SERVICE DESCRIPTION

Managed Security and Compliance (MSC)

Trustwave Managed Compliance Security Services for Hospitality and Retail

Through packaged bundles designed specifically for the demands of the hospitality industry, we make easy for you to address PCI compliance and security without disrupting your focus. Whether you need basic validation services or full network security management with connectivity services, we deliver security the way you want it.

Trustwave Managed Security and Compliance Security Plus Package

Service Description

Trustwave helps you remove the heavy lifting of securing your business and improve the way you achieve and maintain compliance across all your locations. Our Security Plus package delivers the technologies you need to help protect your sensitive data from threats, combined with 24x7x365 expert management and support, and cloud-based management tools. The Unified Threat Management device (UTM) is the foundation of our comprehensive security structure, which assists in securing your business by helping you protect your network against growing and evolving threats.

There are four (4) components that can make up a Managed Security and Compliance (MSC) Security Plus Package

- Security Plus (Managed UTM with the TrustKeeper Portal)
- Compliance Suite
- WiFi Suite
- Endpoint Protection Suite

The Core Service is Security Plus:

- Managed UTM service:
  - Intrusion Prevention System
  - Gateway Anti-Virus / Anti-Spam
  - Centralized logging and reporting
  - Content-based Web Filtering
  - Whitelist Services
- 2FA Remote Access Control (one license per site)

- Site-to-site VPN (One license per site)
- Active UTM Service Subscription and Warranty contract for the term of the Service
- TrustKeeper Portal.

Compliance Suite Option adds:

- Quarterly External and Internal Vulnerability Scans (2 IP's each)
- SAQ Wizard in Portal
- PCI Training in Portal
- $100,000 in Breach Coverage.

WiFi Suite Option adds:

- Secured Client/Guest Wireless (4 SSIDs)
- Family-friendly Category Filtering
- Business First Priority Bandwidth Protection
- Branded Disclaimer Page
- Wireless Access Point Detection.
- A WiFi Access Point the expand WiFi coverage (FortiGate UTM's only) is also an add-on option.

Endpoint Protection Suite Option adds:

- File Integrity Monitoring (FIM)
- Security Health Check & Security Configuration
- Credit Card Data Scanner (DLP)
- Unauthorized Device Monitor
- IP Beacon
- Trustwave AV Option

Connectivity Service Options

Optional high-speed Internet connectivity services for locations are also available. Selecting a connectivity option is not required. Trustwave can work with most ISP providers (except SATCOM). Trustwave connectivity services can be added later if a Client decides to consolidate services with Trustwave.

- **Managed Wired Broadband1**

  Primary Internet connectivity using a broadband service that is managed proactively monitored and supported by Trustwave. (DSL or Cable only)

- **Broadband Management Services**

  The client will retain their current broadband supplier and billing responsibility and Trustwave will act as 1st Line Support and manage all network gateways via UTM and ensure internet connectivity with the broadband router.

- **4G Backup Cellular Broadband**

  Standalone backup Internet service using 4G cellular wireless technology that is used if primary broadband service fails. 3G availability is restricted as most service provides are eliminating their 3G networks. Trustwave no longer offers 3G services on new contracts.

[1]Trustwave Telecom Team will need the addresses of the locations to determine which ISP can provide services in the location.

The Security Plus Service provides monitoring and support 24x7x365 for the managed device and compliance programs. The TrustKeeper Client Portal provides secure easy access to your business information from anywhere with two-factor authentication options. The availability of a record of attack events and subsequent analysis assists the Client in meeting its internal control and compliance requirements. While the service features are designed to assist in meeting compliance requirements, it is not a guarantee that the Client is compliant.

The Security Plus service consists of:

- Service Provisioning – the performance of remote activities required to establish the service within a steady state. Provisioning connects the UTM device(s) to the Trustwave Platform and the features and functionality of the System Management and includes the collection and assessment of the Client Provisioning Questionnaire and the initial configuration of the UTM device(s).
- System Management – the ongoing configuration of the UTM device(s), policies, rulesets, the management, maintenance, health monitoring and the implementation of Security Updates and Product Updates to, the UTM device(s). The Trustwave Security Operations Center (SOC) teams provide these services through globally located facilities.
- Log Collection and Monitoring – UTM, and other applicable audit and security logs are collected, processed, stored and displayed in the TrustKeeper Portal. Client has the option to add any of the Trustwave SIEM Security and Compliance Monitoring services to a MSC package. Those options are outlined in this SOW.

The Security Plus Service includes the following basic service features:

- TrustKeeper Client Portal access providing:
    - Tracking of provisioning progress;
    - 24x7 security event reporting;
    - Change and Support requests creation and management; and
    - Notifications and Security Incident management;
- Supply and Delivery of UTM device(s);
- UTM services turned on-AV/Anti-Spam/IPS;
- Initial Baselining and Tuning of the UTM device(s), policies and rulesets based on Client input;
- 24x7 Log collection and storage;
- If required, Configuration of encrypted communication links. Support provided for both Site-to-Site connections and Remote User VPN Clients. Support for one (1) site-to-site (S2S) VPN connection included.
- If required, Configuration of one (1) local network DMZ segments included.
- Firewall configuration report as available via the UTM.
- The management, maintenance and provision of technical support assistance, for supported UTM device(s) and features.
- A Trustwave Log Relay appliance (TS25) may be included in SOW to collect and forward logs from non-Trustwave UTM's to the TrustKeeper Portal.

Supply & Management models

The UTM Device(s) are managed from a cloud-based infrastructure. UTM Management infrastructures are hosted and maintained by Trustwave within Trustwave data centers.

Client Access Model

The UTM Management Console is not accessible by the Client. The Trustwave SOC has sole access to the managed UTM on site. The Client will have no access to the UTM Configuration, Policies or settings through the UTM Management Console.

Provisioning and Implementation

The provisioning and Implementation teams are the Client's first point of interaction with Trustwave after the contract is executed. Implementation services are provided for remote or onsite implementation assistance depending on the options chosen with this Service.

Service introductions and information gathering

Trustwave provisioning, assurance and delivery teams are assigned to implement and facilitate the successful configuration and rollout of the Security Plus service, which includes the following actions:

- Send an introduction email to the Client providing guidance on how to provide the necessary Client Provisioning Questionnaire prior to a remote kick-off meeting.
- Contact the Client to establish and schedule the timing of the remote kick-off meeting; and.
- Remotely create an instance for, and establish the Client within, the TrustKeeper Client Portal.

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 Provisioning Questionnaire provided;
- Assessment of the provided information and available network diagrams to confirm:
    - UTM placement in network is appropriate
    - Access to the UTM will be available to enable SOC management
    - Client is assigned the appropriate services within the TrustKeeper Portal
- Presentation and confirmation with the Client of:
    - Client's UTM environment, policies and rulesets;
    - Placement and configuration of the UTM device(s); and
    - Services configured in the TrustKeeper Portal are the services the Client has requested as part of this Service.

Managed Device Client Contacts

Client contacts are collected during provisioning and retained to facilitate the change control process for all managed network devices as well as the appropriate notification. The TrustKeeper Portal provides levels of access that can be leveraged by clients if needed to delegate levels of access and responsibility within the organization.

Policy Contact – The policy contact is authorized to make configuration change requests. Policy and configuration changes will not be made on CPE devices unless a client policy contact has authorized the request

in writing or directly through a live conversation with an authorized SOC analyst. These contacts are also able to designate other levels of contacts within their organization. The Policy Contact is authorized to:

- Request and approve device configuration and security policy changes
- Delegate others within the client organization as technical or security contacts

Technical Contact – The technical contact is someone who the SOC analysts will collaborate with regarding the resolution of any technical issues that occur. The technical contact is authorized to:

- Interact with provisioning and SOC analysts to ensure device health, accessibility and availability on the network.
- Interact when necessary during device maintenance or other network related maintenance that could disrupt the availability and effectiveness of the network device.
- Submit support requests or respond to Trustwave initiated support request for the purposes of remediating technical matters with the managed device.

Implementation and delivery

The implementation team is responsible for working with Client to:

- Review and analyze the Client Provisioning Questionnaire;
- Configure the UTM 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 Security Plus Service; and
- Coordinate the provisioning and implementation the UTM Device(s) into the Client's production environment so that the services can be handed over to the SOC for on-going management, maintenance and support.
- Coordinate the provisioning and implementation the Compliance Suite, WiFi Suite or Endpoint Suite if selected by the Client.

The Security Plus service is deemed delivered and operational when:

- SOC has management control of the UTM device(s)
- SOC is able to view the UTM device(s); and
- Client has access to the TrustKeeper Client Portal to view event data, logs and reports.
- Client has access to the Trustwave Compliance, WiFi Suite services, if selected by Client, within the TrustKeeper Client Portal.
- Client has access to the Trustwave Endpoint Protection Agent software from within the TrustKeeper Client Portal if selected by the Client.

Device configuration

Trustwave provisioning will work with Client to verify that the UTM device(s) are integrated into the Trustwave Platform, in a "supported state", confirming:

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

Device baselining

The Provisioning Team will monitor, review and work with the Client to tune and update the configured security policies, in the UTM device(s) to an approved state for Trustwave standard operations, in accordance with the following criteria:

- If the Trustwave UTM is new to the Client environment, the device will be configured to meet the standard Trustwave Gold Configuration. Trustwave will work with the Client on requests for specific policies, whitelist and prevention events to be blocked and the UTM configuration will be updated. Any prevention rules that block traffic will require approval from the authorized Client contact before those rules are made active;
- If the device is an existing Trustwave UTM, and is being upgraded to a newer Trustwave UTM, Trustwave will apply the existing UTM configuration and policies. Any additional changes to the existing configuration will require approval from the authorized Client contact; and
- Once the configuration is optimized, the baselining period ends and the UTM device(s) are prepared for transitioned to Trustwave standard SOC operations, for monitoring and management.

SOC Welcome call

The Trustwave provisioning team will implement the SOC Welcome Call and complete the following actions:

- Schedule a welcome call with the Client.
- During that call introduce the Client to the TrustKeeper Client Portal ensuring that the Client understands how to access and use the services purchased.
- Review the Client's TrustKeeper Client Portal usage understanding including the following actions:
    - Creating change and support requests;
    - Accessing and modifying support tickets;
    - Reviewing available reports and security information;
    - Modifying permissions for other TrustKeeper Client Portal users as appropriate or available to the Client;
    - How to access and leverage applicable applications within the TrustKeeper Client Portal; and
    - How to upload or access documents available for Client.

TrustKeeper Client Portal

The TrustKeeper Client Portal provides the Client with access to the expertise of the SOC staff, security information and analysis and the Trustwave Platform. 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 Client Portal includes the following:

- Designated Client contact information;
- Track progress of the service rollout;
- Provides a method for the Client to securely communicate with the Trustwave MSS provisioning and SOC personnel;
- Access device configuration and status information;
- Security software (such as the TrustKeeper Agent) if applicable to the relevant Trustwave service;
- Upload documentation and security policies;

- View security data and other security related data providing a current security posture of the Clients environment to the extent possible with services provided by Trustwave;
- Review current security events and Security Alerts of Client's Trustwave-monitored network(s), as well as historical data;
- Review and track status of Client change requests to equipment installed on Client's premises or within the Client's environment; and
- Create and track support tickets.

Trustwave responsibilities

- Establish and maintain contact with the Client and navigate the Client through the provisioning process until the UTM device(s) transition to SOC for on-going management, maintenance and support.
- Request and collect initial information provisioning questionnaire from Client
- Initiate provisioning activities with Client and collect, review and assess the necessary information relating to the UTM infrastructure and operating environment as necessary to complete the provisioning process.
- Assess, configure and baseline the UTM device(s) based on information and instructions provided by Client.
- Provide applicable user guides, introduce and review the Clients usage and understanding of the TrustKeeper Client Portal and implement the applicable support process and procedures.
- Verify that:
    - The UTM device(s) are functioning according to the service delivery design; and
    - The UTM device(s) and the management and security event collection are active within the Trustwave Platform.

Client responsibilities

- Respond to requests from the provisioning team when establishing contact and collecting the Client Provisioning Questionnaire.
- Accurately complete the provisioning questionnaire.
- Make available an onsite resource capable of installation and troubleshooting of the UTM.
- Provide remote access to on premise infrastructure to accommodate installation and configuration of any UTM device(s).
- Provide appropriate credentialed access to Trustwave, to the managed UTM device(s) and the Client's environment where applicable, that is compatible with available Trustwave connection standards.
- Develop and complete a comprehensive test plan to review all impacted customer systems associated with the provisioned UTM devices prior to commencement of the Device Baselining activities referred to in this service description.
- Read and confirm the understanding of all provided user guides and documentation.
- Participate in and confirm the understanding of the processes explained during the welcome call.
- Acknowledges that:
    - Trustwave provisioning, management and SIEM 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 Client Provisioning Questionnaire
    - Implement Trustwave's recommended security practices regarding the Service and UTM.

System Management

The Security Plus Service includes the configuration, health monitoring and provisioning of Product Updates to the Trustwave Managed UTM device(s). These management features ensure that the UTM device(s) are performing their function within the Client environment as designed.

The Trustwave SOC managed the UTM device(s) to:

- Ensure that the UTM device(s) are active;
- Track the version of firmware or software that is active on the UTM device(s); and
- Apply Product Updates and Security Updates to the UTM device(s) and the Trustwave Platform.

Health Status Monitoring

The health status monitoring feature of the Security Plus Service, monitors the network availability of the UTM device(s) to ensure it they are available on the network and/or to the Trustwave Platform.

- UTM device(s) are monitored to detect when these devices are no longer showing as active within the Client's environment. This includes Initial steps taken to assess the cause of the offline status of the relevant device and remediate the issue if possible;
- SOC analysts will contact the Client's technical contact or other designated contact to notify the Client if remediation steps available to Trustwave are not successful;
- Notifications sent to the Client regarding the device status will be provided within the time requirements specified in the SLA.
- Analyst will initiate the device Trustwave RMA process when it has been determined the UTM device must be replaced.
    - Analysts will coordinate the shipment of the Trustwave Owned replacement device and request the return of the RMA'ed device.
    - If the device is Client owned, then Trustwave analyst will work with Client contacts to initiate the Client owned RMA process.

Product, Security and Ruleset Updates

The Trustwave SOC will monitor the availability of Product Updates and Security Updates and apply those updates to the managed UTM device(s).

- Product Updates, Security Updates and rule updates are assessed by the SOC to determine the priority of the update and the potential impact to the managed UTM device(s) and the related functionality associated with the changes provided in the update;
- When Product Update, Security Updates becomes available, a Security Plus Service Ticket will be created and assigned to the Client by the Trustwave SOC;
- Product Updates and Security Updates available will be scheduled with the Client for implementation;
- Trustwave SOC will give consideration to accommodate the Client's preferred maintenance window and apply any threat protection features with the least disruption to the UTM, as possible. The Trustwave SOC will implement the relevant Product Updates and Security Updates within timeframe required depending on priority, to ensure that the UTM device(s) are operating, and the Security Plus Service is provided, as designed;
- Security and Product Updates

- All Security Updates and Product updates for UTM software and underlining OS will be completed during any Version upgrades
- Bug fixes will be applied as Product Updates to the UTM only when applicable to that device

Trustwave responsibilities

- Maintain management connection to the UTM
- Monitor the UTM 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
- Coordinate and facilitate the device RMA process.
- Apply Security Updates, Product Updates as they become available and are applicable to UTM device(s) and within timeframe required depending on the relevant update's priority.
- Create a Security Plus Service Ticket and schedule the Product Update, Security Update with the Client.
- Attempt to resolve connectivity or system issues identified in order to return the device to a steady state of operation.
- Where applicable, notifying the Client if a High Availability UTM device has been brought online as part of a support ticket associated with the offline primary device.

Client responsibilities

- Internet connectivity to the UTM's must be maintained for Trustwave to provide Services.
- Inform Trustwave of all Client environment maintenance activity and changes that may impact on Trustwave's ability to provide the Security Plus Service, as designed.
- Submit changes in accordance with the change management process and use and access the TrustKeeper Client Portal to log tickets, receive notifications, schedule updates and view, download and track the status of and respond to, Security Alerts and Security Incidents.
- When requested by Trustwave, provide remote support, for the UTM device(s), to resolve connectivity or support issues.
- If UTM device has been RMA'ed, return the defective device to Trustwave within seven (7) days of receipt of the replacement UTM device.
- The Client acknowledges that:
    - The implementation of necessary Product Updates Security Update or rule update, is not an optional feature of the Security Plus Service; and
    - Failure to allow the implementation of a required Product Update, Security Update or rule update as required, may adversely impact the operation and functionality of the UTM and the Clients network security.
    - Implement Trustwave's recommended security practices regarding the Service and UTM.

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 assesses and implements change requests submitted by the Client to the 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 Security Plus Service are:

- Configuration changes to the UTM device(s) as requested by authorized Client contact or a Threat Analyst in response to a known threat.
- Change reversals as requested by an authorized Client contact.
- Policy and configuration management processes may differ slightly depending on the technology and device being managed. All Configuration change requests are made in the Trustwave Portal.
- Trustwave Portal – Authorized Policy contacts must make any change requests through the portal specifying all details within the request. These requests are authenticated based on portal authentication and processed in accordance with the service SLA.

Trustwave Responsibilities

- 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.
- Determine whether the request is in-scope with 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 and risk.
- 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 if additional charges will apply or if the change request is outside the scope of the Service.

Client Responsibilities:

- Submit change requests using the TrustKeeper Client Portal.
- Provide Trustwave with requested information in the Ticket opened in the Portal.
- Provide resources to review's risk assessment of the 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 will be deemed a project and will be executed as a separate project.

UTM Log Collection

Reporting

UTM logs are collected, processed, stored and displayed in the TrustKeeper Portal. Trustwave Platform receives security events from the UTM device(s) and other potential sources as part of the Security Plus Service. These security events are included within reports available in the TrustKeeper Client Portal as follows:

- 105 days of security events in the security activity page of the TrustKeeper Client Portal
- 2 weeks of all events
- All Logs are stored for 1 year
- All events can be exported to a csv file for use outside of the portal.

Trustwave Responsibilities:

- Provide Client access to UTM logs in the TrustKeeper Portal and Security Incident reports.

Client Responsibilities

View available Logs and reports through the TrustKeeper Client Portal.

Log Collection approach

The Managed Trustwave UTM will forward encrypted logs to the SIEM system for processing. A Managed FortiGate UTM will have a management VPN established and will forward logs over the VPN to the SIEM system for processing. Logs from Workstations will require the Endpoint Protection Suite Agent.

Optional MSC Security Plus Features

Optional features are available to the base Security Plus service described in the above sections of this Service for additional fees. Some options may require an independent Service Description, which provides a more detailed description of the services provided within the option.

Trustwave UTM: Cold Spare Option

Trustwave's Managed UTM and MSC service offers a Cold Spare support option to help reduce down-time and operational interruptions due to the failure of a single, primary UTM device. The Cold Spare UTM appliance is configured with a generic configuration until such time it is needed and then the specific configuration for the down location will be remotely installed by Trustwave SOC personnel. See Cold Spare Installation paragraph below.

Cold Spare Storage and Security

Trustwave Cold Spare UTMs are the property of Trustwave and as such the Client is responsible for ensuring that all appliances are stored in appropriate environmental conditions for computer-based equipment and are expected to be secured in a locked room or storage locker that has restricted access.

Trustwave is not responsible for Cold Spares that are lost or stolen or were not stored and secured properly.

Trustwave will provide the Client with the price to replace a lost or stolen UTM Cold Spare.

Cold Spare Installation

- **Notify Trustwave Support:** The Cold Spare, if it will be a general Cold Spare that could go to any number of multiple sites, will not have the unique site UTM configuration loaded and, as a result, will not work if installed with the generic Trustwave configuration. Trustwave Support must be informed prior to the installation of a Cold Spare. If the Cold Spare is for one designated site, then the initial base site configuration will be installed. However, the configuration must be updated to the most current configuration supported by Trustwave Support and the Trustwave Support Operations must be informed prior to the installation of this Cold Spare. Client will need to provide the location address in need of the cold spare and coordinate a time with Trustwave to perform the remote site configuration installation/update. Installation and use of a Cold Spare, without contacting Trustwave Support, can lead to a security breach of the network and will void the Trustwave Breach Coverage. Trustwave assumes no Liability in this situation.

Return of Trustwave UTM: Client will be required to ship the original UTM back to Trustwave within 30 days or an additional monthly charge will be billed to the account. Shipping instructions will be provided by Trustwave Support.

Platform Replacement: The Trustwave MSS 24 hr. Platform Replacement SLA does not apply to the installation of the Cold Spare hardware. The Cold Spare replacement/installation time will be determined by the Client and when the Client calls Trustwave Support to coordinate a time with Trustwave to perform the remote site configuration installation. Once the coordination call occurs, Trustwave will make commercially reasonable efforts to set up the Cold Spare UTM within 24 hours of the call. The Trustwave MSS 24 hr. Replacement of the Cold Spare that was utilized will occur NLT 10 business days.

Security and Compliance Monitoring Options

Service Description

Trustwave's Security Plus service includes basic log collection and monitoring service that provides for the collection, monitoring and storage of UTM Log Data. Log data is available in the Clients TrustKeeper Portal. Clients can add one of the three (3) Security and Compliance monitoring options to provide additional log alerting and analysis.

Cloud Log Monitoring Option

Overview

Cloud Log Monitoring includes the above services and the following features:

- Collection of selected Log Data on the Trustwave Platform;
- Automated notifications via email of Alerts detected by automated threat detection rules. These rules will analyze collected data in real time and when threats are detected Alerts are created and the Client notified via email. Use cases may include but are not limited to:
  - account lockout events
  - failed administrator authentication events
  - filesystem full events
  - filesystem nearing full events
  - reboot events
  - shutdown events

- audit trail cleared events
- account privileges modification events
- time sync error events
- network traffic anomaly events
- audit system error events
- brute force authentication attempt events
- configuration change events
- security audit trail cleared events
- escalation of high priority IDS/IPS events
- multiple suspected attacks from same source
- multiple suspected attacks to same target
- failed login (same user) on many hosts
- recurring operational errors
- source-specific escalations by event ID
- source or target is in Known Bad Actor watchlist

Trustwave's Threat Detection rules are managed by an internal Content Team and are under continuous improvement and integration. Rules may vary by service level. The above list is a subset and example set. Actual rules in production are subject to change.

- 24x7 access to reports and interactive search functionality for Events and Alerts through the TrustKeeper Client Portal;
- 1-year offline storage of Log Data
- Monthly and Quarterly Event, Security Alert and Incident Summary Reports.

Trustwave responsibilities

- Collect and Monitor Log Data via the Trustwave Platform via automated processes; Review Security Events collected by the Collector(s) and help in identification of potential Security Alerts via automated processes;
- Maintain availability of Events and Security Alerts in the TrustKeeper Client Portal. Generate and publish the relevant reports to the TrustKeeper Client Portal.
- Generate automatic notifications of Security Alerts via email;

Client Responsibilities

- Review Security Event and Security Alert activity in the TrustKeeper Client Portal. Review reports published to the TrustKeeper Client Portal.
- Notify Trustwave if Events or relevant reports are not available in the TrustKeeper Client Portal, as expected.

Managed Compliance Monitoring Service Option

Managed Compliance Monitoring is a base service feature option, which may be selected by the Client and includes the following features:

- Cloud Log Monitoring services as referred to in the previous clause of this service description;

- Trustwave analyst review of Log Data for compliance-related activity on a daily basis. Trustwave's Security Operations Center (SOC) will review the Data Logs on a periodic basis and at least one time per day notify Client as per the agreed escalation procedures, generally an Incident in the Trustkeeper Client Portal.
- 24X7 access to email support;
- Daily, Monthly and Quarterly Reports.

Trustwave Responsibilities

- Collect and Monitor Log Data via the Trustwave Platform via automated processes;
- Review Security Events collected by the Collector(s) and help in identification of potential Security Alerts via automated processes and via periodic review by human analysis;
- Create Incidents and notify Client when security concerns are detected during periodic review.
- Maintain availability of Events and Security Alerts in the TrustKeeper Client Portal. Generate and publish the relevant reports to the TrustKeeper Client Portal.
- Generate automatic notifications of Security Alerts via the TrustKeeper Client Portal.

Client Responsibilities

- Review Security Event and Security Alert activity in the TrustKeeper Client Portal. Review reports published to the TrustKeeper Client Portal.
- Notify Trustwave if Events or relevant reports are not available in the TrustKeeper Client Portal, as expected.

Managed Threat Detection Option

Managed Threat Analysis and investigation is a base service feature option, which may be selected by the Client and includes the following features. The services will only be performed on the contracted in-scope components of the Client's network.

- Cloud Log Monitoring and Managed Compliance Monitoring services as referred to in the previous clause of this service description;
- Collection, correlation and analysis of Log Data from the in-scope components of the Client's network as defined in the contracted scope of work on the Trustwave Platform.
- 24x7 access to reports and interactive search functionality through the TrustKeeper Client Portal, 24x7 telephone support;
- Automated notifications via email of Alerts detected by automated threat detection rules;
- Monitoring and Security Event and Alert notification by the Global Threat Operations team in accordance with the pre-defined escalation procedures set out below; Classification of Security Incidents by GTO analysts;
- 1-year offline storage of Log Data;
- Daily, Monthly and Quarterly Incident Summary Reports.

Trustwave Responsibilities

- Collect and Monitor Log Data via the Trustwave Platform via automated processes; Review Security Events collected by the Collector(s) and help in identification of potential Security Alerts via automated processes;
- Maintain availability of Events and Security Alerts in the TrustKeeper Client Portal. Generate and publish the relevant reports to the TrustKeeper Client Portal.
- Generate notifications of Security Alerts via the TrustKeeper Client Portal.

Client Responsibilities

- Review Security Event and Security Alert activity in the TrustKeeper Client Portal.
- Review reports published to the TrustKeeper Client Portal. Notify Trustwave if Events or relevant reports are not available in the TrustKeeper Client Portal, as expected.

Reporting and data access

The Security and Compliance Monitoring services include the following available self-service reporting features accessed through the TrustKeeper Client Portal:

- Pre-defined reports grouped by device type and/or common compliance guideline;
- Interactive searches: pre-defined filters to assist in searching for Events and Security Events;
- Security Alert notifications: automated Security Event notification by email, as configured;
- 7 days of Events in the security activity page of the TrustKeeper Client Portal;
- Where applicable, 105 days of Security Alerts in the security activity page of the TrustKeeper Client Portal.
- Upon Client request, 12 months of Log Data in csv format, which can be accessed securely through the TrustKeeper Client Portal.

Threat Detection

Trustwave's proprietary threat analysis engine considers client log data and Trustwave and client security and infrastructure information to help identify potential indicators of security attacks and attempts to compromise a Client's network environment.

- Automated analytics are applied to the Security Events sent to the Trustwave Platform by the Collector(s). Based on threat intelligence and correlation rules within the Trustwave analytics engine, a Security Alert is created, and a level of importance is allocated to each;
- Security Alerts that have been escalated by the automated threat analysis engine, are reported on independently within the TrustKeeper Client Portal.
- Sources subscribed to Managed Compliance Monitoring will be subject to periodic review by the Trustwave Global Threat Operations team of security analysts, monitoring for security and compliance concerns. Discovered threats will be escalated to the customer via Incidents in the Trustkeeper Portal.
- Sources subscribed to Managed Threat Analysis receive additional ongoing real-time monitoring and analysis by the Trustwave Global Threat Operations team of security analysts. Discovered threats will be escalated to the customer via Incidents in the Trustkeeper Portal.

NAC on UTM Option

The support for the NAC on UTM option is only available with the Trustwave UTM (TS25 or TS151) and the features below may vary depending on the vendor solution chosen.

- The add-on Network Access Control (NAC)-based service feature of the Managed UTM service provides detection assistance, alerting and optional blocking support of unauthorized (aka "Rogue") devices that attempt to connect to target Client's network segments.
- The feature does not require separate support hardware installation (e.g. wireless card, separate device) at additional cost.
- NAC on UTM supports both wireless and wired device and network services detection assistance for the following:
  - Rogue Device
  - Device-based registration of discovered known devices
  - Alert on and/or block new, unknown devices

- Rogue Gateway
- Unique mechanism for detecting devices acting as routers (wired or wireless)
- Alert on and/or block rogue gateways
- Rogue Services
- Fingerprint OS and service ports on known devices
- Alert on and/or block if a known device opens a new port

Trustwave responsibilities

- Provide NAC related reporting within the TrustKeeper Portal.
- Configure NAC feature based on customer information provided

Client responsibilities

- Provide Trustwave with the accurate information required to identify the authorized devices within the environment. Ensuring the authorized devices have access to the network is essential in identifying unauthorized systems and helping to protect the Client network.
- Implement Trustwave's recommended security practices regarding the Service and UTM.

High Availability Management

Trustwave's Managed UTM service offers a High Availability (HA) failover support option to help reduce availability and operation interruption due to the failure of a single, primary UTM device. Trustwave will configure the UTM's as a HA pair if this option is selected by Client. Trustwave supports an Active/Passive configuration. One active primary device is backed up by a standby or passive secondary device. The failover process is set to be automatic based on state syncing and heartbeat communication between the primary and secondary units that comprise the HA pair. Recovery back to the primary is also set to automate once the designated primary device becomes visible to the secondary device. 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.
- Hardware Support: The UTM HA configuration is based on a pair of identically configured Client UTM appliances, one assuming the role of the active primary and the other the role of the passive secondary. Trustwave can only support the functions that are part of the UTM specifications.
- One-to-One Support: The HA configuration supports communication between one primary and one secondary device. The devices are not peers in this configuration. The secondary appliance does not process network traffic when it is operating in a secondary state.
- Single Entity: The HA pair appears as a single UTM resource to the network, with the primary objective of preserving protective firewall state.

Trustwave responsibilities

Monitor and update HA devices with Product Updates and Security Updates.

UTM Upgrade Option

Clients may choose to upgrade the base Security Plus UTM model (TS25 or FortiGate 60D) for an additional cost to accommodate their more complex network requirements. The Trustwave TS 150 or the FortiGate 100D are the available models. Trustwave will work with Client to define the needs/requirements for the upgraded UTM.

Compliance Suite

The following options are included within the Compliance Suite.

External Vulnerability Scanning

As an Approved Scanning Vendor, Trustwave performs certified quarterly external vulnerability scans to help address PCI requirements and provide critical information regarding potential network security concerns. If required to perform scanning of card-processing environment, the Trustwave proprietary scanning engine becomes an integral component of your compliance process. The activities and Client/Trustwave responsibilities are within the External Vulnerability Scanning service description and are not specified in this service description.

The EVS service consists of:

- Discovery, which is the information gathering and discovery process to understand the Client's System Target(s) and the scope of the required scanning of those targets.
- Scanning helps to identify potential vulnerabilities or weak configurations of the Clients System Target(s).
- Reporting is the provision of results of the Client Target System(s) scans, as a completed report available through the TrustKeeper Client Portal.

Base Features

Basic service features overview

The EVS service includes the following basic service features:

TrustKeeper Client Portal access providing:

- Tracking of provisioning progress
- EVS portal account subscription
- Client Target System entry
- Change management and support requests creation and response
- Reporting

Discovery

During this phase the Client information is collected, and a port scan of the Client's network is completed.

Scanning

Unlimited self-service scans during the EVS Scan Period, based on the predefined Scan Profile selected by the Client is performed on the Client's Target System(s).

Reporting

Predefined reports are available through the TrustKeeper Client Portal, including PCI DSS reports for compliance.

Internal Vulnerability Scanning

Trustwave provides quarterly internal vulnerability scanning to help secure the internal network by proactively identifying weaknesses within your internal network environment. With a Trustwave UTM, IVS software is on the UTM and scanning takes place on the internal segments of the network rather than from the external side of the UTM device. With the selection of a Trustwave FortiGate UTM, IVS scanning will be done down the management VPN set up on the UTM. The activities and Client/Trustwave responsibilities are within the Internal Vulnerability Scanning service description and are not specified in this service description.

The IVS service consists of:

- Discovery, which is the information gathering and discovery process to understand the Client's System Target(s) and the scope of the required scanning of those targets.
- Scanning helps identify potential vulnerabilities or weak configurations of the Clients System Target(s).
- Reporting is the provision of results of the Client Target System(s) scans, as a completed report available through the TrustKeeper Client Portal.

Base Features

Basic Service Features Overview

The IVS service includes the following basic service features:

TrustKeeper Client Portal access providing:

- Tracking of provisioning progress
- IVS portal account subscription
- Client Target System entry
- Change management and support requests creation and response
- Reporting

Trustwave IVS Appliance

The Trustwave UTM acts as the IVS Scanner for use in the Client's Target System(s). With a FortiGate UTM, IVS scans are done down the management VPN.

Discovery

During this phase the Client information is collected, and a port scan of the Client's network is completed.

Scanning

Unlimited self-service scans during the IVS Scan Period, based on the predefined Scan Profile selected by the Client is performed on the Client's Target System(s).

Reporting

Predefined reports are available through the TrustKeeper Client Portal.

Self-Assessment Questionnaire (SAQ)

Trustwave provides a PCI SAQ Wizard in the TrustKeeper Portal to simplify the process of filling out the correct SAQ for submission to the Card processor. Assistance with correctly filling in the questionnaire is available through SOC support analysts. The SAQ is a required document for completion of the PCI submission and compliance requirements.

Information Security Policy

Establish security best practices for your business with the help of our information security policy template. Having a security policy in place is a requirement of PCI. The Trustwave information security policy template allows the Client to have a framework that they can use to incorporate the security policy information that is unique to their environment.

Security Awareness and PCI Compliance Training

Trustwave provides PCI education for employees on credit card security procedures with PCI training module in the TrustKeeper Portal. Having a security training program is a requirement for PCI compliance. The security awareness training is provided through the Trustkeeper Portal making the availability and tracking of the delivery of the training material easy for Clients to help achieve compliance with this PCI requirement.

Wi-Fi Suite

The support for the Wi-Fi option and the features below may vary depending on the vendor solution chosen. The Wi-Fi suite provides the following features:

- **Wi-Fi Hotspot:** Provides customers easy wireless Internet access while keeping business communications and credit card transactions secure. Service features include up to four (4) multiple SSIDs, family-friendly category filtering and a custom guest disclaimer page.
- **Wireless Access Point Detection**: Through regular scanning of the wireless network, wireless access points can be detected. In order to help compliance needs, logs are collected and stored in the TrustKeeper Portal. The Client is responsible to physically inspect their networks to determine if a detected Wireless Access Point is a true Rouge Access Point. A Rogue Access Point is an unauthorized wired or wireless device that is physically attached to the internal network.

Trustwave responsibilities

- Gather custom disclaimer information from the Client and configure device to display.
- Configure content filtering to be active for client devices that connect to the Wi-Fi Suite.

Client responsibilities

- Provide the appropriate disclaimer information to Trustwave to include in the Wi-Fi configuration.

WiFi Access Point Option: For Clients, who wish to extend the range of their WiFi network, multiple Access Points are available. Trustwave will work with Client to determine which AP Model will best meet their needs. Customer will need to purchase the network cables for the AP, run the cables from the current UTM location to the location of the AP and mount the AP. Due to liability, unique building codes and possible union rules; Trustwave cannot provide these services. Access Point Options include:

- Indoor or Outdoor
- Directional or Omni Directional
- AC or PoE power.

Trustwave Endpoint Protection Suite

Trustwave Endpoint Protection Suite is a powerful, cloud-based security solution that delivers integrated anti-malware, policy enforcement and simplified compliance management. By integrating core endpoint protection functions, Trustwave simplifies management and lowers security operational costs for greater adoption and

optimal defense-in-depth against a wide range of threats. Modules for rogue device detection, file integrity monitoring and log collection further enhance your security.

The Standard EPS Agent includes all the below features except the Anti-Virus and Managed Compliance Monitoring features. Both these options can be added to the Standard EPS Agent.

Trustwave Endpoint Protection Suite Feature Descriptions

File Integrity Monitoring (FIM)

Trustwave's FIM service is a solution that monitors additions, modifications, or deletions of sensitive files or other stored data by performing periodic checks and displaying the data for Client through the TrustKeeper portal when a file modification is detected.

FIM Deployment

Trustwave's FIM service can be deployed on POS devices, laptops, desktops and servers as a module on the Trustwave Endpoint Protection Platform to all Microsoft Windows and Linux OS versions currently supported by endpoint protection. Trustwave FIM can report changes to the following object types:

- Files
- Directories
- Registry keys
- Registry values

The FIM service is delivered in the cloud via Trustwave's TrustKeeper portal. All detected changes are collected and delivered to the Trustwave Endpoint Protection backend and visible through the TrustKeeper portal FIM view. Trustwave will maintain 90 days of FIM event data available online in the TrustKeeper portal FIM view, after which the data will be purged. This FIM event data can optionally be forwarded to the MSS SOC for additional analysis if Client is also subscribed to a compatible MSS SIEM service, in accordance with the terms of the SIEM service agreement.

Trustwave FIM deploys as a software module on the Trustwave Endpoint Protection Suite (EPS) platform for both Microsoft Windows and Linux OS platforms. The service can be added to an existing EPS implementation and installed on each supported endpoint automatically. If Client has not deployed the EPS, the client software is installed when the FIM service is deployed.

FIM Template Support

Trustwave will leverage pre-configured templates to enable monitoring of critical system configurations. Customer will be responsible for specifying any additional objects beyond the supplied template.

As a general guideline, a custom FIM template can be developed for any application, on a time and materials basis, as long as all of the following criteria are met:

- Request for FIM template is delivered in writing or via TrustKeeper portal support ticket
- Application is deployed on a supported EPS OS
- Application stores its critical configuration and file objects on the endpoint filesystem or in the Windows registry (registry only supported on Windows OS)
- An existing deployment of the application in the customer's environment, that is the same as production, is available for Trustwave engineers to access, preferably by remote access
- There are no differences in the endpoint used to build the template and the endpoint that is to be monitored

- Customer is responsible for all travel expenses if any on-site work is necessary to build the FIM templates
- Customer understands that custom FIM templates do not support change severity detection

A separate statement of work, or contract addendum, is required for any custom FIM template work. A custom FIM template project is billed on a per-project, time and materials basis.

FIM Event Management

Once Trustwave's FIM service has been deployed to all applicable devices, the monitoring aspect of the service is considered live. Client is responsible for reviewing events from Trustwave FIM through the TrustKeeper portal. Individual FIM events include details of the specific machine, file modified, and time stamp.

Security Health Check & Security Configuration

This feature helps ensure Client's desktop endpoint settings are configured in a secure manner and that proper security policies are in place to provide maximum visibility and control for your entire organization to help meet PCI requirements and deliver powerful protection. This feature also performs a series of health audits on mobile POS devices to proactively protect and defend your fleet.

Windows Log Collection

Offers a simplified method for collecting and centrally storing required endpoint logs for your compliance and security audits, and works with Trustwave SIEM to provide event correlation, alerting and reporting. Once Trustwave's logging service has been deployed to all applicable devices, the monitoring aspect of the service is considered live. All logs are collected and Client reviews log events in the Trustwave MSS portal. *See the Security and Compliance Monitoring Service Description included if this option has been selected.*

Credit Card Data Scanner (DLP)

Fixed endpoints with prohibited and unencrypted credit card data pose a great risk. Eliminate this exposure of data loss, potential fines and remediation costs with the critical assurance that your endpoints are free of unencrypted credit card data.

Unauthorized Device Monitor

Rogue devices are weak links that provide attackers with an easy target to breach your network. This monitor helps ensure only authorized devices are on your network with quick and easy detection of rogue devices that may present a risk of breach, such as unauthorized wireless access points, personal devices and retired equipment.

IP Beacon

Synchronizes dynamic IP address information with TrustKeeper for automated scanning of mobile and fixed endpoints. Available on Windows, macOS, Linux, and Android.

Trustwave AV

Real-time malware protection. Provides real-time protection against threats on the endpoint, remote or removable drives and threats downloaded from the internet – and scans for dormant threats waiting to be activated to protect your organization against advanced targeted attacks. New Endpoint Protection Suite customers can download an installer from the TrustKeeper portal. Existing Endpoint Protection Suite customers can request that Trustwave AV be manually pushed to existing endpoints. Real-time protection is only available on the Windows platform and

is not available on Linux or Android. Trustwave AV on Linux provides daily and on-demand scanning of the device for malware threats. Automatic malware threat quarantining is only available on the Windows and Linux platforms.

Virus Definition Updates: Trustwave will provide anti-virus definitions in real-time via CDN. These updates by default are automatic but can be configured to be delivered on an hourly, daily, or manual basis.

Endpoint Reporting: All Trustwave AV data can be reviewed in the TrustKeeper AV application. In addition, data can be viewed locally on machines where Trustwave AV is installed.

Trustwave AV Deployment

Trustwave's AV service can be deployed on POS devices, laptops, desktops, and servers as a module of the endpoint protection suite to all Microsoft Windows, macOS, and Linux versions currently supported by the Endpoint Protection Suite.

The AV service is delivered in the cloud via Trustwave's TrustKeeper portal. All detected malware threats are quarantined, reported to the TrustKeeper backend, and visible through the TrustKeeper portal AV view. The backend will forward these events to the MSS SOC for additional analysis and alerting. Trustwave will maintain 30 days of AV update history, the most recent plus seven days of full scan data, and all data available online in the TrustKeeper portal AV view. Trustwave will also maintain all AV event data for forensic review for up to one year upon Client request.

Trustwave AV deploys as a software module on the Trustwave Endpoint Protection Suite (EPS) platform. The service can be added to an existing EPS implementation. If Client has not deployed the EPS, the software is installed when the AV service is deployed.

EPS will aggregate and securely relay the AV event data to Trustwave's SOC for processing and analysis. In the event of a network disruption, the EPS application buffers the data until such time as connectivity has been restored.

Trustwave will provide all maintenance of the EPS software as a part of the Trustwave Managed AV service. Updates to the standard AV template are included.

The AV event data is transmitted from Client's site to Trustwave facilities where the data is automatically normalized, aggregated, correlated and scored.

Payment Card Breach Protection

Trustwave, through its insurance broker and carrier, has obtained the option for breach protection that can provide operators with up to $50,000 or $100,000 per merchant ID to cover expenses resulting from a payment card compromise. These costs may include fees for forensics investigations, payment card re-issuance, punitive fines from the card brands, ADCR ("fraud") expenses and other mandatory expenses imposed by the card brands.

Trustwave is not an insurance broker or carrier and is not selling insurance to Client or their remote operators. Rather, Trustwave will procure an insurance policy from an insurance carrier through a licensed insurance broker that will provide insurance coverage as "Additional Locations" under the Trustwave policy to Client's who are identified by Client for Trustwave services and pay the related services fees hereunder. The insurance policy specifically relates to data compromises that occurred due to a security incident as defined in the insurance policy

and Client customer will be provided coverage when, and only when an accurate MID is provided to and accepted by the third-party insurance carrier. Insurance coverage is only effective during the month or months that the accurate MIDs are provided to and accepted by the Insurance Carrier. Trustwave is not responsible for, nor will it assume any responsibly or liability whatsoever for verifying the accuracy of any MIDS provided by either Client or their franchisees. Trustwave does not make and specifically disclaims any and all representations or warranties regarding the insurance policy and Client agrees to look only toward the insurance policy and the carrier for resolution of any associated claims. Client shall indemnify Trustwave for any claims related to non-coverage as a result of an inaccurate or omitted MID.

Trustwave, in its sole discretion, has the right to cancel, terminate, replace or modify the terms of the Trustwave obtained insurance policy or the terms and conditions of obtaining coverage under the policy at any time and without notice. Furthermore, Trustwave shall have the right to replace, supplement, or other change the third-party insurance broker and carrier at any time in its sole discretion. Trustwave or the third-party insurance carrier or broker shall publish a copy of the then-existing insurance policy via the internet for merchant review along with claims processing information. Client and its franchisees agree that any and all coverage shall be subject to the terms of the applicable insurance policy.

Trustwave Managed Broadband Service Options (US ONLY)

Managed Wired Broadband Service

Trustwave can deliver a high-speed Internet connection to your locations. The service provides Internet connectivity using a broadband system that is delivered, managed, proactively monitored and supported by the Trustwave support team. The service installation includes:

- A Cable or DSL business class circuit
- A single static IP address (if applicable) – Static blocks of 5 usable IP addresses or more are available upon request but will incur additional monthly fees.
- If a Cable or DSL business class circuit is not available in the area, Trustwave will evaluate all options with the client before moving forward-Fiber/T1/Cell. This will include offering the option for the client to keep their own broadband connection with either Trustwave management of the circuit for $15/month or client retains management.

Additional cabling will be charged for on a time and material basis. The service cost includes:

- Installation
- Internet modem/equipment rentals and dispatches
- Technical work
- Troubleshooting/support
- Consolidated billing

Trustwave Managed Wired Broadband Service includes 24x7x365 monitoring and support. Trustwave is 1st line of support and the client will not have to deal with any ISP. Trustwave also provides one monthly bill for both the Security Plus and the Managed Broadband service.
Primary Internet deployment can include any combination of the following services (based upon availability):

- Cable: Cable Internet offers high stability; scalability and the ISPs have higher levels of support.

- DSL: DSL is generally available in over 80% of all locations nationwide. We install 6Mbps lines with all carriers where available. We use only “dry” or “naked” lines where available to improve stability and troubleshooting. This means we do not require the use of your existing phone lines.
- Trustwave makes every effort to eliminate expensive one-time construction fees that ISP’s sometime charge to install new lines in areas they do not currently have service in. Any special one-time assessments or construction fees, required by the ISP to provision a site with DSL or cable, will be paid by the Client, as these are permanent site improvements. Trustwave will notify the Client of those special fees, before any commitment is made to the ISP, and work with the Client to explore alternatives

New Site Builds

- For Clients, that are in the process of constructing a new store, it is recommended that they order the Emergency Cell Back Up Service. Many times, the planned opening date is before the ISP can install the internet connection. The Emergency Cell service can provide a bridge for internet service to the new site. See the Emergency Cell service description for details and limitations.

Broadband Service Management

If a client wants to retain their current broadband supplier but would like Trustwave to manage the ISP and any connectivity issues, clients can add the Broadband Service Management option and Trustwave will manage all network gateways via Trustwave UTM and ensure internet connectivity with the broadband router.

The client will retain their current broadband supplier and billing responsibility and Trustwave will manage all network gateways via UTM and ensure internet connectivity with the broadband router. Trustwave will manage this single circuit for $15/month for each internet connection.

This service does not include Trustwave ownership of any circuit and/or payment from Trustwave to any Internet Service Provider nor will Trustwave take over any billing services to the ISP. Trustwave will proactively monitor and manage each circuit, as well as, be responsible for any dealings with the Internet Services Provider regarding the delivery of the internet services to your location and troubleshooting lost connectivity. Trustwave will not be responsible for internet speeds being provided by the ISP or any outages caused by the ISP, their service/equipment, act of nature, or any 3rd Parties. If Trustwave, as part of the managed UTM service, has set up Auto failover on the second WAN port of the Trustwave UTM, Trustwave will provide Broadband support service for that failover circuit. Trustwave assumes no responsibility for any 3rd party Modem or Back up Cell stick hardware. All BuC sticks must be supported by the Trustwave UTM and certain 3G/4G services might require use of a Cradlepoint device. Trustwave can supply the Cradlepoint device at an additional one-time fee. If the BuC circuit is provided by another ISP, different from the primary ISP, an additional charge of $10/month will be added to the base price of $15/month. If the same ISP provides both Primary and Failover service, the price remains $15/month.

In order for Trustwave to provide Broadband Support Services for your existing Internet contract; Trustwave will need the following information:

- The sites current account information to put in our Telco customer data base for Support (account #, latest internet bill for each location)
- Any static IP information (if applicable),
- ISP(s) support Contact information
- ISP(s) Failover information. Who is the provider of the Backup Cell service (3G/4G) and cell stick device information is required.
- Any pins/passwords on the account(s)

- Client will need to call their ISP(s) and add Trustwave SOC members as authorized users on each account in order for us to be able to work with the ISP for troubleshooting.
- If any accounts are bundled with phone/TV/Internet, Trustwave cannot provide Broadband Support Services

Cellular Internet Backup

Trustwave can provide a USB-based, 4G cellular backup Internet connectivity with a Trustwave managed UTM to provide temporary Internet access upon failure of the primary Internet connection. Trustwave cannot use a customer supplied USB Cell stick due to potential incompatibility issues between the Trustwave UTM and cell stick. Trustwave can support a customer Back up Cell under our Broadband Support Service. Back up Cell service is available for U.S. and Canadian-based deployments only. Through a monthly subscription fee priced separately, Trustwave establishes a service contract with the cellular provider and provides USB modem hardware for customer use. 4G cellular backup can only be provided where service is available from Cell providers. The use of a Cradlepoint device will be required with 4G services. Please refer to the Cellular Internet Backup Limitations section of this document for additional detail regarding allowed usage of the Cellular Internet Backup service option.

Cellular Internet Backup Limitations

- Cellular internet backup is a USB-based service using cellular wireless technology that is used if primary broadband service fails. This service is reserved for temporary Internet access support only. It is not to be used as a primary Internet connection, nor leveraged for an extended period of time in the event of continued unavailability of a primary connection or non-existence of a primary connection. In addition, the USB modem will not be removed from the firewall appliance's USB port and/or Cradlepoint device and connected to another device for personal or business Internet access use. Unauthorized removal will require the cell service to be terminated and any usage charges will be applied.
- Trustwave will use commercially reasonable efforts to provide the Cellular Broadband Backup Service to the locations listed herein. If Trustwave is unable to retain the Broadband Services for the Client on terms acceptable to Trustwave at any specific location, then Trustwave reserves the right to cancel the Broadband Services to that location. Trustwave's cancellation of the Broadband Service to a location will absolve Client of any payment obligations for the Broadband Service cancelled by Trustwave.
- Trustwave will monitor cellular modem service usage and will charge Client accordingly for service overuse and misuse including as described above. Overuse and misuse will be determined by Trustwave on an ongoing case-by-case basis, but in general will be flagged over one [1] GB of data usage per month.
- Trustwave will apply overage charges to Client's Monthly Managed UTM subscription fee. Overages are charged at $20/1 GB of Data/Site. In cases where egregious misuse of the service is observed, or Client does not pay the billed overage charges within 30 days, Trustwave reserves the right to cancel the Cellular Internet Backup service. If a USB Cell Stick modem and/or Cradlepoint device is lost or destroyed by Client, a $150 replacement fee for each device will be charged. A reinstallation fee will be assessed separately from the monthly charges and paid by the Client.

Emergency Cellular Internet Backup Kit

Trustwave can provide a temporary USB-based, 4G cellular backup Internet connectivity with the installation of a Trustwave UTM. Service will be identified by Trustwave on availability at the site Location. If Client will also be provisioned with the Trustwave regular Backup Cell Service, once the wired internet connection is established at the location, Trustwave will provision the Emergency Cell service with the same 4G service that will be provided with the regular Back Up Cell service. Under no circumstances will the Cell stick be unplugged from the firewall

appliance's USB port and/or Cradlepoint device and connected to another device for personal or business Internet access use. Trustwave will disconnect the service upon detection of the removal of the cell stick. A reconnection fee of $200 will be charged if the customer wishes to continue use of the service.

This service is limited to 30 days. At the end of 30 days the cell service will be discontinued. Clients are strongly advised to carefully plan the installation of the normal internet service to occur within the 30-day cell service period. One (1) 30-day extension can be approved and the price is the same for the next 30-day period. No extensions beyond 60 days of use. Trustwave cannot prorate the cost due to contractual obligations to the selected ISP provider. This Emergency Backup Cell service is available for U.S. only. Trustwave establishes a service contract with the cellular provider for 30 days and provides USB modem hardware for customer use. USB-based, 4G cellular backup can only be provided where service is available from Cell providers and the use of a Cradlepoint device will be required.

Emergency Cellular Internet Backup Limitations:

Trustwave will use commercially reasonable efforts to provide the Emergency Backup Cell Service to the locations listed herein in the SOW. Emergency service is a 30-day temporary connection until the existing, or new, internet connection is restored or installed. Trustwave will provide up to 6 GB of Data /month/site with the connection speeds up and down provided by the selected Cell Service Provider. Overages are charged at $20/1 GB of Data/Site.

Return of Emergency Cellular Internet Backup hardware. If Client is not continuing with the Trustwave Back up Cell service, Client is required to return, in good working condition, all the hardware provided (USB Cell stick and/or Cradlepoint docking station if provided) within 10 working days after termination of the service to the address provided in the return shipping container. If a USB Cell Stick modem and/or Cradlepoint device is lost or destroyed by Client, a $150 replacement fee for each device will be charged.

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 Managed Services described herein, which are incorporated into this Agreement and include commitments with respect to certain availability of the Managed Services, are set forth at https://www.trustwave.com/SLA/Ver001_Trustwave_MSS_SLA.PDF

Definitions

Incidents are Security Alerts that are investigated by the Global Threat Operations team and is considered a threat, which is escalated to Clients based on the Severity assigned by the Threat Analyst.

Client Provisioning Questionnaire means the Client provided information relating to the UTM environment, policies and rulesets.

UTM means the Client's Source File Device(s) and the Client's Management Console device(s).

Product Updates are vendor provided product and security enhancements to the UTM devices, the Trustwave Platform, 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 means the relevant manufacturer's return and repair warranty applicable to UTM device(s);

Security Alert means one or more security events of certain significance which have been escalated as a Security Alert, where the application of specified correlation rules of certain attributes has identified the security event as having an increased risk of the event being a security threat and requiring further analysis, attention and investigation. Security Alerts are evaluated through an incident management process where they are categorized, and appropriate actions are taken based on the level of severity.

Security Incident means a Security Alerts of certain significance which, having been analyzed and investigated by the Threat Analyst team is identified as a security threat.

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

Security Updates are provided by vendors to add additional protection or update the existing protection engines included with the device. These updates are typically very small in nature but are more frequent than Product Updates.

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

Ticket is a method of capturing activities or alerts and documenting them within the Trustwave TrustKeeper Portal. Tickets are displayed in the Support application within Trustwave TrustKeeper Portal. Tickets can be used to alert clients to support issues or security incidents. Tickets are also used by clients to request configuration changes.

TrustKeeper Portal means the Trustwave's TrustKeeper service management web portal.

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