Trustwave®

Service Description

Security Technology Management (On-Premise/Hybrid)

Version 3.2
Date 10/1/2020

Table of Contents

List of Tables

Service Description

The Security Technology Management service (the "**Service**") provides system management features which enable security technologies to function according to the system design. This description applies to security technologies deployed onsite or deployed via a combined cloud delivery and onsite approach.

Service Management

Service Delivery

As a part of this Service, Trustwave provides the following sub-services:

- **MSS Transition** – please 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.
- **Change Management** – this sub-service provides ongoing configuring of the Managed Technology(ies), policies, rulesets, and the implementation of Security Updates and Product Updates.
- **Incident Management** – this sub-service monitors system health metrics and availability.
- **Backup and Restore** – this sub-service backups and restores activities to maintain the integrity of a system in case of system failure.
- **Trustwave Security and Compliance Monitoring Services** – please refer to Trustwave's Threat Detection services described in the Threat Detection & Response – Managed Detection
- **Trustwave Fusion Portal Access** – provides reporting and interactive features that are related to service components.

Management Models

Client may select from the following management models:

- Trustwave will assume management of the existing Managed Technology(ies) within Client's environment; or
- Where Client has procured and installed a new Managed Technology(ies), Trustwave will assume management of those technologies; or
- Trustwave will manage Managed Technology(ies) through a third-party management system that is located either on Client’s premises or hosted within the Trustwave Fusion Portal.

Client Access Model

Client may select from the following access models for support technologies and features of support technologies for physical or virtual next generation firewalls.

- **Fully Managed Device**: Trustwave fully manages the device(s) within the scope of the Service and Client will not have edit permissions. Client may have the ability to directly view configurations and content from the device(s).
- **Co-Management – Role Base Access**: Client will have limited access to the Managed Technology's management local web user interface and Trustwave will retain full administrative access. Any third party's platform will dictate how Trustwave will allocate permissions to Client to read and edit configurations of supported features.

Service Operations

Change Management

Trustwave maintains an overall change control procedure for its support infrastructure and associated managed security services. Changes that could affect the operation of Client's systems are coordinated with Client's IT staff. Trustwave establishes an email address for each Client contact to support communication with Client or any service contractors responsible for the administration of Client's networks.

The SOC will assess and implement change requests submitted by the Client or the SOC itself through the Trustwave Fusion Portal. The SOC evaluates all requests against industry best practices to help ensure that they will not detrimentally impact the security of the Client's environment.

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

Table 1: Types of Change Requests

Request Type	Characteristics & Process
Emergency Security Change Request	Such requests require immediate security threat mitigation because: • A change is necessary to mitigate security risk(s) identified by the SOC or Client. • The request involves security policy settings and is not an upgrade of software or patch for the Managed Technology. *Example*: Active threat activity detected and requires mitigation by implementing a security rule change.
Standard Change Request	A request for a change that is low risk, relatively common, and follows a specified procedure or work instruction. A Standard Change Request has repeatable implementation steps and has a proven history of success. As such, changes are pre-approved

	and they follow a streamlined process in which approval is not required from group level, peers, or Client's change advisory board (where applicable). This also includes unscheduled changes which are proactive and: • do not have a significant impact on managed technology; or • no not alter the architectural design or functions of managed technology. *Example*: Add firewall rules for new services or new IPS policy to begin inspecting new traffic type due to disclosure.
Complex Change Request	A request for a beneficial change or any change to the Service that is sufficiently more complex to not constitute a Standard Change Request. These changes are most often scheduled outside of defined change blackout windows or during defined maintenance windows. These are large and complex changes that require planning and scheduling of resources to execute the change because such changes could: • significantly impact the functions of the Managed Technology. • alter the architectural design of Managed Technology. • require POC to be completed before scheduling and errors during this change could have significant outage consequences. *Example*: Managed Technology software version upgrades, changing routing configurations, or large scale network architecture changes.

Trustwave will setup a change window for Client's approval to apply changes in Client's environment.

Client-Initiated Change Management

Trustwave will assess and implement change requests submitted by Client through the Trustwave Fusion Portal. All requests are evaluated against industry best practices to help ensure that they will not detrimentally impact the security of Client's environment. Trustwave will plan changes that may be disruptive to Client's environment, and Client will approve or deny these changes. Client acknowledges that denial of a change window may impact Trustwave's ability to provide the Service. Typical change requests under this Service include:

- Change management requests to Managed Technology as requested by an authorized Client contact or a Trustwave threat analyst in response to a known threat.
- Change reversals as requested by an authorized Client contact.
- Applying Product Updates and Security Updates to the Managed Technology when necessary to stay within the supported version policy.
- Facilitation of Technology Replacement

Trustwave-Initiated Change Management

Trustwave will assess and implement change requests submitted by the SOC through the Trustwave Fusion Portal. All requests are evaluated against industry best practices to help ensure that they will not detrimentally impact the security of Client's environment. Typical change requests under this Service include:

- Change Management to Managed Technology in response to a known threat.
- Configuration changes deemed necessary by Trustwave.
- Applying Product Updates and Security Updates to the Managed Technology when necessary to stay within the supported version policy.
- Facilitation of Technology Replacement.

Trustwave will operate within a change window preapproved by Client to apply changes in Client's environment.

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, or patches, as needed, may adversely impact Trustwave's ability to provide the Service.

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 the latest threats and typically do not interfere with the proper function of the Managed Technology.
- **Patches or Hotfixes**: Updates to address immediate and specific product issues initiated by the vendor for such products. Issues addressed by patches often inhibit the proper function of the Managed Technology and should be implemented as soon as possible.
- **Product Feature Updates**: Feature updates provided by the vendor of the applicable product. These updates will typically cause brief downtime or restart of the Managed Technology. The application of these updates requires a predefined change control window coordinated with Client.

The SOC will monitor the availability of Security Updates, Product Updates, and patches and apply such updates to the Managed Technology in accordance with the following policies:

- Trustwave will review updates or security patches that include bug and vulnerability fixes and applied to the Managed Technologies only when the update applies to any active subscriptions or feature set.
- Trustwave will schedule Product Updates and Security Updates available under the relevant valid Managed Technologies application license or maintenance contract with Client for implementation. Version upgrades will include all Security Updates and Product Updates for Managed Technologies software.
- Trustwave will implement the relevant Product Updates and Security Updates depending on Trustwave-determined priority to help ensure that the Managed Technologies and the Service are operating as intended. In scheduling such implementation, Trustwave will consider Client's preferred maintenance window to ensure the least interruption possible.
- When Managed Technologies incorporate an operating system (OS) as a part of the Technology, then the underlying OS updates will also be updated as provided for by the Managed Technology vendor. If the Managed Technologies does not incorporate an OS, then those OS updates will be the responsibility of Client.

Technology Replacement

For issues requiring replacement of technology in a Client's environment, the 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 within the scope of this Service.

For specific solution types where Trustwave can control the shipment of a replacement, Trustwave will also provide SLAs for RMA Process shipment. In such cases, the Technology Replacement must be received by Client and connected to Client's network in such a manner that the SOC can connect and configure the Replacement Technology remotely. Further, the SOC will work to validate that the Replacement Technology is configured consistently with the state before its replacement. After deploying the Replacement Technology and achieving the most current state, Trustwave may resume the Service.

Technology Incident Management

Incident Management is a process utilized by Trustwave to minimize any adverse impact caused by a failure of a Managed Technology and to restore regular service operation as quickly as possible.

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 Technologies. Health monitoring helps ensure that a Managed Technology is available and performing within Client's environment.

The SOC monitors the Managed Technologies to:

- help ensure that Managed Technologies are active; and
- monitor health and availability metrics.

The health status monitoring feature of the Service monitors the network availability of the Managed Technologies to ensure they are visible to the Trustwave Fusion Portal.

Health monitoring metrics supported by Trustwave may vary between different supported platforms. Monitoring health and availability should include multiple aspects of a Managed Technology, such as:

- **Network Availability**: Trustwave determines if the Managed Technology is showing available via the network interface that allows delivery of the Service.
- **CPU Utilization**: Trustwave measures CPU utilization and anticipates overutilized CPU that could threaten the Managed Technology's proper functions.
- **Disk Space**: Trustwave seeks advanced warning of full disk utilization to prevent technology or service degradation, thereby threatening its proper functions.
- **Heat Indicators**: For Managed Technologies which provides this information (often an appliance), Trustwave seeks advanced awareness of extreme temperature changes which may cause failure to help prevent technology or service degradation, thus threatening its proper functions.

Managed Technology monitoring detects when a Managed Technology is no longer showing as active within the Trustwave Fusion Portal or surpasses a threshold that might indicate a health issue. Trustwave will take initial steps to assess the cause and remediate the problem, if possible, as determined by Trustwave. If remediation steps available to Trustwave are not successful and, based on the outage type identified, Trustwave will notify Client within the defined SLAs and provide subsequent updates to Client.

In the event of a complete outage or highly impactful partial outages, Trustwave will create an incident report within the Trustwave Fusion Portal and will provide to Client details related to the disruption. Trustwave will track action to bring the Managed Technology back to production performance and will include in the incident report any changes to the configuration necessary to recover the Service. To close the Ticket, Trustwave will deliver the incident report to Client.

High Availability Management

As a part of the Service, Trustwave offers the option to manage certain supported technologies in a high availability (HA) configuration. HA provides redundancy for Managed Technology by placing a secondary device to create a redundant pair so that if the first Managed Technology fails, the second device can take over the operation. HA management services are offered at additional cost. Where Trustwave and Client agree to include HA management as part of the Service, Trustwave will:

- monitor HA devices ensure they are online and operating as designed;

- monitor and update HA devices with Product Updates and Security Updates; or
- when the primary device is offline and un-recoverable, initiate the HA device to take over the primary device's functions.

Problem Management

Problem Management is focused on service failure analysis and provides a solution designed to outline the 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 per the available information. Root cause analysis reports are available upon Client request without additional cost.

Backup and Restore Policy

Trustwave includes backup and restoration services for Managed Technologies as part of the Service. Trustwave will use regular polling to permit technology configuration and policy backups and to help ensure the latest version of the configuration is available for recovery scenarios. Trustwave will hold Client's backups for ninety (90) days.

Service Responsibilities

Trustwave Responsibilities and Acknowledgements

- Maintain a management connection to Managed Technologies, however, when not possible through no fault of Trustwave's, notify Client within SLA timeframes if management connection is unavailable and Trustwave is unable to restore.
- Monitor Managed Technologies to ensure their active online status and availability.
- Attempt to resolve any connectivity or system issues identified to return the Managed Technology to a steady state of operation.
- Determine when a Technology Replacement is necessary.
- Provide remote assistance, support, and configuration, in respect of any repaired or replaced Managed Technologies, to restore it to a steady state of operation.
- Notify Client if an HA configured device has been brought online as part of a support Ticket associated with the primary device.
- Validate that an authorized Client contact submitted a change request 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 the implementation of the change request and advise Client of the outcome, as necessary (to be determined by Trustwave).
- Notify Client if a change request is outside the scope of the Service and 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 Technologies, as made available by the applicable vendors and within the timeframe reasonably determined by Trustwave based on the 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 Managed Technologies.
- 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 vendors of the appointment of Trustwave as Client's agent to act on its behalf with the RMA Process.
- Confirm delivery of a Technology Replacement.
- Perform the physical installation of a Technology Replacement.
- Contact the SOC to arrange for Trustwave remote support and configuration of any Technology Replacement.
- Inform Trustwave of all Client’s environment maintenance activity and changes that may impact Trustwave's ability to provide the Service.
- Access the Trustwave Fusion Portal to submit change request Tickets, respond to Tickets, and confirm the 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 enable the execution of change management functions.

- Any configuration change management requests for a Managed Technology or Client's environment categorized as a Complex Change Request may be deemed a project and is subject to Client's 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 by Trustwave may adversely impact the operation and functionality of the Managed Technologies.
- Trustwave will not be responsible for any service delivery issues, SLAs, or damages resulting from or arising from Managed Technologies and product versions that are not supported by the solution vendor.
- There are inherited risks associated with change management and Client waives any claim against Trustwave in this regard.

Service Level Agreement

It is Trustwave's goal to respond to security incidents, monitor for outages, and perform configuration changes under 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 https://www3.trustwave.com/SLA/Ver003_Trustwave_MSS_SLA.pdf

Definitions

Capitalized terms used in this service description but not defined herein have the meaning given to them in the Trustwave Master Services Agreement found at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or a similar agreement signed between Trustwave and Client.

IPS means Intrusion Prevention Systems.

Managed Technology(ies) is any technology deployed within the customer's physical/virtual, cloud, or hybrid environment that Trustwave has agreed to manage and support.

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 related 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, seven 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 Portal.

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