



Client Service Description

Web Application Firewall as a Service

05 March 2020 | Document Version 1.2



Client Service Description

Web Application Firewall as a Service

NTT Contact Details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Bob Gordon – Services Product Portfolio Director, Security

Phone: +1 203 446 4942

NTT Limited

✉ bob.gordon@global.ntt

Confidentiality

This document contains confidential and proprietary information of NTT Limited ('NTT'). {ClientFull} ('{Client}') may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that {Client} may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of {Client}'s evaluation of the document. {Client} agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as {Client}. As a condition of receiving this document, {Client} agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

This document is valid until October 1, 2021 and, in the absence of any other written agreement between the parties, NTT and {Client} acknowledge and agree is subject to NTT's standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by {Client}. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.





Client Service Description

Web Application Firewall as a Service

Document Preparation

	Name	Title	Date
Prepared:	Tore Terjesen	Director Service Integration	18 Feb 2020
Reviewed:	Bob Gordon	Services Product Portfolio Director	05 Mar 2020

Release

Version	Date Released	Pages	Remarks
V1.0	06 Mar 2020		Internal Region Review
v/1.1	27 Mar 2020		Updating based on region feedback
V1.2	20 Nov 2020		Added SLA

© 2021 NTT Pty Limited. The material contained in this document, including all attachments, is the copyright of NTT Pty Limited. No part may be reproduced, used or distributed for any purpose, without the prior written consent of NTT Pty Limited. This document, including all attachments, is confidential and use, reproduction or distribution of this document or any part of it for any purpose, other than for the purpose for which it is issued, is strictly prohibited.

This document is only a general description of the available Services. The Services to be supplied are subject to change. For each Client, the Services will be as set out in the contract entered into by the Client and NTT. If there is any conflict between this document and the contract, the contract will prevail.



Client Service Description

Web Application Firewall as a Service

Table of Contents

NTT Contact Details	2
Confidentiality	2
Terms and conditions	2
Document Preparation	3
Release	3
1. Service Description	7
1.1. Overview	7
1.2. Standard Service Variant	7
1.3. Enhanced Service Variant	8
1.4. Benefits.....	9
1.5. Service Matrix.....	10
1.6. NTT’s Managed Security Services Portfolio.....	11
2. Core Service Feature Descriptions	13
2.1. Hours of Operation.....	13
2.2. Security Operations Centres (SOCs).....	13
2.3. Client Portals	13
2.3.1 NTT’s Manage Center Portal	13
2.3.2 Imperva’s WAF as a Service Console	13
2.4. Language Support	14
2.5. Management Options	14
2.5.1 Standard Management (Default)	14
2.5.2 Co-Management.....	14
3. WAF as a Service – Service Features	16
3.1. Standard Service Variant	16
3.1.1 Policy Management	16
3.1.2 Client Notification	16
3.1.3 Portal and Reporting	17
3.2. Enhanced Service Variant	17
3.2.1 Compliance Monitoring Features in Enhanced	17
3.2.2 Cyber Threat Detection Features in Enhanced	18
3.2.3 Client Notification	18



Client Service Description

Web Application Firewall as a Service

3.2.4	Portal and Reporting	19
3.3.	Web Application Security Service Features	19
3.3.1	Web Application Firewall (WAF)	19
3.3.2	WAF Policies	19
3.3.3	Custom Rules	20
3.3.4	Security Policies	20
3.3.5	SSL Support	21
3.3.6	Login Protect (Two Factor Authentication)	21
3.3.7	Content Delivery Network (CDN)	22
3.3.8	Advanced Analytics (Enhanced)	23
3.3.9	Threat Intelligence (Enhanced)	23
3.3.10	Detailed Security Incident Investigation by Security Analyst (Enhanced)	24
3.3.10.1	Event-driven Threat Hunting	25
3.3.10.2	Security Incident Reports Based on Detailed Investigation and Threat Hunting	25
3.3.10.3	Threat Severity	27
3.3.11	Compliance Monitoring (Enhanced)	28
3.4.	Infrastructure DDoS Protection	29
3.4.1	Prerequisites for Infrastructure DDoS Protection	30
3.5.	Service Options	30
3.5.1	Website DDoS Protection (Unlimited)	30
3.5.2	DNS DDoS Protection	30
3.5.3	Single IP DDoS Protection	31
3.5.4	Infrastructure Monitoring	31
3.5.5	SIEM / Log Integration	31
3.5.6	Attack Analytics	32
3.5.7	Dedicated Network	32
3.5.8	Load Balancing and Failover	33
3.5.9	Investigator – Enriched and Aggregated Log Search (Option)	33
3.5.10	Secure Long-Term Log Storage (SLTLS) (Option)	35
3.5.11	Vulnerability Correlation (Option)	36
4.	NTT’s Approach to Service Operations	37
4.1.	Service Experience	37
4.2.	Service Desk	37
4.2.1	NTT’s Manage Portal	37
4.2.2	Online Dashboards and Charts	38



Client Service Description

Web Application Firewall as a Service

- 5. Service Management 40**
- 5.1. Service Level Management40**
- 5.1.1 NTT Service Delivery Manager (SDM)40
- 5.1.2 MSS Technical Account Manager40
- 6. Our Approach to Service Transition 42**
- 6.1. Objectives of Service Transition42**
- 6.2. Transition Methodology42**
- Appendix A Service Level Agreement 43**
- Appendix B WAFaaS Policy Management MACD 46**

List of Figures

- Figure 1 – Global Managed Security Service Platform..... 12
- Figure 2 – Continuous Threat Intelligence Updates 24
- Figure 3 – Security incident investigation life-cycle 24
- Figure 4 - Example Security Incident Report..... 27
- Figure 5 – Threat severity classification using MITRE ATT&CK matrix..... 28
- Figure 6 – Investigator 34
- Figure 7 – Investigator Log Searches..... 35
- Figure 8 – Investigator Search Filtering..... 35

List of Tables

- Table 1 – Service Matrix for Web Application Firewall as a Service (WAF as a Service) 11
- Table 4 – Threat Severity Levels 27



Client Service Description

Web Application Firewall as a Service

Service Description

1.1. Overview

Keeping web applications secure and meeting compliance requirements is a challenge that requires the right set of people, processes and technology. Our Web Application Firewall (WAF) as a Service, based on Imperva's market leading Web Application Firewall, protects your applications in the cloud and on-premise.

Depending on your needs, resources and in-house capabilities, we offer tailored service packages that varies from policy management to compliance monitoring and all the way to cyber threat detection with Security Analyst investigation and validation.

While the Web Application Firewall protects your business critical web applications, the rest of the IT infrastructure and other online business critical applications are still subject to denial of service attacks. We offer Infrastructure DDoS protection of entire subnets or single IP addresses based on Imperva's global Infrastructure DDoS protection services.

Both Web Application Firewall and Infrastructure DDoS are truly global cloud based services without the need for additional infrastructure overlays.

The Service contains two independent service features that can be selected separately or together:

- Web Application Security
- Infrastructure DDoS Protection

The service features are available in packages called service variants. Only one service variant may be selected and will apply to all service features.

- **Standard** (Co-Management option available)
- **Enhanced** (Co-Management option available)

Co-Management is useful for clients with in-house skilled WAF or DDoS resources who are available during business hours and are comfortable with making changes themselves. In a Co-Management setup, you are allowed to make changes to the policies, configuration, view data and statistics. In the default management setup of the Standard and Enhanced service variants, you are provided with read only access and changes are performed by NTT after a change request has been raised by you.

1.2. Standard Service Variant

In the Standard service variant you leverage the selected Imperva features for protection of your web applications and infrastructure, while we provide Service Transition and policy management. We offer expertise, ensuring that the service features are configured to provide maximum protection of your websites and other critical infrastructure.



Client Service Description

Web Application Firewall as a Service

Service management tickets, including service requests, change requests and incidents are available in NTT's Manage Center Portal, which is the main entry point to the Service. From Manage Centre you can access Imperva's WAF as a Service Console via single sign on for information on security, performance, statistics and traffic.

In the Standard service variant we do not ingest event notifications from Imperva into our ticketing system or any logs for compliance monitoring or cyber threat detection. These features are only available in the Enhanced service variant. That implies that in the Standard service variant, any notifications (set up during Service Transition or through change management) are sent to you directly from the Imperva WAF as a Service Console via email.

If you require additional capabilities beyond the native Imperva features, such as detection of new and emerging web application threats or customized compliance monitoring you must subscribe to the Enhanced service variant.

The Standard service variant provides:

- 24/7 Security Operations Centre (SOC) coverage
- Policy management and maintenance by experienced security engineers in NTT's SOCs, supplemented by highly trained security experts as an extension of your own in-house IT team
- Protection of critical online assets including networks, applications, individual IPs and DNS infrastructure - anywhere in the world, on premise or in the cloud (requires purchase of relevant protection licenses)
- Load balancing and failover from the cloud, supporting your application/server availability deployed in hybrid cloud environments (requires purchase of relevant load balancing licenses)
- Detailed real-time and historical views of the performance, security, configuration and availability of all websites, name servers and traffic managed by the Service
- PCI-DSS compliance reporting

1.3. Enhanced Service Variant

The Enhanced service variant includes all the NTT and Imperva service features available in Standard, with the addition of our cyber threat detection and compliance monitoring capabilities - effectively reducing the noise, improving detection of web application threats and enabling customized compliance monitoring.

In order to deliver cyber threat detection and compliance monitoring, event notifications and logs are collected by NTT from Imperva for further processing and validation. Data is collected from Imperva's cloud into NTT's cloud infrastructure without the need for any additional virtual or physical infrastructure components.

Cyber threat detection is delivered by analyzing WAF logs using NTT Advanced Analytics and Threat Intelligence supported by Security Analyst investigation, threat



Client Service Description

Web Application Firewall as a Service

hunting, and validation, resulting in detection of new and emerging threats against your web applications and removal of nearly all false positives as you are only notified of validated security incidents.

The Enhanced service variant also includes additional compliance monitoring and reporting compared to Standard. While both service variants include native PCI reporting from Imperva, the Enhanced service variant provides extended compliance capabilities with the ability to customize business policy compliance rules and event notifications.

The Enhanced service variant also provides additional options for raw log storage, enriched and aggregated log search, and correlation with Qualys vulnerability data (requires purchase of NTT's Vulnerability Management Service).

The Enhanced service variant provides (in addition to Standard):

- Cyber threat detection enhanced by NTT Threat Intelligence
- Advanced Analytics with proprietary machine learning and behavioral modelling
- Security Analyst event driven threat hunting, investigation and validation of cyber threats
- Validated cyber threat detection Security Incident Reports
- Custom business policy compliance use cases and notifications
- Raw log storage (option)
- Extended log viewer for enriched and aggregated log search (option)
- Correlation with Qualys vulnerability data (require NTT's Vulnerability Management Service)

1.4. Benefits

The benefits of Web Application Firewall as a Service include:

- Safeguarding your business by gaining complete visibility into activity across your web servers wherever they are deployed
- Better protection of information assets to minimize any impact on business operations and reduce overall security risk
- Enhanced risk management through effective incident management, incident escalation and rapid response to outbreaks by Security Engineers and Security Analysts using advanced SOC toolsets
- Access to NTT's SOCs for 24/7 engineering and incident lifecycle support
- Improved ability to meet compliance requirements and pass audits
- Content Delivery Network (CDN) and Content Optimization services, benefitting web servers with a 40-70% reduction in bandwidth consumption, and a 50% acceleration in website browsing



Client Service Description

Web Application Firewall as a Service

1.5. Service Matrix

Web Application Security and Infrastructure DDoS Protection are available in tailored service packages called service variants. The selected service variant and options are formalized in a Record of Entitlement that forms part of your Managed Services Agreement.

Service Features	Service Variant	
	Standard	Enhanced
Core Service Features		
<ul style="list-style-type: none"> Hours of Operation (24x7) Security Operations Centres (SOCs) Client Portals Language Support Management Options 	✓	✓
WAFaaS Service Features		
<ul style="list-style-type: none"> Policy Management 	✓	✓
<ul style="list-style-type: none"> Cyber Threat Detection Compliance Monitoring 		✓
Client Notifications		
Automated Imperva Threat Event Notifications (email)	✓	✓
Infrastructure DDoS Notifications (email, text, phone)	✓	✓
NTT Analyst-created Security Incident Reports based on Detailed Investigation and Threat Hunting		✓
NTT Automated Compliance Monitoring Notifications		✓
Web Application Security		
Web Application Firewall	✓	✓
WAF Policies	✓	✓
Custom Rules	✓	✓
Security Policies	✓	✓
SSL Support	✓	✓
Two-factor Authentication (Login Protect)	✓	✓
Content Delivery Network (CDN)	✓	✓
NTT Advanced Analytics		✓
NTT Threat Intelligence		✓



Client Service Description

Web Application Firewall as a Service

Service Features	Service Variant	
	Standard	Enhanced
NTT Detailed Security Incident Investigation by Security Analyst		✓
Infrastructure DDoS Protection		
Always-on	✓	✓
On-Demand	✓	✓
Service Options		
Website DDoS Protection <ul style="list-style-type: none"> Website DDoS Protection (upgrade to unlimited) DNS DDoS Protection Single IP DDoS Protection 	✓	✓
SIEM / Log Integration	✓	✓ ¹
Attack Analytics	✓	✓
Dedicated Network	✓	✓
Load Balancing and Failover	✓	✓
Investigator – Enriched and Aggregated Log Search (Option)		✓
Secure Long-Term Log Storage (Option)		✓
Vulnerability Correlation (Option)		✓
Service Transition		
Client Transition	✓	✓
Service Management		
Service Level Management	✓	✓
Service Desk	✓	✓
Service Delivery Manager (SDM)	✓	✓
MSS Technical Account Manager (Option)	✓	✓

Table 1 – Service Matrix for Web Application Firewall as a Service (WAF as a Service)

1.6. NTT's Managed Security Services Portfolio

The NTT portfolio of Managed Security Services (MSS) helps reduce the burden of constant and proactive network monitoring, advanced security analysis, and global

¹ Pre-requisite for the Enhanced service variant



Client Service Description

Web Application Firewall as a Service

intelligence correlation. All of NTT's Managed Security Service offerings are powered by the NTT Global Managed Security Service Platform (GMSSP), combined with our proven combination of people, process and technology.



Figure 1 – Global Managed Security Service Platform

The MSS portfolio consists of:

- **Threat Detection Services.** The Threat Detection Services includes Standard and Enhanced service variants for advanced detection, investigation, and reporting of security incidents.
- **Enterprise Security Monitoring.** The Enterprise Security Monitoring Services includes Standard and Enhanced service variants for security monitoring of regulatory compliance, security best practices and business policy compliance.
- **Security Device Management Services.** The Security Device Management Services include Standard and Enhanced service variants for management of a broad range of security technologies.
- **Vulnerability Management.** The Vulnerability Management Services deliver customized vulnerability scanning with a variety of compliance and reporting options.
- **Web Application Firewall as a Service.** The Web Application Firewall as a Service protects web applications against cyber threats and network and infrastructure against denial of service attacks.



Client Service Description

Web Application Firewall as a Service

Core Service Feature Descriptions

2.1. Hours of Operation

WAF as a Service is delivered through NTT's Security Operation Centres, which operate 24 hours a day, 7 days a week.

2.2. Security Operations Centres (SOCs)

We will deliver the WAF as a Service from any of our SOCs, at our sole discretion. Your data may be stored in any of the SOCs and on NTT's global infrastructure unless there is prior agreement and approval between NTT and you.

You will be provided with the contact details of the relevant SOC during Service Transition.

2.3. Client Portals

You will have access to the following web-portals:

- NTT's Manage Center Portal
- Imperva's WAF as a Service Console

In the Standard Management (default) set up, all user lists and rights are owned and managed by NTT for all portals. See *2.3.2 Imperva's WAF as a Service Console* and *2.5 Management Options* for more information on Imperva's WAF as a Service Console and Standard Management vs. Co-Management.

2.3.1 NTT's Manage Center Portal

NTT's Manage Centre is a globally available, web-based application which allows you to interact with, manage, and monitor the Managed Security Service.

2.3.2 Imperva's WAF as a Service Console

This portal is only available for NTT's WAF as a Service clients.

The Imperva WAF as a Service Console is a globally available, web-based application which provides specific management, reporting and role-based access for the Service configuration and features for Web Application Security and Infrastructure DDoS Protection, including:

- traffic
- security
- performance
- real-time statistics

We configure the Imperva WAF as a Service Console for you with all relevant Service information.

An account is created for the nominated Service Administrator verified by you.



Client Service Description

Web Application Firewall as a Service

You can be assigned administrative or reviewer entitlements based on your Management Service deployment (Standard Management or Co-Management option).

In the Standard Management (default) set up, you will be assigned a reviewer role (read-only).

In a Co-Management set up, you can be assigned specific permissions to configure and manage the policy of the Service through Imperva's WAF as a Service Console.

In a Co-Management set up, specific conditions apply. For more information refer to 2.5.2 Co-Management.

2.4. Language Support

WAF as a Service is provided in English only, unless there is prior agreement and approval between NTT and the Client.

2.5. Management Options

NTT offers two types of management for the Service configurations:

- Standard Management (default)
- Co-Management²

The type of management is selected by you during Service Transition.

2.5.1 Standard Management (Default)

We maintain all configuration items in the Service.

You will be provided with up to three (3) read-only accounts to access configuration items within scope.

If you expect more read only accounts, we will create a read-only account via move, add, change, and delete (MACD) consumption.

We will create one administrator account for you and will securely store the credentials. In the event of an emergency where we are unable to make a change or access the configuration items/management infrastructure, your nominated Service Administrator will be provided with the credentials and password.

Each time you use the administrative account, we will reset the account with a new password.

2.5.2 Co-Management

Co-Management is available on request at no charge. NTT and the Client and/or its nominated third party and/or an NTT Group Operating Company have access to the

² Excludes Infrastructure DDoS Protection



Client Service Description

Web Application Firewall as a Service

in-scope configuration items with the ability to make updates and configuration item changes.

In a Co-Management set up, you can be assigned a role in Imperva's WAF as a Service Console and may configure and manage Web Application Security policies, configuration, view data and statistics.

You will not be granted access to any configuration item that is not already included in the Record of Entitlement / contracted scope.

Co-Management means that you are responsible for maintaining user accounts and rights in Imperva's WAF as a Service Console. For more information, refer to 2.3 *Client Portals*.

Note: The Management options must be selected during the Service Transition "Planning" phase. You cannot change this selection after the Service "Staging" phase is complete.

You acknowledge only appropriately trained and certified WAF engineers will be granted administrative account rights to perform changes in a co-managed environment.

For the Co-Management option, specific conditions and responsibilities apply as outlined below:

1. Co-Management is only available as an option when you have an appropriately trained, skilled, and certified WAF engineer.
2. WAF configuration and policy changes can only be made by the specific Client engineer, outlined within the Transition Workbook or added by raising a service request via NTT's Manage Center Portal.
3. For us to provide effective support, you must:
 - a. notify us at least 48 hours in advance of scheduling and scope of changes being made to avoid "lost transaction" or collision of change work;
 - b. record all changes to be made via a Request for Change within NTT's Manage Center Portal; and
 - c. if applicable and upon completion, provide a report/status update from your internal change management process to ensure we are aware of all the changes occurring to the configuration items.

You accept any exceptions that may arise due to a deviation from, or circumvention of, the processes described which may result in an unstable configuration(s) and Service. Accordingly, you release NTT from any liability resulting from outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to changes implemented directly by you.

The Co-Management option is not available for Infrastructure DDoS Protection.



Client Service Description

Web Application Firewall as a Service

WAF as a Service – Service Features

The following service features are available in the WAF as a Service:

Service Variant	Web Application Security	Infrastructure DDoS Protection
<ul style="list-style-type: none"> Standard Enhanced 	<ul style="list-style-type: none"> Web Application Firewall (WAF) WAF policies Custom Rules Security Policies SSL support Two factor authentication Content Delivery Network (CDN) NTT Advanced Analytics NTT Global Threat Intelligence Security Analyst Investigation 	<ul style="list-style-type: none"> Always-on On-demand
NTT's Manage Centre Portal and Imperva's WAF as a Service Console		

Table 2 – Service Matrix for Web Application Firewall as a Service (WAF as a Service)

Selection of a service variant is mandatory and applies to all selected service features and options.

Web Application Security and Infrastructure DDoS Protection can be purchased separately or together.

3.1. Standard Service Variant

The Standard service variant is best suited to clients who do not require additional threat detection capabilities or customization of compliance events than what is supported natively in the WAF. For more information about the native WAF functionality refer to *3.3 Web Application Security Service Features*.

The compliance and threat related security events generated by the WAF and Infrastructure DDoS Protection service features are not further processed by NTT.

3.1.1 Policy Management

We manage the policies and configurations of the Web Application Firewall and Infrastructure DDoS Protection service features and options.

3.1.2 Client Notification

You are notified directly from Imperva's WAF as a Service Console via the e-mail address defined in the Transition Workbook.

- Automated Imperva Threat Event Notifications (email)
- Infrastructure DDoS Notifications (email, text, phone)



Client Service Description

Web Application Firewall as a Service

You may elect to receive automated email notifications from the following categories:

- **Website threats:** receive notifications about threats that were detected on your site, such as Layer 7 (application layer) DDoS and backdoor threats. Security events are aggregated, and a notification email is sent at 5-minute intervals
- **Load balancing alerts:** receive notifications when the failure scenarios for load balancing are met
- **Infrastructure DDoS alerts:** receive notifications for the start and end of DDoS attacks against your protected networks

3.1.3 Portal and Reporting

- You will have access to Imperva's WAF as a Service Console that includes access to the last 90 days of traffic, security, performance, and activity log
- You will be able to receive a predefined PCI report on changes to your security rule configuration and compliance with PCI 6.6 requirements. The report is delivered via email (select between weekly, monthly or quarterly delivery)
- You will have access to NTT's Manage Centre portal for the Service Management service features
- Imperva's WAF as a Service Console is accessible via single sign on

3.2. Enhanced Service Variant

The Enhanced service variant is best suited to clients who require customization of compliance events and are looking for detection of advanced web application attacks that require Security Analyst investigation and validation. Clients who subscribe to the Enhanced service variant also benefit from correlation with other NTT Managed Security Services where applicable.

In the Enhanced service variant, logs and events generated by the WAF service features are further processed by NTT as described in the following sections.

Due to the nature of logs and events generated by Infrastructure DDoS Protection these are not applicable for cyber threat detection and compliance monitoring. For more information refer to 3.2.1 *Compliance Monitoring Features in Enhanced* and **Error! Reference source not found.** *Cyber Threat Detection Features in Enhanced.*

3.2.1 Compliance Monitoring Features in Enhanced

In addition to the PCI-DSS reporting available from the Imperva WAF as a Service Console, NTT offers compliance monitoring with the ability to create custom business policy compliance rules.

The service can report on the following categories of security incidents:

- **Regulatory Compliance.** Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls



Client Service Description

Web Application Firewall as a Service

- **Security Best Practices.** Events that indicate a deviation from a pre-defined baseline of NTT's definition of security best practices
- **Business Policy Compliance.** Events that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements

Note: Customized rules/use cases for notification purposes are not available for Infrastructure DDoS Protection. In the event of infrastructure DDoS attacks, notification will be provided by the Service via methods requested in the Transition Workbook.

Detailed information about NTT's Compliance Monitoring capabilities are described in 3.3.11 Service Description Compliance Monitoring (Enhanced)

3.2.2 Cyber Threat Detection Features in Enhanced

In the Enhanced service variation NTT offers cyber threat detection capabilities. Relevant logs are sent from the WAF to NTT for further analysis in NTT's Threat Detection Engine using Advanced Analytics and Threat Intelligence.

Suspicious activities detected by the Threat Detection Engine and all relevant contextual information are presented to a Security Analyst, who engages in threat hunting and threat validation activities to verify the threat and its impact, and to identify additional information associated with the potential breach. Once verified, the Security Analyst creates a detailed Security Incident Report and initiates security incident notifications defined in the Transition Workbook, providing a detailed description of the security incident combined with scenario-specific actionable response recommendations. These actions assist businesses in reducing the time to take informed, responsive measures, lowering associated risks.

Detailed information about NTT's Advanced Analytics, NTT's Threat Intelligence and the importance of the Security Analyst are described in 3.3.8 *Advanced Analytics*, 3.3.9 *Threat Intelligence* and 3.3.10 *Detailed Security Incident Investigation by Security Analyst*.

3.2.3 Client Notification

In addition to the notification options in the Standard service variant, The Enhanced service variant has additional notifications options for compliance monitoring and detection of cyber threats. You are notified based on your selection of supported notification options, including e-mail and phone calls for the following categories:

- Analyst-created Security Incident Reports based on detailed investigation and Threat Hunting
- Automated compliance monitoring notifications

Additionally, tickets may be viewed in NTT's Manage Centre Portal.



Client Service Description

Web Application Firewall as a Service

3.2.4 Portal and Reporting

In addition to the Standard service variant portal and reporting capabilities (refer to 3.1.3) you have access to the following in NTT's Manage Centre Portal:

- Cyber threat detection and compliance monitoring events (last 90 days)
- Cyber threat detection and compliance monitoring security incidents
- Cyber threat detection and compliance reporting

Development of custom reports in NTT's Manage Centre Portal is not included as part of the Service.

Note: All Clients will have access to Imperva's WAF as a Service Console inclusive of options as per purchase order / contract.

3.3. Web Application Security Service Features

The Service provides PCI-DSS certified, cloud-based Web Application Security, through the implementation of a Web Application Firewall (WAF). The WAF will be used to secure key assets against known and emerging threats. The Service detection and mitigation capabilities covers web application attacks, including advanced bot attacks, web defacing, brute force attacks, sophisticated injections, and cross-site-scripting (XSS) site scraping.

This service feature is priced on the number of web sites (domain / URLs) and total network bandwidth (for all sites).

3.3.1 Web Application Firewall (WAF)

The WAF protects you against the most critical Web Application Security risks, such as SQL injection, cross-site scripting, illegal resource access, remote file inclusion and other OWASP top 10³ threats. Security experts behind the Service ensure optimum protection against newly discovered vulnerabilities to prevent disruption to your applications and improve website performance.

This service feature implements an enterprise-grade and PCI DSS-certified WAF.

Once this feature is selected, the following service features are included.

3.3.2 WAF Policies

WAF rules are deployed to protect web applications against advanced threats. Customized security rules can also be implemented to allow tighter enforcement of organizational security policy. These customizations can be based on many parameters including, browser details, IP addresses, header information, web page details, cookies and more. The customization and changes in WAF policies can be implemented via MACD service units.

³ [https:// https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)



Client Service Description

Web Application Firewall as a Service

The actions that can be taken on these requests include alerting, blocking (user, IP address, request) or ignoring a request, session or specific IP address indefinitely or for a specific period of time. The Service can also identify human interactions by providing a CAPTCHA ⁴ mechanism.

Threats

The Service identifies and categorizes threats on your websites into the following:

- Backdoor Protection
- Remote File Inclusion
- SQL Injection
- Cross Site Scripting
- Illegal Resource Access
- DDoS (Limited protection based on request threshold rates. For unlimited DDoS protection refer to *3.5.1 Website DDoS Protection (Unlimited)*).

Based on the policy configured, each threat type may be handled differently, e.g. 'Alert' only or 'Block IP Address'. These settings can be applied on a per site basis. Exceptions / whitelists can also be applied where required.

3.3.3 Custom Rules

Rules in the Service allow you to implement custom policies aligned to business requirements. Rules are applied at the web application site level. The following can be created and performed for security specific or application delivery use cases via MACD service units:

- Prevent bots from accessing a site's registration form
- Restrict access to a specific part of an application based on IP address
- Limit the rate of requests to a website
- Manipulate traffic routes and redirects
- Control a request's URL structure, headers and cookies

Rule actions for security include block, alert, require additional authentication (CAPTCHA, JavaScript and cookie).

Rule actions for application delivery include redirect URL, rewrite (URL, header, cookie) or forward traffic.

Rules created will appear in event logs when triggered and revision control allows rollback to previous versions.

3.3.4 Security Policies

Bot Mitigation

⁴ <https://en.wikipedia.org/wiki/CAPTCHA>



Client Service Description

Web Application Firewall as a Service

Bot Mitigation blocks known bad or suspicious bot activity such as comment spam, scraping and vulnerability scanning, while making sure that legitimate bots such as Google and Facebook can freely access your website. In addition to the improved security, blocking malicious bots also improves website performance as they account for up to 50% of all website traffic.

Bot Mitigation provides several options for handling bad and suspected bots. You can choose to receive an alert, block the bot, or challenge it with a CAPTCHA test to ensure that the visitor is human. Bad bots can be blocked based on the classification and specific sources (countries, URLs, IP address).

White and Black Lists

The Service supports both Black and White Lists. Black Lists are categorized by:

- Geolocation (countries)
- URLs
- IP addresses / subnets / ranges
- Exceptions to the Black Lists can also be added.

White Lists are based on either single or multiple IP Address, IP ranges or subnets.

3.3.5 SSL Support

SSL Support allows the Service to become the intermediary for all HTTP over SSL traffic targeted to your web applications. By allowing the Service to be an intermediary, HTTP over SSL traffic can be decrypted, analyzed, and filtered out for malicious visitors and requests against your web applications.

The Service is compliant with PCI-DSS and uses industry security techniques for secure key handling.

Custom Certificates

The Service certificate is used by default for both Server Name Indication (SNI) and non-SNI supporting clients. You may choose to use your existing domain certificate by uploading the certificate and private keys to Imperva's WAF as a Service Console.

Custom Certificates allows your website to use your own SSL certificate while having SSL traffic inspected.

Note: The Service does not manage the custom certificate. You are responsible for your own certificate lifecycle management.

3.3.6 Login Protect (Two Factor Authentication)

Login Protect' provides a two-factor authentication overlay solution for any website or application that requires a strong authentication mechanism. Login Protect does not require plugin install, code changes or integration with a third-party authentication product. Login Protect provides seamless integration using a one-time passcode sent to the authenticating user and can be introduced as an



Client Service Description

Web Application Firewall as a Service

additional authentication prompt to enforce strong authentication and appropriate access.

For example, access to sensitive pages, site administration, partner access, access to unpublished content, etc.

Login Protect supports the following authentication methods:

- Email
- Text message (SMS)
- Google Authenticator mobile application

You are provided with five (5) Login Protect accounts. Additional Login Protect accounts can be provided at an additional charge and configured using MACD service units.

3.3.7 Content Delivery Network (CDN)

CDN consists of a network of data centers located across the globe that delivers full site acceleration. The service features in CDN are included as part of Web Application Security service features. On average, users will experience 50% acceleration in web site browsing experience. The origin web servers will also benefit from a reduction in web bandwidth consumption between 40% and 70%. This is achieved through a combination of application-aware traffic analysis, dynamic profiling and intelligent caching technologies. The Service's CDN maximizes cacheable content while ensuring that the most frequently accessed resources are served from memory.

Note: This service feature is included with the Service at no charge when purchasing Web Application Security.

Caching and Policies

CDN caching policies are fully customizable to provide you with granular control over your users' web experience. The following pre-defined caching modes are available:

- **Disable caching.** No caching is performed; all content is forwarded from the origin web server
- **Static only.** Only content that has been marked as static (using standard HTTP headers) will be cached
- **Static and dynamic.** The Service applies a learning algorithm, which dynamically profiles the site and identifies what content should be cached
- **Aggressive.** All site content is cached. A time period (in minutes, hours, days or weeks) can be set to determine how often the cache is refreshed

Content Optimization

Content Optimization uses many content and networking optimization techniques to accelerate the web site browsing experience and minimize bandwidth utilization.

These techniques include content 'minification', 'on-the-fly' file compression, image



Client Service Description

Web Application Firewall as a Service

compression, session reuse optimization and TCP optimization and connection pre-pooling.

Content Optimization is included with the Service at no charge when purchasing Web Application Security.

3.3.8 Advanced Analytics (Enhanced)

NTT's Advanced Analytics utilizes proprietary machine learning/behavioural modelling to detect cyber threats in your environment. Advanced Analytics leverages a combination of traditional threat detection techniques (e.g. correlation, pattern matching, reputation feeds) with advanced detection techniques (e.g. machine learning, statistical modelling, kill chain modelling) and Threat Intelligence to enable detection of sophisticated threats using NTT's Threat Detection Engine.

To ensure Service quality, we will continuously make detection tuning decisions based on the validity and relevance of Service generated events and security incidents.

3.3.9 Threat Intelligence (Enhanced)

The Threat Detection Engine and Security Analysts utilize the extensive Threat Intelligence curated and produced by our Threat Intelligence researchers.

Additionally, Advanced Analytics includes continuous threat intelligence updates driven by investigations of actual security incidents.

Threat Intelligence is continuously curated and propagated into the Threat Detection Engine and Security Analyst tool sets from multiple technical and operational sources in an integrated manner that enables efficient and accurate detection of cyber threats.

Product threat data is gathered from the global network of analysis engines monitoring client businesses and NTT Group Networks. As these continuously identify known and unknown threats in specific locations, the threat data is gathered and used to improve the detection logic globally through improving machine learning capabilities, creation of rules, and high confidence Black Lists.

As Security Analysts identify and escalate verified threats as security incidents within the Service, delivery data is automatically gathered and used for the same purposes.

In addition, dedicated Threat Intelligence Analysts teams in the Global Threat Intelligence Center monitor the global threat landscape for new threats, trends and advisories. Upon identifying such scenarios, the team engages in threat research activities to identify additions and modifications to the threat detection capabilities, including:

- Black List additions
- Pattern signature modification, or creation



Client Service Description

Web Application Firewall as a Service

- Correlation signature modification, or creation
- Collaboration with Data Scientists improve machine learning capabilities
- Contextual information of emerging threats to support Security Analyst investigation

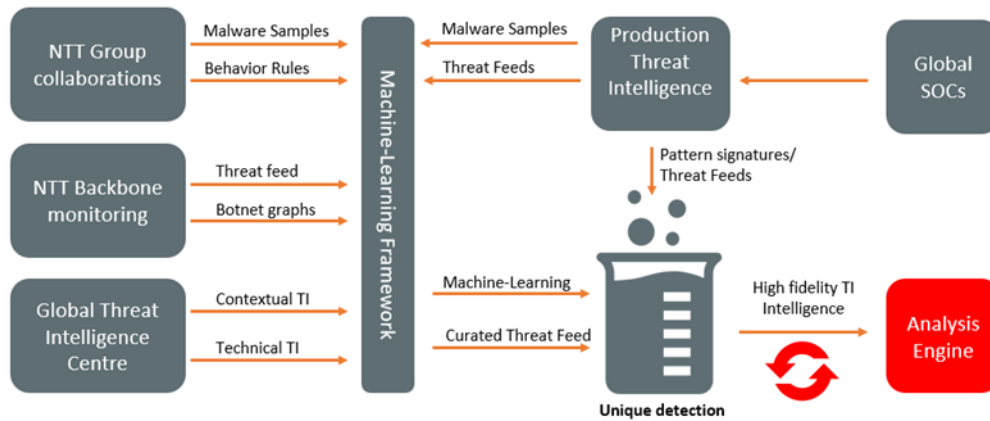


Figure 2 – Continuous Threat Intelligence Updates

3.3.10 Detailed Security Incident Investigation by Security Analyst (Enhanced)

Security events qualified by the analysis engine (or that of reliable signatures triggered by monitored technologies), are presented to the Security Analyst team within the proprietary Threat Hunting and Threat Validation framework called Analyst Workbench. Within this framework the Security Analysts are provided with all the information of the event, the holistic insights across client monitored sources, and strong threat hunting and validation capabilities.

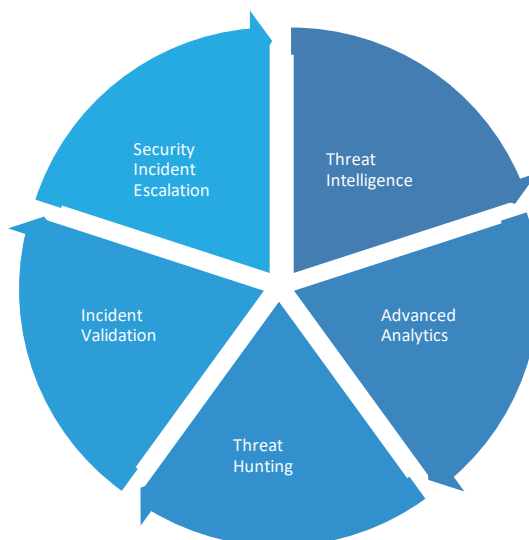


Figure 3 – Security incident investigation life-cycle



Client Service Description

Web Application Firewall as a Service

- Threat Hunting – Analyst Workbench, Big Data
- Incident Validation – Analyst Workbench, Threat Intelligence, Malware Lab, All Historic Incidents

3.3.10.1 Event-driven Threat Hunting

Security Analysts perform event-driven threat hunting activities as part of security incident validation in the Enhanced service variant. Leveraging the proprietary Analyst Workbench toolset, Security Analysts gain full insights of your monitored sources, as well as contextual information and evidence data in one single pane of glass.

Threat Hunting enables not only the ability to follow a threat throughout its life cycle, but also to hunt for additional activities and lateral movement possibly not detected by any of the monitoring capabilities in place. This is critical in understanding the extent of identified threats and the potential impact.

When examining an event that has been triggered in your environment, the Security Analyst has two objectives: Investigate and confirm the validity of the event, and perform additional pivoting of the event to additional monitored sources in order to determine the extent of the potential threat in your environment, answering these questions:

- Is the event that triggered just one indication of a potentially larger incident?
- Is there evidence that additional systems may be impacted?
- Can the root cause of the activity be identified?

Providing Security Analysts with a single view over the entire monitored Client estate and the ability to perform threat hunting activities across these in a responsive manner, offers insight into the entire security incident life cycle.

A view enabled by supporting tools, contextual data and insights into client's sources result in the Security Analyst's ability to offer accurate, relevant and actionable Security Incident Reports.

3.3.10.2 Security Incident Reports Based on Detailed Investigation and Threat Hunting

As security incidents are identified, the Security Analyst provides clients with a Security Incident Report that includes a detailed description of the threat, identified activity, and impact, and are combined with an incident response recommendation.

Response steps to take:

Typical content

- Estimated Threat Severity
- Activity Summary
- Incident Description
- Incident Response Recommendations



Client Service Description


Web Application Firewall as a Service

The contents of which will significantly increase the Client's ability to take swift and informed steps to resolve identified security incidents.

Given that the impacts associated with security incidents are closely tied to the period of time an attacker has until detection and containment receiving an actionable Security Incident Report significantly lower client risks.

Ongoing security incidents will be kept open until confirmation and validation of containment occurs and updates may be provided as new information is identified in relation to open security incidents.

Validated security incidents are categorized classified with appropriate threat severity based on the SOC team's analysis and assessment.

 <p>Critical Multiple compromised hosts</p> <table border="1"> <tr><td>Reference</td><td>INC965373</td></tr> <tr><td>Customer</td><td>Company</td></tr> <tr><td>Category</td><td>Malicious Activity</td></tr> <tr><td>Device(s)</td><td>Multiple</td></tr> <tr><td>First Observation</td><td>2017-NOV-12 23:15 UTC</td></tr> <tr><td>Last Observation</td><td>Ongoing</td></tr> </table>	Reference	INC965373	Customer	Company	Category	Malicious Activity	Device(s)	Multiple	First Observation	2017-NOV-12 23:15 UTC	Last Observation	Ongoing	<p>SOC Update 2017-11-25 22:43</p> <p>The internal host 10.74.68.75 (User: Bob) has triggered through proxy 10.10. signature "PROXY-D.PCK-167: Allowed proxy client session to blacklisted IP SE)".</p> <p>When the SOC downloaded the file, investigation revealed that it looks similar exploitation tool "PowerSploit" which is a collection of PowerShell scripts for lateral movement, executing programs and exfiltrating data.</p> <p>In connection to this the same internal host, 10.74.68.75 (User: Bob), also trig signature "FW-D.PCK-104: Extensive TCP hostscan (accepted privileged port towards the internal host 10.74.68.231 over multiple ports. The traffic was rep allowed. This signature triggers when it detects an extensive TCP hostscan (privileged ports) on internal network.</p> <p>SOC Update 2017-11-25 23:15</p> <p>The internal host "it_depart" (IP: 10.74.68.231) triggered the signature "MySQL Brute Force Attempt" towards "main_db" (IP: 10.74.68.63) over port TCP/3306 TCP/3306 is usually being used for MySQL. The signature "MySQL Authentic Force Attempt" triggers when a host has failed to login to MySQL more than 2 60 seconds. The signature has triggered 25 times within 7 minutes. The activ</p>
Reference	INC965373												
Customer	Company												
Category	Malicious Activity												
Device(s)	Multiple												
First Observation	2017-NOV-12 23:15 UTC												
Last Observation	Ongoing												
<p>Description</p> <p>The external host 80.85.158.147 (Chelyabinsk Signal LCC, Russian Federation) signature "EMAIL_PHISH_SHIPPING_COMPANIES_DOWNLOAD_ATTACH" sending an email towards 98.252.200[.]64 over port TCP/25. The traffic was re allowed. The subject of the email was "Updated Invoice January (URGENT)", a from satoshiii_nakamoto@gmail.com, and the recipient was hr@company.com</p> <p>Attached to the email was an executable "invoice.doc.exe", which when execut sandbox would make requests towards http://silent9.zapto[.]org over port TCP/</p> <p>Around the same time, the internal host 10.15.15.15 triggered the signature "S Executable Mail Attachment" towards 10.74.68.32 and 10.74.68.75. The logs f host 10.15.15.15 indicate that the host is a mail server.</p> <p>A few minutes later, 10.74.68.32 (User: Alice) triggered the signature "Win32/G accessing the file mentioned above ("invoice.doc.exe"). The action was reporte quarantined.</p>	<p>SOC Update 2017-11-26 09:07</p> <p>The internal host "it_depart" (IP: 10.74.68.231) triggered the signature "DNS-D.PCK-032: Continuous suspicious domain requests (Generated domain - DGA3)" by connecting to the external host 198.252.200.59 over port UDP/53.</p> <p>Example of captured data</p> <pre>.D.....YwRtaw46c3VtbaWYfjAxNw==.corporatecertupdate.com.....)..... .3.....23Vlc3Q6Z3VlC3Qe-.corporatecertupdate.com.....)..... m.....ahT6czHjcaV8cDRzc3cwcMq-.corporatecertupdate.com.....).....</pre> <p>When base64 decoding the subdomain in the DNS requests, we get:</p> <pre>admin: Summer2017 guest: guest IT_Adam: s3cretp4ssw0rd</pre>												
	<p>SOC Update 2017-11-26 12:09</p> <p>The internal host "mailsrv" (IP: 10.74.68.230) triggered the signature "PROXY-D.PCK-188 Allowed proxy client session to blacklisted hostname/domain (OTX)" by downloading the https://www.exploit-db[.]com/download/40616.c.</p> <p>When the SOC inspected the file in the Malware Lab, it seems to be an exploit for the vulnerability "DirtyCow" which can be used to get higher privileges on a system. By lookin through the linux_audit logs, the SOC found that the user "IT_Adam" compiled the exploit The following commands were executed from the host 10.74.68.230 in proximity to the ev</p> <pre>- gcc -o cow ./40616.c - ./cow - whoami - cat /etc/shadow</pre> <p>This is highly suspicious and authentication to the server might have been made with the of the previously exfiltrated credentials.</p> <p>Recommendation</p> <ol style="list-style-type: none"> 1. Disconnect the following hosts from the network: 10.74.68.75, 10.74.68.231 and 10.74.68.230 2. If possible re-image the compromised hosts, if this is not possible, follow the below advice. 2.2 Investigate the hosts mailsrv (10.74.68.230) and it_depart (10.74.68.231) for backdoors left by the attacker such as rootkits. 2.3 Run a scan with at least two different anti-malware products on the host 10.74.68.75 belonging to user Bob. 3. Perform 2.3 on the host 10.74.68.32 belonging to user Alice. 4. Perform a reset of passwords for all accounts. 5. Perform a thorough forensic investigation that looks for more possibly compromised hosts related to this activity. 6. Advise the users Bob and Alice on not to open untrusted attachments. 												



Client Service Description

Web Application Firewall as a Service

<p>Details: Action: Q Actual action: Quarantine Performed action: Quarantine Detection method: UNKNOWN App Path: C:\Windows\System32\explorer.exe Malware File Path: C:\Users\alice\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\CASEVGE\invoice.doc.exe User: Alice Target machine: ENS1622 Signature: WORM:Win32/Gamarue Time detected: 11/13/2017 8:48:43 AM Time reported: 11/13/2017 8:49:35 AM Category: Worm</p> <p>No signature triggered from the host 10.74.68.75 (User: Bob). SOC Update 2017-11-25 22:14</p> <p>The internal proxy 10.10.10.100 triggered the alert "AAE-D.PCK-Backdoor_Worm" by POST requests towards http://silent9.zapto[.]org/is-ready over port TCP/7895. Correlate the proxy logs shows that request came from 10.74.68.75 (User: Bob), which can also be seen in the captured data.</p> <p>Example of captured data</p> <pre>POST http://silent9.zapto[.]org:7895/is-ready HTTP/1.1 Accept: */* Accept-Language: en-US User-Agent: 57Ab29C6 <[.]ENS1622[.]Bob[.]Microsoft Windows 7 Professional[.]plus[.]avc[.]true - 25/11/17 Accept-Encoding: gzip, deflate Host: silent9.zapto[.]org:7895 Content-Length: 0 Proxy-Connection: Keep-Alive Pragma: no-cache X-FORWARDED-FOR: 10.74.68.75</pre>	
--	--

Figure 4 - Example Security Incident Report

3.3.10.3 Threat Severity

Each security incident will be assigned one of the following threat severity levels.

Threat Severity	Definition
Low	Observed security related event that could be an indicator of threat or interesting from other perspectives but no direct security incident or threat.
Medium	Minor security incidents with low risk of spreading or propagation. Should be tracked and followed-up but generally medium threat severity incidents require no immediate action.
High	Security incidents where if exploited, these threats could lead to compromise of the system and/or loss of information. Should be investigated in a timely fashion.
Critical	Security incidents with severe impact that threatens to have a significant adverse impact on the affected systems. These issues have a high probability of spreading or propagating, pose a threat to confidential or otherwise sensitive data or assets. Critical security incidents require immediate attention for remediation or mitigation.

Table 2 – Threat Severity Levels

The threat severity levels are to be considered guidance only. The Security Analyst always has the final say in assigning the threat severity while considering the situation and past experiences.

In addition to the above security incident threat severity levels, Security Analysts use the following mapping with the MITRE ATT&CK Matrix to identify the severity of security incidents as an additional reference and guidance.



Client Service Description

Web Application Firewall as a Service

Note: The MITRE ATT&CK Matrix mapping is not referenced in the Security Incident Report or integrated in Security Analyst Workbench.

		ATT&CK													
For pre-ATT&CK and unspecified findings, the TD SOC will only send incidents on special targeted attacks if deemed interesting.		unspecified	Technical Information Gathering (Pre-ATT&CK)	Technical Weakness Identification (Pre-ATT&CK)	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Lateral Movement	Exfiltration (& Destruction)
Category	Subcategory	Low Informational	Medium	High/Serious	Critical										
Unauthorized access	Data exfiltration											✓			✓
Unauthorized access	Vulnerability exploration			✓	✓										✓
Unauthorized access	Cross site scripting			✓	✓										✓
Unauthorized access	SQL injection			✓	✓										✓
Unauthorized access	Host compromise				✓									✓ (depends on the situation)	
Unauthorized access	Evidence tampering														
Unauthorized access	Privilege escalation					✓		✓		✓					✓
Unauthorized access	Brute force attacks									✓					✓
Denial of service	Application DoS			✓											✓
Denial of service	Volumetric DoS			✓											✓
Denial of service	Application DoS			✓											✓
Malicious software	Malware Infection														✓ (depends on malware's function)
Malicious software	Exploitation/Infection attempt				✓										
Malicious software	Adware or spyware	✓													
Improper usage	Instant messaging	✓													
Improper usage	Data leakage														✓
Improper usage	Peer-to-peer activity	✓													
Improper usage	Policy violation	✓									✓				
Reconnaissance activity	Network sweep		✓												✓
Reconnaissance activity	Host port scan		✓												✓
Reconnaissance activity	Network port scans		✓												✓
Other	Phishing				✓										
Other	Account fraud				✓										
Other	Social Engineering		✓												
Anomalies	Network Anomaly	✓													
Anomalies	Host Anomaly	✓													
Anomalies	Application Anomaly	✓													

Figure 5 – Threat severity classification using MITRE ATT&CK matrix

3.3.11 Compliance Monitoring (Enhanced)

For compliance monitoring with custom rules, the Service uses a customized rules and compliance profile to identify compliance deviations and can report on the following categories of security incidents:

- **Regulatory Compliance.** Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls
- **Security Best Practices.** Events that indicate a deviation from a pre-defined baseline of NTT's definition of security best practices
- **Business Policy Compliance.** Events that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements

To ensure Service quality, we continuously make detection tuning decisions based on the validity and relevance of Service-generated events.

The Enhanced service variant leverages automated detection and reporting of compliance-related security incidents.

The Service comes with a set of standard compliance rules sets. Creation of a limited number of custom rules (annually) is included in the Service. Additional rules can be created using MACD service units as described below:

- Use of NTT's Standard Compliance Rule Sets defined for WAF as a Service.



Client Service Description

Web Application Firewall as a Service

- Up to fifteen (15) Standard⁵ or Compound⁶ Rules can be developed and implemented annually. This includes any custom rules developed during Service Transition.
- Additional Standard or Compound Rules can be purchased via MACD service units at a rate of 6 MACDs per rule.
- Development of new Analyzers⁷ can be purchased via the MACD service units at a rate to be determined based upon the level of effort associated with the development of the Analyzer.

3.4. Infrastructure DDoS Protection

Infrastructure DDoS Protection helps to protect key infrastructure components across entire subnet ranges or individual single IP address. All incoming network traffic to the protected IP subnets is inspected and filtered in real-time. Malicious traffic is blocked, where only legitimate traffic is forwarded to the enterprise network via Generic Routing Encapsulation (GRE) tunneling.

In the event of an attack, the Service acts as the Internet Service Provider (ISP) and advertises all protected IP ranges to the Internet. All traffic from the internet will be re-routed through the Service's scrubbing centers, using BGP announcements.

Infrastructure DDoS Protection is asymmetric. Ingress traffic flows through the Service network then is forwarded to the Client's networks via GRE tunnels. Egress traffic goes directly to the Internet from the Client's networks.

This feature (priced) is available as "**Always-on**" or "**On-demand**" and pricing is based on the number of tunnels (connections) and the total amount of clean bandwidth required.

Infrastructure protection plans include up to 32 C-class prefixes and 8 connections (GRE tunnel, Equinix cloud Exchange, Cross Connect, or Internet Exchange).

Always-on – traffic is always routed via the Imperva scrubbing center.

On-demand – traffic is rerouted only when initiated, either automatically (see 3.5.4) or via Client notification.

Note: Infrastructure DDoS can be included (standalone) without any WAF features.

⁵ A detection method that tests a single attribute within a single log line to generate an event (e.g. if a specific message number is identified, then an event should be generated).

⁶ A detection type that tests multiple attributes within a single log line to generate an event (e.g. if a specific user logs into a specific server, then an event should be generated).

⁷ A detection mechanism that requires detailed analysis and development. (e.g. a detection mechanism which triggers an event if a user is created and added to a privileged group in the configured duration, scoped on username).



Client Service Description

Web Application Firewall as a Service

3.4.1 Prerequisites for Infrastructure DDoS Protection

Infrastructure DDoS Protection requires Clients to own a full C-class prefix and BGP routing capability with a public Autonomous System (AS) number.

- Own at least one C-class (/24) range
- Have a route object configured for each IP prefix in at least one of the IRRdatabases (e.g.RADb)
- Have TCP Maximum Segment Size (MSS) adjustment capabilities
- Be able to set up a GRE tunnel
- Use BGP on the network edge (preferred)

Clients who require Infrastructure DDoS and do not own a full public C-class prefix, can utilize IP Protection. For information about the service options, refer to 3.5 *Service Options*.

3.5. Service Options

The DDoS options presented below can be included with both web and infrastructure contracts.

3.5.1 Website DDoS Protection (Unlimited)

The Website DDoS Protection (Unlimited) service option provides security for large and sophisticated DDoS attacks against key websites on network, protocol and application levels (layers 3, 4 and 7). This service feature is built to handle volume-based attacks, such as SYN flood and Domain Name Server (DNS) amplifications. This service feature mitigates sophisticated application layer attacks by implementing advanced and progressive challenge mechanisms.

The DDoS protection mechanism can be set to 'Automatic' where threats are transparently mitigated based on the request rate threshold. The website DDoS protection can be set to 'On', where all DDoS rules are enabled, or 'Off' (disabled). White Lists can also be set.

Pricing is based on the amount of clean bandwidth required for the web sites.

3.5.2 DNS DDoS Protection

The DNS DDoS Protection service option safeguards DNS from DDoS attacks and is deployed as an Always-On service which automatically identifies and blocks attacks seeking to target DNS servers. This service option also accelerates DNS responses. This service option forwards legitimate DNS requests to your original name servers, ensuring that existing processes for managing name servers remain unaltered.

This option can only be added to Web Application Security.

You receive protection for up to 10 DNS zones when purchasing the option Website DDoS Protection (Unlimited).



Client Service Description

Web Application Firewall as a Service

3.5.3 Single IP DDoS Protection

If individual IP address are being protected (Edge IP), the Service provides an Always-On enabled protected IP address for any backend services. This is ideal for services hosted in cloud infrastructure, email, FTP or other non-web or non-DNS services where you do not possess a public routable C-class network range.

Edge IP (Protected IP over TCP/IP)

Edge IP can be used in place of a dedicated network for the use case of DDoS protection for TCP services where non-HTTP traffic needs to be passed to the origin server with no WAF inspections, e.g. proprietary protocols.

Edge IP provides Layer 3/5 volumetric DDoS for TCP whereby the origin server is resolved to a CNAME and an Anycast IP address is assigned. At least one of the identified IPs must respond to ICMP to show status as UP.

Note: If UDP protection is required instead of (or including) TCP, Edge IP can be configured to provide UDP protection. GRE tunnels on Client routers is a prerequisite.

3.5.4 Infrastructure Monitoring

The Infrastructure Monitoring service option is available with an on-demand deployment mode of Infrastructure DDoS Protection.

This option provides two main functions:

- Alerting when under attack – allow you to decide how and when to failover
- Providing network visibility – dashboard to show traffic statistic and analysis

With this option the **On-demand** service can automatically detect DDoS attacks and facilitate the immediate activation of the Service.

This option is not required for Always-On.

The Service monitors the origin network edge routers and firewalls, providing packet level visibility for both clients and Operations teams.

The Monitoring service requires edge routers that support: Netflow (v5,9,10) or sFlow.

Note: If the deployment mode for Infrastructure DDoS Protection is on-demand and the Client needs the Service to notify in the event of DDoS attacks and activate re-routing traffic, purchasing Infrastructure monitoring is mandatory.

3.5.5 SIEM / Log Integration

The SIEM / Log Integration service option is managed by you and securely transmits logs from the Service via a number of supported formats (CEL, LEEF, W3C) and supported SIEM vendors.



Client Service Description

Web Application Firewall as a Service

Detailed security logs are collected and sent in near real-time to your device to permit long term data retention, detailed investigations and to leverage internal use cases that may be developed as part of an on-premise SIEM solution.

Logs that are collected include:

- **Security logs.** Provide a detailed alert for each suspicious event detected by the Service. All logs include site and account ID references
- **Access logs.** Specify every request and response sent between your web server and the Service. This is all the traffic that would have been sent between end users and your origin server, including traffic served from the Service's cache

A number of tools are provided to you such as API integration, log encryption and predefined SIEM packages for leading OEMs.

You are responsible for all configuration of SIEM / Log Integration. We will make logs available in the supported formats.

This service feature is a prerequisite for the Enhanced service variant

3.5.6 Attack Analytics

Attack Analytics is a tool to help speed up the security investigation of WAF alerts. It provides a comprehensive view of attacks and attackers targeting your resources. Attack Analytics aggregates and analyzes your account's security alerts, and identifies common characteristics and groups them into meaningful security incidents.

Attack Analytics takes events from both the on-premise WAF and the cloud WAF and analyzes them to identify related events.

An Attack Analytics dashboard is integrated in Imperva's WAF as a Service Console.

Note: Attack Analytics includes SIEM / Log integration.

3.5.7 Dedicated Network

A Dedicated Network provides you with a unique static IP address for a website. Once a dedicated network is allocated, it is never shared among other clients. This provides additional control over your TLS certificates.

Using a dedicated network is recommended to support the following use cases:

- Non-HTTP traffic needs to be passed to the origin server with no WAF inspection (e.g., proprietary protocols)
- HTTP/S traffic needs to bypass WAF inspection and tunnel directly to a specific origin server (impacting all domains sharing the IP)
- Non-SNI clients, such as APIs, need to be served with a custom SAN certificate for multiple customer domains



Client Service Description

Web Application Firewall as a Service

- Non-SNI clients need to be served with a custom cipher-list or TLS versions
- Only your domains are allowed to appear on the Imperva-generated SAN certificate list, such that no other brands or competitors will share the same certificate
- Only available with Web Application Security.

3.5.8 Load Balancing and Failover

The Load Balancing and Failover service option provides Layer 7 load balancing and failover from the cloud to support your application and server availability deployed in data centers and cross-data centers. This is particularly useful for applications and servers deployed in a hybrid cloud or multi-cloud environment.

Load balancer allows you to manipulate traffic by using application delivery rules.

Load Balancing and Failover is only available with Web Application Security.

Single data center load balancing

Single data center load balancing supports a wide variety of load balancing and traffic distribution methods to maximize performance and distribute the load across a number of servers within the same data center. This supports maximizing application performance and reducing server load.

Sophisticated traffic distribution algorithms are available with or without a 'persistence override' option. Real-time server health and performance checks are used to rapidly detect outages and eliminate downtime. In the event of web server failure, the Service stops routing traffic to the failed server. As soon as the web server resumes operation, traffic forwarding will be re-enabled to the server.

Global Server Load Balancing (GSLB)

GSLB supports automatic failover, selection between multiple sites to enable high availability, ensures consistent performance in multiple geographies, and accelerates disaster recovery. Leveraging a global CDN, GSLB is offered through performance-based (i.e. user is assigned to data center with the best connection time) and geography-based mechanisms (i.e. users are assigned to data centers according to their geographic location).

3.5.9 Investigator – Enriched and Aggregated Log Search (Option)

WAF as a Service clients have the option to include NTT's Investigator log search capabilities. Investigator provides you with access to an interface to perform historical log searches from NTT's Manage Center Portal.

Investigator is only available with Web Application Security Enhanced.

The Investigator Tool ('Investigator') provides cloud-based, real-time access to log data. As NTT collect and analyse logs, it also archives a copy of the logs in a secure, cloud-based repository. Online access to enriched and aggregated logs through the Manage Centre Portal is enabled without the need for additional on-

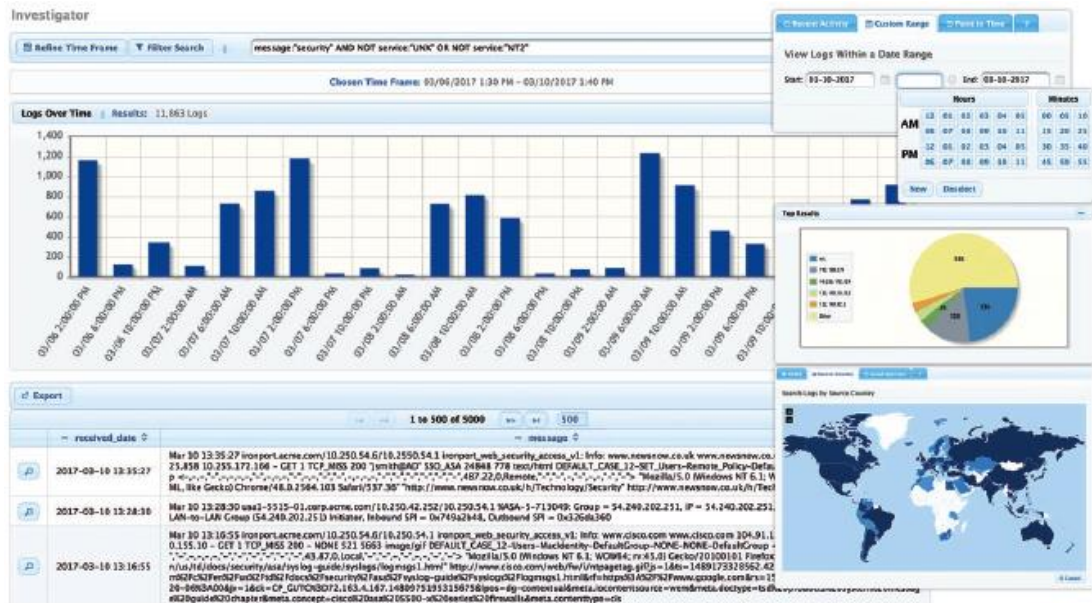


Client Service Description

Web Application Firewall as a Service

premise equipment or an up-front capital investment. This accessibility enables data mining of the logs for efficient security and compliance with incident investigations.

Search results can be filtered and mass exported for further off-line analysis.



INVESTIGATOR LOG DATA IS ACCESSIBLE VIA THE NTT SECURITY PORTAL.

Figure 6 – Investigator

Incident investigations require fast, efficient access to required log data.

Investigator provides a single source to access logs allowing your security team to immediately investigate incidents.

When a deep dive is necessary, Investigator allows users to search for logs. Searches use standardized query language, or the wizard-like filtering tool can be used to narrow specific data points. Recent searches can easily be re-run and frequent searches can be saved by each user.



Client Service Description

Web Application Firewall as a Service

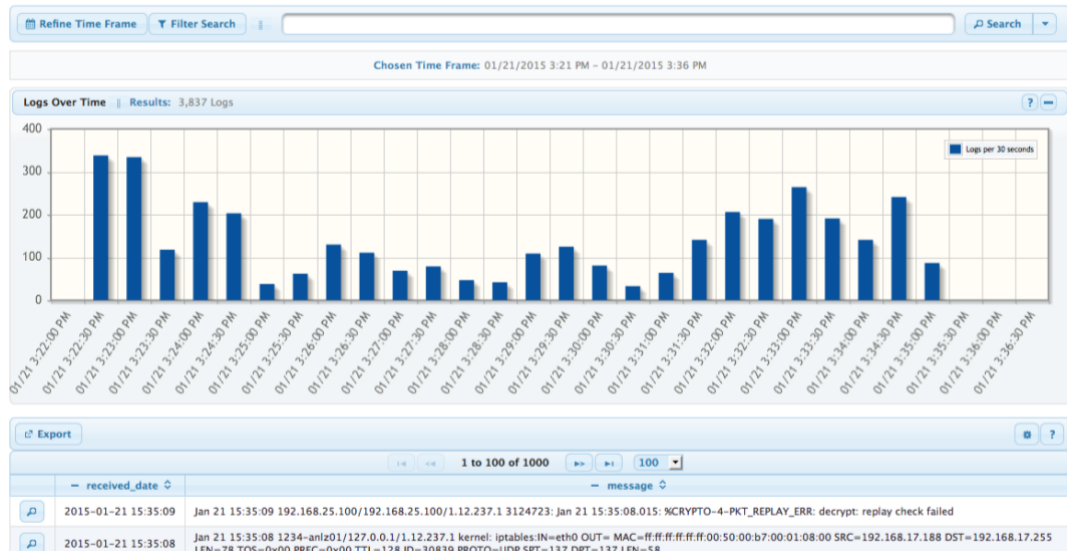


Figure 7 – Investigator Log Searches

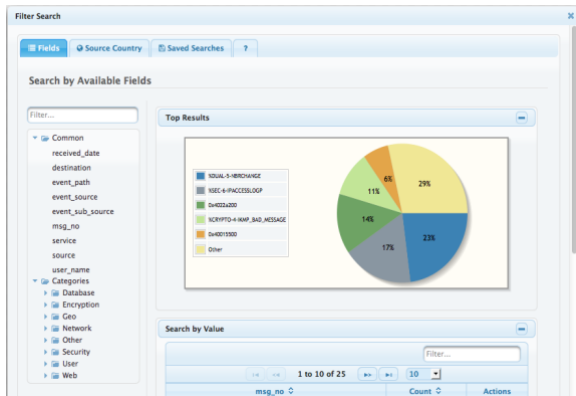


Figure 8 – Investigator Search Filtering

3.5.10 Secure Long-Term Log Storage (SLTLS) (Option)

You have the option to purchase Secure Long Term Log Storage (SLTLS).

By default, Imperva's WAF as a Service Console will only store events for up to 90 days.

This option is only available with the Web Application Security Enhanced service variant.

SLTLS utilizes the MSS infrastructure to store and retrieve raw logs collected by the platform. SLTLS will store logs for all devices in scope for your subscribed monitoring service. SLTLS is not customizable to specific devices or IP addresses.

The SLTLS service utilizes proprietary data storage software to securely store raw logs in originally obtained unaltered format. The SLTLS solution provides 'data encryption at rest' to ensure the privacy of your stored logs. The data encryption at rest feature is a FIPS 140-2 Level 2 validated enterprise-class encryption solution



Client Service Description

Web Application Firewall as a Service

that complies with regulations for sensitive data, such as HIPAA and Sarbanes-Oxley.

A user interface is provided so that you can perform raw log searches. The user interface is located within NTT's Manage Centre Portal. You may specify a date range along with an IP address as required input for log searches. Results from searches are displayed in NTT's Manage Centre Portal as a list of hourly compressed files that can be downloaded.

Log retention can be purchased in increments of 3 months (e.g. 3, 6, 9, 12, 15, 18, etc). Once the retention period has expired, raw logs shall be purged.

SLTLS provides you with the ability to self-service search for raw logs via NTT's Manage Centre Portal. As this is a self-service offering, you are responsible for performing searches and downloading relevant log files.

3.5.11 Vulnerability Correlation (Option)

If you also subscribe to NTT's Vulnerability Management Service for the web servers protected by the WAF as a Service Enhanced service variant, this option (opt-in and free of charge) use the information available to improve the ability to accurately identify cyber threats of relevance.

Opt-in requests are made during Service Transition or raised by you in NTT's Manage Centre Portal during continuous service delivery.

Upon opt-in, the NTT Vulnerability Management Service provides the WAF as a Service Enhanced service variant with added contextual information of the underlying operating system that the web applications are running on, including any vulnerabilities they may have. This additional information increases the Security Analyst's overall ability to understand the relevance of a web application threat and raise the accuracy of Security Incident Reports.

Prerequisites include:

- Client is also subscribed to NTT's Vulnerability Management Service
- Client Qualys subscription includes access to the Qualys API and the API key is provided to NTT for integration purposes
- Client Qualys API subscription is appropriately sized and reflects the size of the organization and its asset estate. Smaller subscriptions may result in limited usages caused by Qualys API restrictions

This option is only available with Web Application Security Enhanced service variant.



Client Service Description

Web Application Firewall as a Service

NTT's Approach to Service Operations

4.1. Service Experience

Our desire is to maximize the value you receive from MSS through effective engagement, communication and information sharing. Our focus is to enhance your Service experience and provide your organization with insight to enable your business decisions.

4.2. Service Desk

NTT's regional Manage Service Centre (MSC) is your primary Service interface, available to you 24/7. The NTT MSC coordinates incidents, and service requests, as well as system administration functions.

The service desk logs, tracks, and closes all tickets (incidents and service requests) in the NTT Service Management System. Tickets can be logged through the following methods:

- event driven (through monitoring of the environment)
- directly reported to us by you through the service desk
- directly reported to us by you via NTT's Manage Portal
- directly reported by CEC via our service desk

4.2.1 NTT's Manage Portal

As part of any Managed Security Service, you are provided with access to NTT's Manage Centre Portal. Manage Centre provides online access to:

- interact with us online by logging incidents, requests and changes
- track, view and submit comments within incident, request, and change tickets
- browse and search our knowledge base
- access the online document repository for contractual documentation, procedural documentation, meeting minutes, etc



Client Service Description

Web Application Firewall as a Service

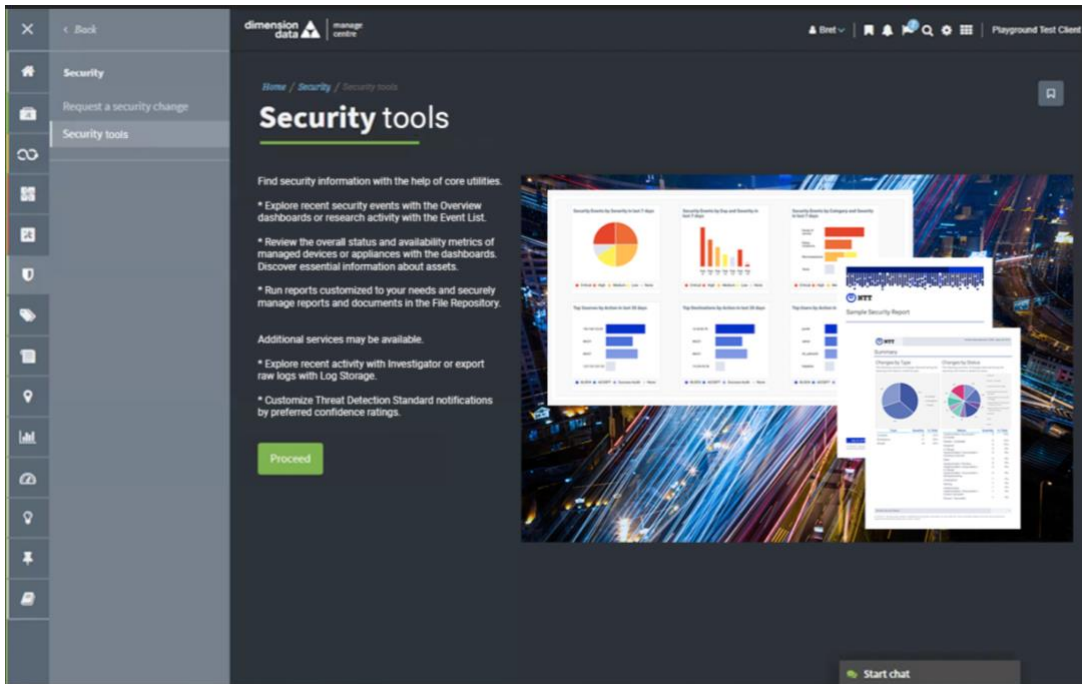


Figure 6 – NTT's Manage Centre Portal

4.2.2 Online Dashboards and Charts

Reporting is provided via NTT's Manage Centre Portal, through a mixture of interactive dashboards, charts and downloadable reports. Through NTT's Manage Centre, you can:

- view summaries and drill down into the detail for analysis.
- focus in on specific time periods.
- export the underlying data for offline analysis or reformatting.

1. ¹NTT's Manage Centre Portal provides a consolidated view of all your NTT managed services. Some reporting such as availability, capacity and performance data do not apply to all Security Services.

Client Service Description

Web Application Firewall as a Service

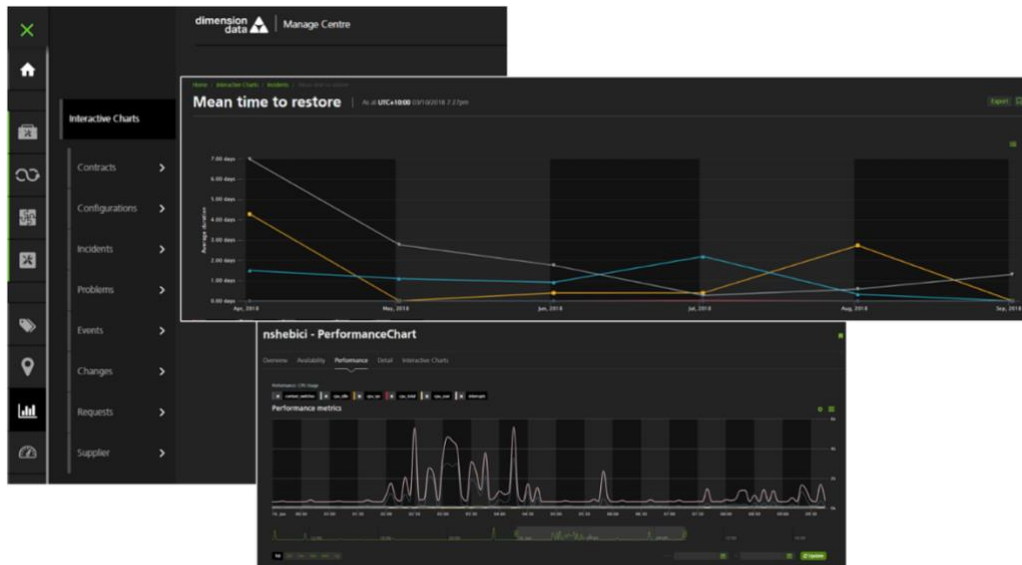


Figure 7 – NTT's Manage Centre dashboards and reports

Interactive reporting is available for:

- service levels, and
- task-related data e.g. incidents, requests, changes.



Client Service Description

Web Application Firewall as a Service

Service Management

5.1. Service Level Management

Depending on the complexity and/or size of your environment, and the mix of products and services, we may recommend additional service delivery management options.

5.1.1 NTT Service Delivery Manager (SDM)

Service delivery management provides governance and control across the various service features, processes, and systems necessary to manage the full lifecycle of the Service.

We will assign a Service Delivery Manager (SDM) to be responsible for service level management, and to act as an advocate for your organization within NTT. The NTT SDM is the primary interface who will manage the service delivery relationship between your organization and NTT. The SDM is responsible for scheduling, running all service management review meetings, and ensuring all processes and documentation are in place to manage your services.

Deliverables of the NTT SDM include:

- establish client relationship
- capture and manage minutes, agenda items, actions, and decisions
- change management issue management
- escalation management
- risk management
- service level monitoring, reporting and management
- service review meeting

5.1.2 MSS Technical Account Manager

The MSS Technical Account Manager is a security management function that provides technical and risk-based oversight and advocacy services for you. The Service is delivered through the NTT MSS Technical Account Manager team who assign and designate Technical Account Managers to clients who subscribe to the service providing the full depth and breadth of NTT's cybersecurity capabilities.

The MSS Technical Account Manager team leverages security best practices and an expansive knowledge base to deliver globally consistent security programs tailored to your specific needs and regulatory requirements. They are committed to developing long-term relationships with you to gain a deep understanding of your business objectives. This includes understanding your strategic initiatives, risk profile by industry or sector and cybersecurity maturity level assessments. This knowledge and level of technical engagement ensures you benefit from an optimized service aligned with your organization's business imperatives.



Client Service Description

Web Application Firewall as a Service

The MSS Technical Account Manager team are an additional component of the NTT MSS delivery model who provide cybersecurity insights beyond the Managed Security Services. Coupled with our 24/7 SOC teams, the MSS Technical Account Manager team provides operational support and consultative guidance in alignment with your business priorities and technology roadmaps.

The MSS Technical Account Manager team provides increased client intimacy by being available on-site (if Geo permits) as needed to provide technical guidance and to operate as an extension of your security team. Clients benefit from the MSS Technical Account Manager team support of internal and external stakeholder management while they face challenges implementing security controls across their enterprises.

The MSS Technical Account Manager team are the client advocates who identify and track action items and service requests that have been raised via the service desk to reduce the time to respond to your requests. The MSS Technical Account Manager Team also provides a quality control function to ensure delivery excellence, maintain high levels of client satisfaction, achieve project success, and drive continual service improvement.

The SOC provides 24/7 support for clients and although the MSS Technical Account Manager Team are not a 24/7 resource, the MSS Technical Account Manager Team is included in the escalation path for security incidents whereby intimate knowledge and proximity to you provides further context to aid in assessment and response activities. Overall, the team share observations and makes recommendations to improve your cybersecurity maturity and help you to manage risk.



Client Service Description

Web Application Firewall as a Service

Our Approach to Service Transition

Our approach to transition aims to ensure that both organizations enter the transition with a clear idea and understanding of the goals and objectives of the transition.

6.1. Objectives of Service Transition

- To ensure the absolute minimal disruption to your business during the onboarding of the managed service
- To determine and manage realistic transition timeframes
- To establish an operational baseline for the global MSS delivery organization that will be responsible for delivering the Service post-transition
- To align your expectations with service delivery capabilities and constraints
- To ensure our people understand your business from the onset to deliver a reliable, stable and excellent service

6.2. Transition Methodology

We use a formal transition methodology, developed in-house from industry-leading best practices and years of practical experience.

NTT's Service Transition Manager is responsible for managing the transition process with you and your organization and coordinating back with our Transition Team. The Transition Team is responsible for running the service onboarding and activation process to enable service operations. As part of the service activation process, the required tools and systems are set up and activated for the managed service to go live.

The typical duration for Service Transition is 10 elapsed weeks, although timing will depend on the size and complexity of the environment.



Client Service Description

Web Application Firewall as a Service

Appendix A Service Level Agreement

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Request Response	NTT will assign a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT's Service Desk.	P1&P2	60 Mins	5% of Monthly Service Fee	N/A	N/A
		P3&P4	4 Hours			
Request Complete	NTT will resolve a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT's Service Desk	P1	2 Business days	95% Service Units of the Request	95% Service Units of the Request	N/A
		P2&P3	5 Business days			
		P4	10 Business days			
Incident Management – Response	NTT will assign a Incident ticket with priority ____ within ____ minutes of receiving the ticket at NTT's Service Desk.	P1&P2	30 Min	N/A	N/A	24/7
		P3&P4	60 Min			
		P2	8 hrs			
		P3&P4	24 hrs			
		P2	16 Hours			
		P3&P4	48 Hours			
Emergency Change Response	NTT will assign an Emergency Change ticket within ____ minutes of receiving the ticket at NTT's Service Desk	N/A	30 Min	N/A	N/A	N/A
Change Response	NTT will assign an Change ticket within ____ minutes of receiving the ticket at NTT's Service Desk	N/A	60 Min	N/A	N/A	N/A
Change Implementation – Complete	NTT will complete changes before the end of the change window as mutually agreed upon between client and NTT.	N/A	95%	N/A	N/A	



Client Service Description

Web Application Firewall as a Service

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Resolve Notification (Service Level Objective) – Notify	NTT will provide a resolve notification for every Incident ticket within ____ minutes of restoring the service.	N/A	30 Min	N/A	N/A	

Table 3 – Service Level Agreements



Client Service Description

Web Application Firewall as a Service

Appendix B



Client Service Description

Web Application Firewall as a Service

Appendix C WAFaaS Policy Management MACD

Task	MACD	Comment	Justification (Notes)
WAF as a Service			
Onboarding	10	WAF Protection Single Website onboarding	2 hours for preparation/communication and 0.5 hour for implementation
Onboarding	16	WAF Protection multiple Websites onboarding (Up to 3 Websites)	2.5 hours for preparation/communication, 0.5 hour for implementation for each site
Onboarding	8	Log Integration for Website	1 hour for preparation/communication, 0.5 hour for implementation, 0.5 hour for testing
Onboarding	15	Log Integration for Multiple Websites (up to 3 sites)	1 hour for preparation/communication, 0.5 hour for implementation for each site, 1 hour for testing
Reporting	3	Ad hoc Report Generation from Portal	0.5 hour for preparation/communication, 0.25 hour for implementation
Website Setting	7	Renew/Upload custom SSL certificate for single Website	1 hour for preparation/communication, 0.5 hour for implementation
Website Setting	9	Renew/Upload custom SSL certificate for multiple Websites (up to 3 sites)	1.5 hour for preparation/communication, 0.25 hour for implementation for each site
Website Setting	3	Change Website setting	0.5 hour for preparation/communication, 0.25 hour for implementation
Website Setting	5	Change multiple Websites setting (Up to 3 sites)	0.5 hour for preparation/communication, 0.25 hour for implementation for each site
Account Setting	3	Change Client account setting on Incapsula	0.5 hour for preparation/communication, 0.25 hour for implementation
Account Setting	3	Create, Remove or Update account user	0.5 hour for preparation/communication, 0.25 hour for implementation
Account Setting	11	Create Error page/Login Protect page	2 hours for preparation/communication, 0.25 hour for implementation, 0.5 hour for testing



Client Service Description

Web Application Firewall as a Service

Task	MACD	Comment	Justification (Notes)
Account Setting	2	Change Log Level	0.25 hour preparation/communication, 0.25 hour implementation
WAF tuning	3	Change Security Setting, including Add or update IP/URL/Bot/country to White List/Black List	0.5 hour for preparation/communication, 0.25 hour for implementation for each site
WAF tuning	5	Change Security Setting for multiple Websites, including Add or update IP/URL/Bot/country to White List/Black List (up to 3 sites)	0.5 hour for preparation/communication, 0.25 hour for implementation for each site
WAF tuning	2	Manage WAF setting, including create or update White List/Black List	0.25 hour for preparation/communication, 0.25 hour for implementation
WAF tuning	9	Create or update Rule	1 hour for preparation/communication, 0.25 hour for implementation, 1 hour for testing
WAF tuning	11	Create or update Rule for multiple Websites (up to 3 sites)	1 hour for preparation/communication, 0.25 hour for implementation for each site, 1 hour for testing
API	3	API management, including generate API Key and permission management	0.5 hour for preparation/communication, 0.25 hour for implementation