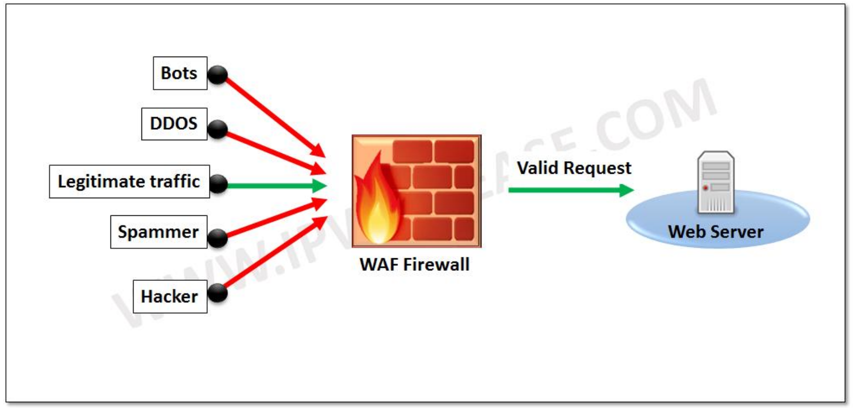
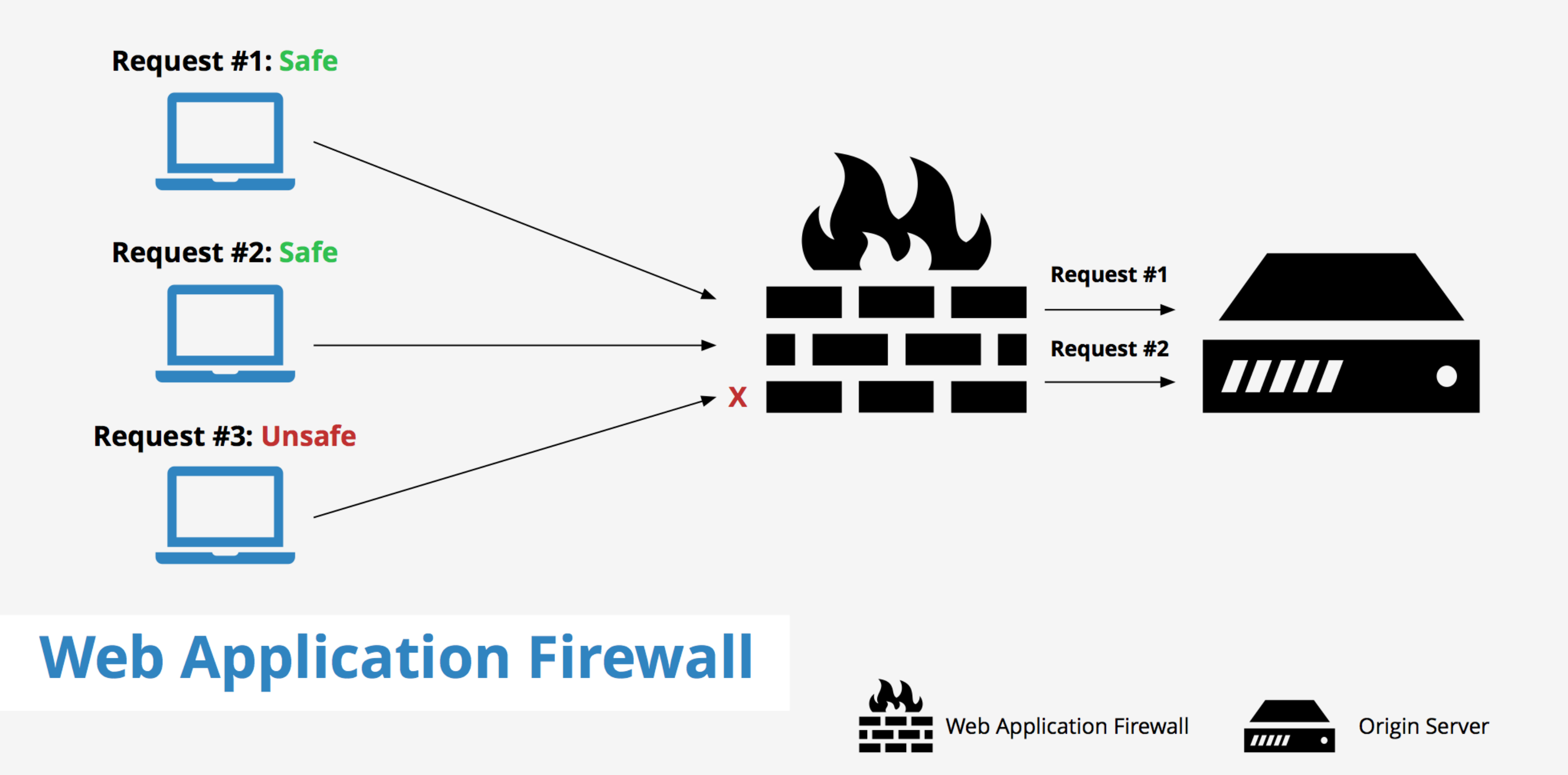


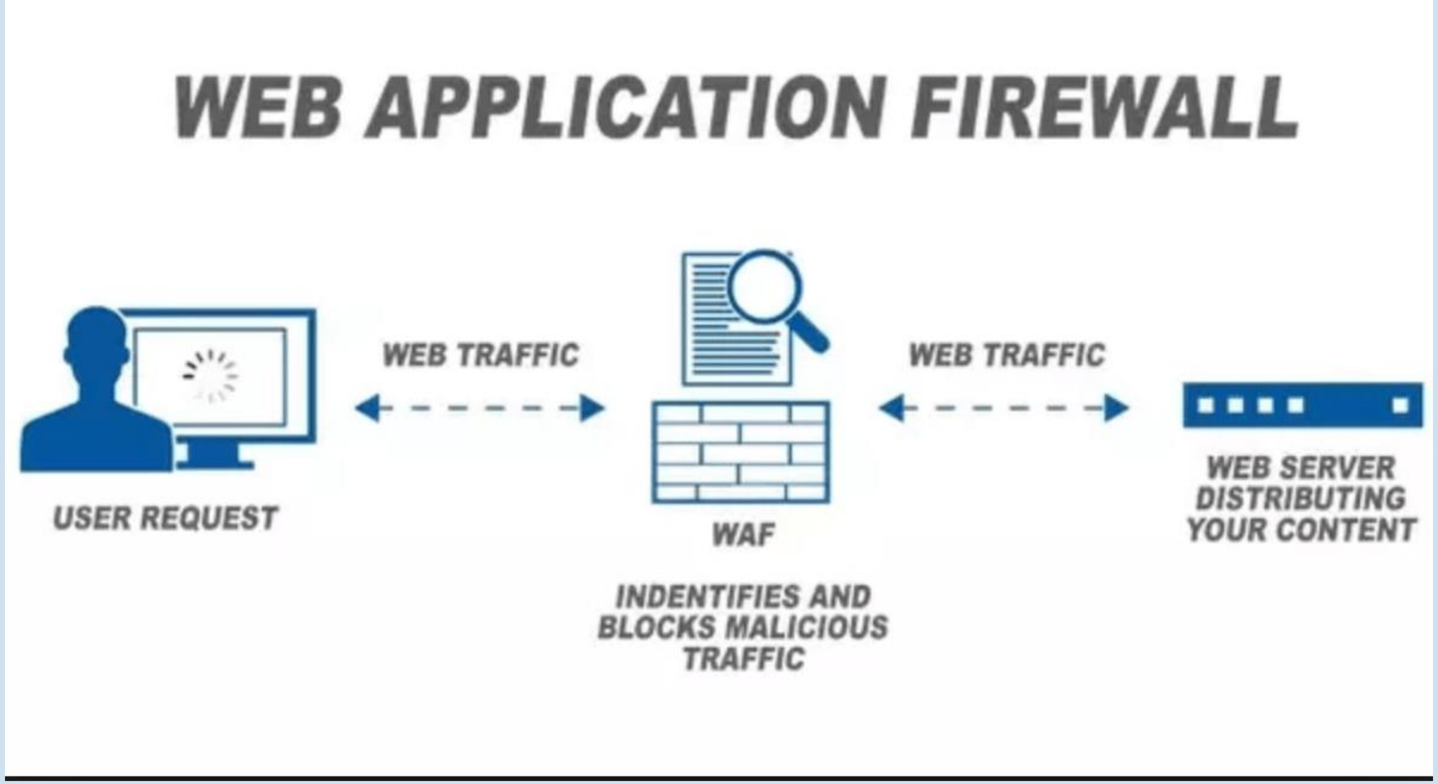
# Web Application Firewall (WAF)

Barış Karaer

# WAF (Web Application Firewall)



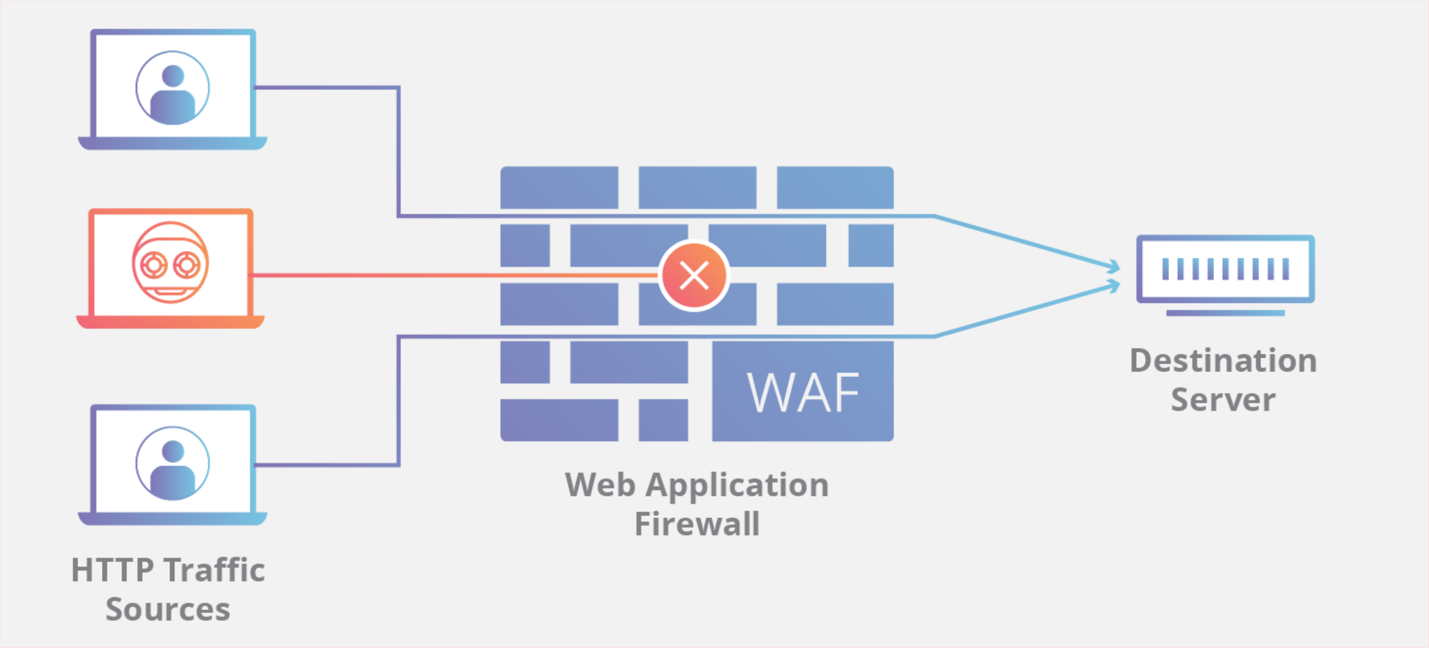
# WAF (Web Application Firewall)


WEB APPLICATION FIREWALL
USER REQUEST
WEB TRAFFIC
WAF
INDENTIFIES AND BLOCKS MALICIOUS TRAFFIC
WEB TRAFFIC
WEB SERVER DISTRIBUTING YOUR CONTENT

- A web application firewall filters, monitors and blocks HTTP traffic to and from a web application.

- WAF is able to filter the content of spesific web applications while regular firewalls serve as a safety gate between servers.

# WAF (Web Application Firewall)

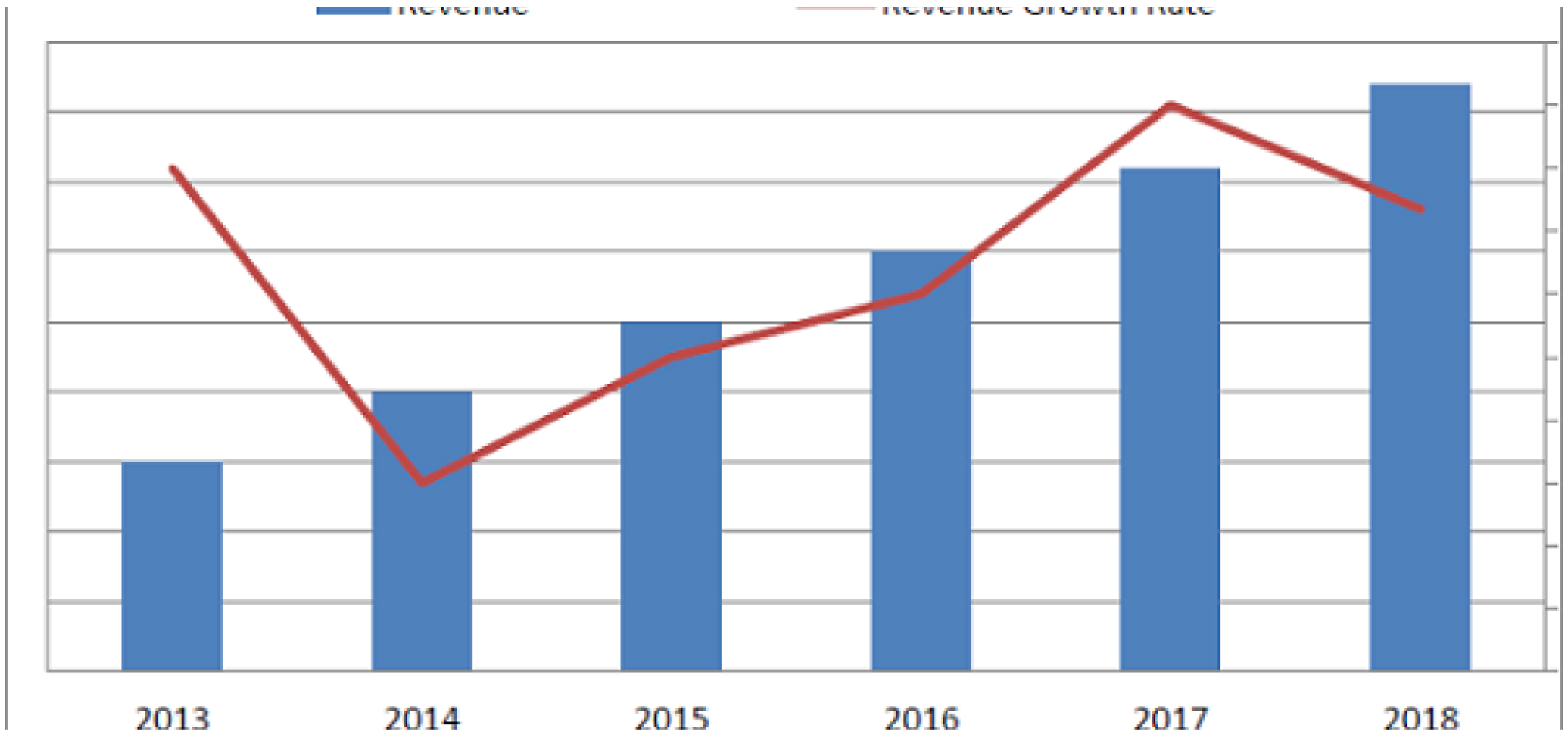


- WAF can prevent SQL injection, cross site scripting, file inclusion and security misconfigurations by inspecting HTTP traffic.

# Detailed List of the WAF Protection

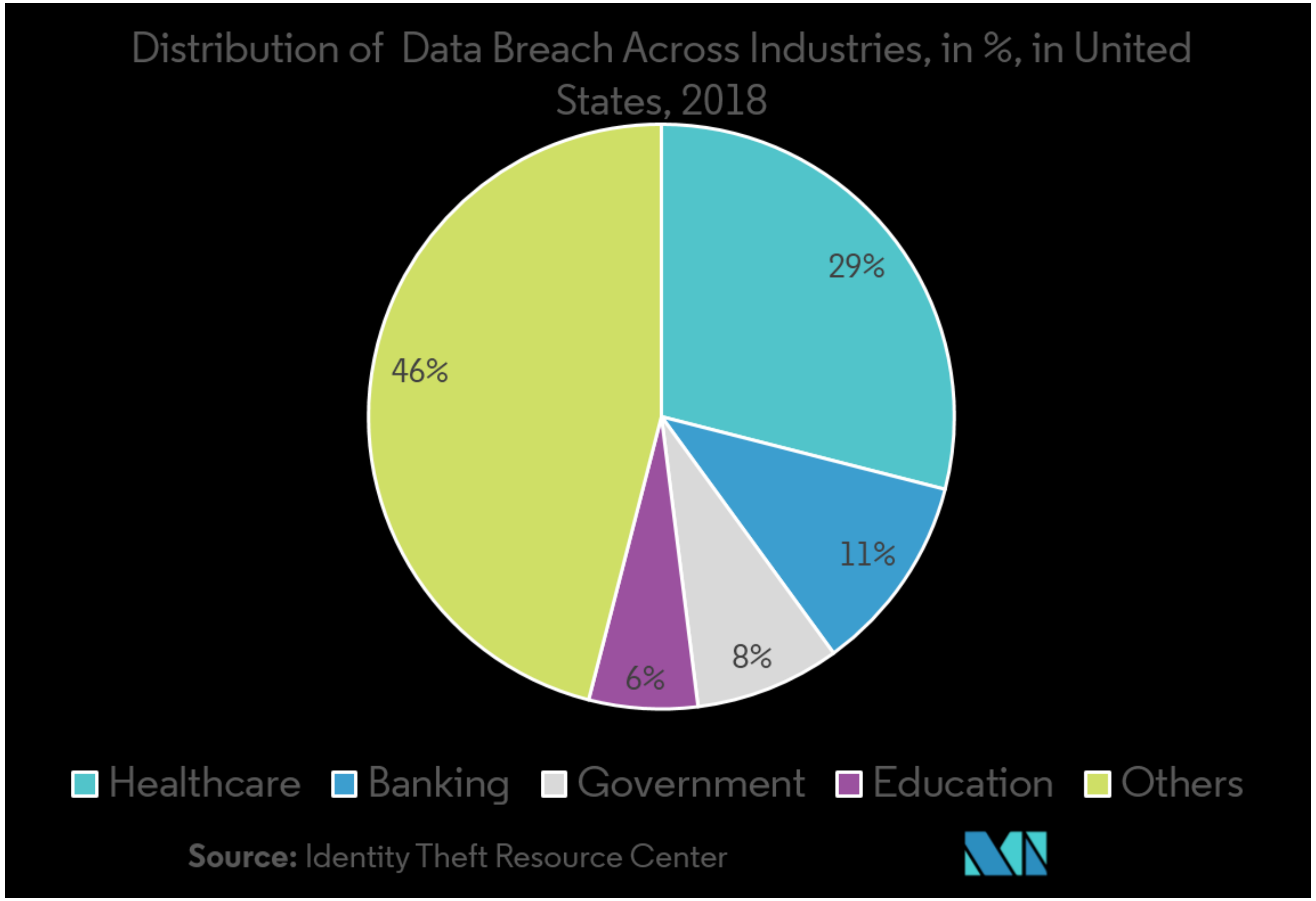
- **Cross-Site Scripting (XSS)** – malicious HTML code inserted into a web page input field by a hacker
- **Hidden field manipulation** – hackers rewrite the source code of a web page to alter values held in hidden fields and then post the amended code back to the server
- **Cookie poisoning** – altering parameter values held in cookies to corrupt data passed between web pages
- **Web scraping** – automated data extraction from web pages
- **Layer 7 DoS attacks** – overwhelming a web server by recursive application activity
- **Parameter tampering** – altering values in the parameters to a web page call
- **Buffer overflow** – user input that overwrites the code in memory
- **Backdoor or Debug options** – developer feedback reports for web page testing that can be used by hackers for access to the processor
- **Stealth commanding** – an attack on the operating system of a web server
- **Forced browsing** – the hacker gains access to backup or temporary folders on the webserver
- **Third-party misconfigurations** – manipulation of content inserts provided by other companies
- **Site vulnerabilities / SQL injections** – queries entered in user authentication fields

# Global Web Application Firewall Market (2018)



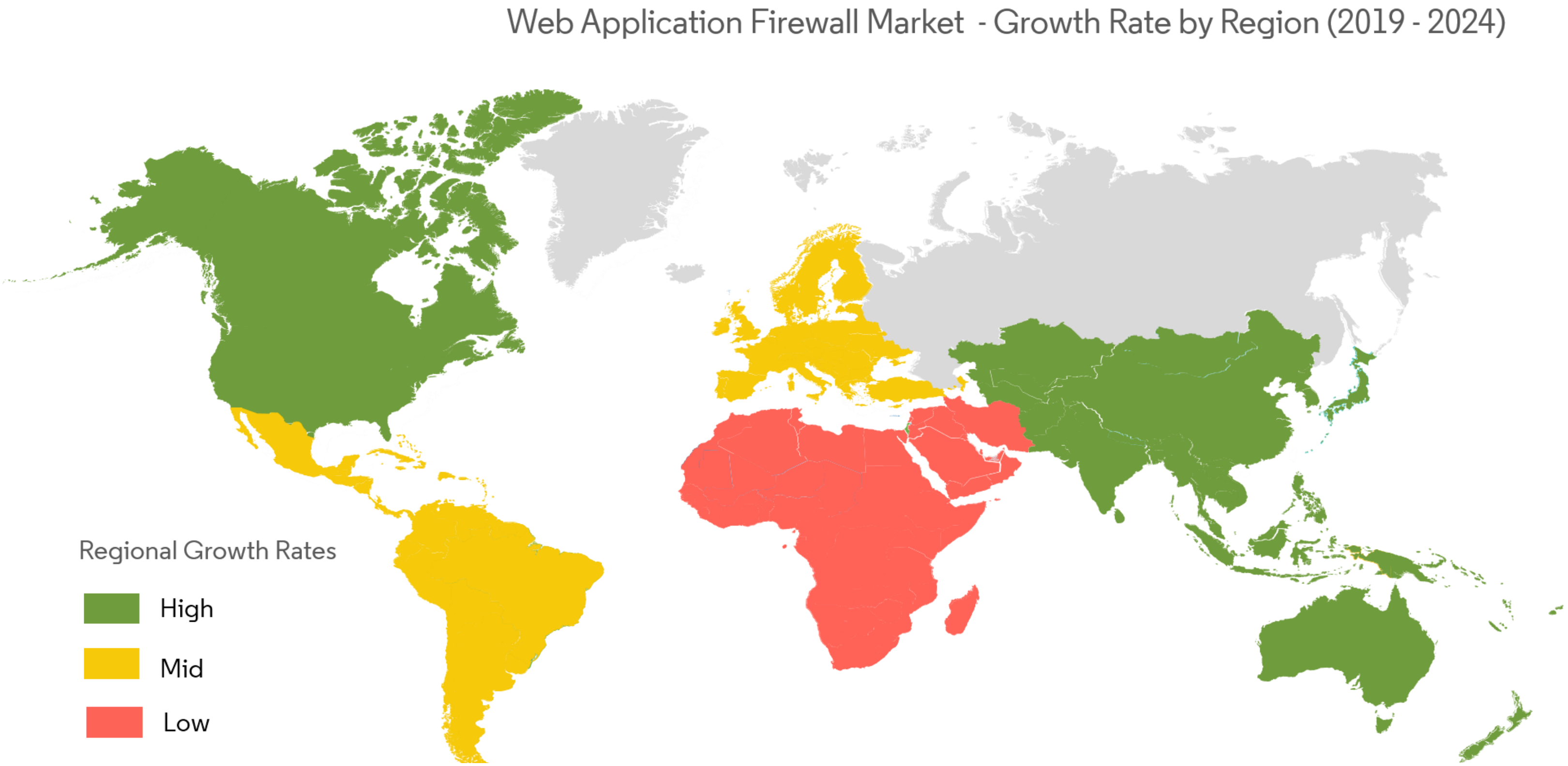
# The Largest Share in WAF

- **North America Holds the Largest Share in Web Application Firewall Market**
- Due to the security breach incidents and the presence of cyber security vendors, North America is considered the most advanced region for technology adoption and infrastructure.  Awareness about the threats is a critical economic and security challenge in the region. The growing concern to ensure the protection of sensitive data has increased corresponding government intervention in recent years.



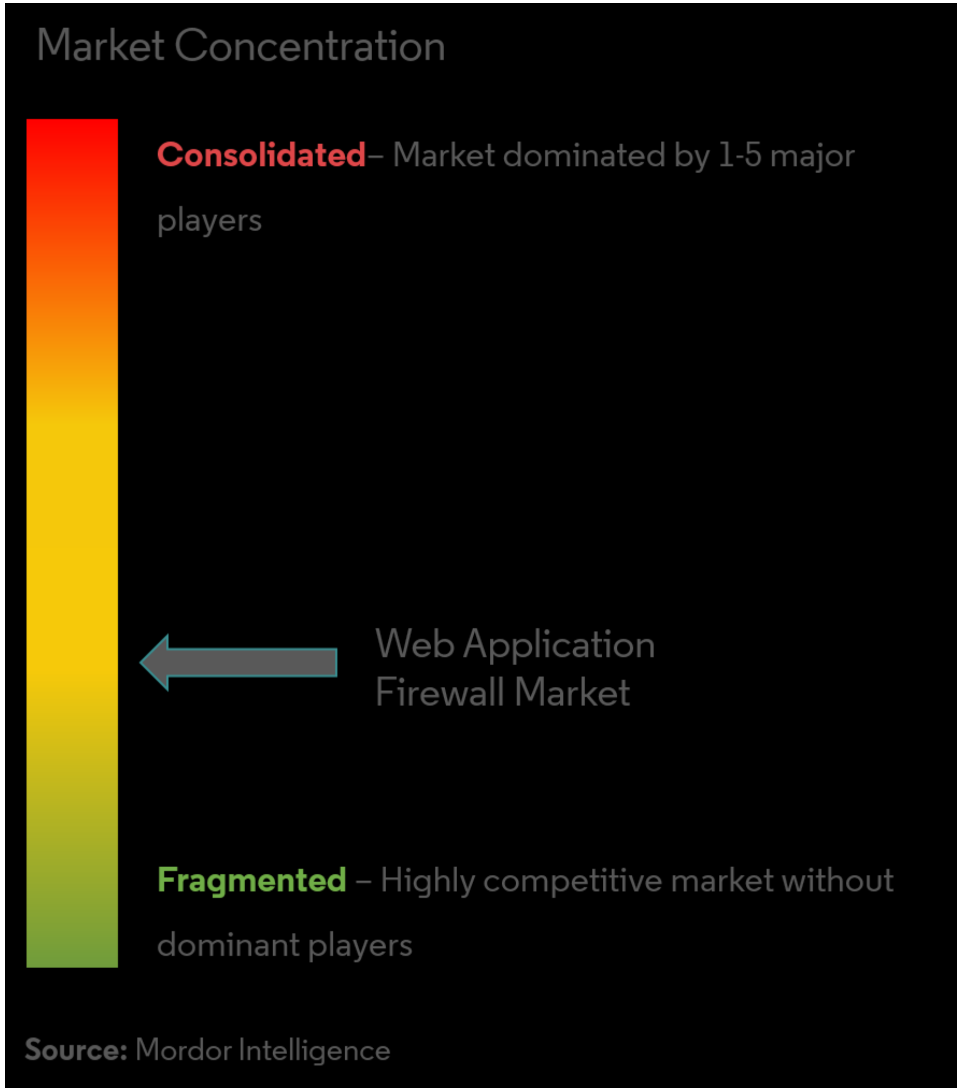
**Source:** Identity Theft Resource Center

# WAF Growth Rate By Region


Web Application Firewall Market - Growth Rate by Region (2019 - 2024)
Regional Growth Rates
🟩 High
🟨 Mid
🟥 Low

# Major Players

- Akamai Technologies INC
- F5 Networks INC
- Imperva INC
- Barracuda Networks
- Cloudflare INC



Market Concentration

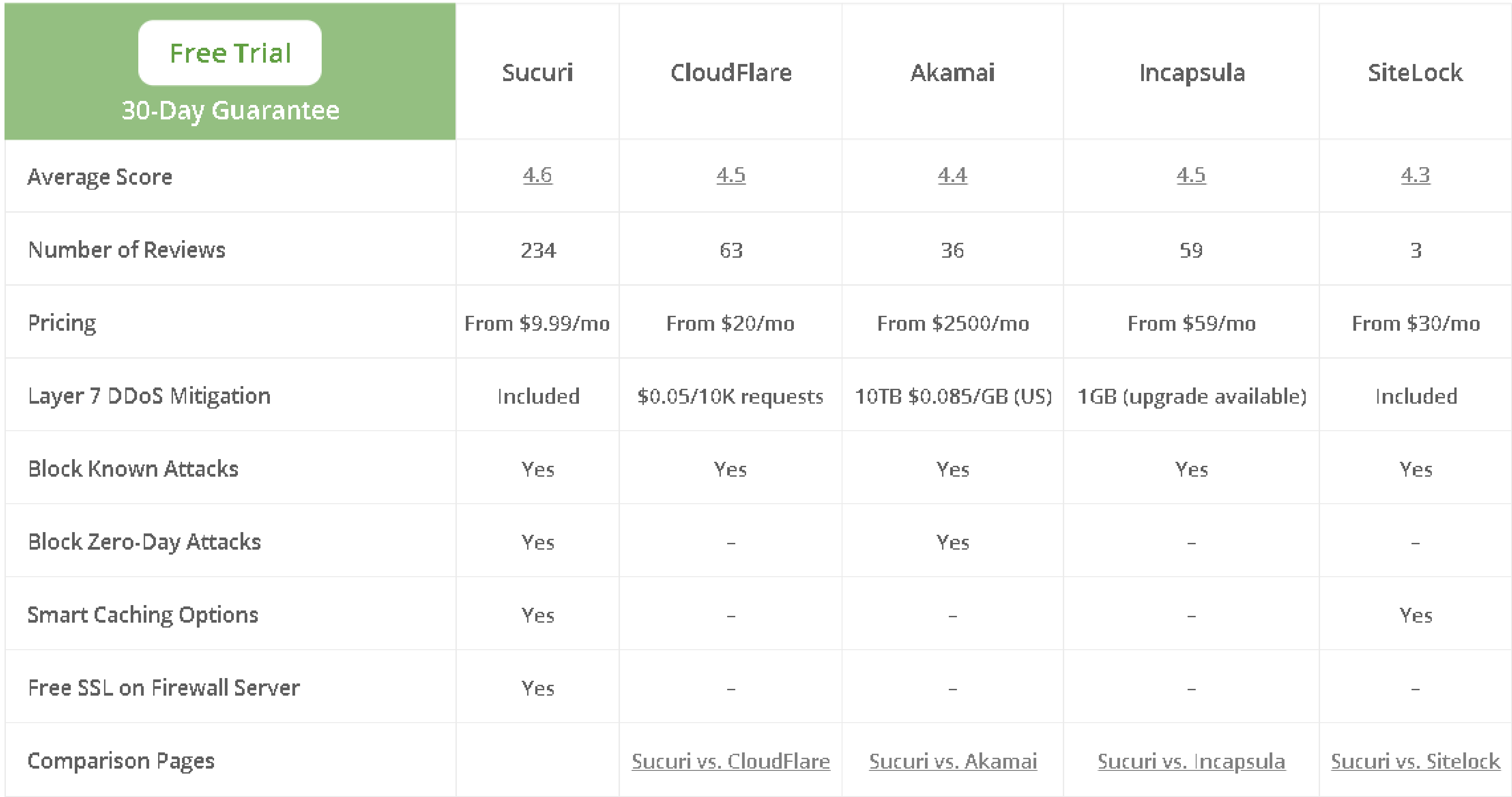
**Consolidated**– Market dominated by 1-5 major players

Web Application Firewall Market

**Fragmented** – Highly competitive market without dominant players

**Source:** Mordor Intelligence

# Top WAF Vendors Compared



| Free Trial<br>30-Day Guarantee | Sucuri | CloudFlare | Akamai | Incapsula | SiteLock |
|---|---|---|---|---|---|
| Average Score | 4.6 | 4.5 | 4.4 | 4.5 | 4.3 |
| Number of Reviews | 234 | 63 | 36 | 59 | 3 |
| Pricing | From $9.99/mo | From $20/mo | From $2500/mo | From $59/mo | From $30/mo |
| Layer 7 DDoS Mitigation | Included | $0.05/10K requests | 10TB $0.085/GB (US) | 1GB (upgrade available) | Included |
| Block Known Attacks | Yes | Yes | Yes | Yes | Yes |
| Block Zero-Day Attacks | Yes | – | Yes | – | – |
| Smart Caching Options | Yes | – | – | – | Yes |
| Free SSL on Firewall Server | Yes | – | – | – | – |
| Comparison Pages | | Sucuri vs. CloudFlare | Sucuri vs. Akamai | Sucuri vs. Incapsula | Sucuri vs. Sitelock |

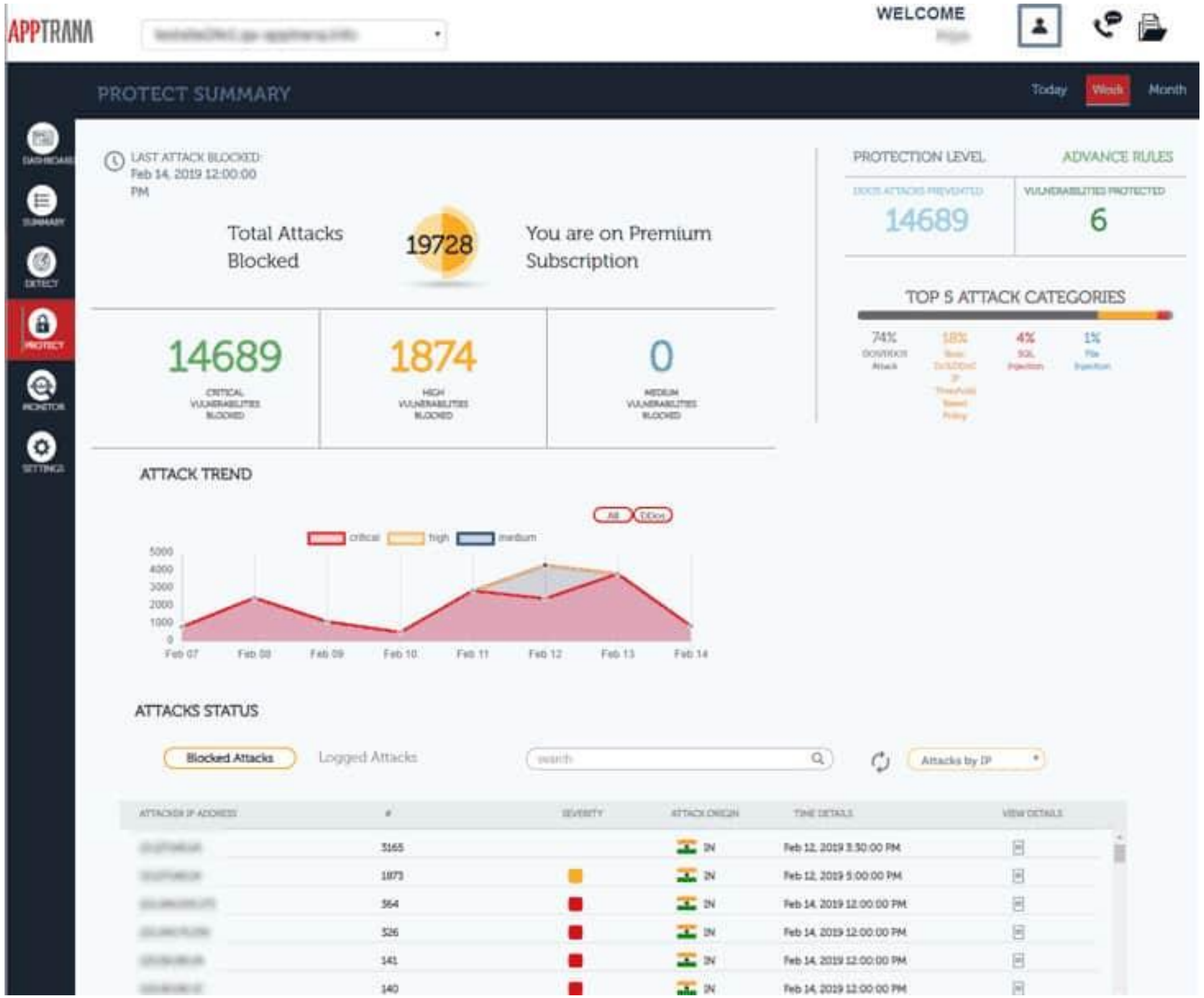
# The Best Cloud Based WAF’s

- 1. Apptrana Managed Web Application Firewall
- 2. StackPath Web Application Firewall
- 3. Sucuri Website Firewall
- 4. Cloudflare WAF
- 5. Akamai Kona Site Defender
- 6. Amazon AWS WAF
- 7. Incapsula Web Application Firewall

# Apptrana Managed Web Application Firewall

- It provides a fully managed Web application firewall bundled with content acceleration and CDN over the cloud.

- All the customers have to do is route the traffic via the AppTrana service hosted in multiple regions in AWS data centers by Indusface.



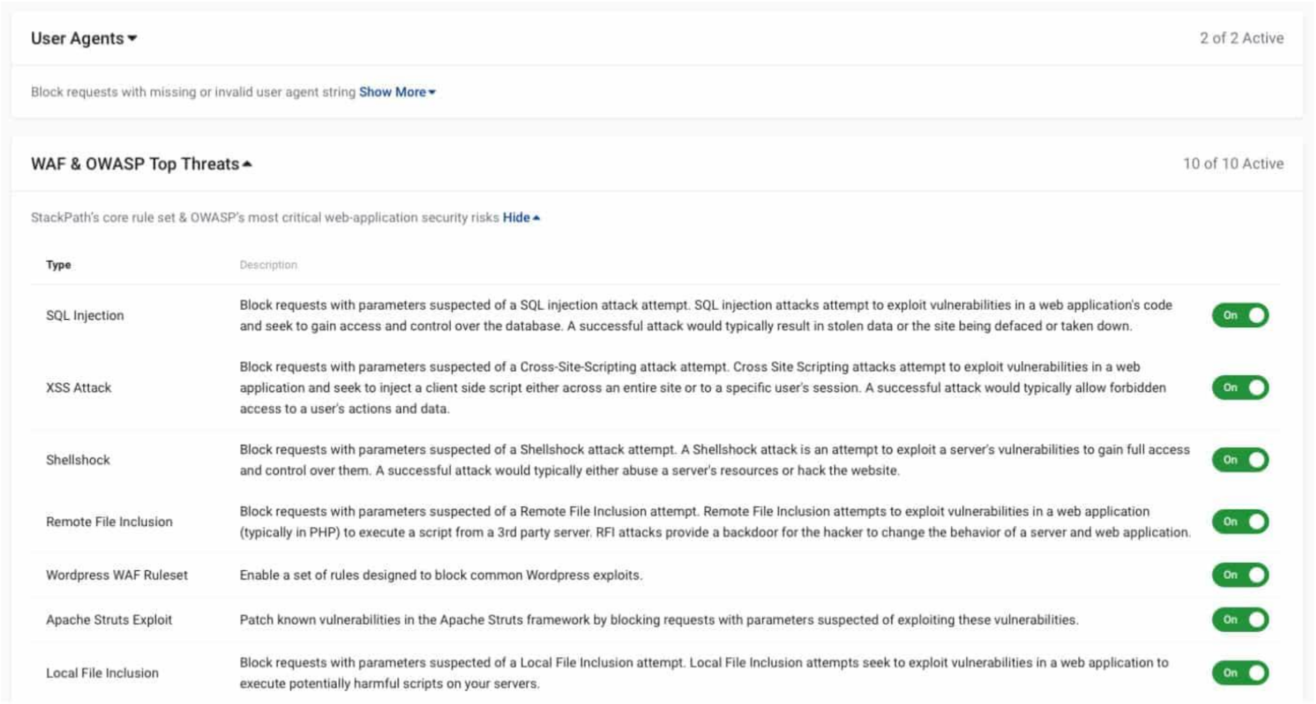
| ATTACKER IP ADDRESS | # | SEVERITY | ATTACK ORIGIN | TIME DETAILS | VIEW DETAILS |
|---|---|---|---|---|---|
| [redacted] | 3165 | | IN | Feb 12, 2019 3:30:00 PM | |
| [redacted] | 1873 | 🟧 | IN | Feb 12, 2019 5:00:00 PM | |
| [redacted] | 364 | 🟥 | IN | Feb 14, 2019 12:00:00 PM | |
| [redacted] | 326 | 🟥 | IN | Feb 14, 2019 12:00:00 PM | |
| [redacted] | 141 | 🟥 | IN | Feb 14, 2019 12:00:00 PM | |
| [redacted] | 140 | 🟥 | IN | Feb 14, 2019 12:00:00 PM | |

# StackPath Web Application Firewall

- Specialize in “edge technology”

- This term refers to the technique of pushing services out to the edge of your network, and then and little beyond. StackPath is a subscription-based Cloud service that **captures all of your traffic before it reaches your Web server**.

- The offsite configuration of StackPath provides extra protection for your Web server as any **malicious code doesn’t even get a chance to touch your resources**.



**User Agents** ▾ 2 of 2 Active

Block requests with missing or invalid user agent string **Show More** ▾

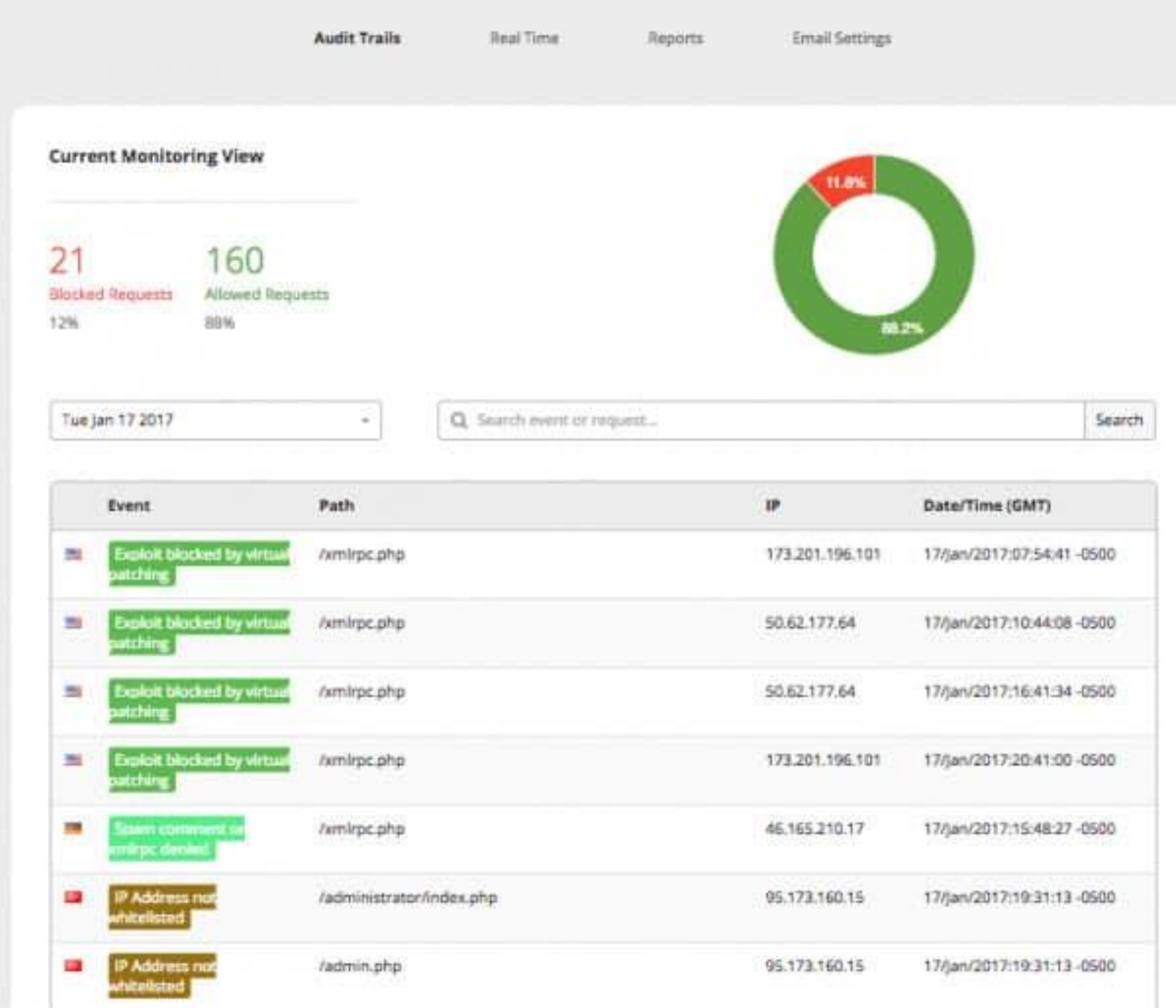
**WAF & OWASP Top Threats** ▴ 10 of 10 Active

StackPath’s core rule set & OWASP’s most critical web-application security risks **Hide** ▴

| Type | Description | |
|---|---|---|
| SQL Injection | Block requests with parameters suspected of a SQL injection attack attempt. SQL injection attacks attempt to exploit vulnerabilities in a web application's code and seek to gain access and control over the database. A successful attack would typically result in stolen data or the site being defaced or taken down. | On |
| XSS Attack | Block requests with parameters suspected of a Cross-Site-Scripting attack attempt. Cross Site Scripting attacks attempt to exploit vulnerabilities in a web application and seek to inject a client side script either across an entire site or to a specific user's session. A successful attack would typically allow forbidden access to a user's actions and data. | On |
| Shellshock | Block requests with parameters suspected of a Shellshock attack attempt. A Shellshock attack is an attempt to exploit a server's vulnerabilities to gain full access and control over them. A successful attack would typically either abuse a server's resources or hack the website. | On |
| Remote File Inclusion | Block requests with parameters suspected of a Remote File Inclusion attempt. Remote File Inclusion attempts to exploit vulnerabilities in a web application (typically in PHP) to execute a script from a 3rd party server. RFI attacks provide a backdoor for the hacker to change the behavior of a server and web application. | On |
| Wordpress WAF Ruleset | Enable a set of rules designed to block common Wordpress exploits. | On |
| Apache Struts Exploit | Patch known vulnerabilities in the Apache Struts framework by blocking requests with parameters suspected of exploiting these vulnerabilities. | On |
| Local File Inclusion | Block requests with parameters suspected of a Local File Inclusion attempt. Local File Inclusion attempts seek to exploit vulnerabilities in a web application to execute potentially harmful scripts on your servers. | On |

# Sucuri Website Firewall

- Your website’s address gets hosted at Sucuri’s server, also all of your Web traffic goes there first.
- The company maintains a database of attack signatures, which is constantly updated, so **your website benefits from protection strategies learned by Sucuri when it is defending other sites**.



Current Monitoring View

21
Blocked Requests
12%

160
Allowed Requests
88%

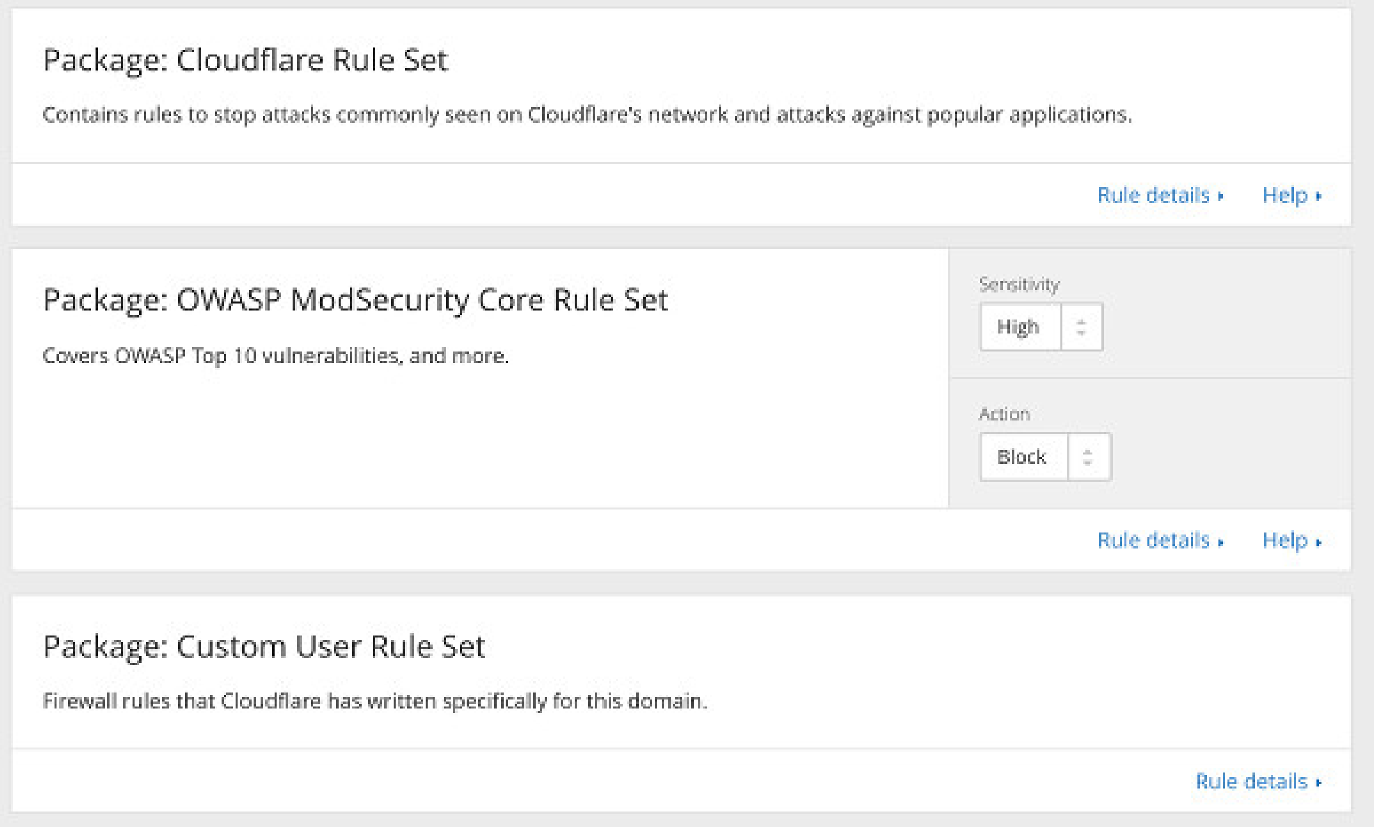
Tue Jan 17 2017

| | Event | Path | IP | Date/Time (GMT) |
|---|---|---|---|---|
| | Exploit blocked by virtual patching | /xmlrpc.php | 173.201.196.101 | 17/jan/2017:07:54:41 -0500 |
| | Exploit blocked by virtual patching | /xmlrpc.php | 50.62.177.64 | 17/jan/2017:10:44:08 -0500 |
| | Exploit blocked by virtual patching | /xmlrpc.php | 50.62.177.64 | 17/jan/2017:16:41:34 -0500 |
| | Exploit blocked by virtual patching | /xmlrpc.php | 173.201.196.101 | 17/jan/2017:20:41:00 -0500 |
| | Spam comment or xmlrpc denied | /xmlrpc.php | 46.165.210.17 | 17/jan/2017:15:48:27 -0500 |
| | IP Address not whitelisted | /administrator/index.php | 95.173.160.15 | 17/jan/2017:19:31:13 -0500 |
| | IP Address not whitelisted | /admin.php | 95.173.160.15 | 17/jan/2017:19:31:13 -0500 |

# Cloudflare WAF

Cloudflare has become very successful at protecting web hosts from DDoS attacks and they extend their protection with a web application firewall.

**An attack attempt on one customer instantly ripples through to a blacklist entry for all web servers protected by Cloudflare.**



Package: Cloudflare Rule Set

Contains rules to stop attacks commonly seen on Cloudflare's network and attacks against popular applications.

Rule details ▸ Help ▸

Package: OWASP ModSecurity Core Rule Set

Covers OWASP Top 10 vulnerabilities, and more.

Sensitivity: High

Action: Block

Rule details ▸ Help ▸

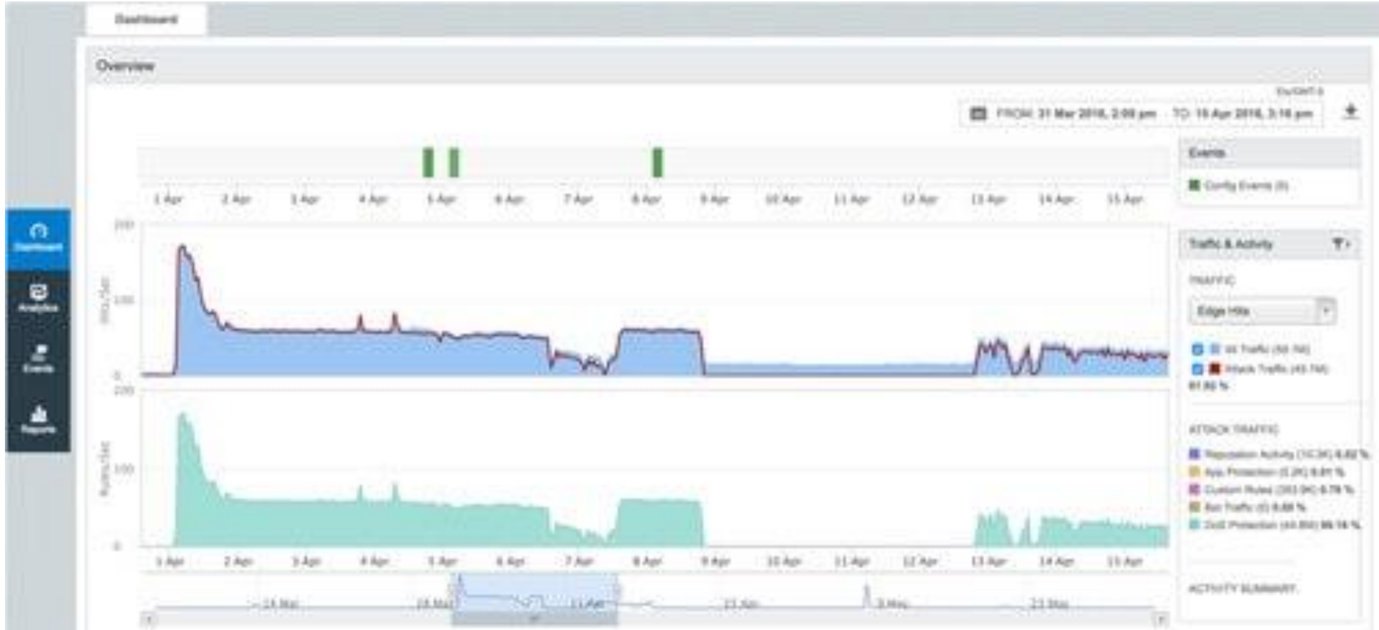
Package: Custom User Rule Set

Firewall rules that Cloudflare has written specifically for this domain.

Rule details ▸

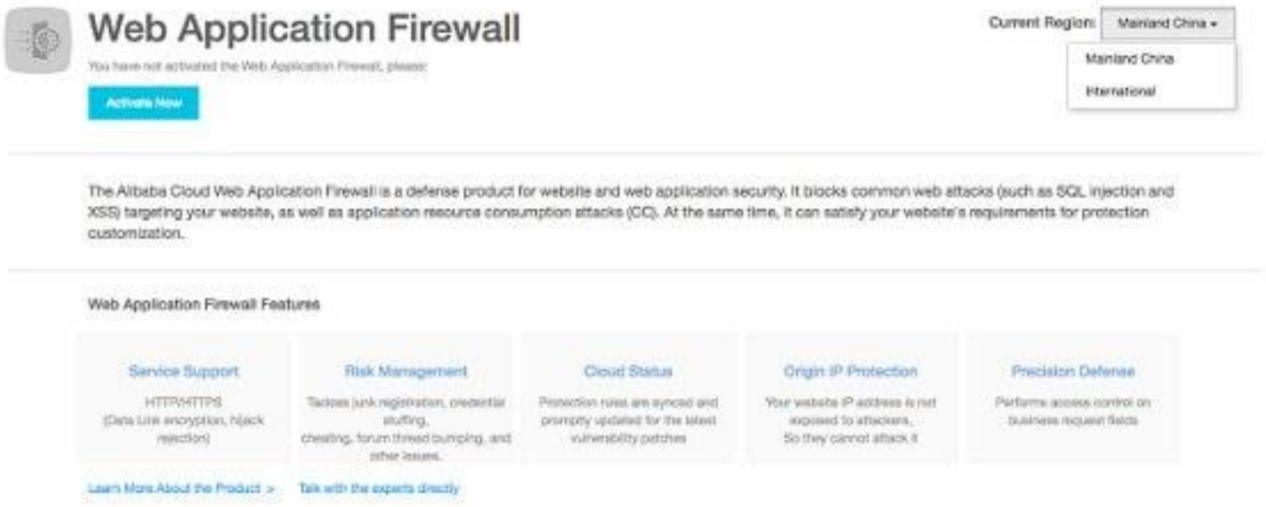
# Akamai Kona Site Defender

- Akamai is a world leader in DDoS mitigation and it integrates full DDoS protection with its web application firewall in a cloud service called Site Defender.
- You **won’t need to have your traffic routed through two different companies** in order to get genuine requests arriving at your web server.
- Akamai often is the first to discover new exploits.



# Amazon AWS WAF

- The Amazon AWS web application firewall (or AWS WAF) is only available to customers of the company's Web Services.
- **You don't pay a lump sum each month.**
- Instead, you get charged for each security rule that you set up and for the number of web requests that your server receives in a month.



Web Application Firewall

You have not activated the Web Application Firewall, please:

Activate Now

Current Region: Mainland China ▾

Mainland China

International

The Alibaba Cloud Web Application Firewall is a defense product for website and web application security. It blocks common web attacks (such as SQL injection and XSS) targeting your website, as well as application resource consumption attacks (CC). At the same time, it can satisfy your website's requirements for protection customization.

Web Application Firewall Features

Service Support

HTTP/HTTPS
(Data Link encryption, hijack rejection)

Risk Management

Tackles junk registration, credential stuffing,
cheating, forum thread bumping, and other issues.

Cloud Status

Protection rules are synced and promptly updated for the latest vulnerability patches

Origin IP Protection

Your website IP address is not exposed to attackers,
So they cannot attack it

Precision Defense

Performs access control on business request fields

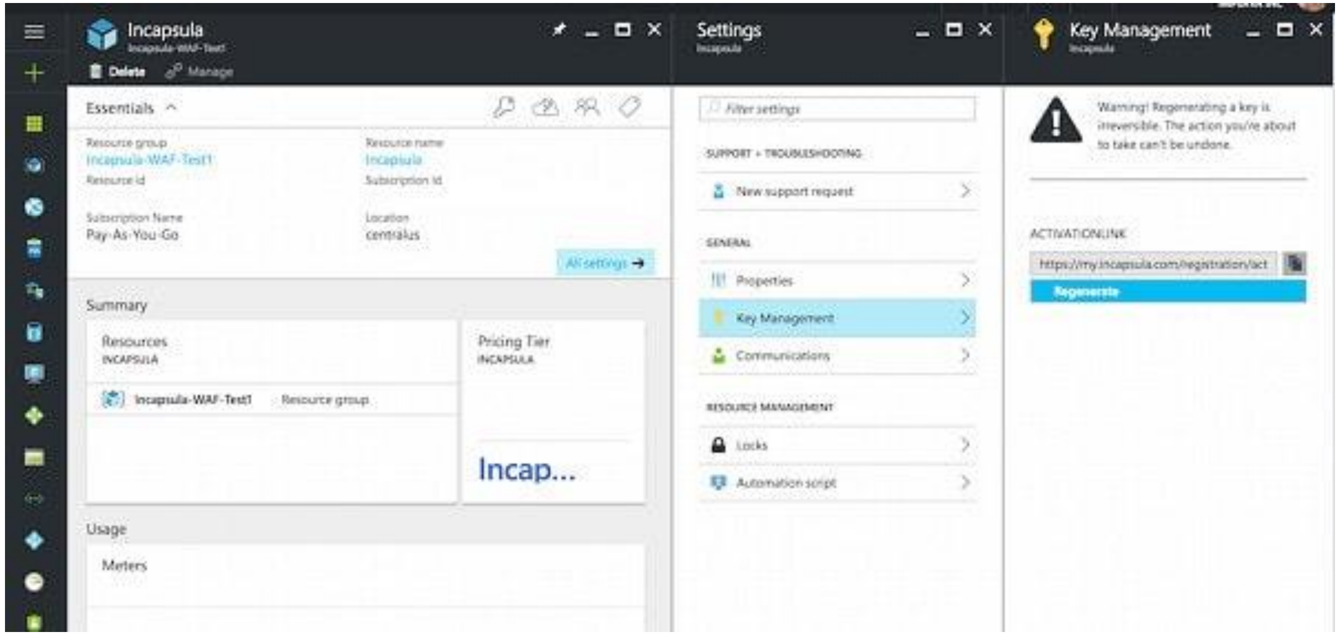
Learn More About the Product >

Talk with the experts directly

# Incapsula Web Application Firewall

- Incapsula is a leader in DDoS protection and the company adds full DDoS filtering to its WAF, not just application-layer protection.

- The cheapest WAF plan offered by Incapsula works out at $300 per month.



Resource group
Incapsula-WAF-Test1

Resource name
Incapsula

Resource id

Subscription id

Subscription Name
Pay-As-You-Go

Location
centralus

Resources
INCAPSULA

Incapsula-WAF-Test1 Resource group

Pricing Tier
INCAPSULA

Incap...

Warning! Regenerating a key is irreversible. The action you're about to take can't be undone.

ACTIVATIONLINK
https://my.incapsula.com/registration/act

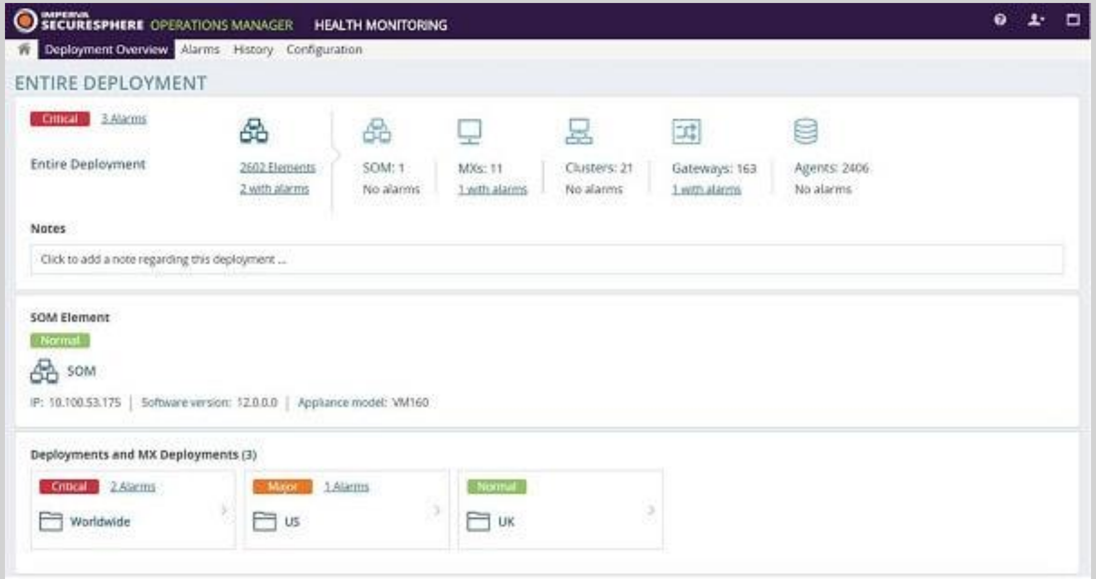
# The Best Hardware Based WAF’s

- The hardware solution to web application firewalls involves a piece of network equipment that needs to go in front of the web infrastructure.

- 1. Imperva SecureSphere
- 2. Barracuda Web Application Firewall
- 3. Citrix NetScaler Application Firewall
- 4. Fortinet FortiWeb
- 5. F5 Big-IP ASM

# Imperva SecureSphere

- This WAF is aimed at smaller businesses with units that have a throughput of 100 Mbps dealing with 440 SSL TPS, going up to a model that can process 10 Gbps and 9,000 SSL TPS.



ENTIRE DEPLOYMENT

Critical 3 Alarms

Entire Deployment

2602 Elements
2 with alarms

SOM: 1
No alarms

MXs: 11
1 with alarms

Clusters: 21
No alarms

Gateways: 163
1 with alarms

Agents: 2406
No alarms

Notes

Click to add a note regarding this deployment ...

SOM Element

Normal

SOM

IP: 10.100.53.175 | Software version: 12.0.0.0 | Appliance model: VM160

Deployments and MX Deployments (3)

Critical 2 Alarms
Worldwide

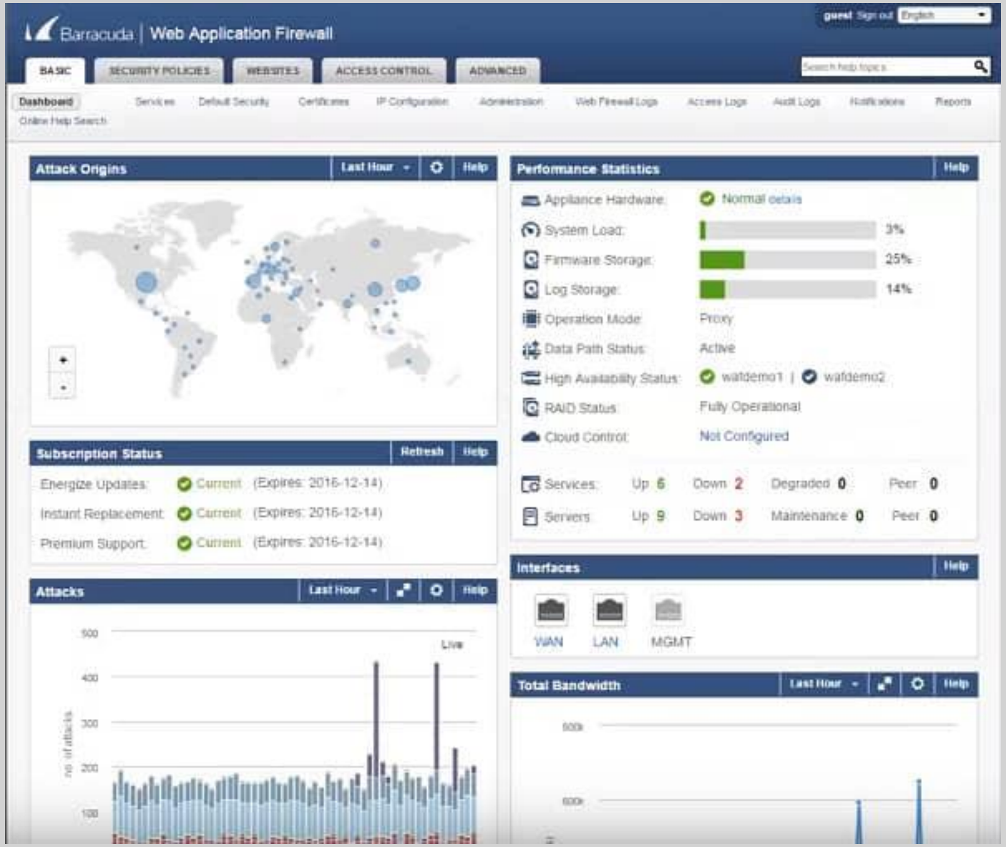
Major 1 Alarms
US

Normal
UK

# Barracuda Web Application Firewall

- Barracuda is a good solution for a small- to mid-sized web-based business. This appliance is a little pricey, but the purchase price includes a full year of system updates.

- The Barracuda box has some extra features, which include caching for faster content delivery and load balancing.



Performance Statistics

Appliance Hardware: Normal details

System Load: 3%

Firmware Storage: 25%

Log Storage: 14%

Operation Mode: Proxy

Data Path Status: Active

High Availability Status: wafdemo1 | wafdemo2

RAID Status: Fully Operational

Cloud Control: Not Configured

Services: Up 6 Down 2 Degraded 0 Peer 0

Servers: Up 9 Down 3 Maintenance 0 Peer 0

Subscription Status

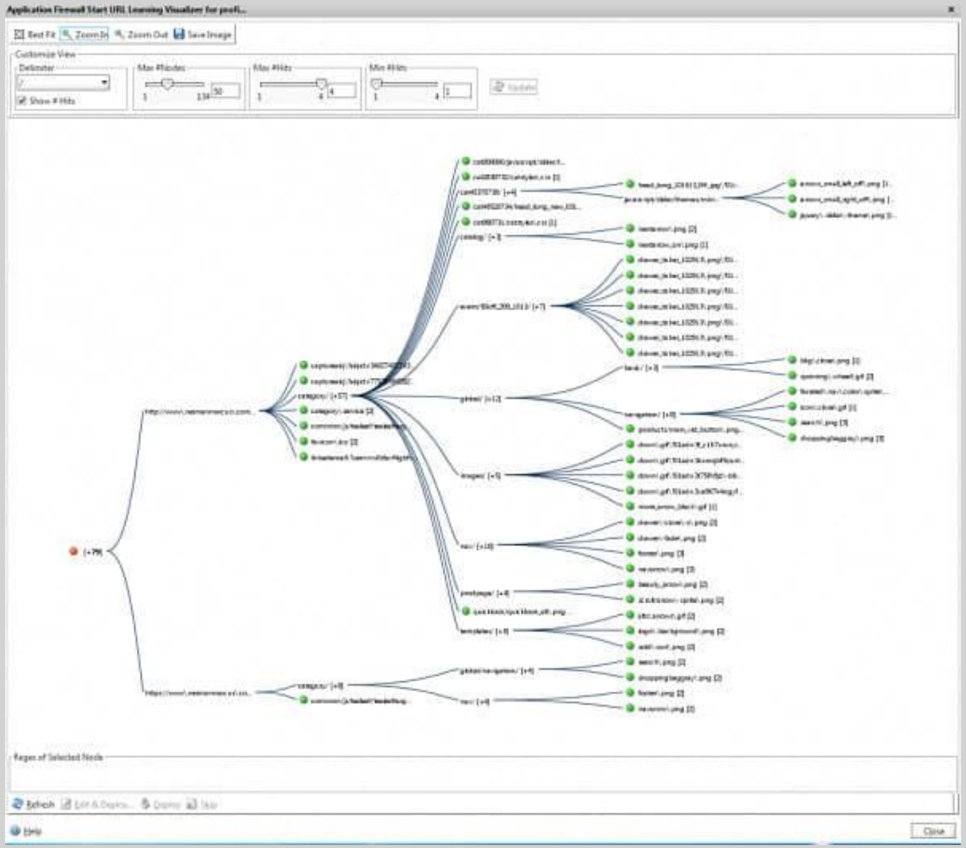
Energize Updates: Current (Expires: 2016-12-14)

Instant Replacement: Current (Expires: 2016-12-14)

Premium Support: Current (Expires: 2016-12-14)

# Citrix NetScaler Application Firewall

- Range comes with capacities ranging from 500 Mbps up to 200 Gbps.
- The cheapest model is the MXP 5550, which gives you a throughput of 500 Mbps and can cope with 1,500 SSL TPS. This unit costs $4,000.



Application Firewall Start URL Learning Visualizer for profi...

Customize View

Delimiter: /

☑ Show # Hits

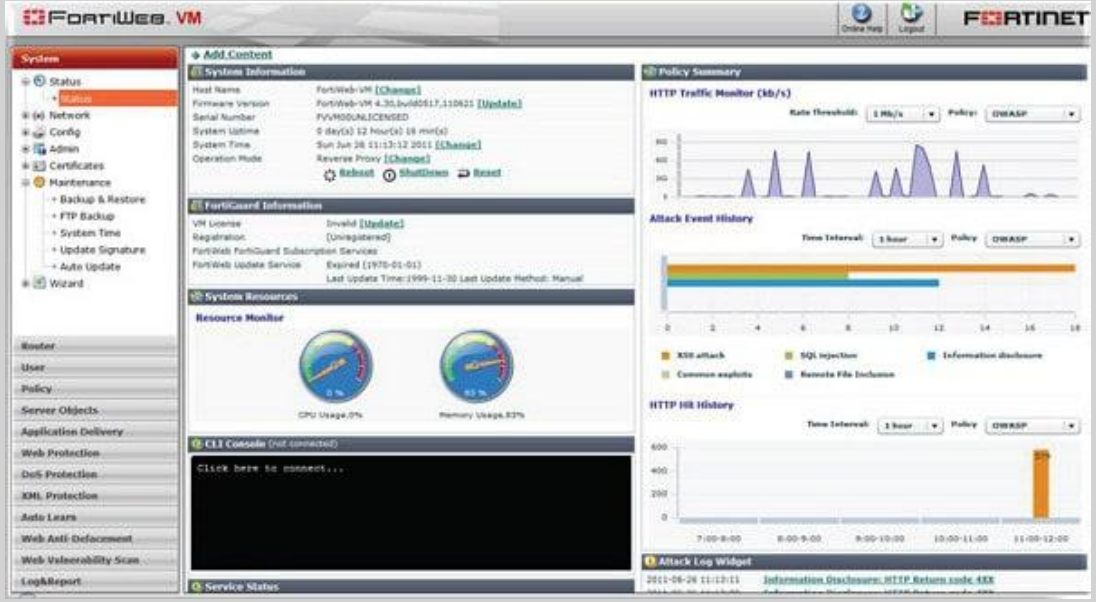
Max #Nodes: 50

Max #Hits: 4

Min #Hits: 1

# Fortinet FortiWeb

- **This device integrates the WAF with a load balancer and an SSL offloader**.
- The entry-level model is 100D. This has a throughput rate of 25 Mbps.



**System Information**

Host Name: FortiWeb-VM [Change]
Firmware Version: FortiWeb-VM 4.30,build0517,110621 [Update]
Serial Number: FVVM00UNLICENSED
System Uptime: 0 day(s) 12 hour(s) 16 min(s)
System Time: Sun Jun 26 11:13:12 2011 [Change]
Operation Mode: Reverse Proxy [Change]

**FortiGuard Information**

VM License: Invalid [Update]
Registration: [Unregistered]
FortiWeb FortiGuard Subscription Services
FortiWeb Update Service: Expired (1970-01-01)
Last Update Time:1999-11-30 Last Update Method: Manual

**System Resources**

CPU Usage,0%
Memory Usage,83%

**CLI Console** (not connected)

```
Click here to connect...
```

**Service Status**

Rate Threshold: 1 Mb/s ▾ Policy: OWASP ▾

Time Interval: 1 hour ▾ Policy: OWASP ▾

Time Interval: 1 hour ▾ Policy: OWASP ▾

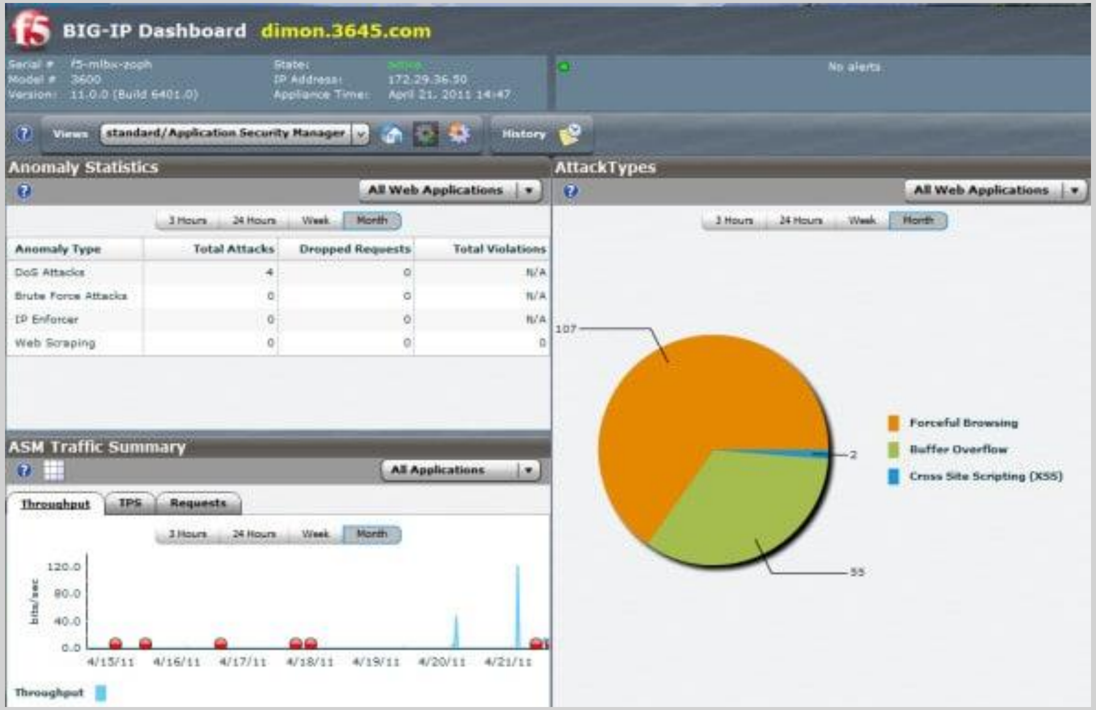
**Attack Log Widget**

2011-06-26 11:13:11 Information Disclosure: HTTP Return code 4XX

# F5 Big-IP ASM

- The BIG-IP ASM is aimed at large companies.

- Unfortunately, F5 doesn't give an SSL TPS rate for its models, but an HTTP one instead. The 10200 model can process 75,000 HTTP TPS and has a throughput of 5 Gbps.



BIG-IP Dashboard dimon.3645.com

Serial #: f5-mlbx-zoph
Model #: 3600
Version: 11.0.0 (Build 6401.0)
State: [illegible]
IP Address: 172.29.36.50
Appliance Time: April 21, 2011 14:47

No alerts

Views: standard/Application Security Manager

## Anomaly Statistics

All Web Applications

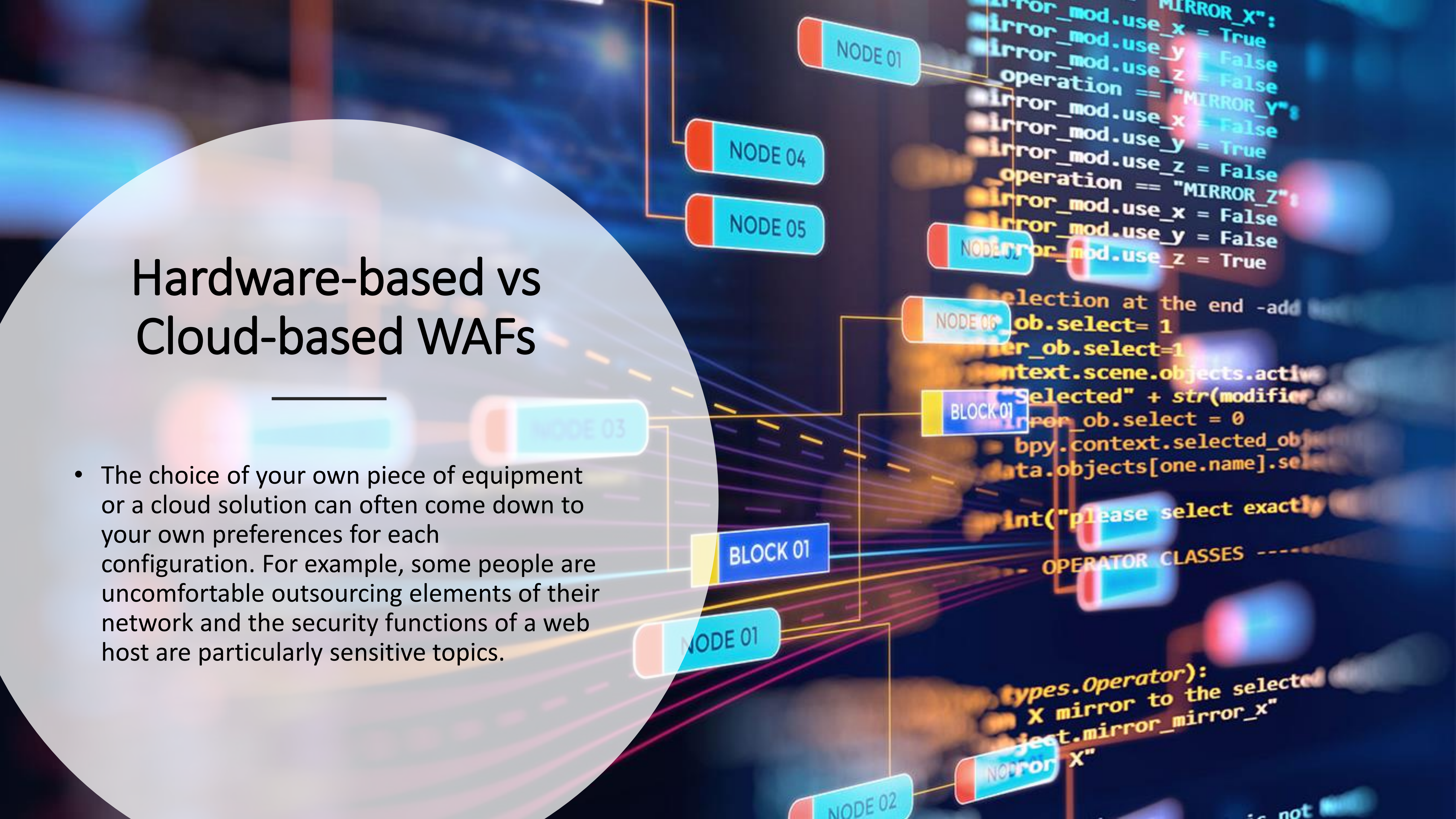
| Anomaly Type | Total Attacks | Dropped Requests | Total Violations |
|---|---|---|---|
| DoS Attacks | 4 | 0 | N/A |
| Brute Force Attacks | 0 | 0 | N/A |
| IP Enforcer | 0 | 0 | N/A |
| Web Scraping | 0 | 0 | 0 |

## ASM Traffic Summary

All Applications

## AttackTypes

All Web Applications



# Hardware-based vs Cloud-based WAFs

- The choice of your own piece of equipment or a cloud solution can often come down to your own preferences for each configuration. For example, some people are uncomfortable outsourcing elements of their network and the security functions of a web host are particularly sensitive topics.

# Choosing a Web Application Firewall

- Whether you prefer to have your own WAF on your network, or you think it would be better to go for a cloud-based WAF solution, this presentation has given you five options to consider. Selecting new equipment, software, and services for a company can be very time-consuming.

You can choose a WAF based on the growth and size of your company.

# Sources

- Mordor Intelligence
- Wikipedia
- Whatec
- Comparitech