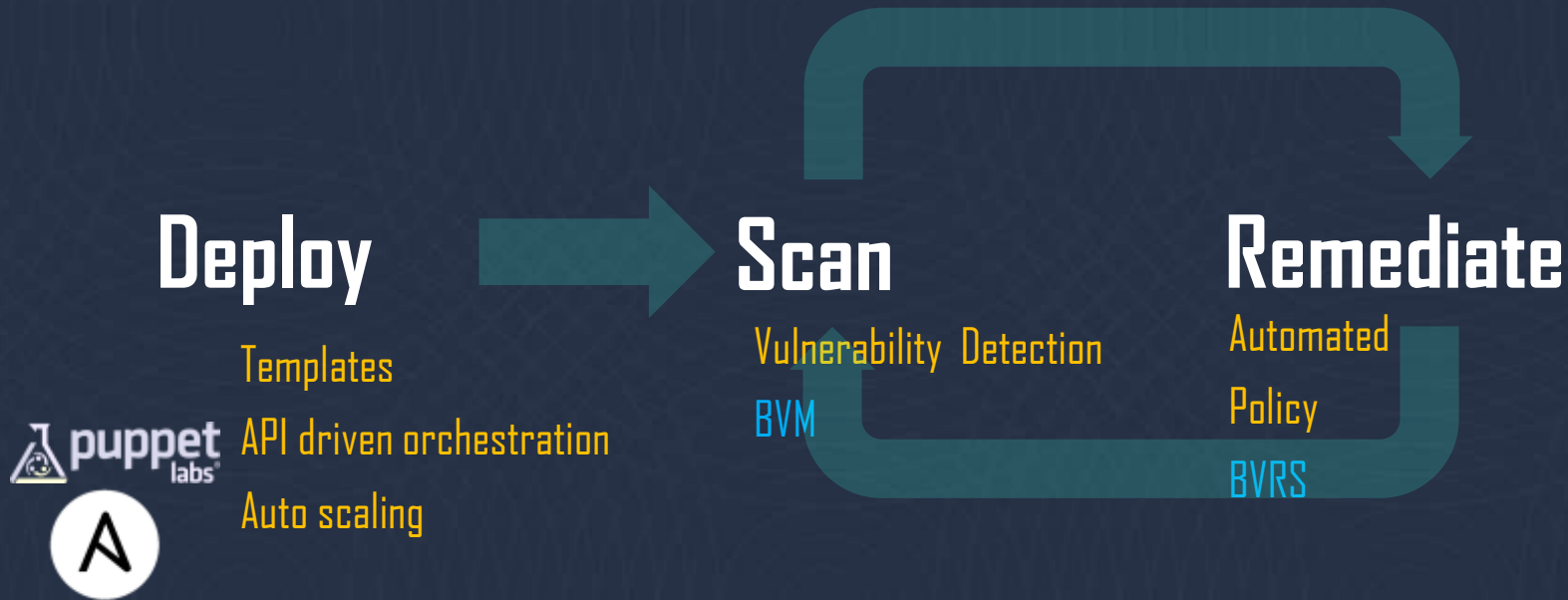
Centralized Management

Cost Effective

WAF Deployment



Security Automation



Integration with Vulnerability Remediation Service

SCHEDULABLE or on demand

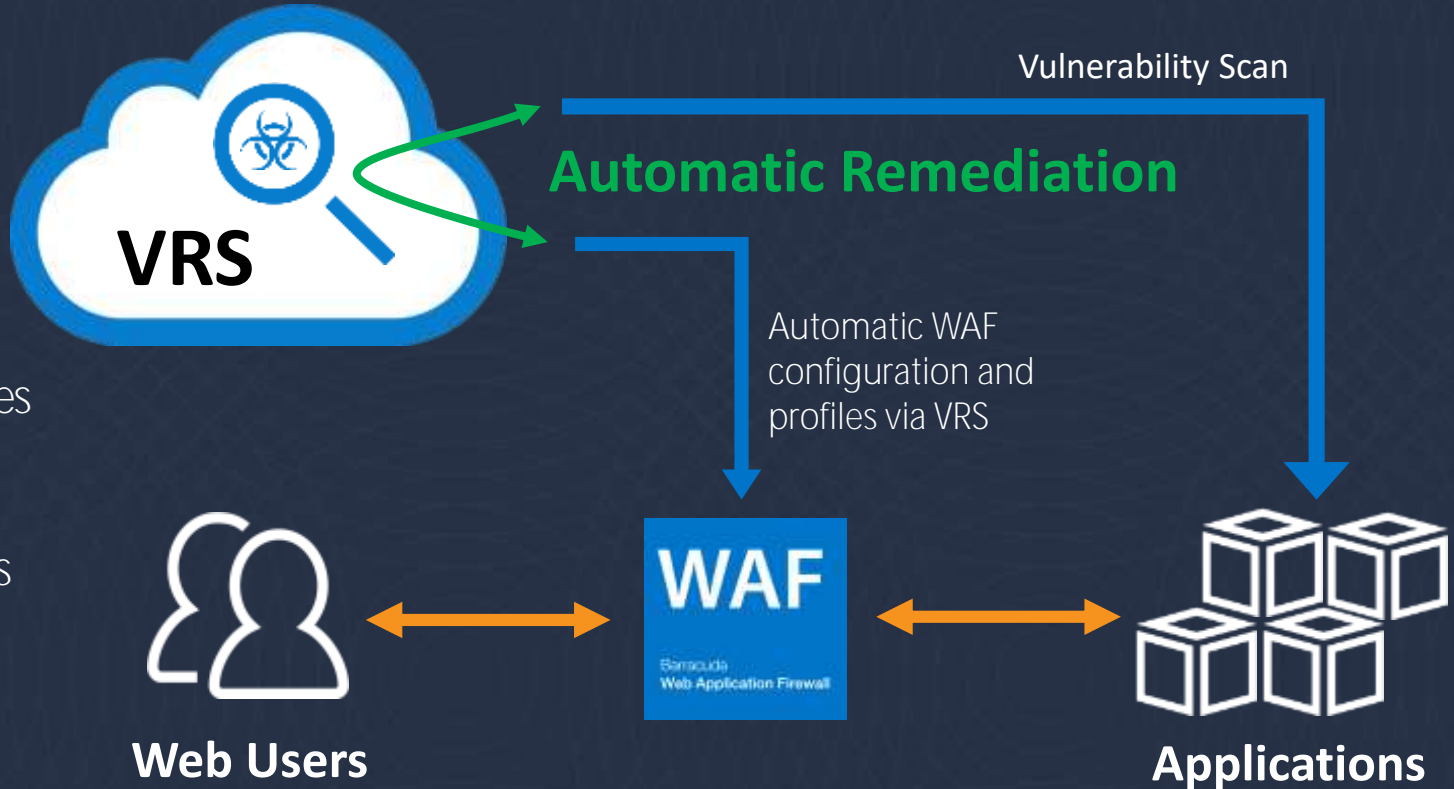
SCAN applications and report vulnerabilities

MANAGE vulnerability workflow/lifecycle

REMEDiate vulnerabilities automatically on the WAF

MONITOR vulnerabilities with scheduled scans

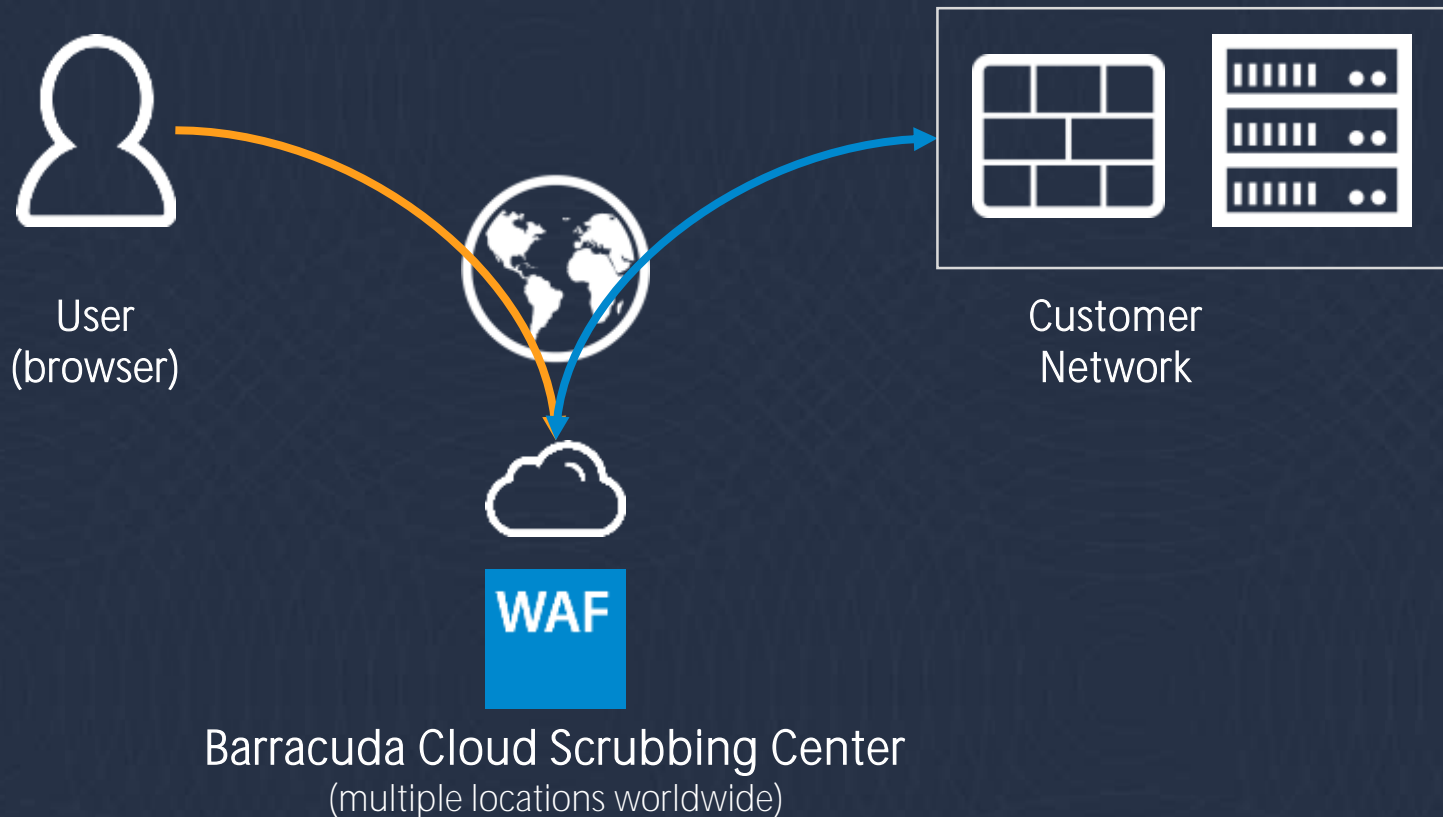
Currently Free



Barracuda WAF-as-a-Service



What is WAF-as-a-Service?



WAF-as-a-Service vs WAF

- Nothing to deploy
- Nothing to size or scale
- No firmware to upgrade
- No hardware to replace



Simple easy to use 5 step deployment

Add Application

✓

✓

✓


✓

5

WebsitesIP AddressBackend ServerSelect ModeChange DNS

Visit your hosting provider's dashboard to change your A Record to the following.
Not sure which hosting provider to use? [Check the Registrar section here](#)

Important: Changing your A records causes no interruption or site downtime. The change can take up to 24 hours, but is seamless for you and your users. interruption. Your site will remain available throughout the switch.

DOMAIN	CURRENT A RECORD	CHANGE A RECORD TO	
 www.barracuda.com	64.235.144.155	64.113.50.88	CLICK TO COPY

CLOSE



Adding Additional Endpoints

New Endpoint

Domains

baracuda.com

+

www.baracuda.com

+

-

baracuda.net

+

-

www.baracuda.net

+

-

Protocol

HTTP

IP Address

☒ Use a unique IP Address for this service

72.13.148.93 : 443

☐ Use the same IP Address as another service

Private Key

Paste the private key including the BEGIN and END lines shown below

-----BEGIN PRIVATE KEY-----
MIIEYDCCAGwAwIBAgJINLQgTzPxtvR6M6DCsgO083DQ3B883pAAwRqRtqewC7YD
-----END PRIVATE KEY-----

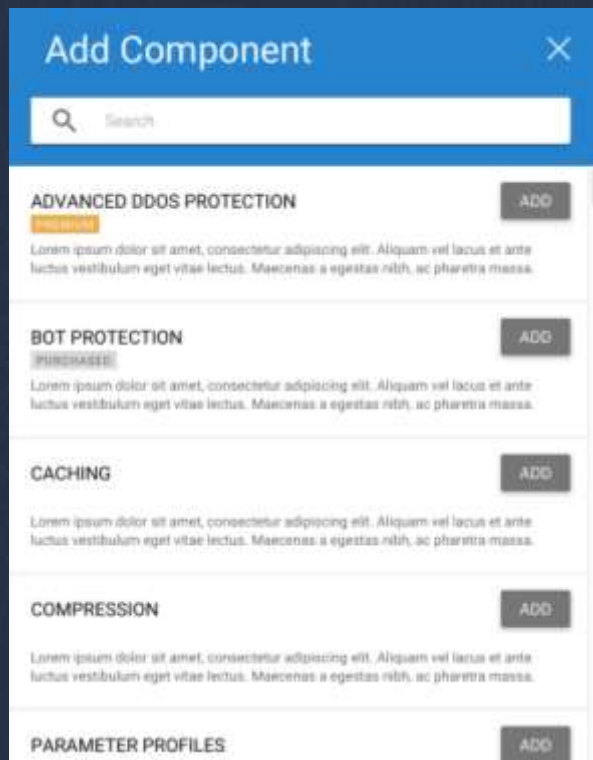
Certificate

Paste the certificate and optional certificate chain including the BEGIN and END lines

-----BEGIN CERTIFICATE-----
MIIDETCCA2gAwIBAgJINLQgTzPxtvR6M6DCsgO083DQ3B883pAAwRqRtqewC7YD
-----END CERTIFICATE-----



Adding Additional Components



Dashboard

OVERVIEW

APPLICATIONS

REPORTS

Applications

Search by name

ADD APPLICATION

NAME	DNS STATUS	SERVER STATUS	BLOCK ATTACKS	ACTIONS
My First Application	<div><div></div>Update Pending details</div>	<div><div></div>3 Servers Up details</div>	<div><div></div>OFF</div>	<div><div></div></div>
My Second Application	<div><div></div>Configured details</div>	<div><div></div>1 of 3 Servers Down details</div>	<div><div></div>YES</div>	<div><div></div>Rename</div>
My Third Application	<div><div></div>Configured details</div>	<div><div></div>All Servers Down details</div>	<div><div></div>YES</div>	<div><div></div>Delete</div>

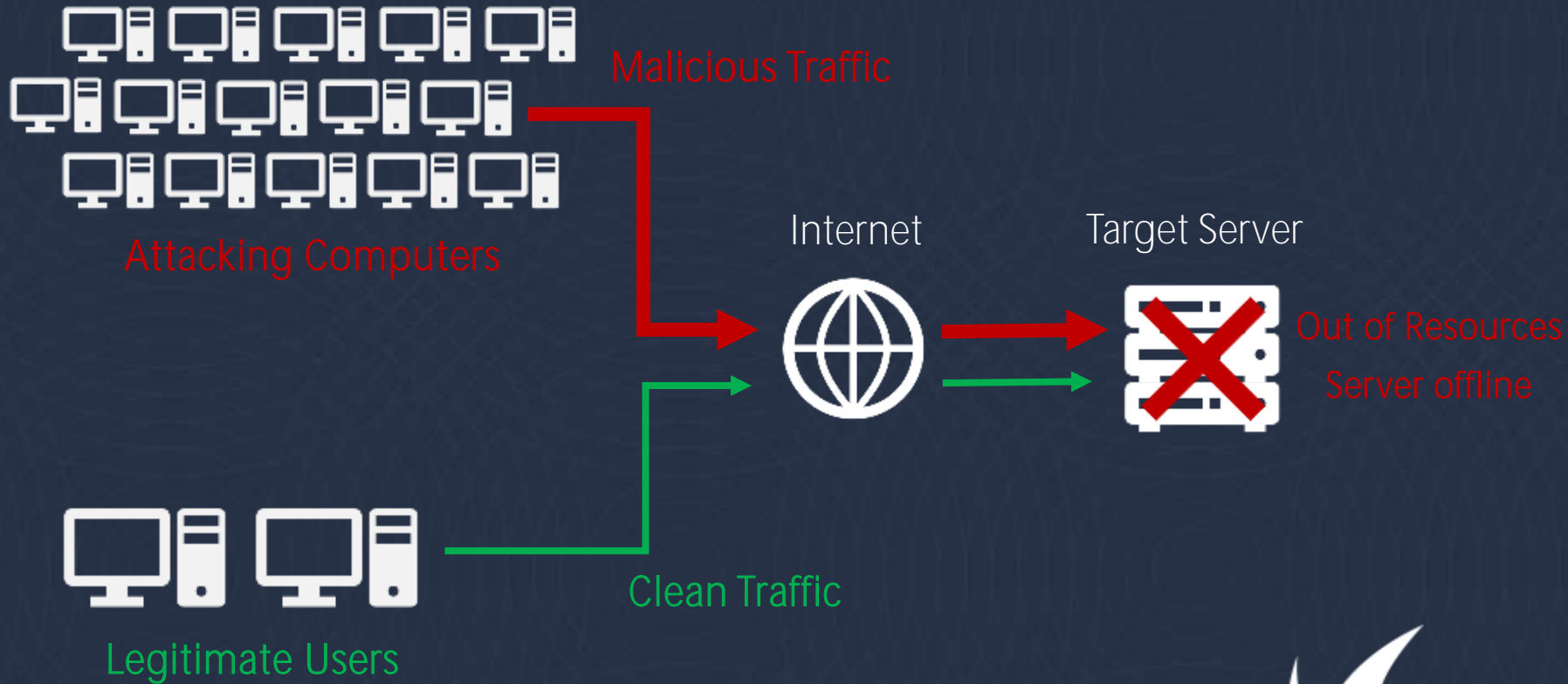
© 2017 Barracuda Networks, Inc. All rights reserved. | [Privacy Policy](#)

Barracuda

DDoS Attacks & Prevention



What is DDoS? Distributed Denial of Service



Effects of DDoS attacks



\$22,000 per min for
single SMB attack



54 minute
average downtime



Volumetric DDoS
attacks range
200-400 Gbps



Barracuda Active DDoS Prevention (ADP)

Always-on DDoS solution that prevents volumetric DDoS attacks from ever reaching a customer's network

- ✓ Add-on subscription to WAF
- ✓ Priced at 30% the cost of WAF





DASHBOARD



BASIC



ALLOW LIST



BLOCK LIST



BRUTE FORCE



WEB SCRAPING



SLOW CLIENT



CLIENT EVALUATION



Dashboard

10 minutes



Status ⓘ

Last 10 minutes

Under Attack Service Down Service Up

Under Attack

10:02AM 10:04AM 10:06AM 10:08AM 10:10AM

Service Up

Service Down

10:02AM 10:04AM 10:06AM 10:08AM 10:10AM

Blocked IP Addresses ⓘ

Last 10 minutes



Requests ⓘ

Last 10 minutes

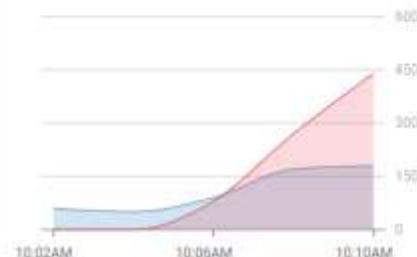
Allowed Suspicious



Connections ⓘ

Last 10 minutes

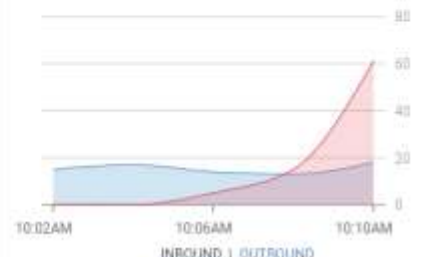
Valid Spoofed



Bandwidth ⓘ

Last 10 minutes

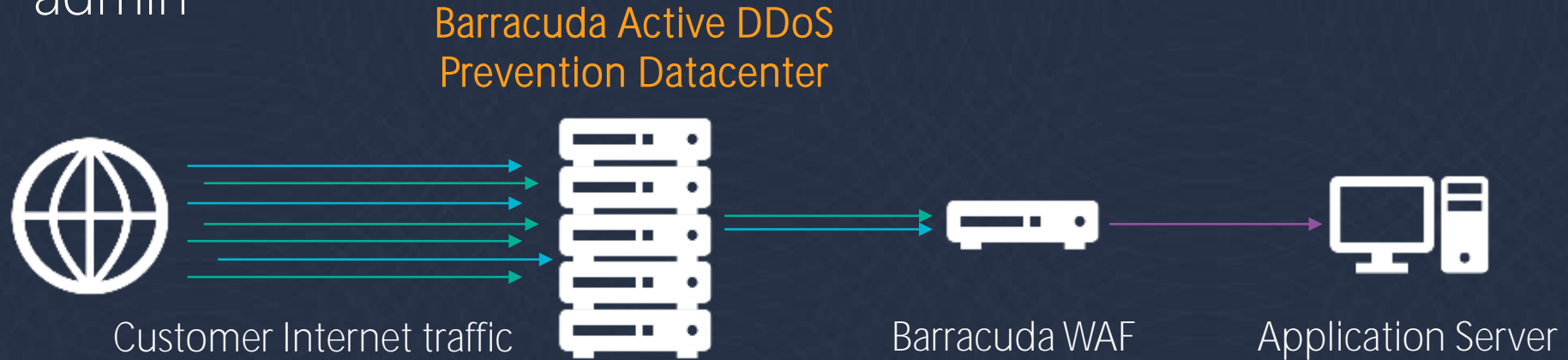
Allowed Blocked



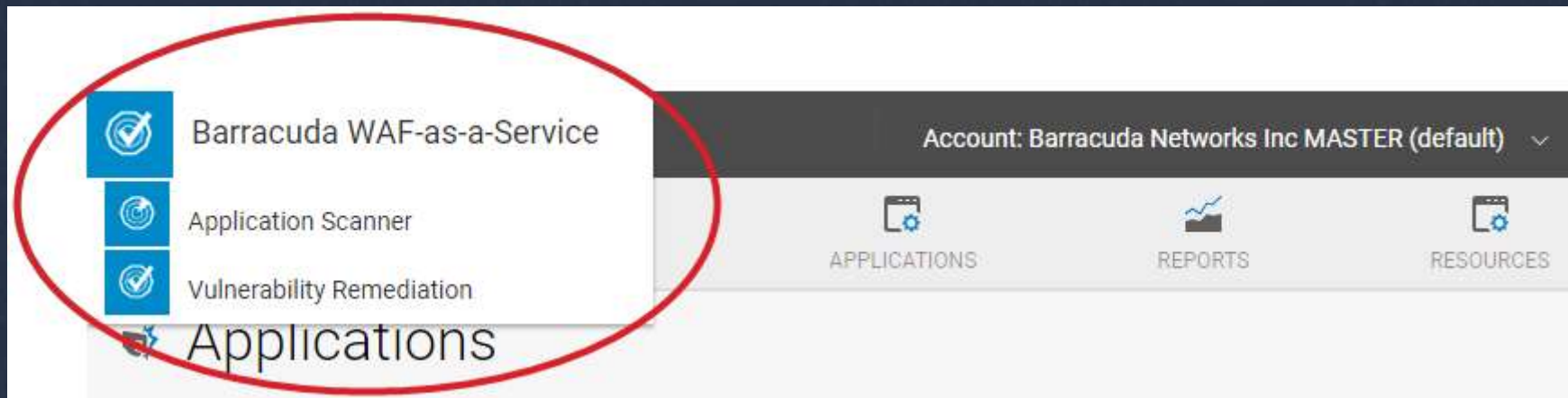
INBOUND | OUTBOUND

How it works

1-step setup: Point DNS record to DDoS service in WAF admin



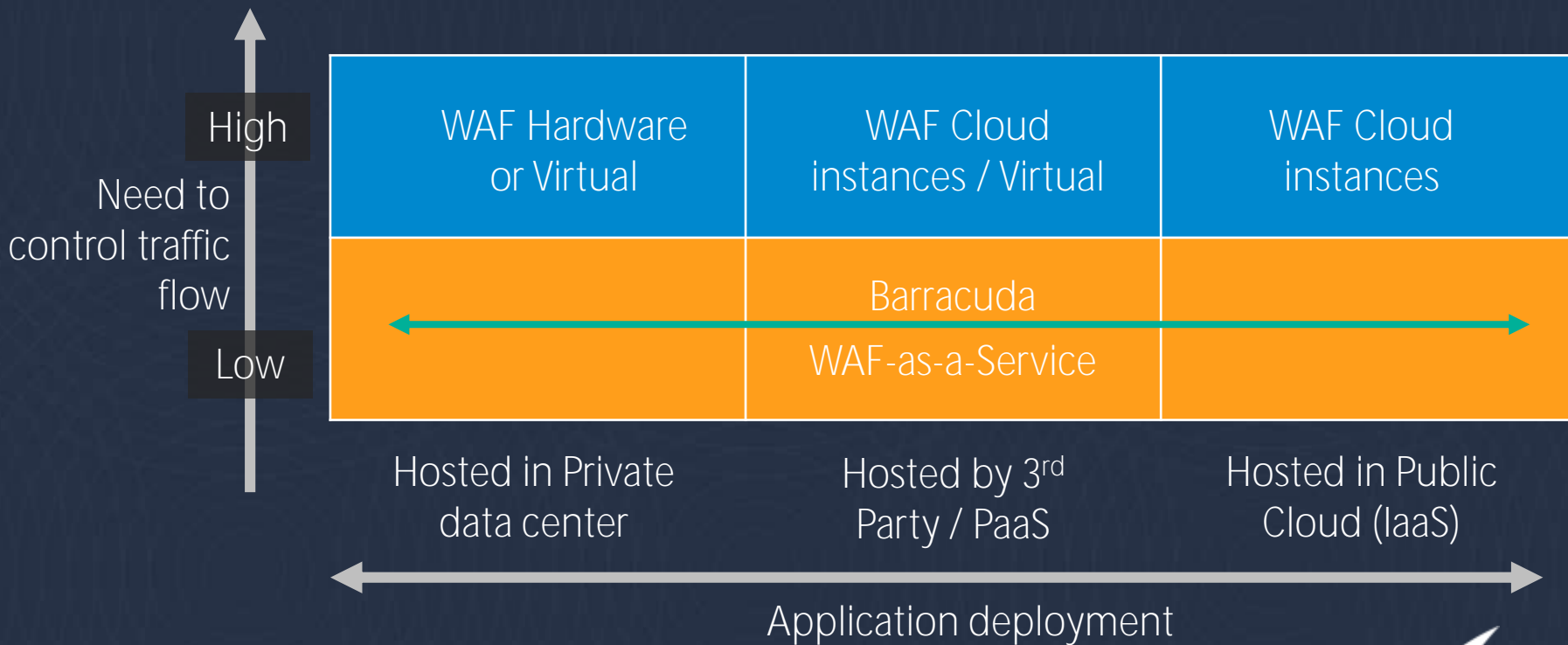
VRS is built right in to WAF-as-a-Service



WAF vs. WaaS



Choosing the right deployment option



Who should use which?

Should use WAF-as-a-Service

"I'm not an application security person; I want something that's easy to configure." (SMB)

"My apps are not all born-in-the-cloud; I have on-premises applications, or applications that are lifted-and-shifted to the cloud."

"I want to set-it-and-forget-it." (SMB)

"I want to point and click, not use APIs and templates."

Should use WAF

"I am very particular about who touches my data and what countries it passes through." (regulatory)

"I am comfortable with complexity and want full control of all features, at the cost of more configuration work." (some large enterprises)

1

Start with an account

€0 new Account SKU	
BWFS000a	€0

+

2

Add ANY # of Apps

SKU	Total # of Apps	Price (EUR)
BWFS1-APP-c12	1 Application	€258

Examples ->

7 Apps? €258*7 = €1,806
23 Apps? €258*23 = €5,934

+

3

Add ONLY 1 bandwidth SKU

SKU	Total Bandwidth Required	Price (EUR)
BWFS025a-e12	25 Mbps Bandwidth	€4,312
BWFS050a-e12	50 Mbps Bandwidth	€7,546
BWFS075a-e12	75 Mbps Bandwidth	€10,511
BWFS100a-e12	100 Mbps Bandwidth	€12,936
BWFS250a-e12	250 Mbps Bandwidth	€21,560
BWFS500a-e12	500 Mbps Bandwidth	€32,340
BWFS1000a-e12	1 Gbps Bandwidth	€43,120
BWFS5000a-e12	5 Gbps Bandwidth	€161,700

Select ONLY ONE SKU for Bandwidth

Pricing is simple and only requires 2 pieces of information:

- 1) The total number of websites and web apps being protected
- 2) The total bandwidth of all those sites and apps combined. If a customer doesn't know their needed bandwidth, we can answer it for them at the end of their free trial.

New account + # of Apps + 1 Bandwidth SKU + Add-ons =
total annual cost for Barracuda WAF-as-a-Service

Barracuda WAF-as-a-Service Add-on Pricelist (1 year price)

SKU	ATP Add-on	Price (EUR)
BWFS025a-a12	ATP (For 25 Mbps Bandwidth)	€1,725
BWFS050a-a12	ATP (For 50 Mbps Bandwidth)	€3,019
BWFS100a-a12	ATP (For 100 Mbps Bandwidth)	€5,175
BWFS250a-a12	ATP (For 250 Mbps Bandwidth)	€8,624
BWFS500a-a12	ATP (For 500 Mbps Bandwidth)	€12,936
BWFS1000a-a12	ATP (For 1 Gbps Bandwidth)	€17,248

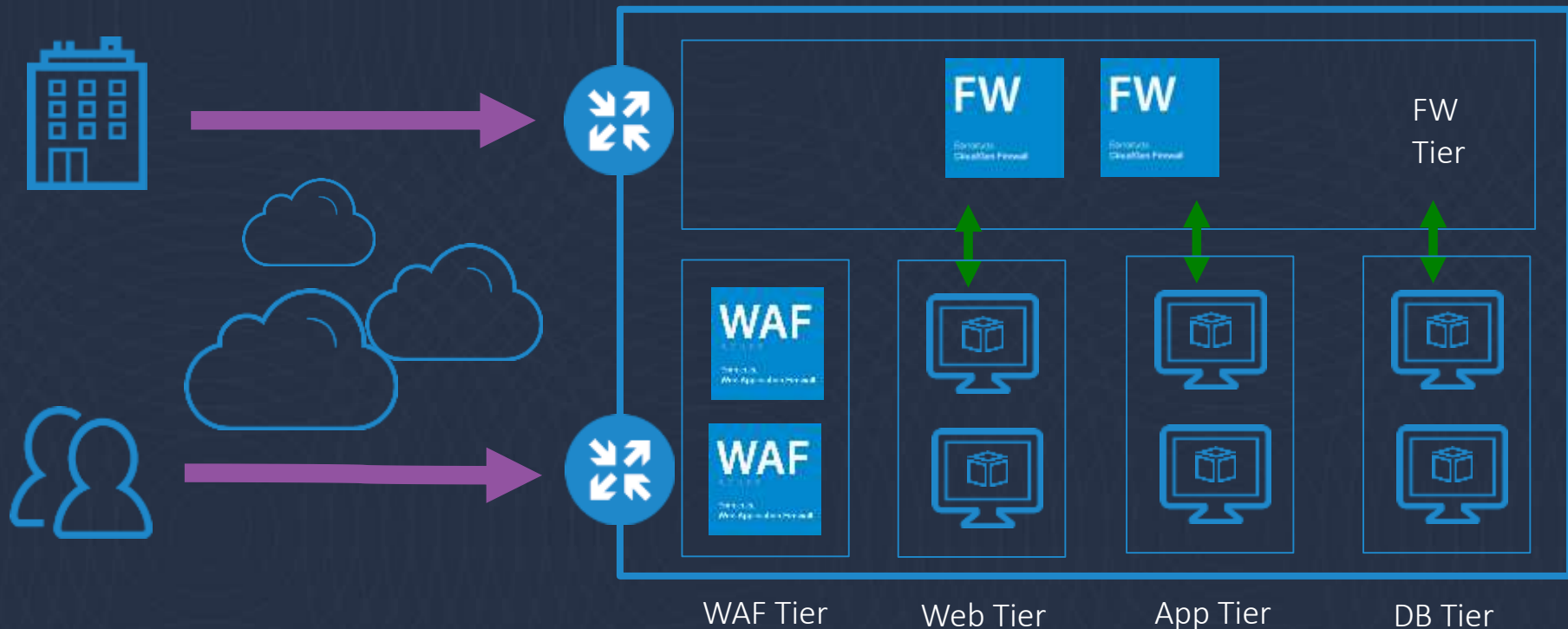
Premium support not available for bandwidth under 100Mbps.		
SKU	Premium Support Add-on	Price (EUR)
BWFS100a-p12	Premium Support (For 100 Mbps Bandwidth)	€5,175
BWFS250a-p12	Premium Support (For 250 Mbps Bandwidth)	€8,624
BWFS500a-p12	Premium Support (For 500 Mbps Bandwidth)	€12,936
BWFS1000a-p12	Premium Support (For 1 Gbps Bandwidth)	€17,248
BWFS5000a-p12	Premium Support (For 5 Gbps Bandwidth)	€64,680

Cloud Architectures



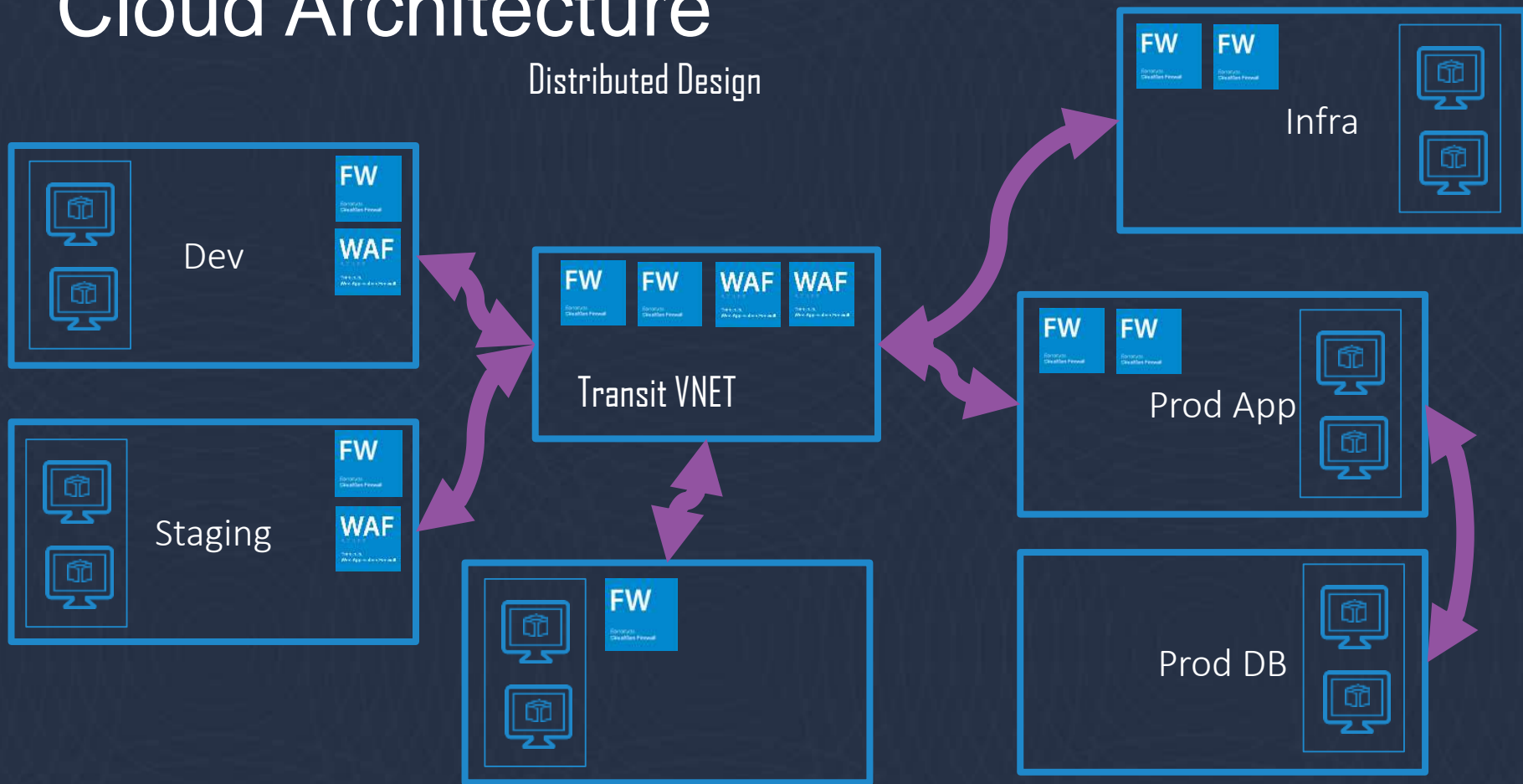
Cloud Architecture

Single VNET – Reference Architecture



Cloud Architecture

Distributed Design

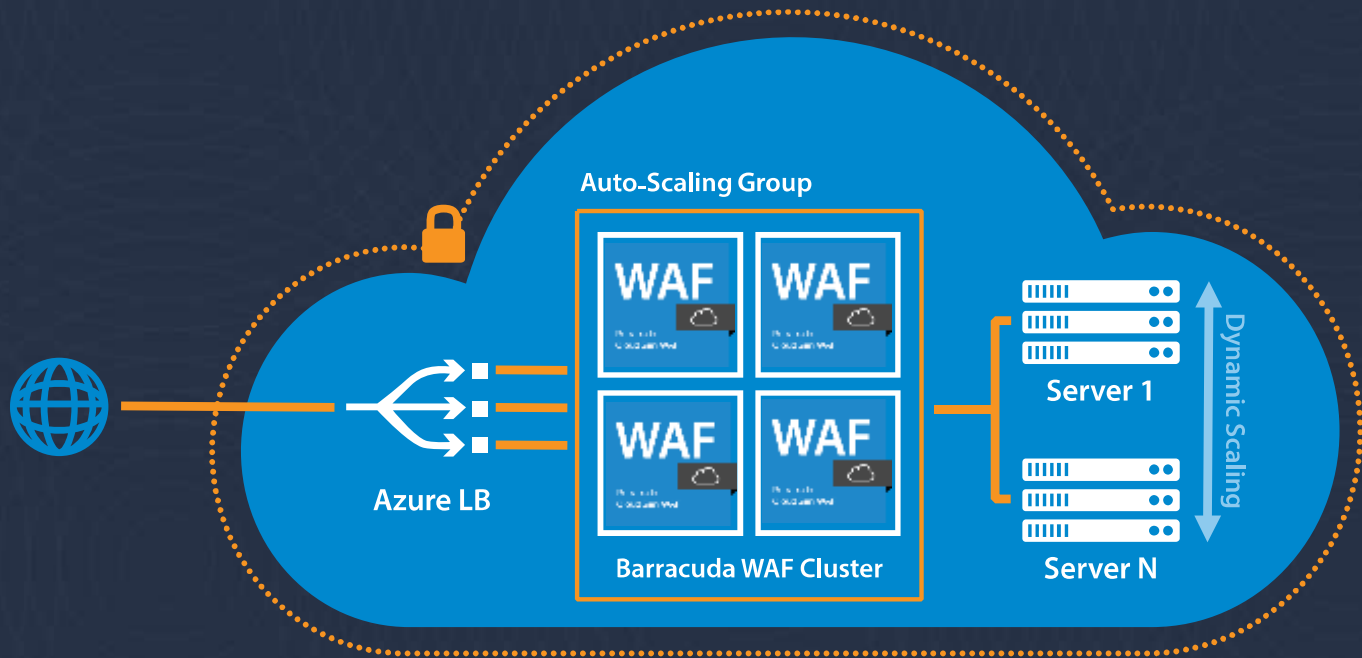


Dynamic Scaling in Azure

Protect multiple applications with a single cluster of WAFs

WAF

Powered by
CloudGen WAF



Next Steps

Barracuda Vulnerability Manager

<https://bvm.barracuda.com>

Free trials

<https://www.barracuda.com/products/webapplicationfirewall>

Partner Resources (collateral, battle-cards, sales tools)

<https://www.barracuda.com/partners>



Thank You

