Cloudreach™
an atos company

Managed Web Application Firewall Service

Service Specification

Cloudreach
an atos company

Service Specification

Service Name:	Managed Web Application Firewall Service
Service Level Hours:	Refer to section 1.1
Unit of Charge:	Monthly Fee
Prerequisites:	Infrastructure Reliability or Infrastructure Essentials
Supported Cloud Platforms:	AWS, Azure and GCP
Product Codes:	
Version Number:	1.1
Status:	Live
Published Date:	August 2022

The Small Print

Definitions

The definitions for all capitalised terms used throughout this Service Specification are set out in the Cloud Operations Service Definitions document which forms a part of this Service Specification and the Cloudreach Order Form to which this Service Specification relates.

Cloudreach
an atos company

Table of Contents

1.0 Web Application Firewall Service Overview

Cloudreach Managed Web Application Firewall (WAF) service is designed to keep Customer web applications secure from vulnerabilities. Cloudreach cloud-based managed WAF service offers a holistic, proven and layered protection against known zero day application attacks keeping all application types secure against application attacks. The Cloudreach Managed WAF Service is conditional on Customer having procured Infrastructure Reliability or Essentials Service.

1.1 Service Levels

Services	Service Level Hours
Onboarding	Business Hours (9x5) (*PDT time zone if the Customer is based in NA and GMT time zone if the Customer is based in EEA & UK*)
Managed Web Application Firewall Service	24x7

2.0 Web Application Firewall Onboarding

2.1 Onboarding Tiers

Transition of deployed applications into support will be approached in two distinct tailored methods to fulfil the requirements of the Customer, depending on the level of involvement desired.

Onboarding Enterprise - This service includes the onboarding of the relevant application(s) into the Managed WAF service, Cloudreach providing an alert report from the implemented rules to the Customer, Cloudreach analysing that report and making recommendations in collaboration with the Customer to what rule changes should be implemented. This option is most suitable for a Customer that requires a more comprehensive onboarding, including collaborative efforts in both assessment and configuration.

Onboarding Essentials - This service includes the onboarding of the relevant application(s) into the Managed WAF service, Cloudreach providing an alert report from the implemented rules to the Customer, Customer analysing that report and making recommendations of what should be updated to the rules. This option is most suitable for a Customer that is content with self-assessment and configuration of WAF rules.

2.2 Onboarding Terms

Once the service is ready for onboarding, Cloudreach will assign a team member to manage the project of onboarding the Managed WAF Service. Please note that Cloudreach will only perform onboarding of service during Business Hours.

2.3 Deployment Strategy

The policies and controls that are required for the delivery of the Managed WAF service are covered in the Deployment Strategy Document provided as part of Infrastructure Reliability and/or Essentials.

The WAF deployment and configuration may be provisioned through CSP-native offerings.

2.4 WAF Monitoring Configuration

As part of the service, Cloudreach analysts shall fine-tune the Customer's WAF solution by monitoring their web application traffic, whitelisting valid requests and data, and building a policy that blocks malicious web traffic and other undesired activity.

As such, Cloudreach shall be responsible for the configuration of monitoring and alerting on any WAF deployments. Alerting incidents and thresholds will be informed during onboarding, and will be noted in Customer WAF specific runbooks for use during remediation events (each, a "Runbook"). Each Runbook will include, but will not be limited to:

- a Recovery Point Objective ("RPO") which shall be informed by the observed values provided by the portal once the environment is supporting production workloads. The RPO shall be used for monitoring and alerting purposes.
- a handover contact within the appropriate Customer team for activities in which the Customer wishes to own remediation.

3.0 Managed Web Application Firewall Service

The Customer's public cloud application(s) will be maintained as part of the Infrastructure Reliability or Infrastructure Essentials service including configuration management and any trouble-shooting that may be required to address issues with availability and accessibility of the application(s).

3.1 Core Functionality

Cloudreach's WAF solution caters to a variety of security posture essentials, designed to ensure an experience that is both seamless and reliable. The solution includes, but it not limited to:

- **Zero-day Emerging Threat Detection** - A broad signature set, which allows for the capture of zero-day and emerging threats

- **Traditional and behaviour based detection** - Leveraging usage-based application learning to analyse behaviour and large signature set of traditional vulnerabilities, enabling the WAF solution to provide a highly effective defence from web application attacks.

- **Full Featured WAF services** - The Cloudreach WAF solution provides a full set of features including end-to-end encryption, rate limiting data masking, and connection throttling in addition to others.

3.2 Incident & Change Management Process

The Incident Management and Change Management Processes detailed in the Customer's existing Infrastructure Reliability or Infrastructure Essentials specification shall apply to the Managed WAF service.

Incidents and Changes will be managed using the corresponding ticketing tools and procedures in accordance with Runbooks and/or process(es) documented, ensuring appropriate steps are taken and any handovers to the Customer team take place. As new threats emerge and Customer's application and portfolio change, the Cloudreach team will update the Customer's policies as needed or required.

The managed WAF service will be specifically focused on any changes required to Web Application Firewalls. Changes related to the Managed WAF service will be limited to 5 per month. This includes, but is not limited to configuration changes or changes to firewall rules or policies. For the avoidance of doubt, any changes pertaining to active threat remediation are not included in this total. .

4.0 Document Management

4.1 Revision History

Version	Description of Changes	Revision Date
1.0	Document creation	September 2021
1.1	Document Revised. Clarification of change management process	June 2022

4.2 Approvals

This document requires the following approvals:

Name	Title	Approval Type	Approval Date	Version
Stephanie Leopold	Head of Compliance	Global Sign off		1.1
Caroline Griffiths	Senior Product Manager - Managed Services	Global Sign off	17th August 2022	1.1
Michael Hogg	Senior DevSecOps Manager	Global Sign off	17th August 2022	1.1