



Always Secure. Always Available.

新一代WEB應用程式防護

A10 技術經理

Allen Lin

The State of Web Application Security

- 應用程式和資料洩漏的風險提升
 - 法規的罰鍰
 - 智財權的損失
 - 永久的商譽損害
- 因為WAF的誤判導致安全團隊的負擔
- 現代應用程式架構導致部署和維運的複雜
- API大量的增加/使用



WAF管理的困境



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%**

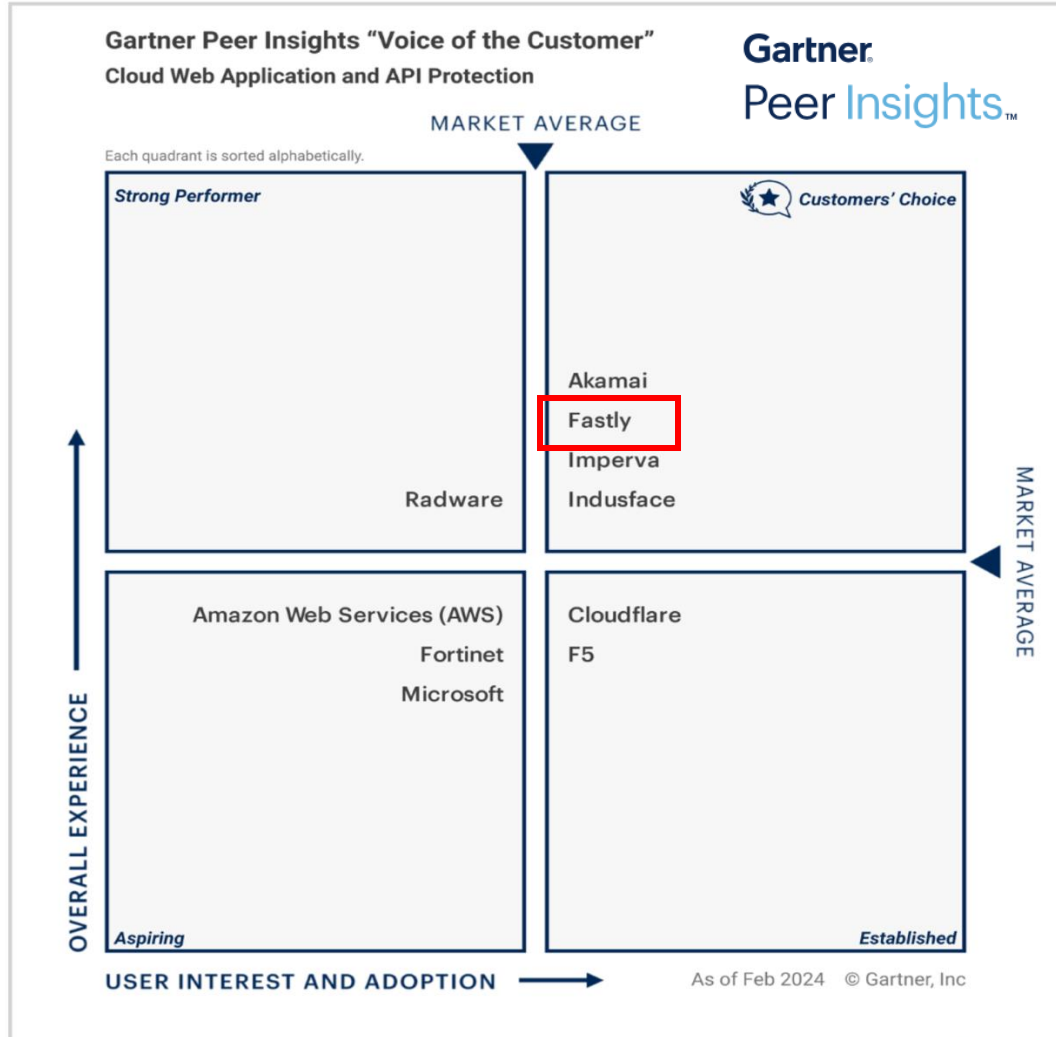


Consolidation

WAF & ADC are
separated devices

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

Market Positioning



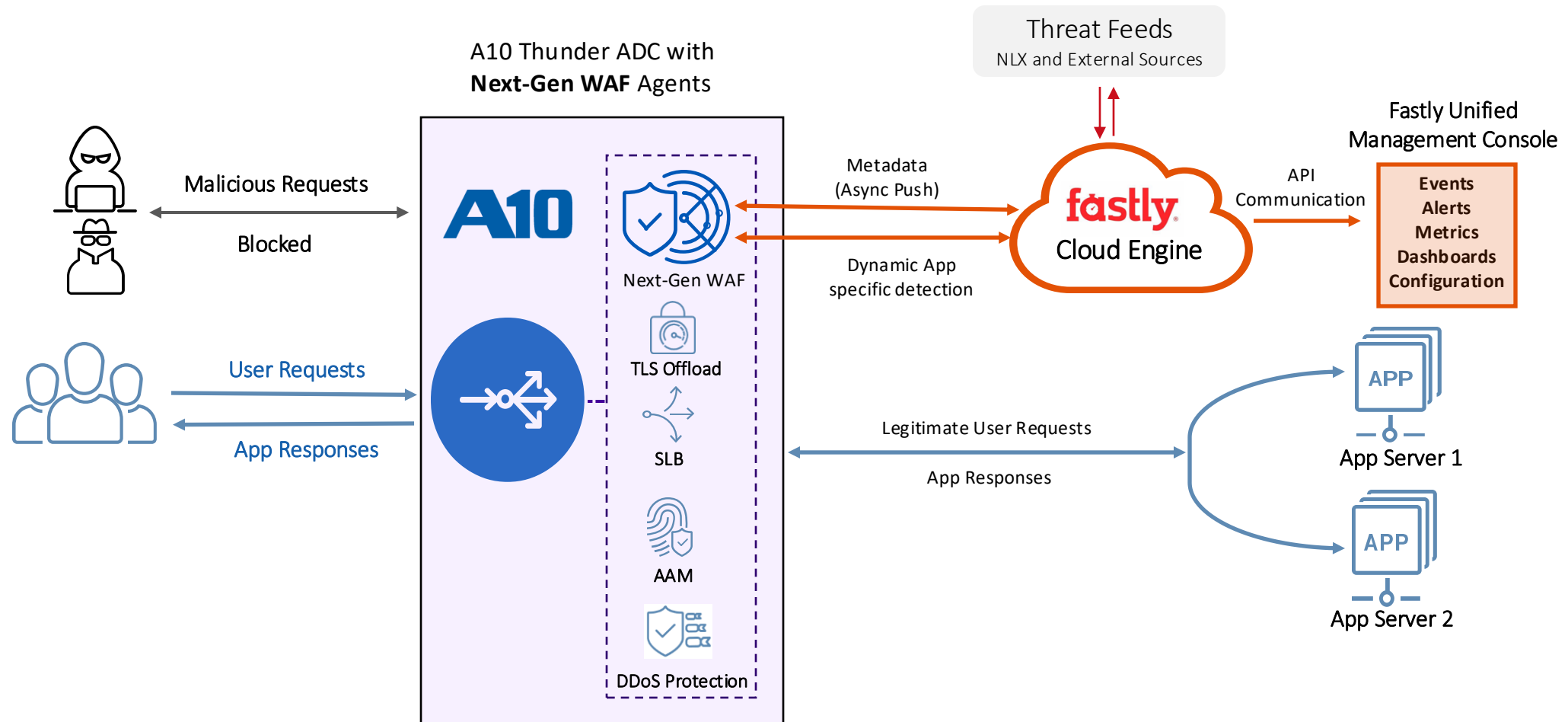
Gartner Peer Insights Customers' Choice
for WAF for the past 6 years



A10 + fastly®

<https://www.gartner.com/reviews/market/cloud-web-application-and-api-protection> **Gartner.**

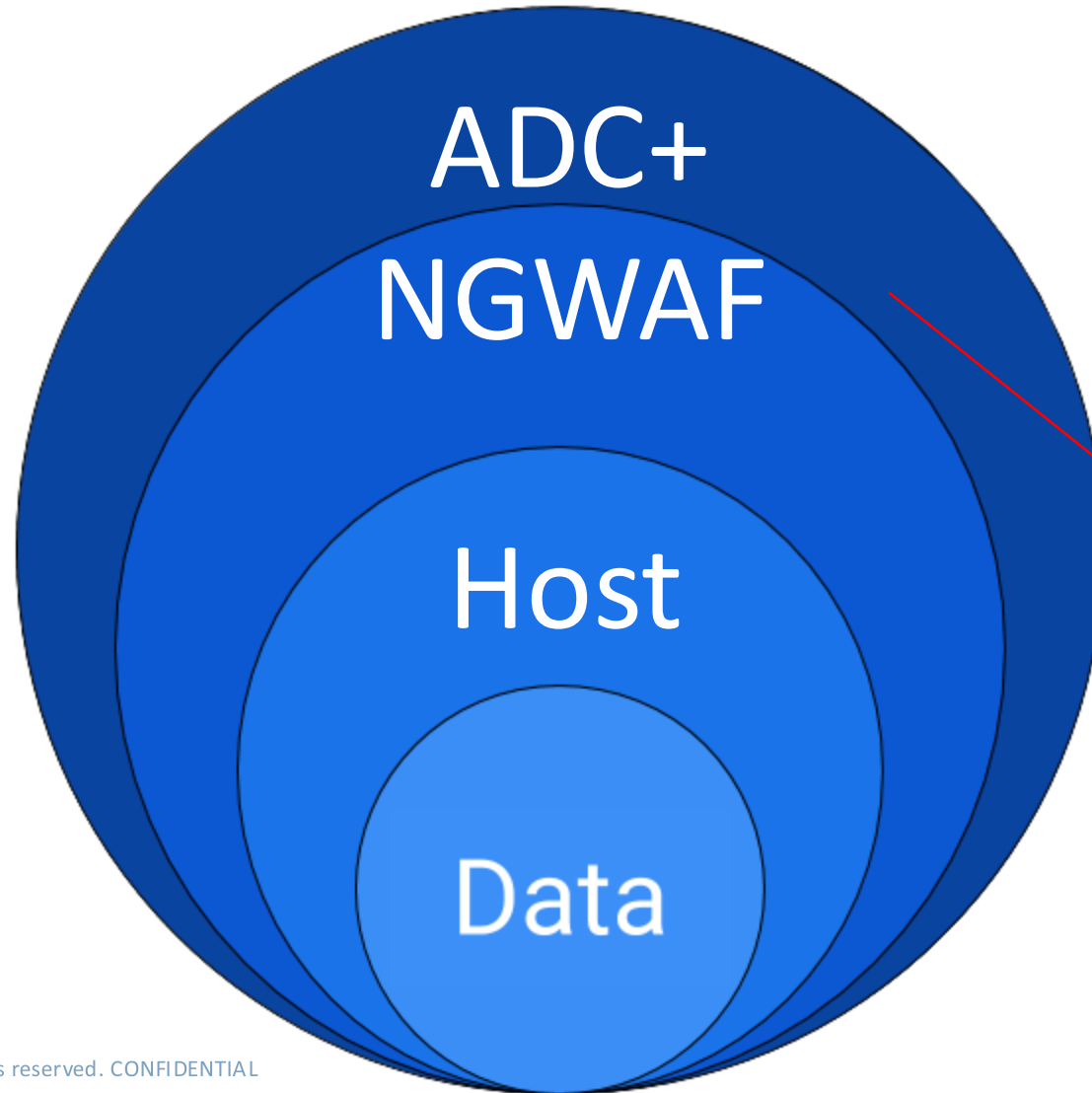
<https://www.gartner.com/reviews/market/cloud-web-application-and-api-protection/vendor/fastly>



Defense in Depth

FW/IPS

防火牆規則
應用程式識別
入侵防護



應用服務優化
應用服務存取政策
全域負載均衡
服務快速平行擴展
Web應用程式保護
Web API防護
Web DDoS防護
IP Reputation
合規
L3/L4 DDoS防護

A10 Next-Gen WAF 關鍵技術

Smart Parse

- 高精度的檢測方法
- 評估每個請求的上下文及其執行方式
- 實現近乎零的調整，無需學習，並且能夠立即開始偵測威脅

Threshold based blocking

- 預先定義的基於時間的閾值允許自動阻止
- 可以針對特定於使用者 Web 應用程式和業務邏輯的閾值、時間、有效性等變數進行自訂

Network Learning Exchange

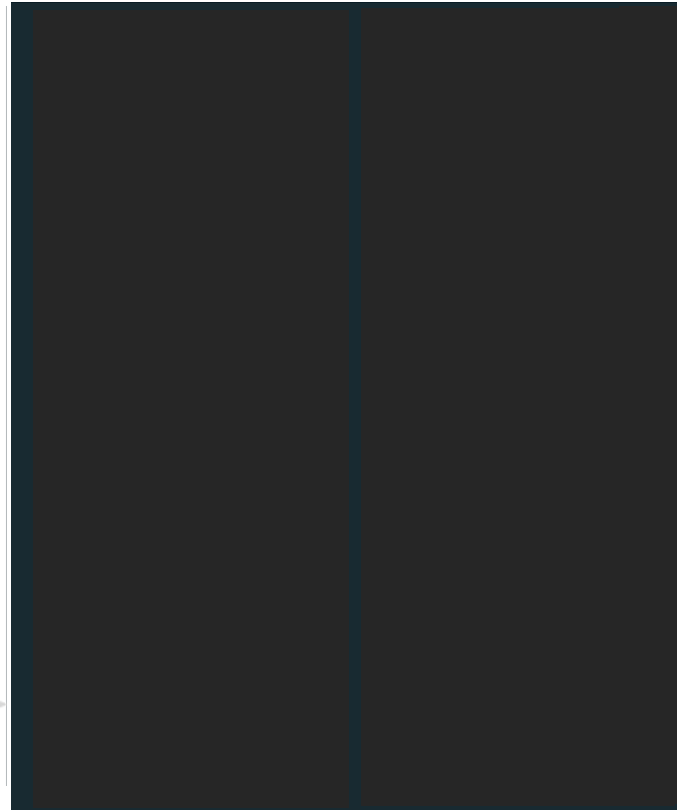
- 精準情報
- 聚合並關聯 Fastly 用戶的匿名攻擊訊息
- 識別潛在威脅並在它們對您的網站構成威脅之前向您發出警報

智能化解析 SmartParse



Web Example 1

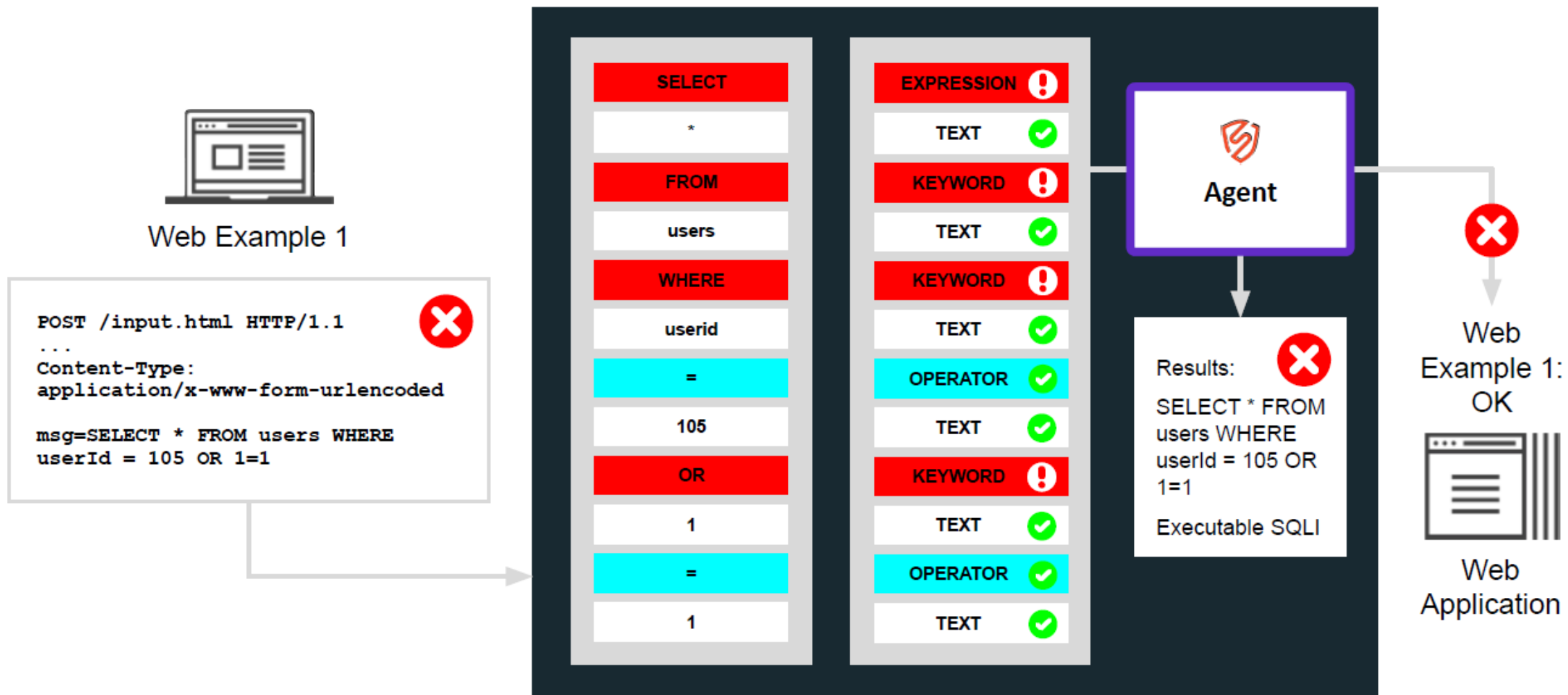
```
POST /input.html HTTP/1.1
...
Content-Type:
application/x-www-form-urlencoded
msg=SELECT * FROM users WHERE
userId = 105 OR 1=1
```



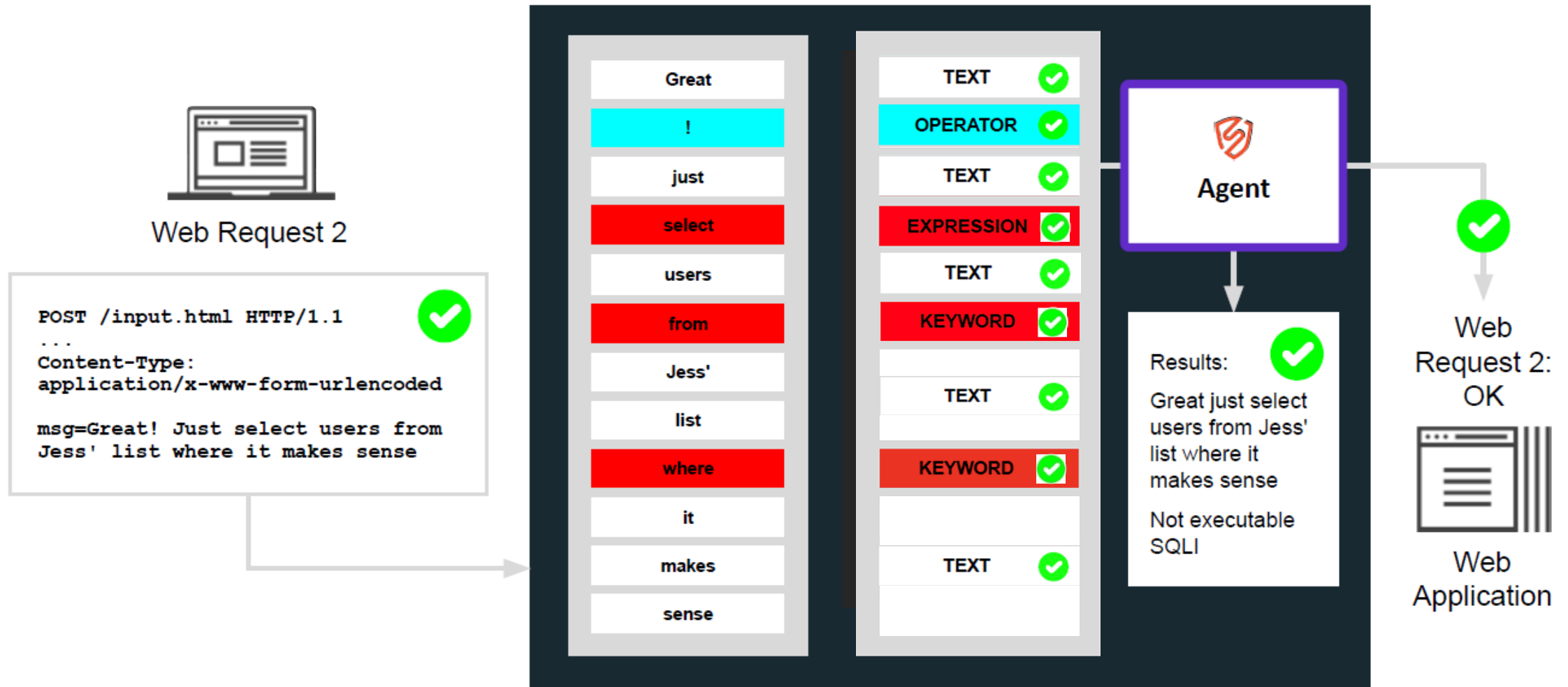
This means that the request is broken up into multiple pieces, and then **tokenized as different categories** (text, operator, expression, and keyword).

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

低漏判率 Near-zero false negatives



低誤判率 Near-zero 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

System Anomaly Signals (default enabled)

Anomaly signals are labels that describe abnormal requests. While not inherently malicious, abnormal requests may be indicative of unwanted or abusive traffic. Examples include malformed request data and requests originating from known scanners.

Long name	Short name	Usable in	Description
Abnormal Path	ABNORMALPATH	- Lists - Rate Limit Rules - Request Rules - Signal Exclusion	Abnormal Path indicates the original path differs from the normalized path (e.g., <code>/foo/. /bar</code> is normalized to <code>/foo/bar</code>)
Bad Hop Headers	BHH	- Lists - Rate Limit Rules - Request Rules - Signal Exclusion	Bad Hop Headers indicate an HTTP smuggling attempt through either a malformed Transfer-Encoding (TE) or Content-Length (CL) header, or a well-formed TE and CL header
Blocked Requests	BLOCKED	None	Requests blocked by Signal Sciences

Code Injection PHP	CODEINJECTION	- Lists - Rate Limit Rules - Request Rules - Signal Exclusion	Code Injection is the attempt to gain control or damage a target system through arbitrary application code commands by means of user input.
Compression Detected	COMPRESSED	- Lists - Rate Limit Rules - Request Rules - Signal Exclusion	The POST request body is compressed and cannot be inspected. For example, if a Content-Encoding: gzip request header is specified and the POST body is not plain text.
Datacenter Traffic	DATACENTER	- Lists - Rate Limit Rules - Request Rules - Signal Exclusion	Datacenter Traffic is non-organic traffic originating from identified hosting providers. This type of traffic is not commonly associated with a real end user.

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)

Suspicious IPs

IPs approaching thresholds

10.10.10.15

SQLI 2% in 1 minute

3 minutes ago

[View all suspicious IPs](#)

追蹤可疑來源

Events

Monitor activity that exceeds your defined thresholds. [Learn more](#)

Threshold based blocking

IP

Filter by IP

Status

Select...

Signal

Select...

Search

Malicious IP tracking

192.168.100.96	Expired
abir-ratelimit-lab1 (site)	
14 days ago	
192.168.100.96	Expired
abir-ratelimit-lab1 (site)	
14 days ago	
192.168.100.96	Expired
abir-ratelimit-lab1 (site)	
15 days ago	
192.168.100.10	Expired
Attack Tooling	
20 days ago	

Blocked requests from 192.168.100.10

Status	Expired
Country	Unknown
Signal	Attack Tooling
Action	No new relevant requests from this IP while flagged
Host	Unknown
User agents	Mozilla/5.0 (Hydra)

Blocked requests from 192.168.100.10

Prev event Next event

 IP marked Suspicious on this site with **Attack Tooling**
May 11, 2023, 3:08:38 PM GMT+8

 **80 requests tagged** from this IP with **Attack Tooling** within 1 minute
100% of site threshold

 Flag applied to IP
May 11, 2023, 3:08:39 PM GMT+8

 Blocking malicious attacks from this IP
● Agent mode is Blocking

 No new relevant requests from this IP while flagged

 Flag expired by rsamleti@a10networks.com
May 11, 2023, 8:24:09 PM GMT+8

 IP blocking ended
May 11, 2023, 8:24:09 PM GMT+8

 Current status: Event expired

blocking malicious attacks
as exceed threshold

Sample request

[View this request](#)

Request line GET http://192.168.100.100/dvwa/vulnerabilities/brute/

Signals **Attack Tooling** Mozilla/5.0 (Hydra)
HTTP 404 404

Tagged Requests

Time ▾

Attack signals ▾

Anomaly signals ▾

Response codes ▾

Search

[Show search examples](#)

1-12 of 12 results

Refresh

Attack signals

REQUEST	SIGNALS / PAYLOADS	SOURCE	RESPONSE
Nov 15, 9:49:30 AM GMT+8 POST 172.16.1.142 /.bash_history View request detail	Private File /.bash_history SQLI category=Gifts'-- XSS CMDEXE () { ;; }; /bin/eject	172.16.1.160 private network host () { ;; }; /bin/eject	Agent: 200 Server: 200 Status: Allowed Response size: 0B Response time: 16 ms
Nov 15, 9:49:29 AM GMT+8 POST 172.16.1.142 /.bash_history View request detail	Private File /.bash_history SQLI category=Gifts'-- XSS CMDEXE () { ;; }; /bin/eject	172.16.1.160 private network host () { ;; }; /bin/eject	Agent: 200 Server: 200 Status: Allowed Response size: 0B Response time: 16 ms

高效率誤判排除

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, like Gecko) Chrome/104.0.0.0 Safari/537.36

Request

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

Method GET

Convert to rule

Convert to rule

Conditions

Each selection will create a rule condition

- ☐ **Agent Name**
ACOS-6.0.1-CFW-WAF-35-shared
- ☐ **Country**
N/A
- ☐ **Domain**
10.10.10.111
- ☐ **IP Address**
10.10.10.7
- ☐ **Method**
GET
- ☐ **Path**
/DVWA/dana-na/./dana/html5acc/guacamole/././././././etc/passwd
- ☐ **Protocol Version**
HTTP/1.1
- ☐ **Scheme**
http
- ☐ **User Agent**
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36

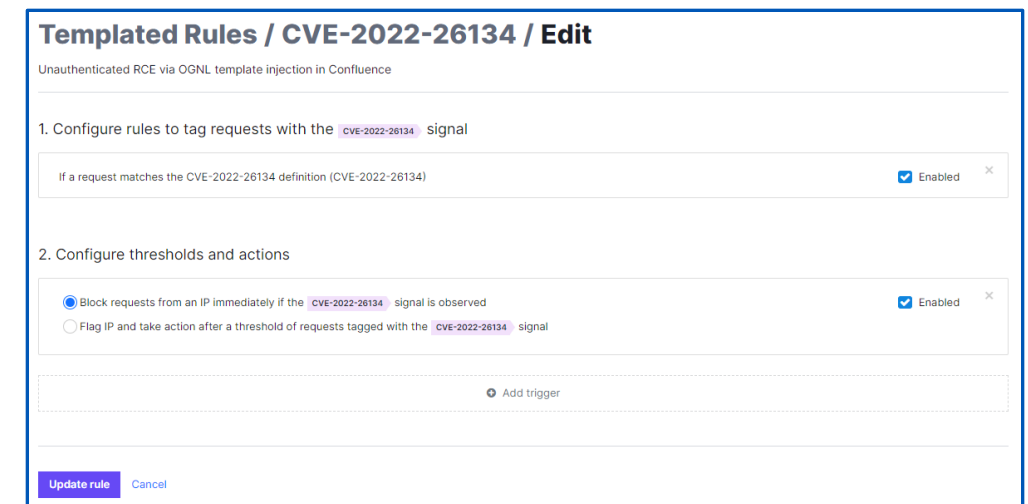
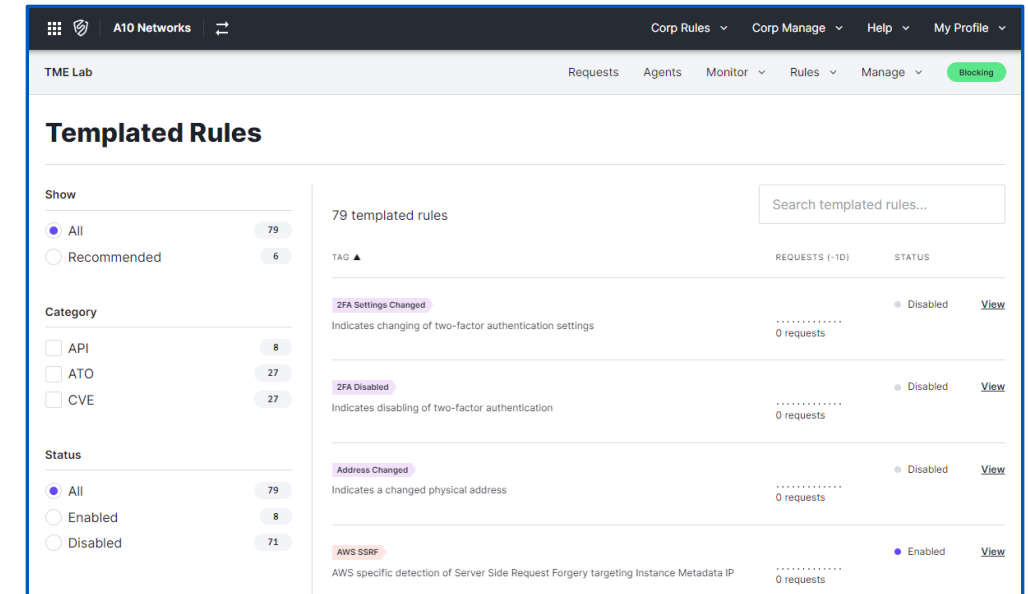
Continue

Cancel

You will be able to edit the rule in the next step

Templated Rules

- Templated rules are of 3 categories
 - Virtual Patching (CVE)
 - Account Takeover (ATO) Protection
 - API Protection
- Built-in virtual patching rules immediately block specific common vulnerabilities (CVE)
- ATO protection enables to identify account takeover attacks on the application
- API protection enable to detect patterns of malicious API requests
- Benefits
 - Built-in rules makes it simple to manage and save time
 - Easy to use rule builders to implement customization
 - Provides visibility into requests through signal tags



Corp/Site Overview

Request Volume

All requests for this site

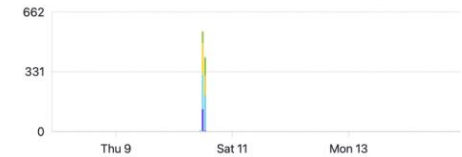
0.01 average RPS



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

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

Showing 3 of 11



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)

Signal Dashboard

☒ OWASP Injection Attacks

- ☒ SQLI
- ☒ XSS
- ☒ CMDEXE
- ☒ Traversal

☒ Scanners

- ☒ Forceful Browsing
- ☒ Backdoor
- ☒ Attack Tooling
- ☒ Private File

☒ Traffic Source Anomalies

- ☒ Tor Traffic
- ☒ Malicious IP
- ☒ SigSci IP
- ☒ Datacenter

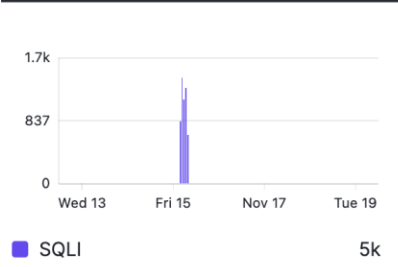
☒ Request Anomalies

- ☒ Allowed Request
- ☒ Impostor
- ☒ No UA
- ☒ Null Byte
- ☒ Invalid Encoding
- ☒ Blocked Request
- ☒ Body Parser Evasion
- ☒ Out-of-Band Domain

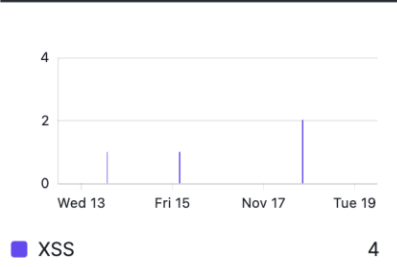
☒ Response Anomalies

- ☒ HTTP 4XX
- ☒ HTTP 403
- ☒ HTTP 404

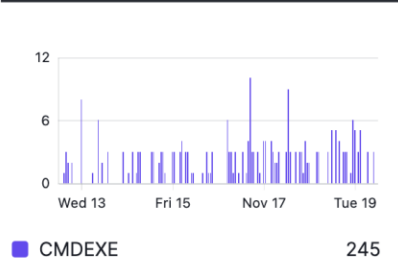
SQLI



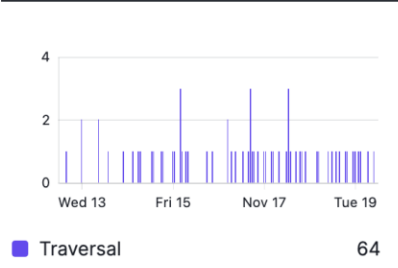
XSS



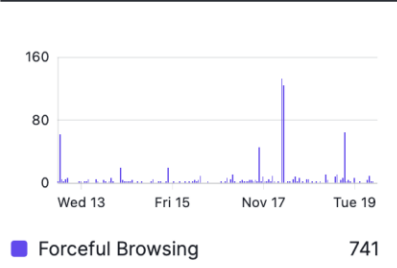
CMDEXE



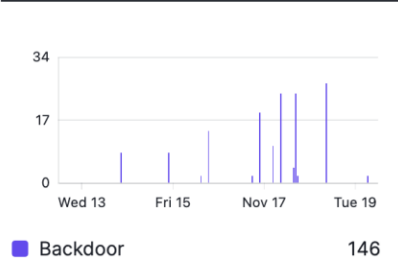
Traversal



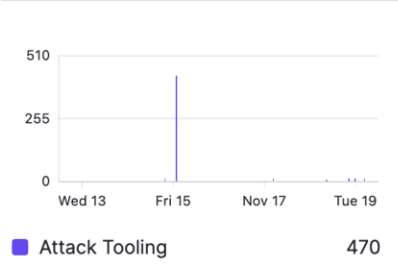
Forceful Browsing



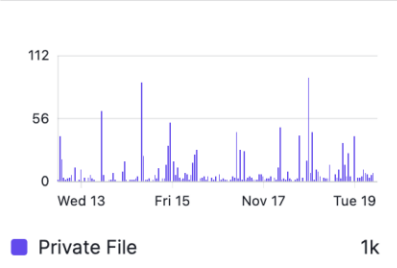
Backdoor



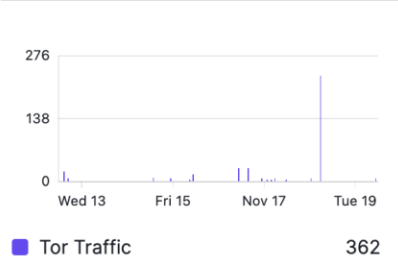
Attack Tooling



Private File



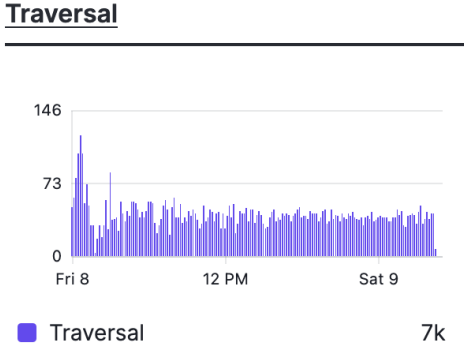
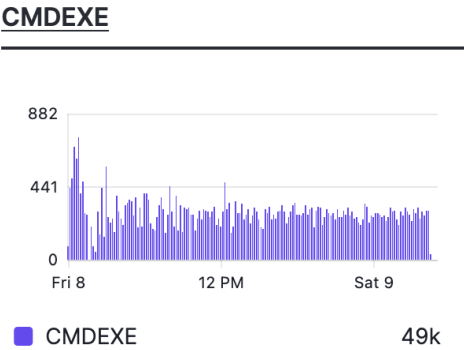
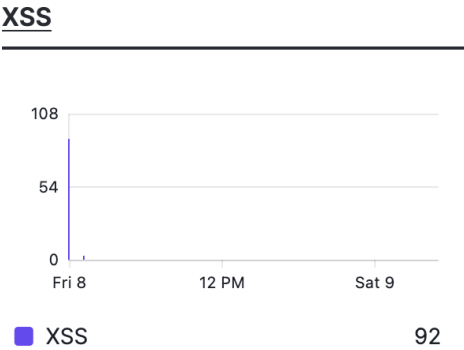
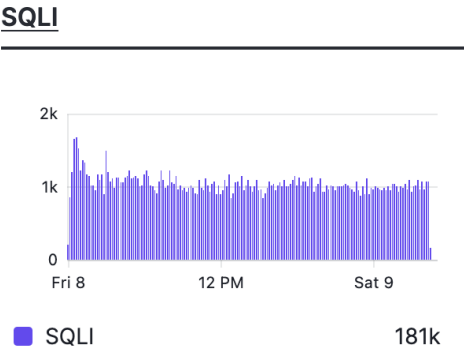
Tor Traffic



Attack Type (Signal) Tracking

Attack Types (Signal) :

SQLi : 181K CMDEXE : 49K Traversal : 7K XSS : 92



Next-Gen WAF Simulator

- Simulator offers expert support in debugging and testing rule creation
- Allows users to pass sample requests and responses and help identify whether user requests would be blocked or allowed as per current rule set
- Simulation output presents details of response code and triggered signals
- Benefits
 - Empowers users to create custom rules that fit the organization's needs confidently
 - Prevents misconfiguration and improves efficacy
 - Speeds up investigation and simplifies troubleshooting for quicker results

Sample Request

```
POST /?userId=117+or+1=1 HTTP/1.1
Host: sample.foo
Accept-Encoding: gzip, deflate
Accept-Language: en-us
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 10000
Cookie:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.6 Safari/605.1.15
Cache-Control: max-age=0
X-Forwarded-For: 127.0.0.1
X-Forwarded-Proto: https
```

Sample Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 21 Aug 2015 21:30:50 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 0
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
pragma: no-cache
x-frame-options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Request-ID: 123456789
```

Simulation Output

```
WAF Response: 406
Signals (4):
1. SQLI (Detector: LIBINJECTIONV5, Location: QUERYSTRING, Value: userId=117 or 1=1)
2. site.owasp-top-10 (Detector: 63c83d99d18c4601d4a63f19)
3. site.sqli (Detector: 63c84bfe53478f01d40f9151)
4. BLOCKED (Detector: 63c84bfe53478f01d40f9151, Value: 406)
```

Compliance – Industry Standard Certifications



Next-Gen WAF is PCI DSS compliant as a Level 1 service provider & fulfill PCI requirement 6.6



Next-Gen WAF is audited against the relevant sections of security and privacy rules of the HIPAA



Next-Gen WAF is audited against the trust services criteria for security, availability, and confidentiality as established by AICPA



Next-Gen WAF is audited against key articles of the GDPR, mapped to data protection and privacy controls

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

- One management plane for centralized policy enforcement and analytics/visibilities
- Doesn't require expert skills to operate

The logo for A10, featuring the letters 'A10' in a bold, white, sans-serif font. The background of the entire slide is a dark blue night cityscape with numerous skyscrapers and streets illuminated. Overlaid on the right side of the cityscape are numerous vertical lines of light in shades of blue and purple, each with small dots at the top, resembling data points or digital signals.

A10

Always Secure. Always Available.

Thank You