

## TRUSTWAVE SECURITY SERVICES

# Secure Web Gateway

## Scope, Features, and Responsibilities

Trustwave Security Services provides a comprehensive set of solutions for Secure Web Gateway (SWG). SWG provides threat and data protection, and ease of compliance with regulatory policies. Trustwave offers the following Trustwave Security Services (the “Services”) across the full solution lifecycle of an SWG project.

### Managed Security Services

- The Managed Security Services operations activities and responsibilities are described in detail within the Security Technology Management service description, subject to the following:

**Table 1: Applicable Security Technology Management Service Description**

Type of CASB Architecture Set-up	Applicable Service Description
Fully Cloud-based – Cloud Portal only (with/without endpoint agents)	Security Technology Management (Cloud)
Hybrid – Cloud Portal with On-premises virtual appliances (with/without endpoint agents)	Security Technology Management (On Prem/Hybrid)

- Integration to core 24x7 threat detection capabilities is provided by the Managed Detection service.

**Table 2: Applicable Threat Detection and Response Service Description**

Monitoring Service Options	Applicable Service Description
Managed Detection Essentials	Threat Detection and Response: Managed Detection
Managed Detection Complete	

### Consulting & Professional Services

- **(Mandatory)** Implementation of supported SWG technologies is provided by the Trustwave Professional Services team, including:
  - Advisory, Activation & Adoption
  - Design and implementation of Trustwave designed default policies and configurations
- **(Desired)** Professional Services custom packages, designed to support Trustwave SWG Clients with bespoke environments:
  - Migration of existing custom rules, available as packages with two iterations/reviews.
  - Regular policy & architectural reviews and updates

## Service Responsibilities

Full-service features described in the following RACI chart below.

Please note:

- Trustwave services do not provide direct support to end users. Client shall assume responsibilities for end user helpdesk services and any communications of procedures for self-registration of credentials to Client's end users. Trustwave will support Client IT staff with technical enquiries.
- Client should also ensure the availability of an active directory for import and synchronization of user and user groups on the platforms.
- Service features described in the RACI chart below correspond to the full suite of services offered. Actual service features that are applicable to Client is dependent on the actual services subscribed.

**Table 3: RACI**

		Customer	Trustwave
<b>Implementation</b>	Implementation project kick-off and Discovery, including advising on configurations, policies & reporting	I	RAC
	Creation of administrator accounts	I	RAC
	Provision, installation of virtual appliances (on-premises if applicable)	RA	CI / RA <sup>1</sup>
	Configuration of cloud portal, virtual appliances (if applicable), and Trustwave-managed assets/ Trustwave-managed 3rd party solutions (if applicable) <sup>2</sup>	CI	RA
	Creation and Implementation of Trustwave designed default policies and whitelists	CI	RA
	Customisation of aesthetics and content descriptions on Client template pages and notification templates, as per client's request <sup>4</sup>	CI	RA
	Deployment and distribution of clients (or PAC files, certificates, or any other files and software, if applicable) on Client's endpoints	RA	CI
<b>MSS Provisioning</b>	Rack, stack, and installation of Trustwave connector appliances, if applicable	RA	CI
	Establishment of connectivity between Trustwave ASOC and cloud portal to enable event collection, security monitoring and change management	I	RAC
	Establishment of connectivity between Trustwave ASOC and virtual appliances (if applicable) to enable security monitoring, health monitoring, and device management	I	RAC
	Creation of Trustwave Fusion Portal accounts and account users	I	RAC
	Creation, change, or deletion of administrator accounts	I	RAC
<b>Ongoing Operations</b>	Threat detection and notification	I	RAC
	Health monitoring, backup and restoration, certificate management, product and security updates for on-premises virtual appliances (if applicable)	I	RAC
	Configuration of existing virtual appliances (if applicable) as part of change requests	I	RAC
	Configuration of cloud portal and Trustwave-managed assets/ Trustwave-managed 3rd-party solutions, as part of change requests <sup>3</sup>	I	RAC

	Configuration and/ or software and adapter installation on customer's cloud apps and customer-managed assets/ customer-managed 3rd-party solutions, as part of change requests <sup>3</sup>	RA	CI
	Updating of DLP, Compliance, and Threat Protection policies and profiles, SSL Decryption policies, URL filtering policies, Forensic profiles, Classification of devices (corporate vs non-corporate) and IP whitelists, as described by a change request	CI	RA
	Updating of Threat Protection policies and profiles, as recommended by Trustwave security analysts	I	RAC
	Customisation of aesthetics and content descriptions on client template pages and notification templates, as described by a change request	CI	RA
	Deployment, distribution or removal of endpoint clients (or PAC files, certificates, or any other files and software, if applicable) to/ from end-users	RA	CI
	Generation and viewing of reports	RA	CI
	Technical assistance	I	RAC
<b>Support Services</b>	Escalations to solution vendor	I	RAC
	Policy and configuration reviews and updates	I	RAC
<b>Professional Services Custom Packages</b>	Design and implement <i>net new</i> policies, architecture and configurations	CI	RA
	Migration of existing SWG custom rules	CI	RA

R - Responsible, A - Accountable, C - Consulted, I - Informed

<sup>1</sup> Clients may perform the installation of virtual appliances themselves, with guidance from CPS. Alternatively, CPS may also be engaged to perform the installation on-site, subject to resource availability. For all on-site engagements, Travel and Expense charges incurred are to be borne by Client and will be quoted separately.

<sup>2</sup> Includes activities to enable:

- Setting up of traffic steering mechanisms
- Integration with directory tools

<sup>3</sup> Includes modification of settings around:

- ration of SWG and supported 3rd-party technologies (eg. EDR, ATP, MDM, DLP, IRM, etc)
- Integration with directory tools

<sup>4</sup> Available as an additional service on a T&M basis.