A10

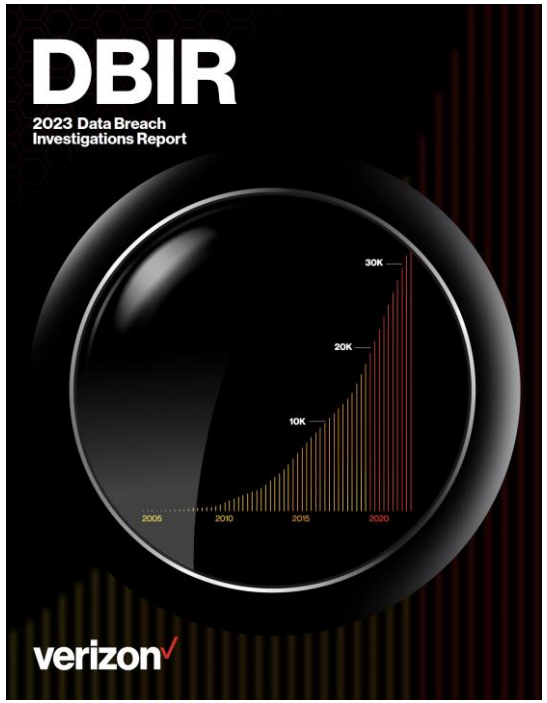
Always Secure. Always Available.

下一代 Web 應用程式防護

Web 應用程式攻擊趨勢

1. 網路攻擊事件近20%是 Web Application Attacks.

2. Web Application Attacks 趨勢持續成長 2019 ~ 2022



2023 Data Breach Investigations Report

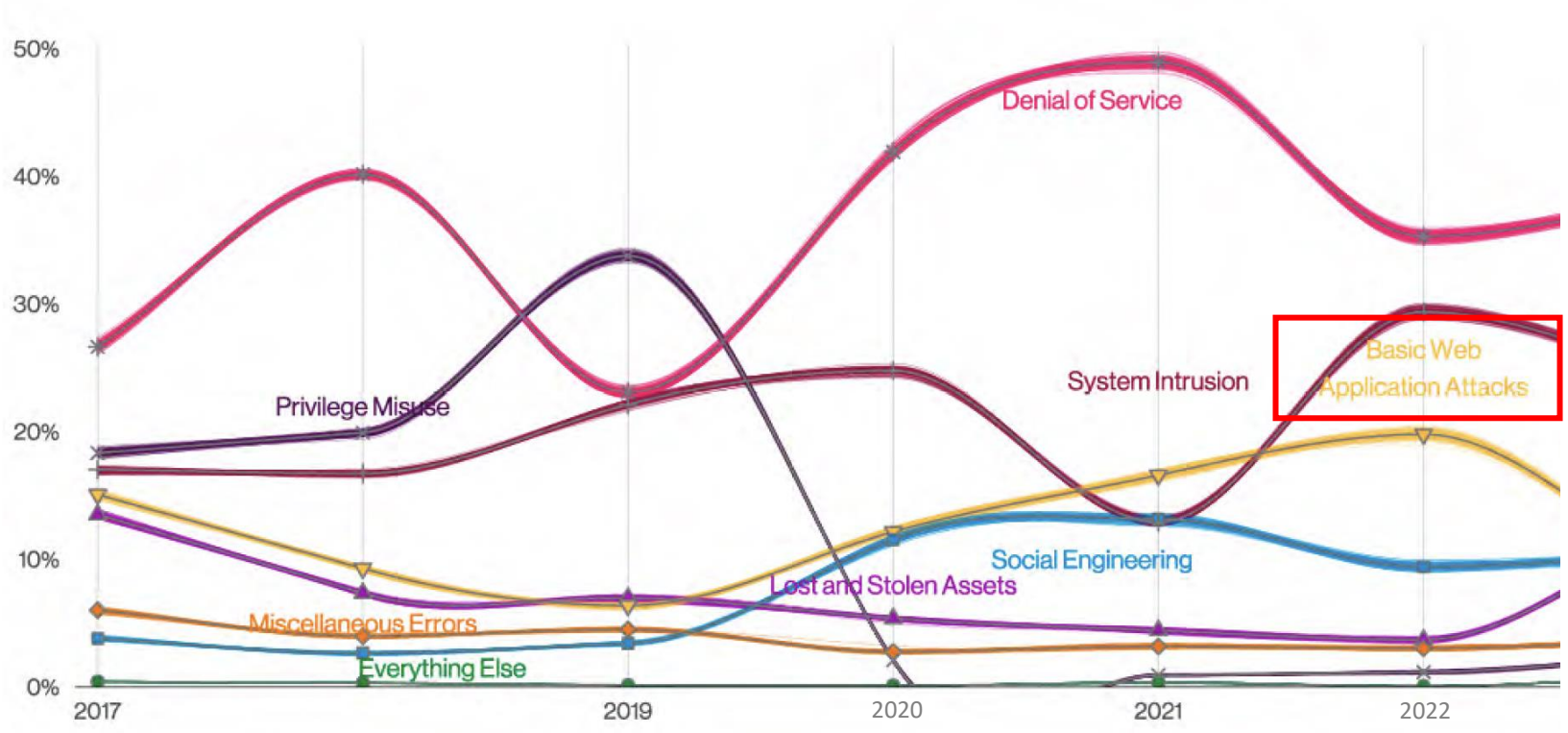


Figure 25. Patterns over time in incidents

傳統 WAF vs Next-Gen WAF

50%

of generated alerts are false positives

- Positive security model combined with custom rules helps keep false positives rate of **1%**

57%

deploy WAF in full blocking mode

- **90%** of Fastly customers deploy WAF in full blocking mode

25%

efficacy without heavy tuning

- No learning mode required
- With advanced tactics like ML and context-based detection, efficacy can rise to high end of **95%**

Consolidation

WAF & ADC are separated devices

- Consolidation of solutions WAF, load balancing
- Simplify SSL certificate management for all apps at one place

"A10's Next-Gen WAF, powered by Fastly, enhances web application defense, while reducing false positives / false negatives and operation efforts, resulting in an always secure and always available security solution for enterprises."

Market Positioning

Gartner Magic Quadrant for WAAP 2022

Gartner Peer Insights Customers' Choice for WAF for the past five years

Gartner peerinsights customers' choice 2019

Gartner peerinsights customers' choice 2020

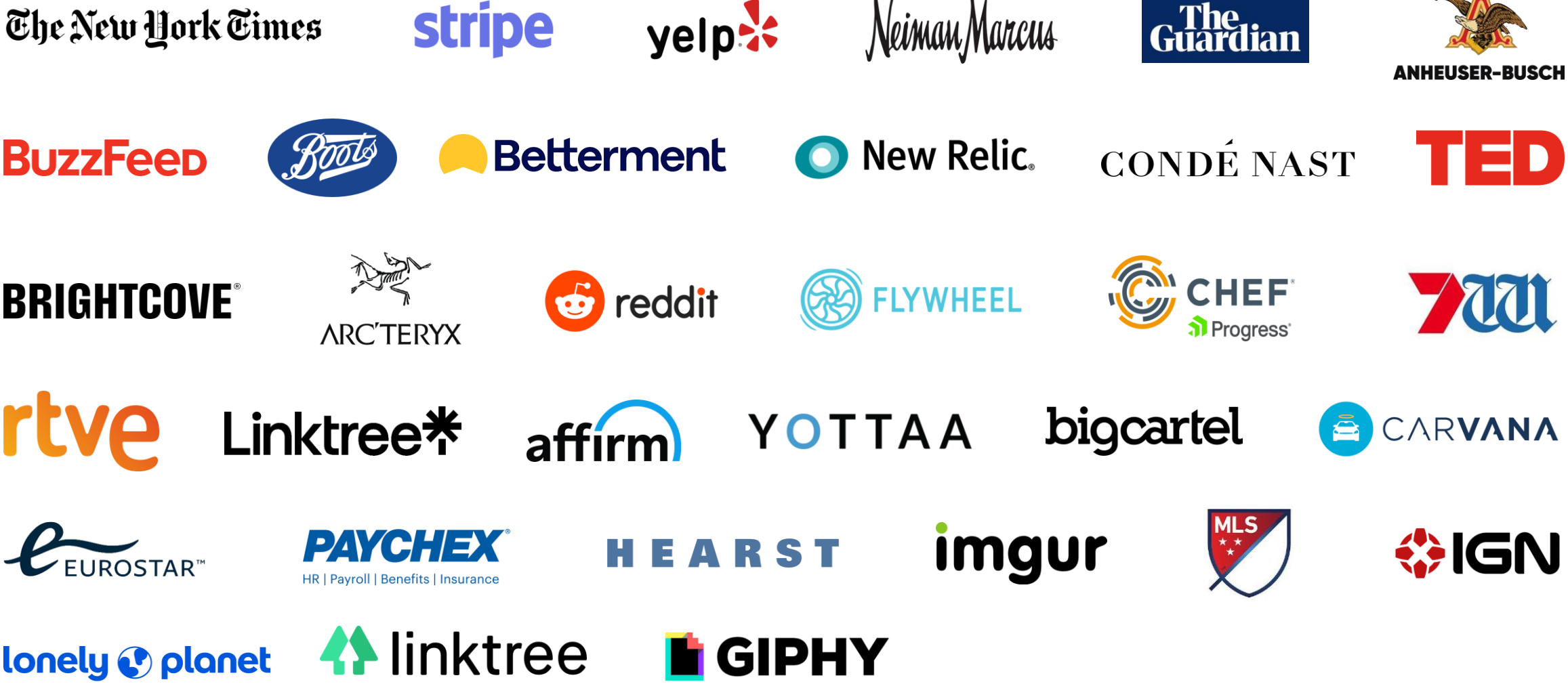
Gartner Peer Insights Customers' Choice 2021

Gartner Peer Insights Customers' Choice 2022

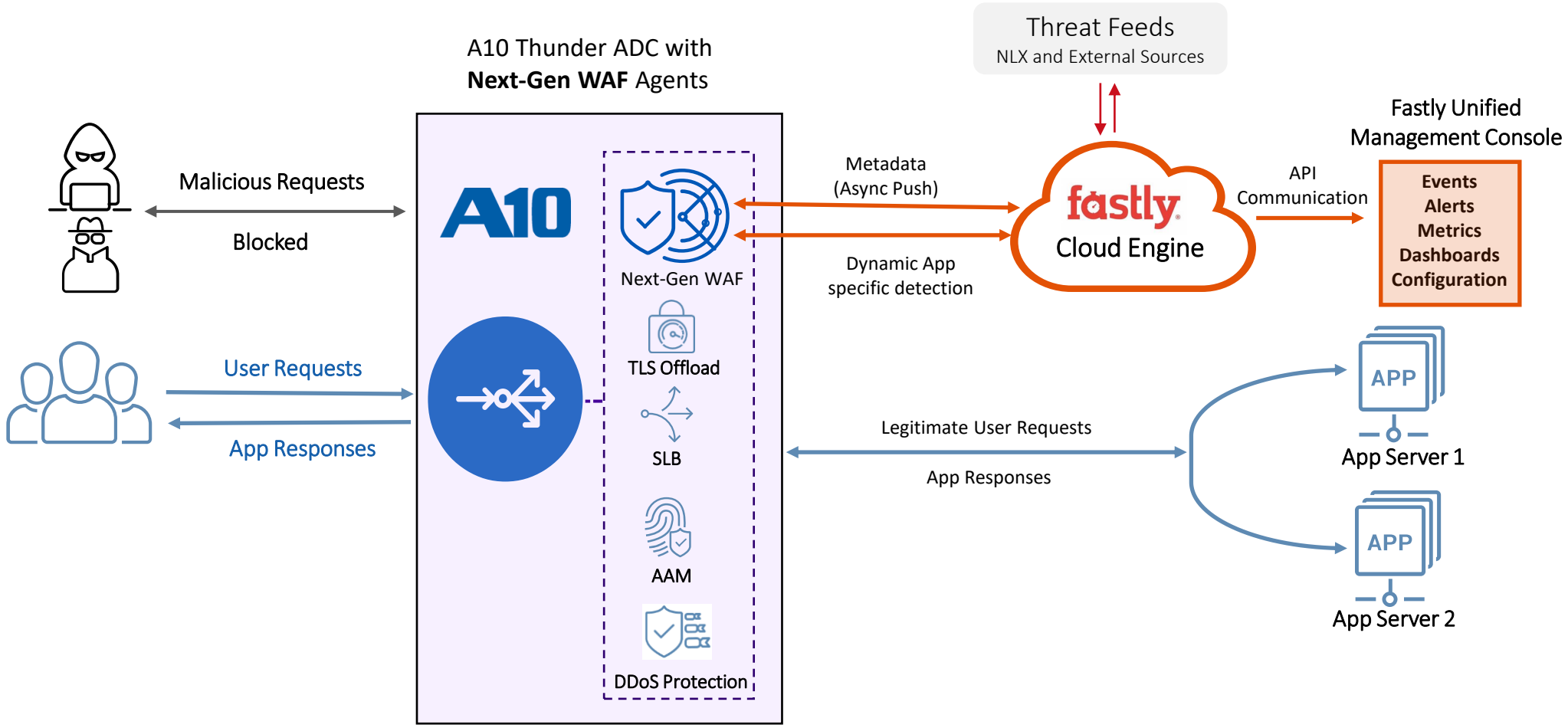
Gartner Peer Insights Customers' Choice 2023

A10 + fastly

客戶參考



A10 + fastly



A10 Next-Gen WAF 關鍵技術

Smart Parse

- A highly accurate detection method
- Evaluates the context of each request and how it would execute
- Enables near-zero tuning, no learning required and the ability to start detecting threats immediately

Threshold based blocking

- Predefined time-based thresholds allows automated blocking
- Can be customized on variables like threshold, time, validity specific to users' web application and business logic

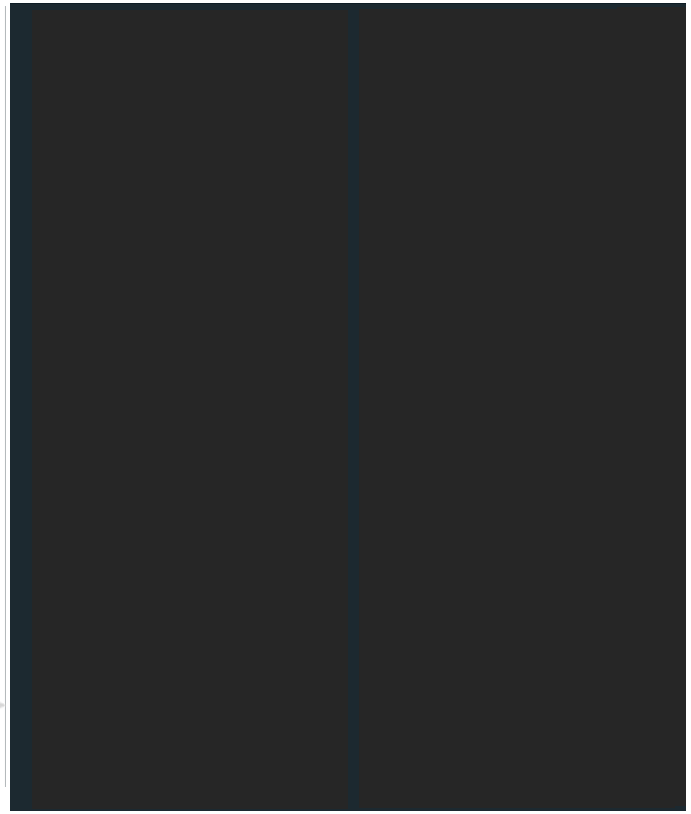
Network Learning Exchange

- Accurate Intelligence
- Aggregates and correlates anonymized attack information across Fastly users
- Identifies potential threats and alerts you before they are a threat to your sites

Smart Parse – How It Works

Web Example 1

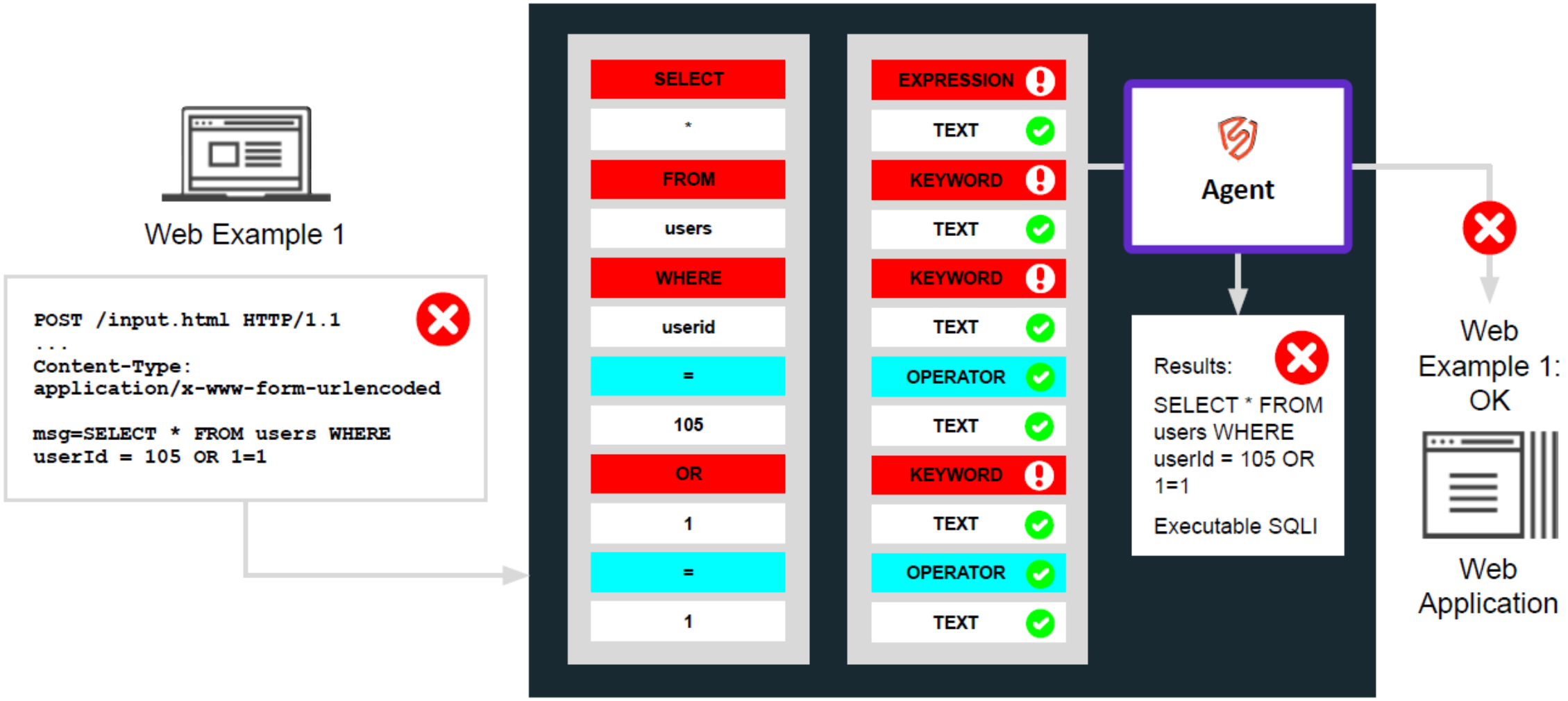
```
POST /input.html HTTP/1.1
...
Content-Type:
application/x-www-form-urlencoded

msg=SELECT * FROM users WHERE
userId = 105 OR 1=1
```



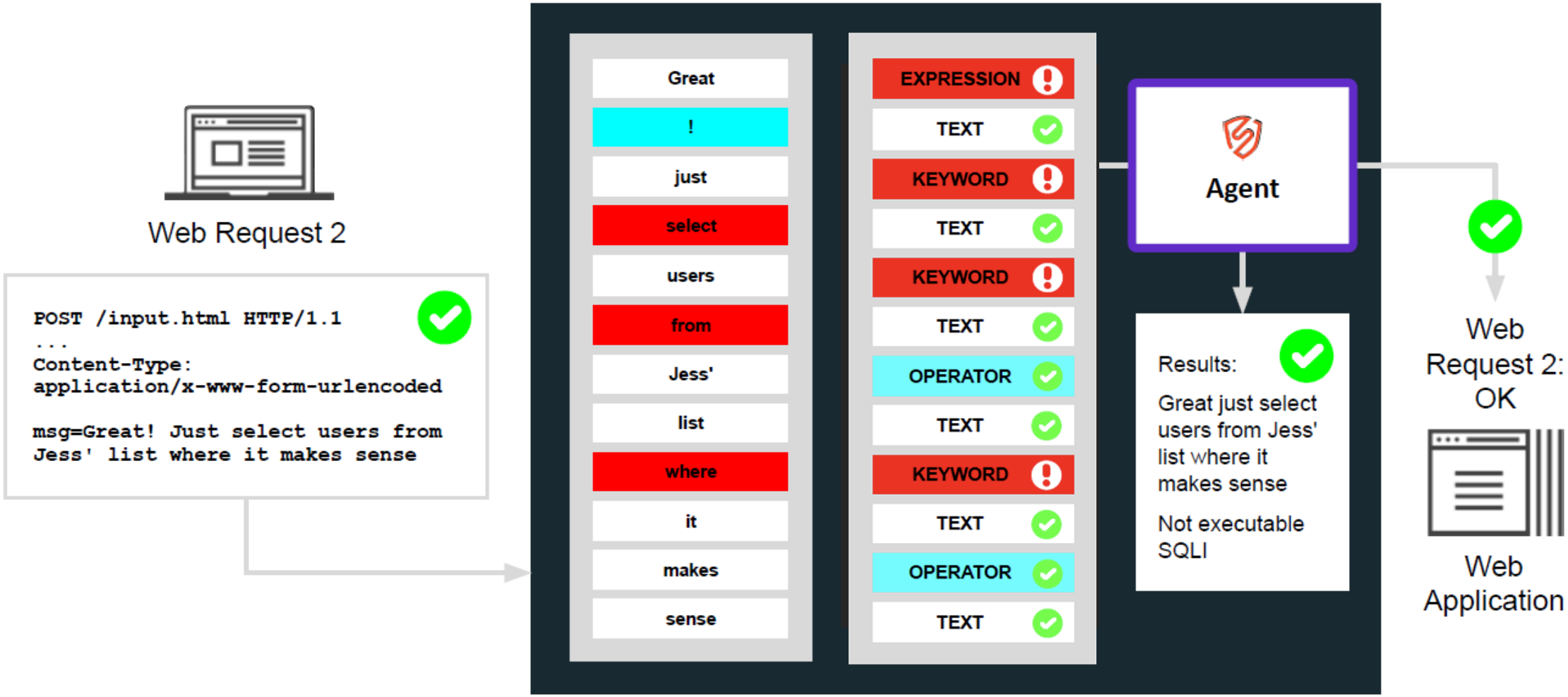
This means that the request is broken up into multiple pieces, and then tokenized as different categories (text, operator, expression, and keyword).

These tokenized patterns are then analyzed to see if they are executable. Thereafter, the agent makes the decision to block (or allow) requests

Example – No false negatives



Example – No false positives



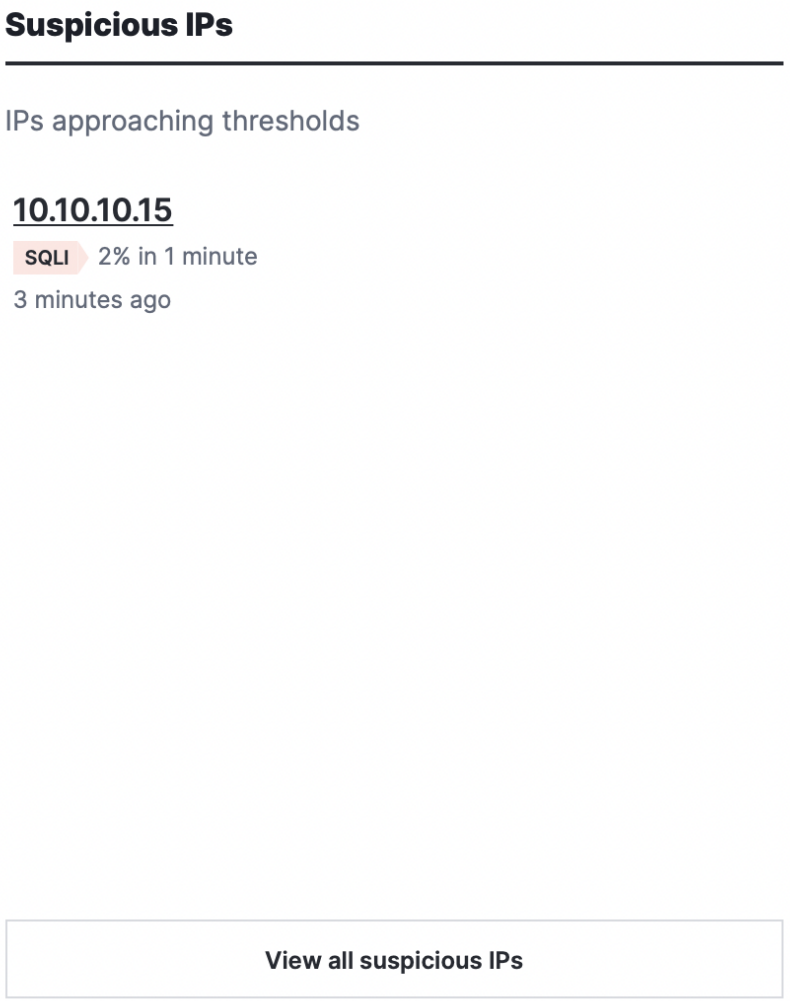
System Attack Signals (default enabled)

Attack signals are labels that describe malicious requests that contain attack payloads designed to hack, destroy, disable, steal, gain unauthorized access, and otherwise take harmful actions.

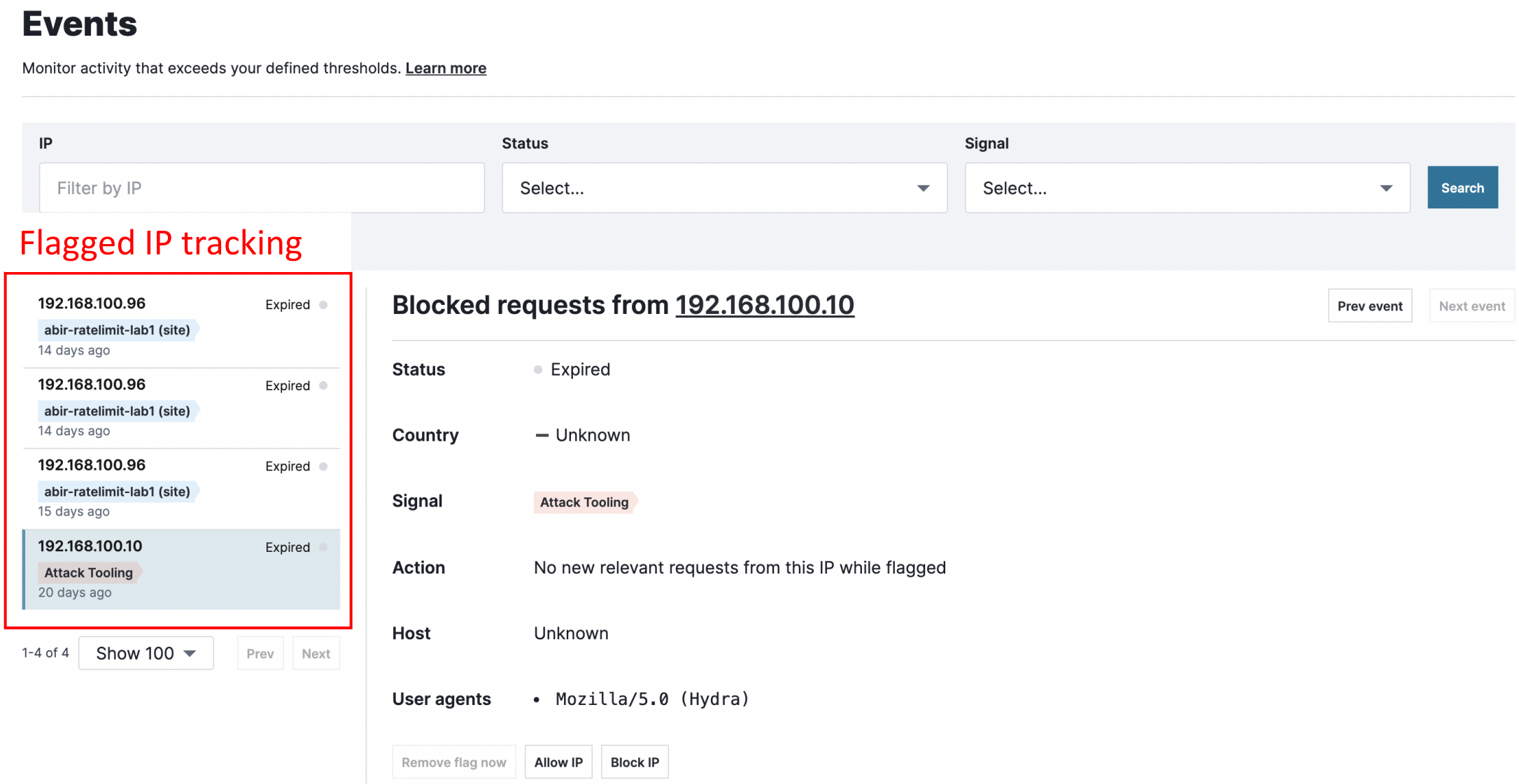
Long name	Short name	Usable in	Description
Attack Tooling	USERAGENT	• Lists • Rate Limit Rules • Request Rules • Signal Exclusion	Attack Tooling is the use of automated software to identify security vulnerabilities or to attempt to exploit a discovered vulnerability
AWS SSRF	AWS-SSRF	• Templated Rule	Server Side Request Forgery (SSRF) is a request which attempts to send requests made by the web application to target internal systems. AWS SSRF attacks use SSRF to obtain Amazon Web Services (AWS) keys and gain access to S3 buckets and their data.
Backdoor	BACKDOOR	• Lists • Rate Limit Rules • Request Rules • Signal Exclusion	A backdoor signal is a request that attempts to determine if a common backdoor file exists on a system. The signal generally matches known backdoor filenames. Traditionally these filenames appear with PHP file extensions like `admin.php` and `r57.php`. For many users, when these paths return a 200 or a larger response than expected, it may indicate that their system has been compromised or they are unknowingly hosting a backdoor file.
Command Execution	CMDEXE	• Lists • Rate Limit Rules • Request Rules • Signal Exclusion	Command Execution is the attempt to gain control or damage a target system through arbitrary system commands by means of user input
Cross Site Scripting	XSS	• Lists • Rate Limit Rules • Request Rules • Signal Exclusion	Cross-Site Scripting is the attempt to hijack a user's account or web-browsing session through malicious JavaScript code
Directory Traversal	TRAVERSAL	• Lists • Rate Limit Rules • Request Rules • Signal Exclusion	Directory Traversal is the attempt to navigate privileged folders throughout a system in hopes of obtaining sensitive information

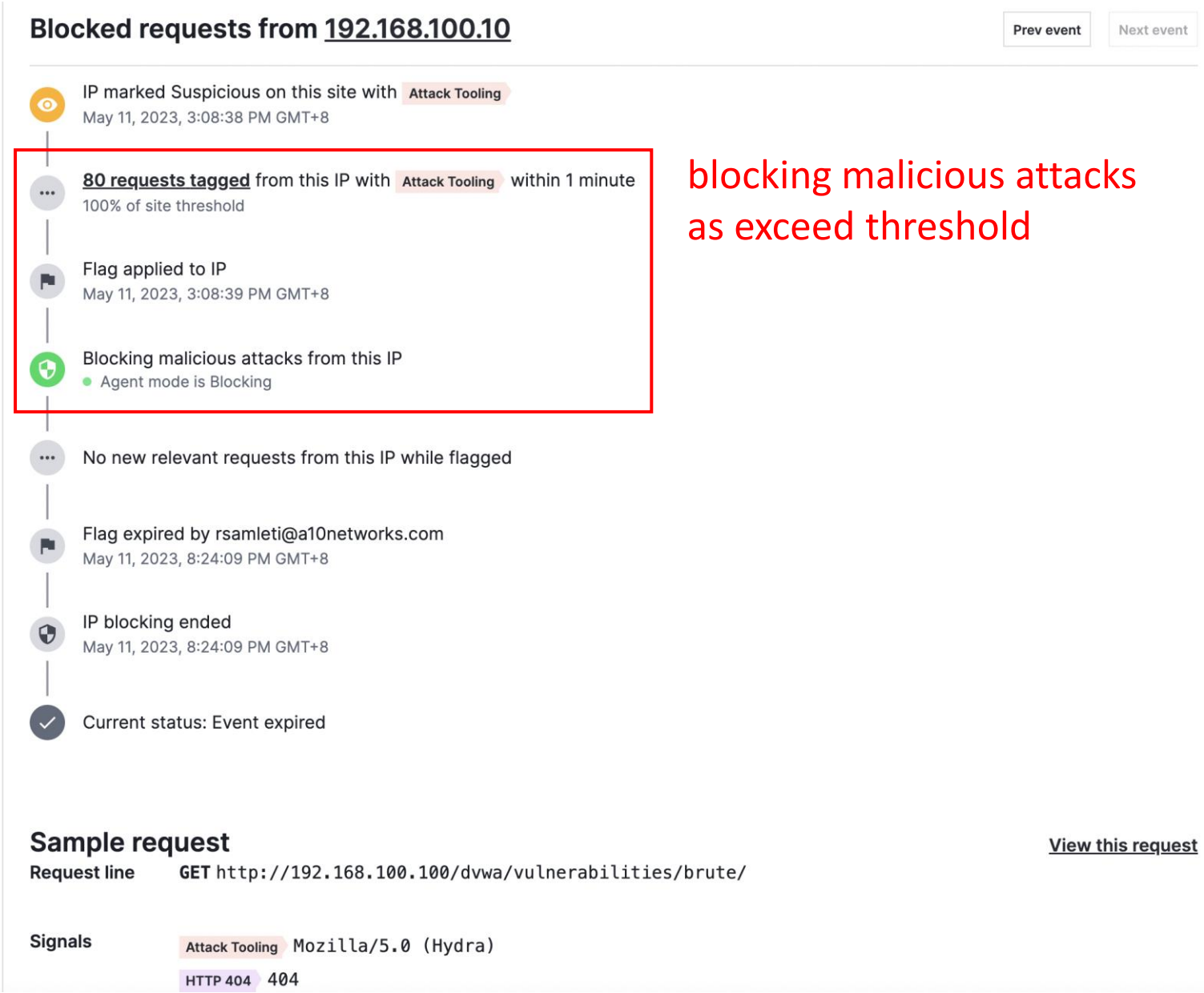
Suspicious IPs

- User IP is suspicious once matching the system signals under thresholds.
- NGWAF identifies a user by it's source IP
- Default threshold:
  - 50/1 minute (check every 20 seconds)
  - 350/10 minutes (check every 3 minutes)
  - 1800/1 hour (check every 20 minutes)



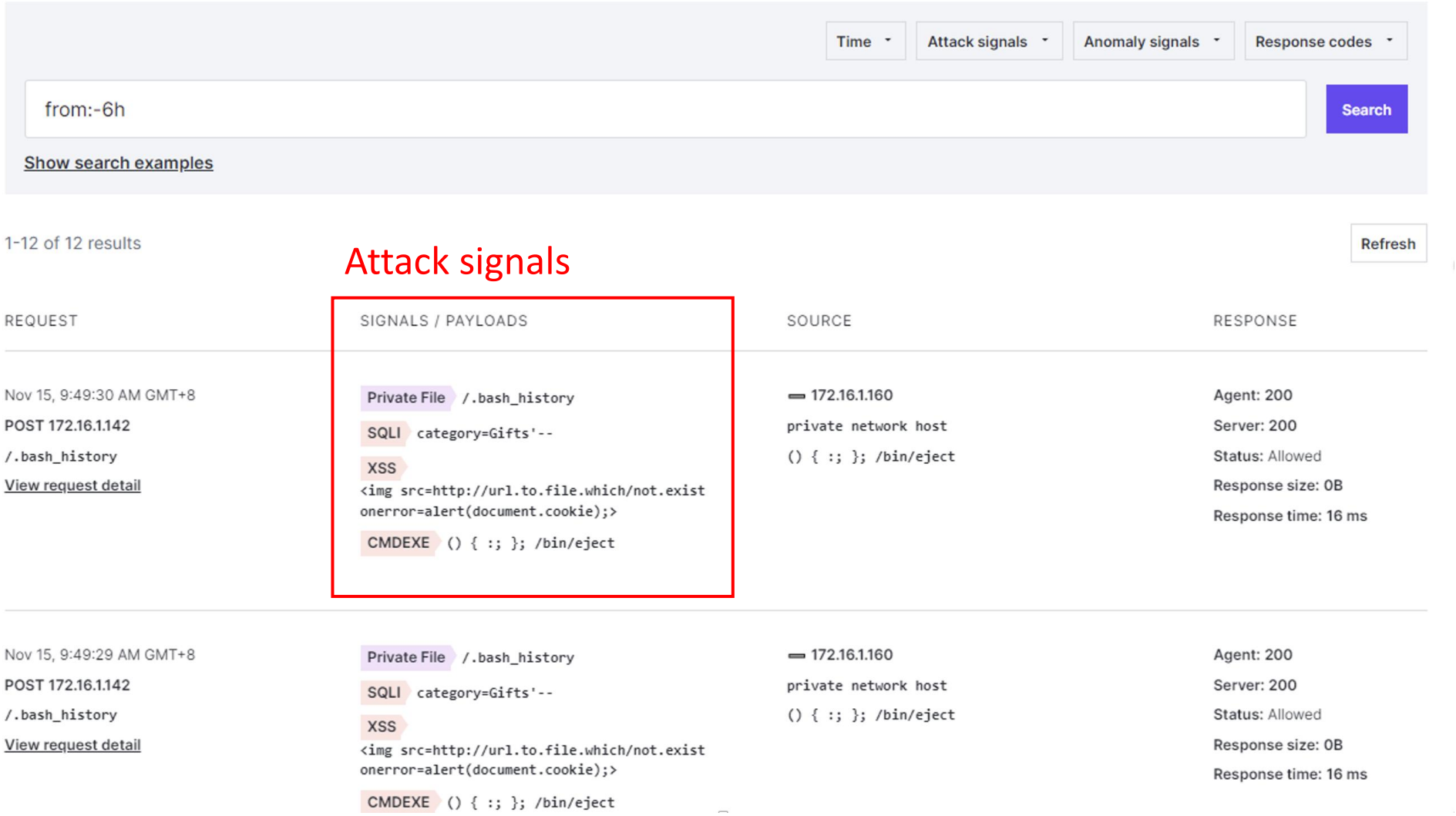
Flagged IP & Threshold based blocking





blocking malicious attacks as exceed threshold

Tagged Requests



False positive convert to rule

Requests / View

Server

Server hostname ACOS-6.0.1-CFW-WAF-35-shared

Remote Client

Remote address 10.10.10.7

Remote hostname private network host

Remote country code N/A

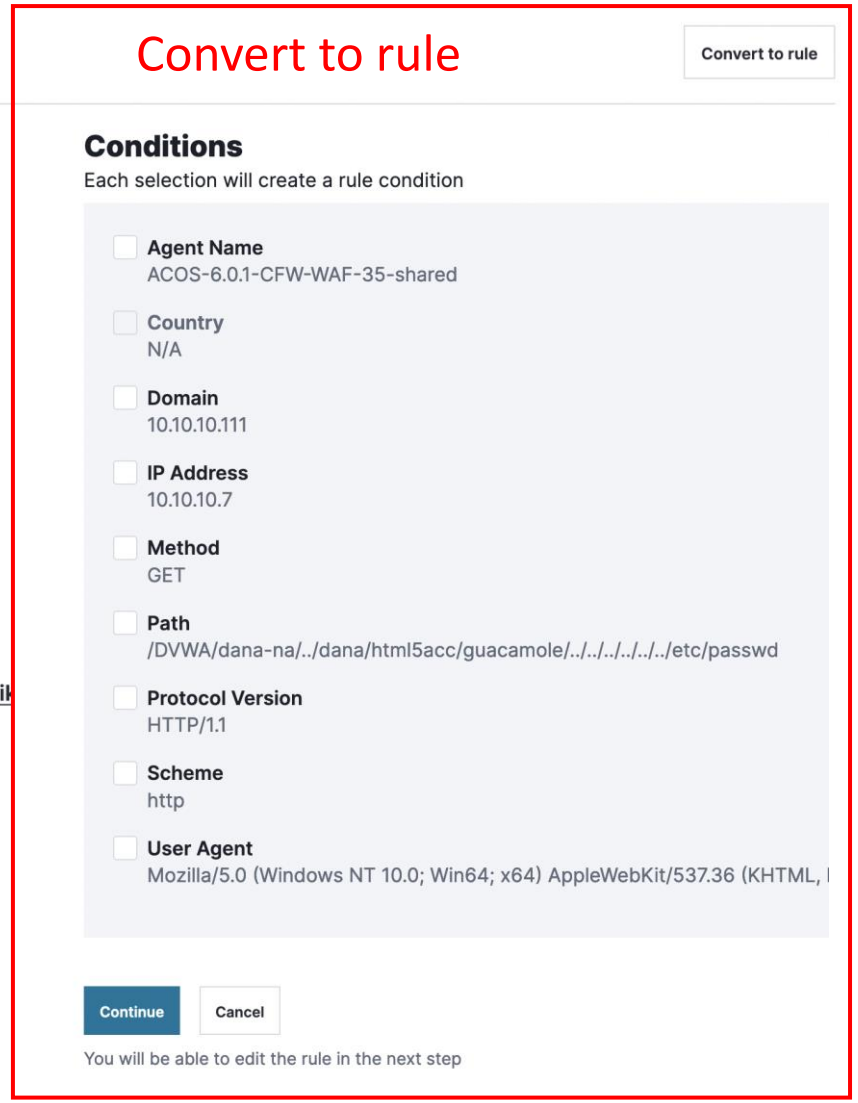
User agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik

Request

Timestamp Aug 17, 4:24:08 PM GMT+8

Method GET

Convert to rule



Site Overview

Request Volume

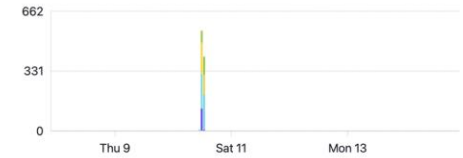
All requests for this site

0.01 average RPS

Total Requests	7k

OWASP Injection Attacks

The most common attacks from OWASP Top 10



SQLI	122
XSS	389
CMDEXE	284
Traversal	166

Quick look | View requests

OWASP TOP 10

Latest feature announcements

Agent management functionality - Beta
Our agent management functionality now includes a service that auto-updates agent versions and a plugin for Vault that stores and rotates agent keys.

Professional Plan Edge Deployment Updates
Custom signals, dashboards, lists, templated rules, and custom response codes are now available for Professional plan customers using edge deployment.

Announcing New Protection for CVE-2022-42889
Use the new virtual patch to protect yourself from the recent Apache Commons Text library code execution vulnerability.

View all announcements

OWASP TOP10

Top 10:2021 List

A01 Broken Access Control

A02 Cryptographic Failures

A03 Injection

A04 Insecure Design

A05 Security Misconfiguration

A06 Vulnerable and Outdated Components

A07 Identification and Authentication Failures

A08 Software and Data Integrity Failures

A09 Security Logging and Monitoring Failures

A10 Server Side Request Forgery (SSRF)

Scanners

Commercial and open source scanning tools

Attack Tooling	3k
Backdoor	0
Forceful Browsing	523
Private File	253

Traffic Source Anomalies

Requests from unusual or suspicious sources

SigSci IP	0
Tor Traffic	0
Datacenter	0
Malicious IP	26

Events

IPs flagged for exceeding thresholds

44.144.222.189	Attack Tooling 4 days ago	Expired
60.49.127.60	SQLI 4 days ago	Expired
154.233.62.85	Attack Tooling 4 days ago	Expired

Showing 3 of 11

目標客戶

Target	Why/The Big Issues	Vertical Specific Challenges	Solved With
E-commerce Companies (電商)	Online transactions (payment systems), complex APIs involved, lower security awareness	Brute force attacks, DDoS, limited management and bandwidth due to limited security team	• Advanced Rate-limiting, Syn Cookies, ATO and DDoS Protection • 0 learning period; simplified deployment • PCI-DSS compliant, SOC 2
Finance and FinTech (金融)	Sensitive financial information, large attack surface, strict compliance regulations (less security)	Bank account numbers, SSNs, credit card fraud	• ADC shrink attack surface, • Improves application performance • PCI-DSS/SOC 2/HIPAA/GDPR • IDP integration enforces continuous monitoring and auth • Protects against known CVEs
Healthcare Providers (醫療)	Cripple critical infrastructure, strict compliance regulations, sensitive personal information, large attack surface	SSNs, HIPAA and GDPR regulations, ransomware attacks, obtain confidential medical research	• ADC shrinks attack surface • TLS/SSL offload • HIPAA/GDPR compliant • Sensitive data redaction • Protects against known CVEs
Government Agencies (政府)	Critical data involved, political motivations, strict compliance regulations	Tax filings, voting, permit applications	• GDPR compliant • Context-aware detection can halt malicious code from being injected • TLS/SSL offloading improves web application performance

A10 vs F5

	A10 Next-Gen WAF	F5 BIG-IP Advanced WAF
Superior Blocking Approach – Context based	✓ (Smart Parse and Threshold based blocking)	✗ (Rely on Regex matching)
No Learning mode required	✓	✗
DevOps Integrations	✓	Partial
User-friendly Centralized Management & Analytics (for WAF)	✓	✗ (Need to purchase a separate BIG -IQ)
Threat IP Intelligence derived from network of customers	✓ (Network Learning Exchange)	✗ (Add on subscription with Third Party Intelligence Services)
Threat feed/New Signature and Rule updates	✓	✓
Comprehensive OWASP coverage	✓	✓
Account Takeover Protection	✓	✓
Virtual Patching	✓	✓

A10 vs F5

	A10 Next-Gen WAF	F5 BIG-IP Advanced WAF
PCI 6.6 Compliance	✓	✓
Effective blocking in production	✓ (Near zero or very minimal false positives)	Partial (generates false positives)
Fast time to value without rules tuning	✓	Partial
Geolocation-based Blocking	✓	✓

A10 vs Imperva

	A10 Next-Gen WAF	Imperva WAF Gateway
Superior Blocking Approach – Context based	✓ (Smart Parse and Threshold based blocking)	✗ (Regex Matching)
No Learning mode required	✓	✗
User-friendly Centralized Management & Analytics (for WAF)	✓	✗ (Need to buy separate management device)
Threat IP Intelligence derived from network of customers	✓ (Network Learning Exchange)	✗ (Add on subscription with Third Party Services)
Threat feed/New Signature and Rule updates	✓	✗ (Add on subscription is required)
Comprehensive OWASP coverage	✓	✓
Account Takeover Protection	✓	✓
Virtual Patching	✓	✓
Geolocation-based Blocking	✓	✓
PCI 6.6 Compliance	✓	✓

A10 vs Imperva

	A10 Next-Gen WAF	Imperva WAF Gateway
ADC integrated	✓	Partial (basic ADC)
Effective blocking in production	✓ (Near zero or very minimal false positives)	Partial (generates false positives)
Fast time to value without rules tuning	✓	Partial

下一代 Web 應用程式防火牆

進階式應用層防禦

- OWASP Top 10
- SmartParse - Context-aware detection
- Account Takeover (ATO)
- Virtual patching (known CVEs)

整合於單一設備

- Consolidation of solutions WAF, load balancing, caching, DDoS protection
- Simplify SSL certificate management for all apps at one place

符合資安法規

- Protect web apps that store sensitive data such as PII credit card and healthcare data
- PCI-DSS 6.6
- SOC2
- HIPAA
- GDPR

提高資安管理效率

- No learning mode required
- One management plane for centralized policy enforcement and analytics/visibilities
- Doesn't require expert skills

A10

Always Secure. Always Available.

Thank You