White Paper

Sense Defence™

WEB SECURITY WITH REAL INTELLIGENCE

Next generation self learning AI powered WAF

Sense Defence
Next Gen WAF

Intelligent
Bot Protection

Advanced
Rate Limiting

Application DDoS
Protection

Sense Defence
Hybrid WAF

Guaranteed
TLS Protection

10 Key Capabilities of Sense Defence Next-Gen WAF

Sense Defence is a powerful web application security technology that can provide modern software teams with advanced protection against the ever-evolving threats they face.

By providing greater control and visibility, enhanced threat detection capabilities and automated defence measures, it offers an effective solution for shielding applications from malicious attacks.

- Flexible Deployment Options for Any Architecture
- Installs Easily Behind Existing Edge Security Tools
- Safeguards Your Apps Without Destroying Them
- Identifies and Blocks Bots and Scrapers
- Helps Engineers to Fix the Right Things
- SSL is a Standard Feature for All
- Advanced AI-based DDoS Protection as a Standard
- Out-of-the-box Integration With External Tools
- Powerful Architecture to Ensure Performance and Speed
- Automated Blocking that Scales

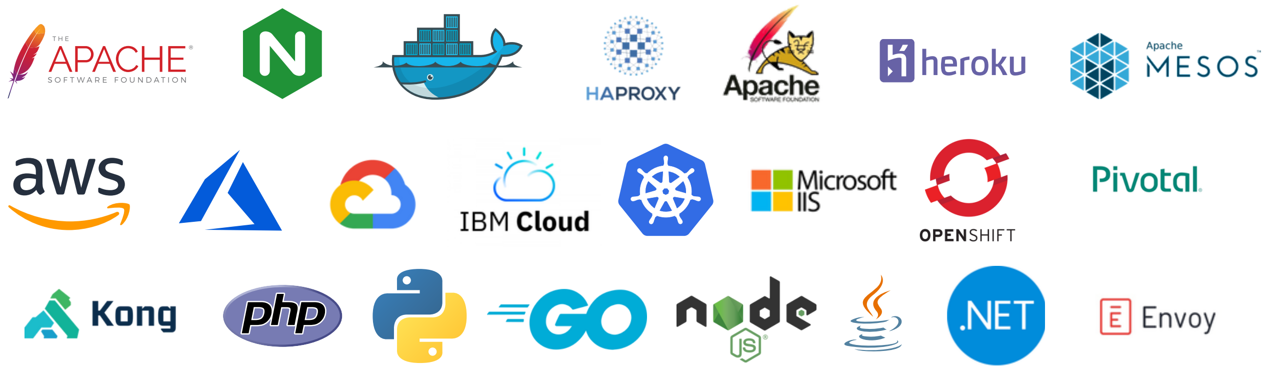
Flexible Deployment Options for Any Architecture

Applications are deployed everywhere by modern software teams, including in containers, on numerous and hybrid clouds, load-balanced across many CDNs, and everywhere in between.

With Sense Defence, you gain visibility and protection regardless of where your apps, APIs, and microservices are located and regardless of the language in which they are written, whether you use Amazon Web Services (AWS), Microsoft Azure, Google Cloud, a combination of these, or something entirely different.

Additionally, Sense Defence can function as a reverse proxy to safeguard legacy apps. Sense Defence is the cornerstone of a future-proof strategy that supports your architecture now as well as where and how you choose to run your apps in the future.

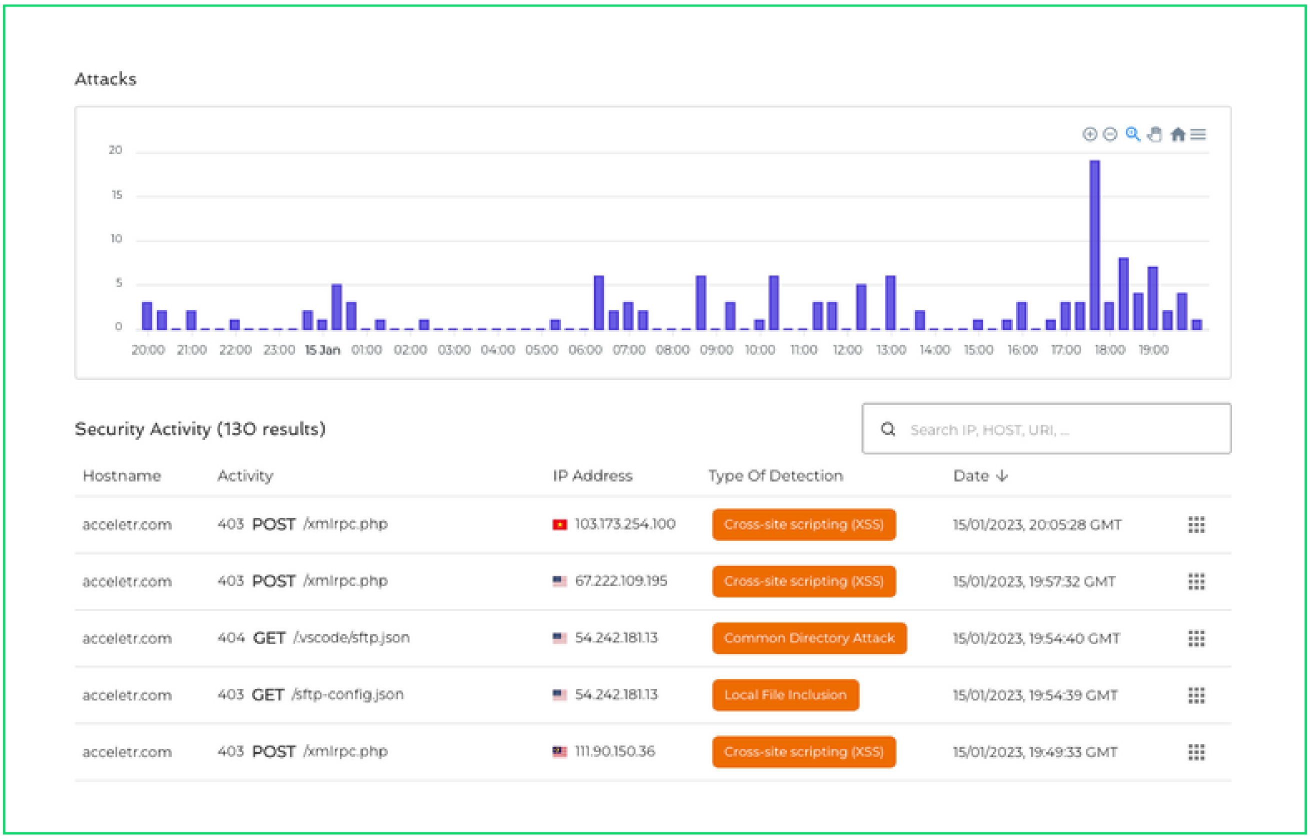
It offers the industry's greatest choice of installation options and a single control panel to monitor all of your apps.



Installs Easily Behind Existing Edge Security Tools

It's not unusual for your company to have invested much money in a CDN or appliance-based WAF. Many operations engineers believe that installing a WAF at the network edge makes sense because cached content is used to reduce the strain on web and application servers.

By identifying and thwarting particular attacks that these existing technologies are unable to, Sense Defence can be installed behind them to supplement current WAF deployments. You may instrument critical business logic processes using Sense Defence to inform you if an attempt is made to exploit them.



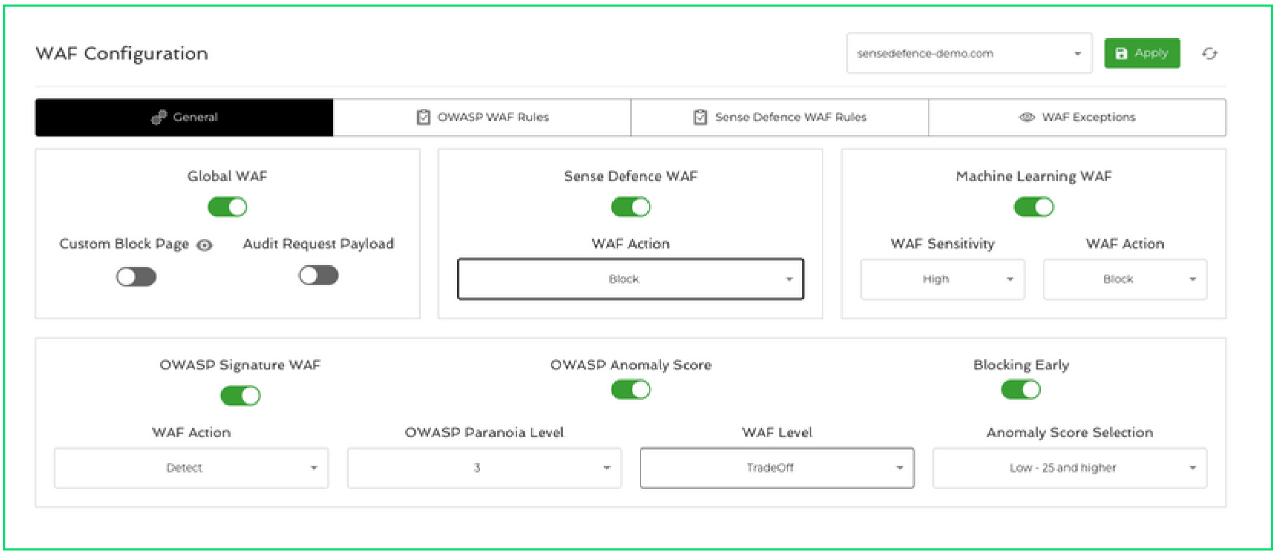
Security Activity (130 results)

Hostname	Activity	IP Address	Type Of Detection	Date ↓
acceletr.com	403 POST /xmlrpc.php	103.173.254.100	Cross-site scripting (XSS)	15/01/2023, 20:05:28 GMT
acceletr.com	403 POST /xmlrpc.php	67.222.109.195	Cross-site scripting (XSS)	15/01/2023, 19:57:32 GMT
acceletr.com	404 GET /.vscode/sftp.json	54.242.181.13	Common Directory Attack	15/01/2023, 19:54:40 GMT
acceletr.com	403 GET /sftp-config.json	54.242.181.13	Local File Inclusion	15/01/2023, 19:54:39 GMT
acceletr.com	403 POST /xmlrpc.php	111.90.150.36	Cross-site scripting (XSS)	15/01/2023, 19:49:33 GMT

Safeguards Your Apps Without Destroying Them

Sense Defence uses a threshold approach to blocking, allowing you to run our solution in full, automated blocking mode in production with virtually no false positives: 90 percent of our customers rely on us to do so.

Unlike other legacy WAFs products, threshold blocking does not make a decision on each request but instead examines suspicious payloads over time and with context to determine whether an actual attack is taking place.



WAF Configuration

sensedefence-demo.com

Global WAF: on
Custom Block Page: off
Audit Request Payload: off

Sense Defence WAF: on
WAF Action: Block

Machine Learning WAF: on
WAF Sensitivity: High
WAF Action: Block

OWASP Signature WAF: on
OWASP Anomaly Score: on
Blocking Early: on

WAF Action: Detect
OWASP Paranoia Level: 3
WAF Level: TradeOff
Anomaly Score Selection: Low - 25 and higher

Identifies and Blocks Bots and Scrapers

Automation and botnets are used by attackers to obtain valuable data, particularly from content-rich sites in the media, e-commerce, and technology industries. You can leverage Sense Defence AI to establish rate-limiting rules around an abusive activity like content scraping and remove providing material and resources to harmful users, potentially saving money on infrastructure costs.

You can prevent high-volume, malicious requests with rate-limiting rules activated without a single false positive. The same threshold-based strategy can be used to prevent harmful automated attacks via bots used to perform application DDoS and account takeovers.

Sense Defence bot management AI can detect and prevent bad bots and malicious bot traffic.

99% detection accuracy and less false positives

Behaviour Analysis for detections

Powerful AI algorithm to detect and block bots

Advanced finger printing to accurately classify bots

Rich Analytics and logs for better understanding

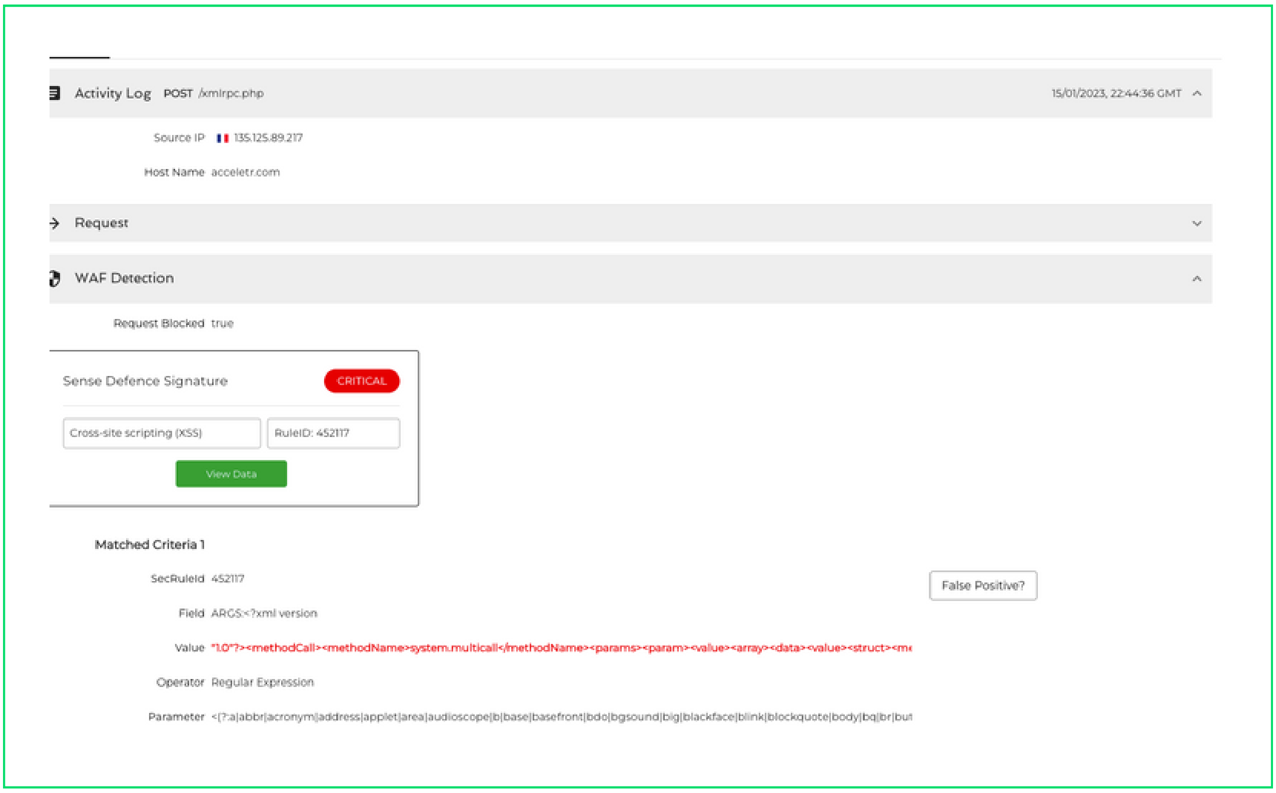
Out of the box module for Layer 7 DDoS prevention

Helps Engineers to Fix the Right Things

Sense Defence provides clear reports on the most common attack types and targets to help your teams focus on what exactly is under attack.

Engineering and security managers use this real-time data to best utilize their resources, including what types of training need to be reinforced depending on the attack tactics used against their apps and APIs in production.

Developers and security engineers are able to self-service data to get a better understanding of the bigger picture of attacks against their code.



POST /xmlrpc.php 15/01/2023, 22:44:36 GMT

Source IP 135.125.89.217

Host Name acceletr.com

Request Blocked true

Sense Defence Signature

Cross-site scripting (XSS) RuleID: 452117

Matched Criteria 1

SecRuleId 452117

Field ARGS:<?xml version

Value "1.0"?><methodCall><methodName>system.multicall</methodName><params><param><value><array><data><value><struct><m

Operator Regular Expression

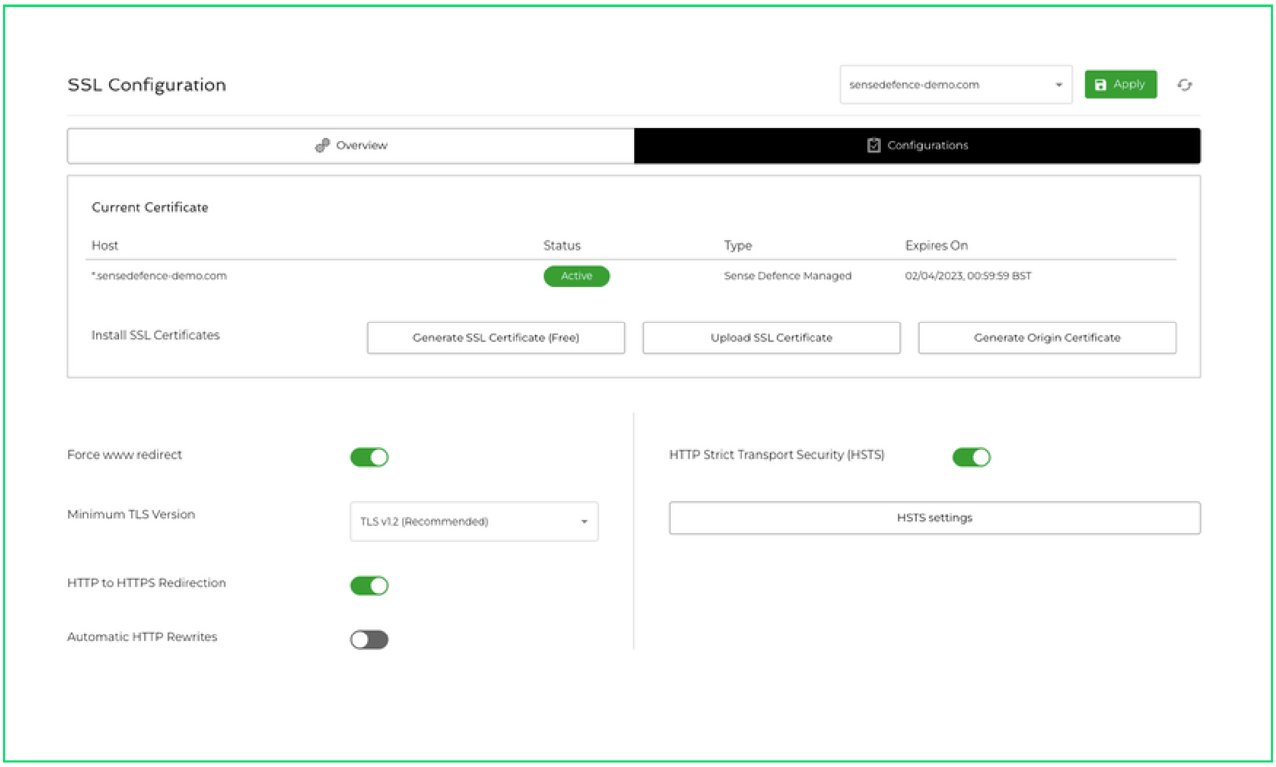
Parameter <(?:a|abbr|acronym|address|applet|area|audioscope|b|base|basefront|bdo|bgsound|big|blackface|blink|blockquote|body|bq|br|bu

SSL is a Standard Feature for All

Sense Defence provides SSL certificates FREE of cost for all the domains and subdomains onboarded to Sense Defence.

By default, all sites onboarded to Sense Defence are enabled with standard recommended security standards. There are no additional configurations needed to get an A+ rating in Qualys SSL labs

Sense Defence SSL certificates are managed certificates which are renewed automatically without any hassle.



SSL Configuration

Current Certificate

Host	Status	Type	Expires On
*.sensedefence-demo.com	Active	Sense Defence Managed	02/04/2023, 00:59:59 BST

Install SSL Certificates

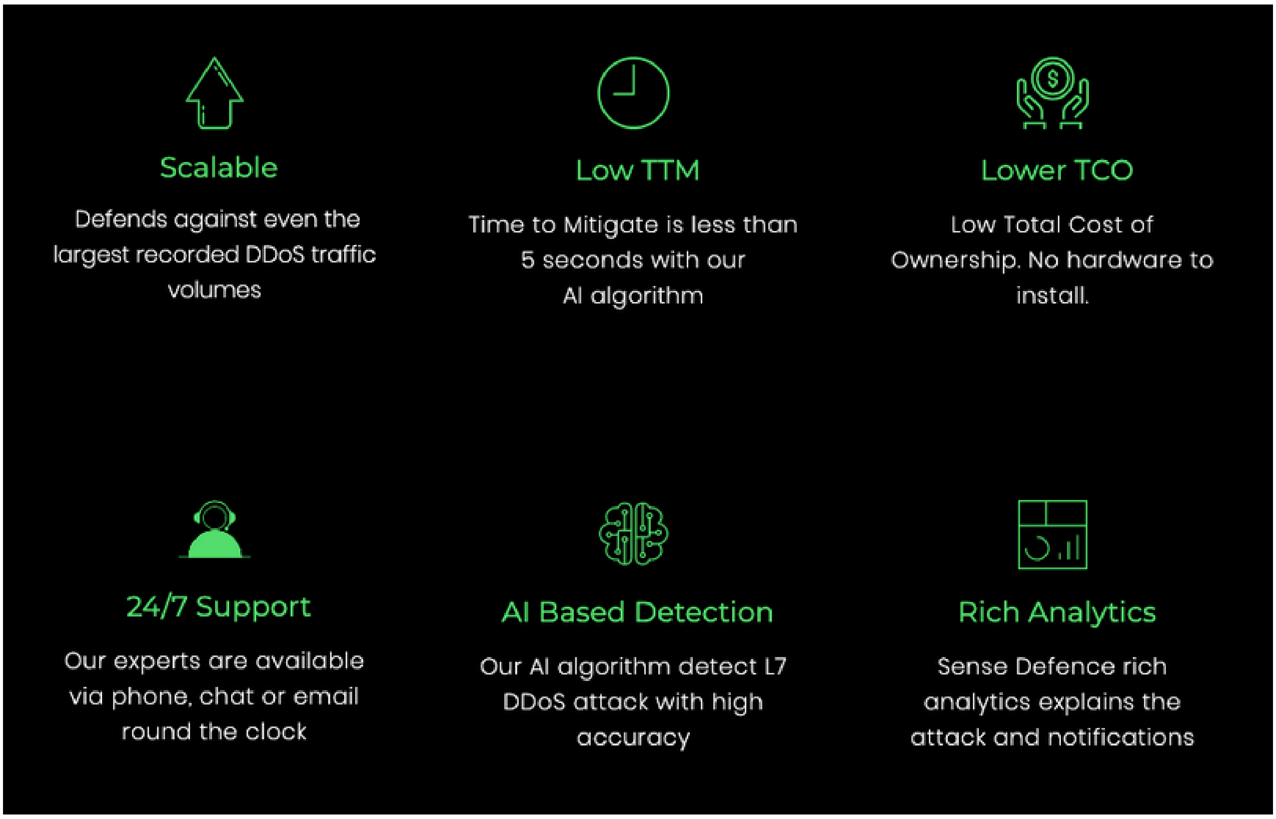
Force www redirect	●
Minimum TLS Version	TLS v1.2 (Recommended)
HTTP to HTTPS Redirection	●
Automatic HTTP Rewrites	○
HTTP Strict Transport Security (HSTS)	●

Advanced AI-based DDoS Protection as a Standard

Sense Defence Layer 7 DDoS protection offers a highly-scalable attack mitigation service that helps you tackle today's sophisticated and high-volume Layer 7 DDoS attacks.

It works across your enterprise environment to alleviate the burden on your network and perimeter systems, and helps maintain continued availability to your customers.

Sense Defence DDoS protection is scalable automatically based on the traffic volume. It will start the mitigation and clean the traffic, no matter what the attack volume is.



Scalable

Defends against even the largest recorded DDoS traffic volumes

Low TTM

Time to Mitigate is less than 5 seconds with our AI algorithm

Lower TCO

Low Total Cost of Ownership. No hardware to install.

24/7 Support

Our experts are available via phone, chat or email round the clock

AI Based Detection

Our AI algorithm detect L7 DDoS attack with high accuracy

Rich Analytics

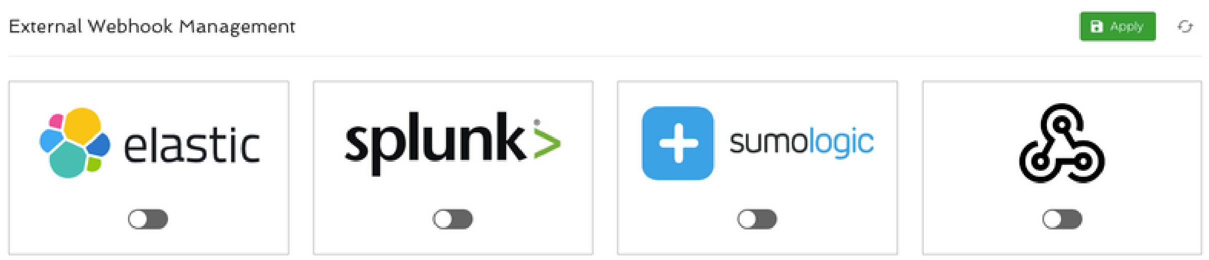
Sense Defence rich analytics explains the attack and notifications

Out-of-the-box Integration With External Tools

Security cannot be an afterthought. Aligning security, dev, and ops teams are crucial for all three groups to understand the requirements of security in the development lifecycle before issues arise that impact you and your bottom line.

Teams can easily create alerts when critical thresholds are triggered, sending messages through to the systems they use. Examples of how we enrich your current toolset include:

- **SIEM integration**s into Splunk, ArcSight, Sumo Logic, and others with fully documented REST/JSON APIs
- **Webhooks** to common DevOps tools like Slack, PagerDuty, Datadog, and Jira provide full event details of alerts

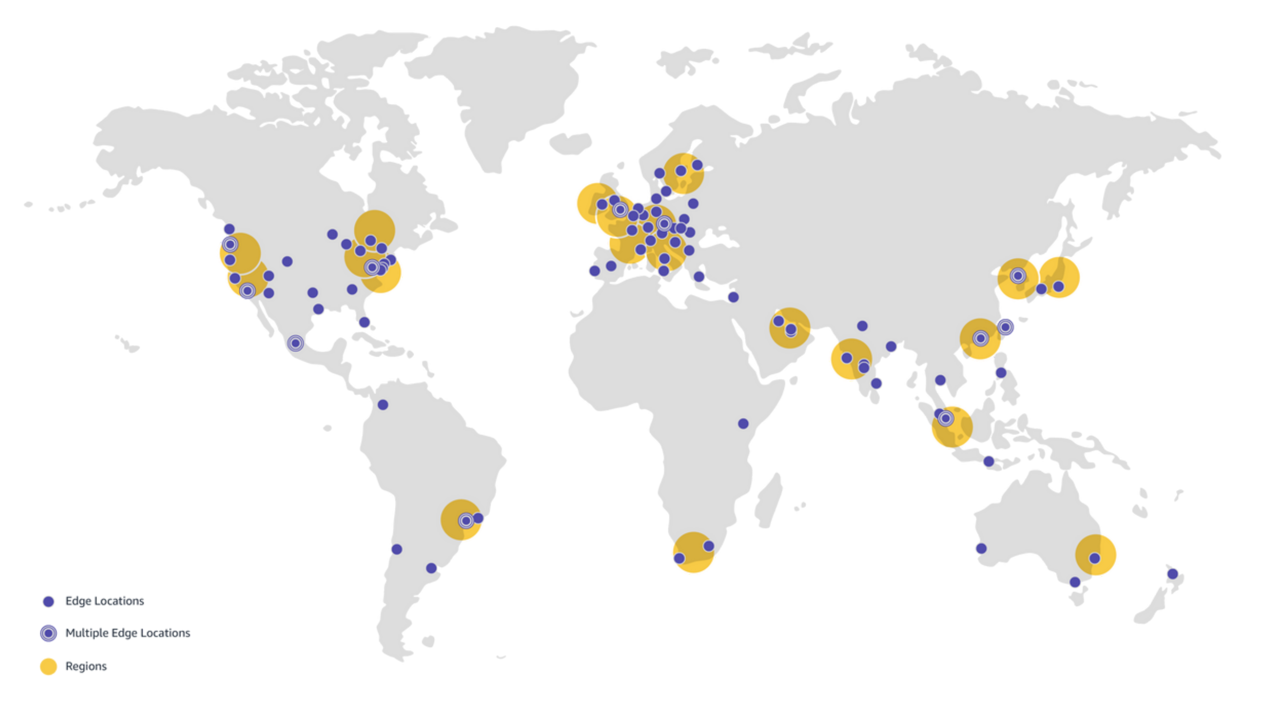

External Webhook Management

Powerful Architecture to Ensure Performance and Speed

Sense Defence leverages global edge network technology which uses AWS global network of 104 Points of Presence in 88 cities across 48 countries.

Sense Defence has a fault-isolating design that increases the availability of your applications. It uses the vast, congestion-free global network to route your web traffic to a healthy endpoint in the closest Region to the user.

Using this well-architected framework, Sense Defence speed up your application performance by 60%, along with providing high-class security.

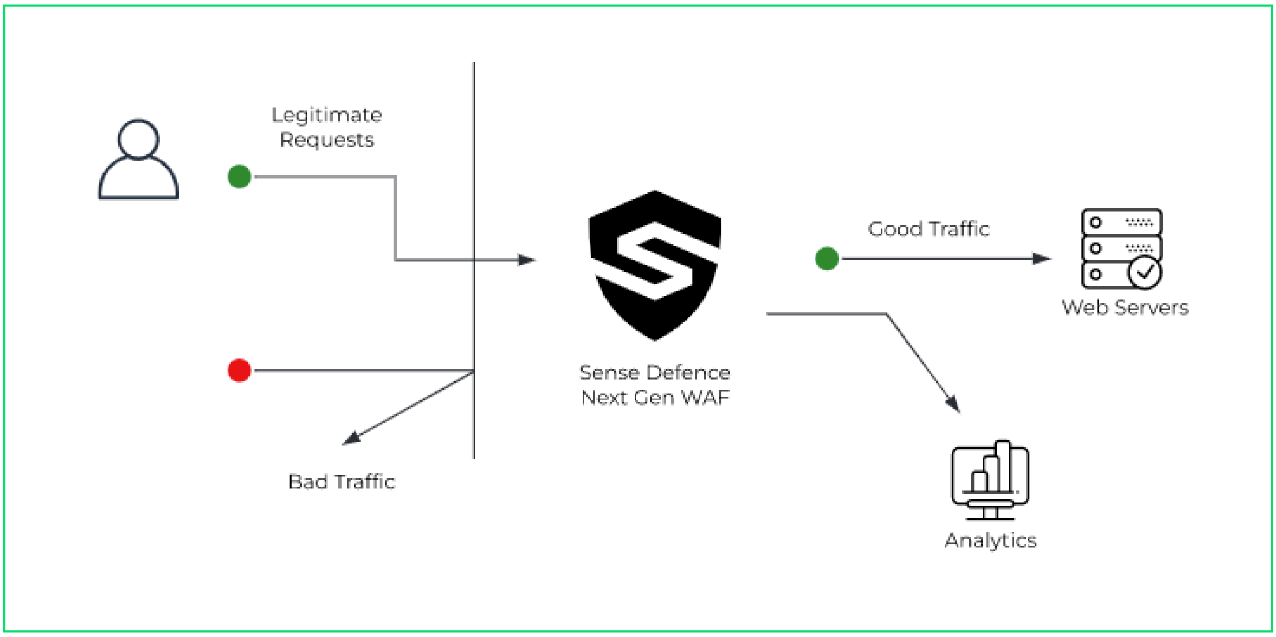


Automated Blocking that Scales

With legacy WAFs, which require learning mode and constant signature tuning to rule out false positives, the aggressiveness of blocking rules gets tuned down or completely turned off for fear of breaking the application.

Sense Defence AI algorithm is designed in a way that it can detect attacks from the moment it is onboarded without worrying about false positives.

You can scale protection without having to deal with the maintenance burden that legacy WAFs require thanks to our detection approach, which requires no tuning or configuration and virtually eliminates false positives.



Sense Defence™

Web Application Firewall

128 City Road
London, EC1V 2NX
United Kingdom

www.sensedefence.com

hello@sensedefence.com