SERVICE DESCRIPTION

Security Technology Management (Cloud)

Service Description

The Security Technology Management service (“Service”) focuses on system management requirements to provide a set of features so that the Client’s cloud-based security technology (“Managed Techology(ies)”) functions according to the system design.

Service Management

Service Delivery

The Service provides the following components:

a) Trustwave Transition Services – Refer to Trustwave's Transition Service description for further information regarding activities and deliverables related to the provisioning and implementation activities required to bring a managed technology to a steady state of service delivery.

b) Change Management – The ongoing configuration of the Managed Technology(ies), policies, rulesets and the implementation of Security Updates and Product Updates.

c) Trustwave Security and Compliance Monitoring services - Refer to Trustwave’s Security and Compliance Monitoring Services for further information regarding service delivery related to Threat Detection services.

d) Trustwave Fusion Platform – Provides reports and interactive features that are related to the service components.

Management models

Trustwave will assume management of Client’s Technology using a cloud-based management portal after being provisioned for Client use by solution provider.

Client access model

Trustwave will provision Client with limited read-only access to the solution unless otherwise allowed under a different service provided by Trustwave.

Service Operations

Change Management

Trustwave maintains an overall change control procedure for its support infrastructure and associated managed services. Changes that could affect the operation of Client systems are coordinated with appropriate Client IT staff.

The SOC will assess and implement change requests submitted by Client through the Trustwave Fusion Platform. All requests are evaluated against industry best practices to help reduce adverse impacts to the security of the Client's environment. Typical change requests for the Service include:

a) Change management requests to Managed Technology as requested by an authorized Client contact or a Trustwave threat analyst in response to a known threat.

b) Configuration changes deemed necessary by SOC analyst.

Changes requested by the Trustwave SOC are categorized and handled according to the following types:

Table 1: Types of Change Requests

Type of Request	Constructs
Emergency Security Change Request	Immediate Security threat mitigation when: a) A change is necessary to mitigate a security risk(s) identified by the Trustwave SOC or Client; or b) It involves security policy settings.
Standard Change Request	Non-scheduled changes which are proactive in nature which: a) Are not a significant impact on Managed Technology; or b) Do not alter architectural design or functions of Managed Technology.
Complex Change Request	Large changes that are planned and scheduled appropriately because such changes: a) could significantly impact the functions of the Managed Technology; b) Could alter the architectural design of the Managed Technology. c) Could require POC to be completed prior to scheduling. Errors during this change could have significant outage consequences.

Trustwave will setup a change window to apply changes in the Client environment. The change window will be available for the following regions as set forth below.

Table 2: Change Management Windows

Region	Time-Zone	Start Time	End Time	How often
Americas	CST	12:00AM	6:00AM	Every Tuesday & Thursday
EMEA	CET	12:00AM	6:00AM	Every Tuesday & Thursday
APAC	PHT	12:00AM	6:00AM	Every Tuesday & Thursday

Problem Management

Problem Management is focused on service failure analysis and provides solution designed outline to underlying causes of one or more service interruptions.

Trustwave provides a root-cause analysis report, which is a post-mortem technical report that relies on incident Ticket notes to identify the probable causes of the service failure in accordance with the available information. Root cause analysis reports are available upon Client request.

Service Exclusions

The following features are not included in the Service:

Technology Availability and Health Monitoring

This service addresses management of cloud-based security platforms. Availability of the cloud provider's platform can affect the Service. Please contact your cloud solution vendor for any service level agreements for platform availability. The Service does not include Availability and Health monitoring for the cloud provider's infrastructure.

Change Management

- Any change management process described as part of the Service described does not apply for Client owned third party solutions (endpoint, infrastructure, cloud resources, etc.)
- Any configuration change management request on supported solution categorized as a complex change may be deemed a project and is subject to Client acceptance of separately quoted additional charges.

Backup and Restore

For cloud-based security platforms, backup and restoration of the environment configuration is not included in the Service. Please contact your cloud provider for any backup and restoration solutions that can be utilized independently of the Services.

Service Responsibilities

Trustwave responsibilities and acknowledgements

- Validate that a change request was submitted by an authorized Client contact, and notify Client if validation is not successful.
- Perform assessment based on Trustwave's risk level and change categories and determine whether a change request is in-scope within the terms of the Service.
- Source additional information as necessary to support the implementation of the change request.
- Assess the potential risk that will result from implementation of the change request and advise Client of the outcome as necessary.
- Notify Client if a change request is outside the scope of the Service and/or if additional charges will apply to a change request.
- Perform change management activities when requested and in compliance with Trustwave policies and inform Client of implemented changes.

Client responsibilities and acknowledgements

- Procure and maintain valid vendor software licenses and maintenance contracts applicable to the Managed Technology(ies).
- Access the Trustwave Fusion Platform to submit change request Tickets, respond to Tickets, and confirm scheduled change windows.
- Work in collaboration with Trustwave regarding risk factors related to a change request as part of change risk classifications and provide requested information in a reasonable timeframe.
- Review and assess changes that Trustwave proposes, and promptly provide Trustwave with approval or rejection of the proposed change.
- If required, provide pre-determined change control windows during which change management functions can be executed
- Client acknowledges that any configuration change management requests for Technology or Client environment that are categorized as a complex change may, in Trustwave's sole discretion, be deemed a project and would require a written addendum between the parties.

Service Level Management

It is Trustwave's goal to respond to security incidents, monitor for outages, and perform configuration changes in accordance with the Service Level Agreement. The Service Level Agreements ("SLAs"), for the Services, which are incorporated into this Service Description and include commitments with respect to certain availability of the Services, are set forth at http://www3.trustwave.com/SLA/Ver003_Trustwave_MSS_SLA.pdf

Definitions

Managed Technology(ies) or Technology(ies) means Client's Technology(ies) and Client's Management Console Technology(ies) covered under the service.

POC means Proof Of Concept.

SLA means the service level agreement targets referred to in this Service description.

SOC means Security Operations Center, the Trustwave operational and security incident management facilities operated 24 hours a day, 7 days a week, 365 days a year.

Ticket is a record of activities or alerts and documented within the Fusion platform.

Trustwave Fusion Platform means the Trustwave managed security service infrastructure utilized in providing the Service.