SERVICE DESCRIPTION

Security Technology Management (On-Premise/Hybrid)

Service Description

The Security Technology Management service (the “Service”) focuses on system management requirements to provide a set of features so that the security technologies function according to the system design. This description applies for technologies deployed on-premise and/or for a hybrid deployment with a combined cloud delivery and on-premise components.

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) Incident Management – the monitoring of system health metrics, and availability.

d) Backup and Restore – backup and restore activities which provide for the integrity of the system in case of system failure.

e) Trustwave Security and Compliance Monitoring Services - Refer to Trustwave’s Threat Detection services described at the Managed Detection service description.

f) Trustwave Fusion Platform access – Provides reporting and interactive features that are related to service components.

Management models

Client may select from these management models for the managed technology:

a) Trustwave will assume management of the existing Client Technology(ies) within Client’s environment; or

b) After Client has procured and installed new Technology(ies), Trustwave will assume management of those technologies; or

c) Management of Client Technology(ies) through third party management system that is located either on Client premises or hosted within the Trustwave platform.

Client access model

Client does not have access to modify data on managed Technology(ies) regardless of the deployment model implemented 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. Trustwave establishes an email address for each Client contact to support communication with Client and/or any service contractors responsible for administration of Client networks.

The SOC will assess and implement change requests submitted by Client or SOC through the Trustwave Fusion Platform. All requests are evaluated against industry best practices to help ensure that they will not detrimentally impact the security of the Client 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.

c) Change reversals as requested by an authorized Client contact.

d) Applying Product Updates and Security Updates to the Managed Technology(ies) when necessary to stay within the supported version policy.

e) Facilitation of Technology Replacement.

Changes requested by 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 security risk(s) identified by the Trustwave SOC or Client.

	b) It involves security policy settings and is not an upgrade of software or patch for the Managed Technology. i.e. Active threat activity detected and requires mitigation by implementing a security rule change.
Standard Change Request	Non-scheduled changes which are proactive in nature which: a) Are not a significant impact on Managed Technology. b) Do not alter architectural design or functions of Managed Technology. i.e. Add firewall rules for new services, new IPS policy to begin inspecting new traffic type due to disclosure.
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. i.e. Managed Technology software version upgrades, changing routing configurations, Client large scale network architecture changes.

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

Product and Security Updates

The service includes the application of Security Updates, Product Updates and patches. The implementation of necessary Security Updates, Product Updates and patches is not an optional feature of the service, and failure to implement a required Security Updates, Product Updates and patches as required may adversely impact the operation and functionality of the Managed Technology(ies)

Each type of Product Update follows a different process:

- Security Content Updates: New content for protection engines, initiated by the vendor of such protection engines, to address latest threats and typically do not interfere with proper function of the technology.

- Patches or hotfixes: Updates to address immediate and specific product issues initiated by the vendor for such products. Issues being addressed by patches often inhibit proper function of the technology and should be implemented as soon as possible.
- Product Feature Updates: Feature updates provided by the vendor of the applicable porduct. These updates will typically cause brief downtime or restart of the technology. Application of these updates requires a pre-defined change control window coordinated with Client.

The Trustwave SOC will monitor the availability of Security Updates, Product Updates and patches and apply such updates to the Managed Technology(ies).

a) Updates or security patches that include bug and vulnerability fixes will be reviewed by Trustwave and applied to the Managed Technology(ies) only when the update applies to any active subscriptions or feature set.

b) Product Updates and Security Updates available under the relevant valid Managed Technology(ies) application license or maintenance contract will be scheduled with Client for implementation. All Security Updates and Product Updates for Managed Technology(ies) software will be completed during version upgrades.

c) Consideration is given to accommodate Client's preferred maintenance window to ensure the least disruption possible. Trustwave will implement the relevant Product Updates and Security Updates depending on priority to help ensure that the Managed Technology(ies) are operating, and that the service is provided as designed.

d) If the operating system (OS) is incorporated as part of the Managed Technology(ies), then the underlying OS updates will also be updated as provided for by the Managed Technology vendor. If the underlying OS is not included with the vendor technology, then those OS updates will be the responsibility of Client.

Technology Replacement

For issues requiring replacement of technology at a Client environment, Trustwave SOC can act on behalf of Client and contact a third-party vendor to activate an RMA Process. Trustwave will provide remote assistance, support and configuration, in respect of any repaired or replaced technology.

For specific solution types which Trustwave can control the shipment of the replacement for, the service will also provide SLAs for RMA shipment. The Technology Replacement must be received by the Client and connected to the network in such a manner that the Trustwave SOC can connect and configure the Technology remotely. The Trustwave SOC will work to validate that the Technology is configured consistent with the state prior to its replacement. The Service will resume only after the Technology is deployed and up to date to its previous state of operation prior to the replacement.

Technology Incident Management

Incident Management is the process utilized by Trustwave to minimize any adverse impact and to restore normal service operation as quickly as possible in the event of a failure.

The Incident Management process involves:

- Incident identification
- Categorization and classification
- Initial diagnosis and troubleshooting

- Notification
- Restoration, resolution and closure

Health Status Monitoring

The service includes health and availability monitoring of the Managed Technology(ies). This helps ensure that the Managed Technology is available and performing within Client environment.

The Trustwave SOC monitors the Managed Technology(ies) to:

- Help ensure that the Managed Technology(ies) are active;
- Monitor the health and availability metrics.

The health status monitoring feature of the service monitors the network availability of the Managed Technology(ies) to ensure they are visible to the Trustwave Platform.

Health monitoring metrics supported by Trustwave may vary between different supported platforms. Monitoring health and availability should include multiple aspects of the Managed Technology.

- Network Availability: Determines if the technology showing available via the network interface that allows service delivery.
- CPU Utilization: Provides measurement of CPU utilization and warns for overutilized CPU that could threaten the technology's proper functions.
- Disk Space: Advanced warning of full disk utilization can prevent the technology from failing, thereby threatening its proper functions.
- Heat Indicators: For technology which provide this information (often an appliance) advanced awareness of extreme temperature causing failure can help prevent the technology from failing, thus threatening its proper functions.

Managed Technology is monitored to detect when it is no longer showing as active within the Trustwave Platform or surpasses a threshold that might indicate a health issue. Initial steps are taken to assess the cause and remediate the issue if possible. If remediation steps available to Trustwave are not successful and, based on the technology outage type identified, Trustwave will provide notification to Client within the defined SALs/SLOs and provide subsequent updates to Client

In the event of a complete outage or a highly impactful partial outages, an incident report will be filed and will provide details related to the outage. Mitigations taken to bring the technology back to production performance, and any changes to configuration necessary to recover the service will be included in the incident report. The incident report will be delivered as part of the closing process of the Ticket.

High Availability Management

The Service offers the option to manage supported technologies in a high availability (HA) configuration. This provides redundancy for Managed Technology by placing a secondary device to create a redundant pair, so that if the first technology fails, the second device can take over operation.

- HA devices are monitored to ensure they are online and operating as designed.
- HA devices are monitored and updated with Product Updates and Security Updates.
- When the primary monitored device is offline and not able to be recovered the HA device will be enabled.

Problem Management

Problem Management is focused on service failure analysis and provides a solution designed to outline 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.

Backup and Restore Policy

Trustwave will apply backup and restore as part of the Service to Managed Technology(ies). Technology configuration and policy backup will take place through regular polling and will help ensure the latest version of the configuration is saved if a recovery is required. Backups are kept for ninety (90) days.

Service Responsibilities

Trustwave responsibilities and acknowledgements

- Maintain management connection to the Managed Technology(ies).
- Monitor the Managed Technology(ies) to ensure their active online status and availability.
- Notify Client within SLA timeframe if management connection is unavailable and cannot be restored by Trustwave.
- Attempt to resolve any connectivity or system issues identified in order to return the technology to a steady state of operation. Trustwave will determine when Technology Replacement is necessary.
- Provide remote assistance, support and configuration, in respect of any repaired or replaced Managed Technology(ies) to restore technology to steady state.
- Notify Client if a HA configured device has been brought online as part of a support Ticket associated with the offline primary device.
- Validate that 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.
- Apply Security Updates and Product Updates applicable to Managed Technology(ies) as made available by the vendor and within the timeframe required depending on the relevant update's priority and criticality.

- Create a service Ticket and schedule the Product Update, Security Update, or rule update with Client for any update that may cause downtime and requires a change control window.

Client responsibilities and acknowledgements

- Procure and maintain valid vendor software licenses and maintenance contracts applicable to the Managed Technology(ies).
- Provide access to vendor portals to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of Client for management and maintenance purposes.
- Notify relevant third-party vendors of the appointment of Trustwave as Client's agent to act on its behalf in relation to the RMA Process and:
    - Confirm delivery of Technology Replacement;
    - Perform the physical installation of Technology Replacement; and
    - Contact the SOC to arrange for Trustwave remote support and configuration of Technology Replacement.
- Inform Trustwave of all Client environment maintenance activity and changes that may impact on Trustwave's ability to provide the Service.
- Access the Trustwave Fusion Platform to submit change request Tickets, respond to Tickets and confirm scheduled change window.
- Work in collaboration with Trustwave regarding relevant risk factors related to a given change as part of change risk classifications and provide requested information in a reasonable timeframe.
- For changes proposed by Trustwave: review, assess and notify Trustwave of approval or non-approval.
- If required, provide pre-determined change control windows that provide opportunities for required change management functions to be executed
- Client acknowledges that:
    - Any configuration change management requests for technology or Client environment categorized as a complex change may be deemed a project and is subject to Client acceptance of separately quoted additional charges.
    - The implementation of necessary Product Updates and Security Updates is not an optional feature of the Service; Failure to implement a required Product Update or Security Update as required may adversely impact the operation and functionality of the Managed Technology(ies).
    - Trustwave will not be responsible for any service delivery issues, SLAs, or damages resulting or arising from Technology(ies) and product versions that are not supported by the solution vendor.

Service Level Agreement

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

Client Initiation Information means Client-provided information relating to Client environment and Client's Technology policies and rulesets.

IDPS means Intrusion Detection and Prevention Systems.

IPS means Intrusion Prevention Systems.

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

NGFW means Next Generation Firewall solution.

POC means Proof of Concept.

Product Update(s) are vendor-provided product and security enhancements to the Managed Technology(ies), that come in the form of firmware updates or new versions of the software. These updates typically include new or enhanced features, product improvements and security patch fixes.

RMA Process means the relevant manufacturer's return authorization process for the refund, replacement, or repair during the relevant product's warranty period.

Security Update(s) are vendor-provided security enhancements that add additional protection or update the existing protection engines included with the technology. These updates are typically smaller in size but more frequent than Product Updates.

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.

Technology Replacement means a repaired or replaced Managed Technology.

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

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