SERVICE DESCRIPTION

MSS Transition

Provisioning and Implementation

Service introductions and information gathering

Transition and delivery teams are assigned to help Clients facilitate the successful configuration and rollout of the Clients managed service.

Welcome call

The provisioning team will schedule a welcome call with the Client for an introduction to the TrustKeeper Client Portal ensuring the Client understands how to access and use the services purchased.

Provisioning and implementation for Managed Device

- The provisioning team is responsible for working with Client to review and analyze the Client's responses to the Provisioning Questionnaire;
- Configure the Managed Device(s) to ensure that normal day-to-day device operations are working properly and all supported capabilities are able to be managed by the SOC in a manner that allows Trustwave to meet service responsibilities and SLA's for the Managed service;
- Ship the managed device to the client supplied address, if applicable;
- Coordinate and schedule installation or takeover of the managed device with the client;
- Provision and implement the Managed Device(s) into the Client's environment, if applicable, so that the services can be handed over to the SOC for on-going management, maintenance and support;
- The managed service is deemed to be delivered and operational when the SOC is able to view and has management control of the Managed Device(s); and
- The Client has access to the TrustKeeper Client Portal to view Log Data, Log Events, Alerts and reports.

Provisioning and implementation for Cloud Services

- The provisioning team is responsible for working with the client to review and analyze the Client's responses to the Provisioning Questionnaire;
- Configure the Cloud back-end to allow for further customer premise configuration;
- Providing instructions to the Client on the install of any required agents or configuration modifications required to activate service functionality;
- The managed service is deemed to be delivered and operational when the Cloud back-end is setup and Client receives instructions to complete final setup tasks;

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.

Device and environment assessment

- Trustwave transition engineers work with the Client to help ensure optimal placement and configuration, including assessment of the completeness of the Client's responses to the Provisioning Questionnaire and Client provided information. Trustwave transition engineers confirm with the Client of the Client's environment, policies and rulesets and assessment of the configuration of the Managed Device(s) to determine if current version and features are consistent with Trustwave supported device requirements.
- If Clients require additional assistance in planning the integration of the managed device(s) in their environment, additional on-site or remote consulting services may be provided at additional cost.

Device configuration

Trustwave transition engineers will work with the Client to verify that the Managed Device(s) are integrated into the Trustwave Platform, in a "supported state". This includes the following:

- Confirming any Product Updates required to the Managed Device(s) required to meet Trustwave's supported device requirements.
- The Managed Device(s) communicate with Trustwave Platform for log data collection, device management and control;
- An active secure connection between the Trustwave Platform and the Managed Device(s);
- Client has completed a comprehensive test plan to review all impacted Client systems associated with the Managed Device(s) and/or Managed service.

Device tuning

Transition engineers will review and work with the Client to tune and update the configured security policies, in the Managed Device(s) to an approved state for Trustwave standard operations, in accordance with the following criteria:

- If the device is new to the Client environment, the device will be configured in accordance with the initial provisioning process and then monitored to ensure correct operation of the Managed Device(s). Fine-tuning of rulesets will continue until steady state operation has been achieved.
- If the Managed Device(s) is an existing Client device and already configured based on the Client's existing policy, that policy will be monitored and recommendations made for fine-tuning.
- Once the configuration is optimized the baselining period ends and the Managed Device(s) are prepared for transition to Trustwave standard SOC operations, for monitoring and management.

TrustKeeper Client Portal

The TrustKeeper Client Portal provides access to features of the managed device services. The available features and functionality of the TrustKeeper Client Portal set out below may differ depending on the relevant Trustwave managed security service acquired by the Client. The TrustKeeper Portal allows clients to:

- Review current and historical security events and alerts of Client's Trustwave-monitored device(s);
- Create and track support tickets and status of Client change requests to equipment installed on Client's premises or within the Client's environment;
- Provides a method for the client to securely communicate with the Trustwave MSS Transition and SOC personnel and Access device configuration and status information;
- Allows for the access to Trustwave user guides and upload of documentation and security policies; and
- Track progress of the service rollout.

Trustwave responsibilities

Layer one – Customer facing service responsibilities:

- Navigate the Client through the provisioning process until the SOC has ongoing management control of the Managed Device(s).

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.

- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to the Managed Device(s) and operating environment as necessary to complete the provisioning process.
- Provide applicable user guides, introduce and review the Client's usage and understanding of the TrustKeeper Client Portal and implement the applicable support process and procedures and verify that client has access to portal.

Other provisioning and implementation responsibilities

- Supply and deliver the Managed Device(s) if applicable
- Create a Client account in the TrustKeeper Client Portal
- Assess, configure and baseline the Managed Device(s) based on information and instructions provided by Client.
- Verify the Managed Device(s) are:
    - functioning according to the service delivery design; and
    - are generating Log Data, Log Events and Log Alerts and is visible to the Trustwave Platform.

Client Responsibilities

- Accurately complete the Provisioning Questionnaire and respond to requests from the provisioning team when establishing contact and collecting the Provisioning Questionnaire.
- Make available an onsite resource capable of installation of the Managed Device(s) and troubleshooting and Client environment. Trustwave can provide onsite resources if Client is unable to perform this duty.
- Provide remote access to on premise infrastructure to accommodate configuration of any Managed Device(s).
- Provide appropriate credentialed access to Trustwave, to the Managed Device(s).
- Provide and maintain a secure connection between the Managed Device(s) and the Trustwave Platform, which is compatible with available Trustwave connection standards.
- Develop and complete a comprehensive test plan to review all impacted customer systems associated with the provisioned Managed Device(s) prior to commencement of the Managed Device(s) tuning activities referred to in this service description.
- Read and confirm the Client's understanding all provided user guides and documentation and participate in and confirm the Client's understanding of the processes explained during the welcome call.
- Procure valid licenses and maintenance contracts for Managed Client owned Device(s) and all relevant configuration data.
- Review Security Event and Security Alert activity in the TrustKeeper Client Portal;
- Adhere to Trustwave's recommended security practices with respect to the Device and service.
- The Client acknowledges that:
    - The Trustwave provisioning, management and threat analysis services are performed remotely. Any on-site provisioning or support services required by the Client would be acquired separately as a Trustwave consulting service;
    - Trustwave is not responsible for delays in provisioning due to delays or inaccurate Provisioning Questionnaire responses and Client provided information;
    - The consolidated features and functionality of the Device(s) may not include all of the functionality and features of equivalent standalone appliance or services.
    - Failure to implement and comply with Trustwave recommended security practices, may adversely impact the operation and functionality of the Managed Device(s) and the Managed Service.
    - It has made its own enquiries as to the available features and functionality of the Device(s) and the suitability of the Managed service to meet the Client's requirements.
    - Client will not have access to the Managed Device(s) unless otherwise specified.

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.