TRUSTWAVE SECURITY SERVICES

Cloud Access Security Broker

Scope, Features, and Responsibilities

Trustwave Security Services provides a comprehensive set of solutions for Cloud Access Security Broker (CASB). CASB serves as a gateway to cloud services, providing visibility of cloud activities, 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 a CASB 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

- **(Required)** Implementation of supported CASB technologies is provided by the Trustwave Professional Services team, including:
    - Deployment in API, forward proxy, or reverse proxy mode
    - Integration with 3rd party technologies supported by the platform
    - Consult, design, and implementation of policies and configurations
- **(Optional)** Professional Services retainer, which can be utilized for a range of post-implementation professional services, including:
    - Regular policy & configuration reviews and updates

- Onboarding of new cloud apps
- Consult, design, and implementation of new policies and configurations

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: CASB RACI

		Customer	Trustwave
Implementation	Implementation project kick-off and discussion, including consulting on DLP requirements	I	RAC
	Provision of information required to implement the technology	RA	CI
	Creation of administrator accounts	I	RAC
	Provision of the hardware, hypervisor, and processing requirements necessary for the installation and running of the virtual appliances (if applicable)	RA	CI
	Installation of virtual appliances on-premises (if applicable)	RA	CI / RA [1]
	Configuration of cloud portal, virtual appliances (if applicable), and Trustwave-managed assets/ Trustwave-managed 3rd party solutions (if applicable) [2]	I	RAC
	Configuration and/ or software and adapter installation on customer's cloud apps and customer-managed assets/ customer-managed 3rd-party solutions [2]	RA	CI
	Creation and Implementation 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	I	RAC
	Customisation of aesthetics and content descriptions on client template pages and notification templates, as per client's request	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
MSS Provisioning	Provision of information required to set up the service	RA	CI
	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

Ongoing Operations	Creation, change, or deletion of administrator accounts	I	RAC
	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 [3]	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 [3]	RA	CI
	Onboarding of new cloud apps, including new custom apps, via API Integration, Forward Proxy (if there are IDP changes), or Reverse Proxy	Provided via Professional Services. Refer to "Professional Services (Retainer) Engagement" section	
	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
Support Services	Technical assistance	I	RAC
	Escalations to solution vendor	I	RAC
Professional Services (Retainer) Engagement	Policy and configuration reviews and updates	I	RAC
	Custom parser creation, import, export, and testing for log parsing/ cloud app discovery purposes	I	RAC
	Onboarding of new cloud apps, including new custom apps, via API Integration, Forward Proxy (if there are IDP changes), or Reverse Proxy	I	RAC
	Application of any necessary configurations on customer's new cloud apps	RA	CI
	Consult, design, and implementation of new policies and configurations	I	RAC

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

[1] 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.

[2] Includes activities to enable:
- Log parsing/ cloud app discovery
- API integration between CASB and customer's cloud apps
- Setting up of forward/ reverse proxy mechanisms
- Onboarding of custom applications
- Integration of CASB and supported 3rd-party technologies (eg. EDR, ATP, MDM, DLP, IRM, etc)
- Establishment of encryption and key management
- Integration with directory tools

[3] Includes modification of settings around:
- Log parsing/ cloud app discovery
- Integration of CASB and supported 3rd-party technologies (eg. EDR, ATP, MDM, DLP, IRM, etc)
- Encryption and key management
- Integration with directory tools