Data Sheet

Managed Security Services

Web Application Firewall as-a-Service

Our **Web Application Firewall as-a-Service** provides the expertise and skills that ensure your web application firewall is configured to provide the highest level of protection for your websites.

Unattended firewalls won't stay standing for long; finding the time it takes to support them can seem impossible.

Dealing with malicious attacks to your system takes time and energy, both to handle and identify, especially when they arrive hidden amongst legitimate traffic. Poorly fortified systems are often overwhelmed by the traffic load, unable to distinguish between the two forms in a timely fashion and consequently resulting in slow connectivity for your end users.

This is just the front end of the problem; behind the scenes, badly maintained firewalls will have trouble mitigating bot attacks and have great difficulty operating in the new hybrid/multi-cloud environment. A busy IT support team may not have the time for thorough incident diagnosis, and few solutions on the market today offer truly 'granular' control of a security solution.

Our Web Application Firewall as a Service (WAFaaS) is specially designed to handle these problems. A worldwide managed service supporting your online business requirements, WAFaaS provides a comprehensive solution to the broad range of issues inherent to managing a complex security network, including:

- Web security – threat detection and prevention (vendor native)
- Denial of service for web and network-based attacks

Our Web Application Firewall as-a-Service provides:

- Detection of based on our advanced analytics, threat intelligence and incident validation and remediation recommendations by skilled security analysts
- Distributed Denial of Service (DDoS) attack protection against website, infrastructure, single IP address, and name server through web-based cloud services.
- Content Delivery Network (CDN) and optimizer services, benefiting web servers with a 40-70% reduction in bandwidth consumption, and a 50% acceleration in website browsing.
- Load balancing and failover from the cloud, supporting your application/ server availability deployed in hybrid cloud environments.
- Management and maintenance by experienced security engineers in NTT's Security Operations Center (SOC), supplemented by highly-trained security experts as an extension of your own in-house IT team.
- High level of network access and information availability, integrity, and privacy.
- Detailed real-time and historical views of the performance, security, configuration and availability of all websites, name servers and traffic managed by the service.

Service level	Client benefits
Standard	• Safeguarding with visibility of all activity across your web servers • Better protection of information assets Access to our SOCs for 24x7 support and engineering • PCI DSS compliance reporting • Enhanced risk management through effective incident management
Enhanced	• Security incident detection with advanced analytics • NTT Ltd. Threat Intelligence • Threat hunting by Security analyst Security incident reports with remediation recommendations • Business and regulatory compliance reporting

Standard WAFaaS

NTT Ltd. provides expertise to ensure that your WAF is configured to provide maximum protection of your websites using the native features of the WAF. Notifications are sent to you directly from the WAF via email. All WAF related reporting is available in the WAF Portal.

Service management tickets, including service requests, change requests and incidents are available in our Manage Center. The WAF Portal is available directly from our Manage Center via single sign on.

A weekly report of summary activity will be provided, along with access to the WAF as a Service portal that includes access to 90 days of events. You will have the ability to generate a PCI report or define a schedule to email (weekly, monthly, quarterly).

Enhanced WAFaaS

The Enhanced WAFaaS variant is specially designed for those users who require cyber-attack detection, customization of alerts and correlation with our other services.

Logs and events generated by the WAF are further processed; our service uses customized rules and an anomaly-based detection and compliance profile to identify and report on the following categories of security incidents:

- **Cyber threat detection** - Advanced analytics based on machine learning, behaviour and kill chain modelling power by our threat intelligence. Identified threats gets investigated by skilled security analyst that perform event driven threat hunting. Notification with remediation recommendations of the validated security incidents.
- **Security best practices** – Events that indicate a deviation from a predefined baseline of our definition of security best practices.
- **Business policy compliance** – Events that indicate a deviation from a predefined baseline of an organization's custom business policy compliance requirements.

To ensure service quality, **we continuously fine-tune detection decisions** based on the validity and relevance of service-generated events and incidents.

Features of our Standard and Enhanced WAFaaS

WAFaaS capabilities	Standard	Enhanced
Management of WAF policies	✓	✓
DDoS for infrastructure	✓	✓
PCI DSS reporting	✓	✓
Automated notifications threats/load/alerts/infrastructure status	✓	✓
Detection of cyber-attacks validated by security analyst		✓
Security best practice and regulatory compliance reporting		✓
Custom business compliance reporting		✓
DDoS protection for websites, DNS, single IP	Optional	Optional
SIEM integration, attack analysis, dedicated network, load balancing	Optional	Optional