SERVICE DESCRIPTION

Managed Network Access Control (NAC)

Service Description

The Trustwave Managed Network Access Control (NAC) service provides managed network access control and monitoring of endpoint access to the Client's network. The Managed NAC service helps the Client manage their endpoint device assets and Client network integrity and assist the Client to maintain internal control and meet industry standard compliance requirements to meet.

The Managed NAC service consists of:

- **Service Provisioning** – the performance of remote activities required to establish the service within a steady state. Provisioning connects Managed NAC Device to the Trustwave Platform. The Managed NAC service includes the collection and assessment of the Client Initiation Information and the initial configuration of the Managed NAC Device(s).
- **Device Management** – the ongoing configuration of the Managed NAC Device(s), policies, rulesets, the management, maintenance, health monitoring and the implementation of Security Updates and Product Updates to, the Managed Enterprise Firewall Device(s). The Trustwave Security Operations Center (SOC) teams provide these services through globally located facilities.
- **Collection and Monitoring** – the collection and monitoring of Log Data to help identify unauthorized access or modification of the Client's network.

Base Features of Service

The Managed NAC service includes the following base service features;

- Supply and deployment of a NAC Device(s), 24 x 7 technical support for the Managed NAC Device(s);
- TrustKeeper Client Portal access providing Tracking of provisioning progress and 24x7 System Event reporting;
- Change and support requests creation and management.
- Implementation of Product Updates; and
- Reporting and access to Log Data.

Provisioning and Implementation

Implementation and delivery

The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with the Client to implement the Managed NAC Service. Please see the Trustwave Provisioning Guide for additional details on the service implementation.

Device and environment assessment

- Trustwave provisioning 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 and Trustwave confirmation with the Client of the Client's NAC system environment, policies and rulesets; and
- Assessment of the configuration of the Managed NAC Device(s) to determine if current version and features are consistent with Trustwave supported device requirements;

Device configuration

- Trustwave provisioning will work with the Client to verify that the Managed NAC Device(s) are integrated into the Trustwave Platform, in a "supported state", confirming any Product Updates required to the Managed NAC Device(s) required to meet Trustwave's supported device requirements;
- That the Managed NAC 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 NAC Device(s);
- Client has completed a comprehensive test plan to review all impacted Client systems associated with the Managed NAC Device(s) and/or Managed NAC service.

TrustKeeper Client Portal

The TrustKeeper Client Portal allows the Client to view security data providing a current security posture of the Client's environment to the extent possible with services provided by Trustwave. 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 security events and alerts of Client's Trustwave-monitored network(s), as well as historical data;
- Create and track support tickets and status of Client change requests to equipment installed on Client's premises or within the Client's environment; and
- Provides a method for the client to securely communicate with the Trustwave MSS provisioning and SOC personnel and Access device configuration and status information;
- Allows for the Upload documentation and security policies;
- Track Progress of the service rollout.

Trustwave Responsibilities

- Navigate the Client through the provisioning process until the SOC has ongoing management control of the Managed NAC Device(s).
- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to the Managed NAC Device(s) and operating environment as necessary to complete the provisioning process.
- Supply and deliver the Managed NAC Device(s) if applicable.
- Create a Client account in the TrustKeeper Client Portal and verify that client has access to portal.
- Assess, configure and baseline the Managed NAC Device(s) based on information and instructions provided by Client.
- 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.
- Verify thatThe Managed NAC Device(s) are functioning according to the service delivery design; and Managed NAC Device(s) is generating Log Data, Log Events and Log Alerts and 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 NAC Device(s) and troubleshooting and Client environment.
- Provide remote access to on premise infrastructure to accommodate configuration of any Managed NAC Device(s).
- Provide appropriate credentialed access to Trustwave, to the Managed NAC Device(s).
- Provide and maintain a secure connection between the Managed NAC 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 NAC Device(s) prior to commencement of the Managed NAC 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 NAC Device(s) and all relevant NAC 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 NAC 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 NAC 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 NAC Device(s) and the Managed NAC Service.
- It has made its own enquiries as to the available features and functionality of the NAC Device(s) and the suitability of the Managed NAC service to meet the Client's requirements.
- Client will not have access to the Managed NAC Device(s).

Device Management

- The Managed NAC service includes the configuration, health status and provision of Product Updates to Managed NAC Device(s). These management features ensure that the Managed NAC Device(s) are performing their function within the Client environment as designed.

Policy and Configuration Management

- Trustwave maintains an overall change control and configuration management procedure for the Managed NAC Device(s). Changes that could affect the operation of the Client systems are coordinated with appropriate Client contacts.
- Configuration change requests are made by the Client by the following methods:

  - **Trustwave Portal** – Policy contacts can make policy change requests through the TrustKeeper Client Portal specifying all details within the request. These requests are authenticated based on the pre-determined contact information.
  - **Telephone** – Policy contacts can make policy change requests by contacting the SOC and providing the security passphrase previously established.
  - **Email Request** – Policy change requests sent by email must be confirmed as being sent by authorised Client Personnel via phone confirmation or noted in the relevant Ticket.

Device Health and Status Monitoring

- The Trustwave SOC monitors Managed NAC Device(s) to detect when Managed NAC Device(s) are no longer showing as active on the Client's network and to monitor the version of firmware or software that is present on the Managed NAC Device(s). The Managed NAC Device(s) is considered the demarcation point for health monitoring, Client network devices connected to the Managed NAC Device(s) are not in scope for health monitoring.

Product Updates

- The SOC will monitor the availability of third party vendor Product Updates and apply those updates to the Managed NAC Device(s) and the Central Manager.
- Product Updates are assessed by the SOC to determine the priority of the update and the potential impact to the Managed NAC Device(s) and the related functionality associated with the changes provided in the update.
- When a Product Update becomes available, a Ticket will be created and assigned to the Client by the SOC; Product Updates available under the relevant valid Managed NAC Device(s) application license or maintenance contract will be scheduled with the Client for implementation;
- The SOC will give consideration to accommodate the Client's preferred maintenance window and apply threat protection features with the least disruption to the Managed NAC Device(s), as possible. The SOC will implement the relevant Product Updates within timeframe required depending on priority, to ensure that the Managed NAC Device(s)) are operating as designed.

Trustwave Responsibilities

- Maintain management connection to the Managed NAC Device(s). Monitor the Managed NAC Device(s) to ensure their active online status and that they are available.
- Notify Client within SLA timeframe if management connection is unavailable and cannot be restored by Trustwave.
- Manage the third party vendor support and maintenance contracts applicable to the Managed NAC Device(s) and Central Manager, to identify available Product Updates within timeframe required depending on the relevant update's priority.
- Provide remote assistance, support and configuration, in respect of any repaired or replaced Managed NAC Device(s).
- Attempt to resolve any connectivity or system issues identified in order to return the Managed NAC Device(s) to a steady state of operation.
- Create a Ticket and schedule the Product Update with the Client.

Client Responsibilities

- Inform Trustwave of all Client environment maintenance activity and changes that may impact on Trustwave's ability to provide the Managed NAC service, as designed.
- Provide, when necessary to Trustwave, technician, access to vendor portals to allow for software and license downloads and provide necessary authorisations for Trustwave to act on behalf of the Client for management and maintenance purposes.
- Access the TrustKeeper Client Portal, respond to Tickets and confirm scheduled implementation of Product Updates and Security Updates.
- When requested by Trustwave, provide onsite support, for the Managed Managed NAC Device(s)(s), to resolve connectivity or support issues.
- In relation to the RMA Process: Confirm delivery of an RMA Device, Perform the physical installation of an RMA Device; and Contact the SOC to arrange for Trustwave remote support and configuration of an RMA Device.

- Access the TrustKeeper Client Portal, respond to Tickets and confirm scheduled implementation of Product Updates.
- The Client acknowledges that the implementation of necessary Product Updates Update is not an optional feature of the Managed NAC service; and
- Failure to implement a required Product Update, may adversely impact the operation and functionality of the Managed NAC Device(s).

Collection & Monitoring

- Monitoring activities related to the Managed NAC Device(s) help identify unauthorized access or modifications of the system and help assist with internal control and compliance requirements. Log Data will be collected from the Managed NAC Device(s) and retained for a defined period of one year from the date of collection.

Log Data Retention

- Log Data is securely collected and stored at Trustwaves secure data centers. The Client can view System Events for forensic or maintenance purposes as follows:
    - Previous 30 days' worth of Log Data is available for immediate viewing through the TrustKeeper Client Portal
    - Up to the previous 90 days' worth of Log Data can be requested for viewing through the TrustKeeper Client Portal
    - Log Data older than 90 days and up to 1 calendar year is available in csv format, and accessed through the TrustKeeper Client Portal.

Change Management

- Trustwave maintains an overall change control and configuration management 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 that is used to support communication with the Client and its service contractors responsible for administration of its networks.
- The SOC will assesses and implements change requests submitted by the Client or SOC through the TrustKeeper Client Portal. All requests are evaluated to help ensure that they are aligned with the features included with the service and will not detrimentally impact the security of the Client environment. Typical change request for the Managed NAC Service are:
    - Configuration changes to the Managed NAC Device(s) as requested by authorized Client contact or a GTO analyst in response to a known threat.
    - Change reversals as requested by an authorized Client contact.

Trustwave Responsibilities

- Allow authorized Client personnel to submit Security Incidents through the TrustKeeper Client Portal, as needed. Determine whether the request is in-scope with the terms of the Service.
- Perform change management activities when requested and in compliance with Trustwave policies.

- Validate that the request was submitted by an authorized Client contact, and notify Client if validation is not successful.
- 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. Confirm Client approval to implement the change request after reviewing risk assessment results with Client.
- Confirm Client acceptance of implemented changes.
- When authorized Client personnel request that Trustwave roll back or reverse a change request:
    - Confirm receipt of Client's request for a change reversal.
    - Confirm completion of the change rollback upon successful execution of change reversal activities.
    - Execute joint testing with Client to validate the rollback is aligned to Client's request, and gain Client confirmation of the same.
    - Update the change request with information on rollback changes.
    - Notify Client a change request is outside the scope of the service and or if additional charges will apply to a change request.

Client Responsibilities

- Nominate Client Personnel authorised to request and or approve configuration and security policy changes and nominate other authorised Client Personnel.
- Submit change requests using the TrustKeeper Client Portal.
- Where the Client does not agree with a Security Incident priority, submit a change management request to change the priority of the relevant Security Incident.
- Provide Trustwave with requested information in a reasonable timeframe.
- Provide resources to review the risk assessment relating to requested changes.
- Review, assess and notify Trustwave of approval or non-approval to a proposed change request.
- When required, authorized Client personnel may request that Trustwave roll back or reverse a change request.
- Submit reversal requests using the TrustKeeper Client Portal, emailing or phoning the Trustwave support team.
- Provide resources to execute joint testing and confirm the change reversal is aligned with the Client-submitted request.
- Confirm completion of the change rollback request.
- The Client acknowledges that change requests that exceed two (2) man days of effort is deemed a project and is subject to acceptance by the Client of separately quoted additional charges.