WEB APPLICATION FIREWALL WITH REAL INTELLIGENCE

Sense Defence AI powered next generation Cloud WAF provides complete protection for web applications and APIs hosted in customer premises or in cloud.

10x

REDUCED COST

Sense Defence allows you to maximise your limited security resources by simplifying and automating crucial security actions, without expensive security hires.

80%

REDUCED WORKLOADS

Sense Defence WAF algorithm is designed and trained to reduce the number of false positives while detecting the true positives with 99% detection accuracy

15x

REDUCED DEPLOYMENT TIME

Sense Defence can be deployed rapidly and comes fully configured out of the box, providing exponential value from day one.

Sense Defence™

CAPABILITY BRIEF

Sense Defence Web Application Firewall is a comprehensive solution offering a full range of features to manage web application security at an individual and enterprise level. Web Applications are a prime target of cyber-attacks because they are readily accessible and offer an easy entry point to sensitive data. Organizations need to protect web applications from existing and emerging cyber-threats without affecting performance, time to market, or uptime. Rapid changes to applications can make it very difficult for security teams to keep up with updating rules that properly secure web assets

SENSE DEFENCE NEXT-GEN WEB APPLICATION FIREWALL

The Sense Defence WAF Gateway empowers organizations to protect their critical business web applications through automated web security and easy deployment. WAF Gateway provides complete protection and granular capabilities, making it the ideal solution to secure web assets, achieve compliance and provide enhanced protection against OWASP Top 10 security attacks.

Legitimate
Requests

Good Traffic

Sense Guard
Next Gen WAF

Web Servers

Bad Traffic

Analytics

CAPABILITY BRIEF
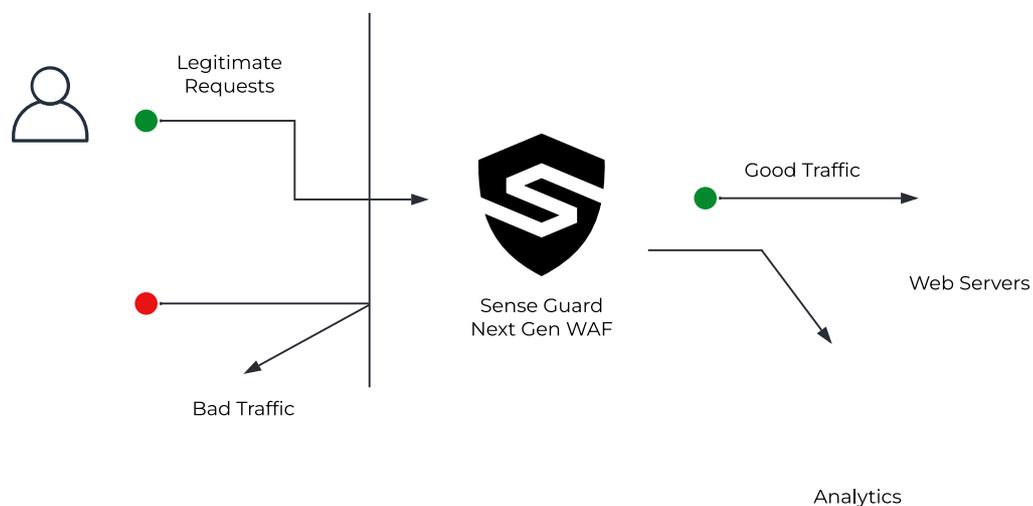
SENSE DEFENCE WAF CAPABILITIES

- Dynamic profiling learns protected applications and user behavior, automatically applying mitigations
- Flexible deployment to support hybrid environments (on-premises and cloud)
- Updates web defenses with research-driven intelligence on current threats
- Correlates security violations to detect sophisticated, multi-stage attacks
- Designed to protect critical business applications, including existing legacy applications and custom APIs from complex attacks while respecting data privacy requirements
- Proactive protection against known and unknown threats that can lead to data loss, sabotage, L7 denial of service (DoS) (Upcoming)
- Proven effective against OWASP Top 10 attacks
- Ability to sign, verify signature, encrypt, decrypt, modify any part or entity of request or response
- Standard security based on generic patterns and scoring mechanism complemented by advanced security engines for more granular and accurate detection
- Log replay for policy testing and forensics analysis
- Proactive bot detection and mitigation Upcoming release
- IP Geolocalization, IP Reputation
- Powerful log analysis allows drilling down to a specific security issue
- Competitive pricing with modules as compared to
- Rapid deployment, requires few minutes to deploy with no wait time on learning the datasets
- Low noise or lesser number of false positives comparatively
- Integration with SIEM tool and other generic web hook to receive WAF events in real time
- More adaptive to customer requirements when it comes to scalability and planning for future

CAPABILITY BRIEF

A different approach, for protecting web applications
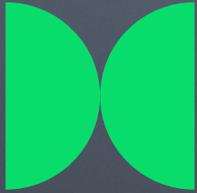
INTEGRITY

We build trust through
responsible actions and honest
relationships.

INNOVATION

We encourage thoughtful,
creative and inspirational
ideas.

ACCOUNTABILITY

Each of us is responsible for
our words, our actions, and our
results

Sense Defence™