Trustwave®

SERVICE DESCRIPTION

Managed Detection and Response Essentials

Overview

Trustwave's Managed Detection and Response (MDR) Essentials service ("**Service**") provides (i) 24x7x365 monitoring, correlation, analysis, investigation, and detection of specific Client log sources, and (ii) threat response. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

The Service includes the following features:

24x7 Threat Analysis, Investigation and Response

Trustwave will use its proprietary threat analysis engine to help identify potential indicators of attack and external efforts to compromise Client's environment. The Service includes both (i) automatic, globally deployed, threat-focused detection capabilities and (ii) human-led threat monitoring.

Threat Analysis and Investigation

The Trustwave Fusion platform ingests event data from Client's supported log sources and processes such data through threat intelligence and threat-focused detection. Any potential threat findings from this process ("**Threat Findings**") are either (i) initially reviewed by Trustwave representatives and then escalated as needed or (ii) automatically escalated according to Trustwave algorithms.

Escalated Threat Findings are deemed "**Actionable Threat Findings**" and the Trustwave Fusion platform will generate an incident ticket in the system ("**Incident**"). Client will receive notifications according to the Incident's assigned priority (see below). Incidents may include a request for Client to authorize recommended actions based on the type of Managed Technology and its configurations.

Threat Findings which are not escalated are deemed "**Non-Actionable Threat Findings**" and no Incident is created. Client may review Trustwave's Incident closure notes relating to Non-Actionable Threat Findings in the Trustwave Fusion platform. These closure notes may document (i) implemented or recommended service tuning or (ii) managed or unmanaged security technology policy updates (each provided at Trustwave's discretion).

Incident Priority Levels

Trustwave will assign a priority level (P1 – P4) to each Incident. Subject to any notification procedures separately agreed in a SOW or Order Confirmation, Trustwave will notify up to five (5) Client-

designated point(s)-of-contact for each Incident and according to the notification procedure and its assigned priority.

Priority	Notification Procedure	Priority Description
Critical (P1)	Phone call & Email	Incidents at this level are actionable, potentially pose a high security risk to Client's environment, and signal an active compromise, extensive damage, or total disruption of operations to high value assets in Client's environment. Investigations that result in this priority require the Client to take immediate containment, response, or recovery actions to contain the Incident.
High (P2)	Phone call & Email	Incidents at this level are actionable, potentially pose a high security risk to Client's environment, and signal a potential compromise, severe damage, or disruption of operations to high value assets in Client's environment. Investigations that result in this priority require Client to take nearly immediate defensive actions to contain the Incident.
Medium (P3)	Email	Incidents at this level are actionable, potentially pose medium-level security risk, and signal the potential for limited damage or disruption to standard assets in Client's environment. Investigations that result in this priority require Client to take timely, but not necessarily immediate, action to contain the Incident.
Low (P4)	Email	Incidents at this level are not immediately actionable and may require further investigation by Client to determine possible actions. Investigations that result in this priority require additional context or may signal known risks and deviations from security best practices.

Client may request that Trustwave follow additional or different notification policy standards as a set of guidelines. Such guidelines have no binding effect on Trustwave.

Threat Response

Trustwave and Client will co-develop a "**Response Runbook**" containing:

- authorizations on a per asset basis using traffic light protocols (TLP) which will identify pre-approved actions for Trustwave to implement without additional approvals from Client during the Term.
- Up to five (5) Client contacts for Incidents which Trustwave will use when following the notifications procedures above.

The TLP designations for each asset will indicate whether Trustwave may

- contain a direct threat to a Client asset; or

- notify Client that Trustwave recommends a response which Trustwave is not pre-approved to take. Trustwave will not act unless Trustwave receives separate approval from Client.

The Response Runbook is stored within the Trustwave Fusion platform. Notwithstanding anything in this section, Trustwave and Client agree to the following:

- **Undefined Assets** – Where the Response Runbook does not address a specific Client asset which may require response action, Trustwave will assume no response actions are authorized without separate approval from Client.
- **Non-Asset Basis Responses** – Certain threats may be separately classified and approved for Trustwave response action on a non-asset basis (e.g. systemic threats).
- **Changes** – Any changes to the Response Runbook by Client must be submitted by an authorized representative of Client and follow the policy change request procedures set out in Trustwave's SLAs (available at https://www.trustwave.com/en-us/legal-documents/contract-documents/).

Threat containment actions may include host isolation but vary based on the Managed Technology (see definition below) and depend on the Trustwave Fusion platform's capabilities with regard to Client's connected security solutions.

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- review Threat Findings, Incidents, and reports as made available in the Trustwave Fusion platform;
- notify Trustwave if events or reports are not available in the Trustwave Fusion platform as reasonably expected;
- work with Trustwave to resolve each Incident by providing relevant personnel and ensuring support and engagement of third parties, as reasonably required by Trustwave;
- provide Trustwave with requested information and confirmations in a timely manner. Client acknowledges failure to do so may inhibit Trustwave's ability to provide the Service;
- request changes in accordance with Trustwave's change management process;
- identify Client personnel authorized to request and or approve threat containment actions, configuration, and security policy changes; and
- promptly respond to Trustwave recommendations for threat responses which Trustwave does not have pre-approval to take.

Trustwave Obligations

For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will

- collect and monitor log data from agreed log sources via the Trustwave Fusion platform;
- maintain availability of events and Threat Findings in the Trustwave Fusion platform according to Trustwave's data retention procedures and service level agreements);
- monitor, analyze, and attempt to remediate issues identified by Trustwave in Client's environment (to the extent pre-approved by the Response Runbook);
- maintain updated status of Incidents in the Trustwave Fusion platform and record all communications between Client and Trustwave pertaining to such Incidents;
- manage the process in developing a Response Runbook that will outline Client's priorities and pre-approved response actions;
- allow authorized Client personnel access to the Trustwave Fusion platform to interact with

Trustwave personnel and to monitor service deployment. The Trustwave Fusion platform will also be used as a repository for Client-approved policies and change management activities;
- confirm that tickets request was submitted by an authorized Client contact and notify Client if unauthorized requests are received;
- request additional information as necessary from Client to support the implementation of any change request; and
- assess the potential risk that may result from implementation of a change request and advise on such assessment. Confirm Client approval to implement such a change request after reviewing risk assessment results with Client.

Systems Management

Trustwave will manage and monitor the configuration of those Client security solutions which are included in the Service as indicated in the applicable SOW or Order Confirmation ("**Managed Technology**") according to the following terms:

Policy and Configuration Management

Trustwave will abide by the following change-control and configuration management procedures for standard change requests to the Managed Technology during the Service:

Client-Initiated Change Management

Trustwave will assess and implement change requests submitted by Client through the Trustwave Fusion platform. Trustwave evaluates such requests against industry best practices and with regard to the change's potential impact on the Client's security environment. Trustwave will schedule and notify Client of changes that may disrupt Client's environment, and Client will approve or deny these scheduled change windows. Client acknowledges that denial of a scheduled change window may impact Trustwave's ability to provide the Service.

Client acknowledges that any configuration change management requests for Managed Technology or Client environment that are categorized as a complex change may, in Trustwave's sole discretion, be deemed a project and would require a written addendum between the parties.

Trustwave-Initiated Change Management

Trustwave will implement Trustwave-initiated changes through the Trustwave Fusion platform. Trustwave determines the applicability of such changes against industry best practices and with regard to the change's potential impact on the Client's environment.

Trustwave will perform the change according to the change schedule agreed between Client and Trustwave.

Endpoint Management

Trustwave will monitor the Managed Technology through its management console primarily and only periodically review connectivity status of the Managed Technology's endpoints. Trustwave will, at its discretion, recommend periodic version updates to be rolled out to the Managed Technology. For the avoidance of doubt, Trustwave will not conduct continuous monitoring of endpoints or health status checks. Client will be responsible for promptly implementing such updates or risk disruption to the Service.

Co-Managed Access Change Management

Trustwave may provide Client with access to the Managed Technology. While receiving the Service with such co-managed access, Client agrees to the following shared change and change audit process:

- Before implementing any changes to the Managed Technology, Client will create a ticket in the Trustwave Fusion platform identifying which policies and configuration settings will change and of any other planned effects. Upon receiving the ticket, Trustwave may review changes made by Client and make recommendations.
- Client acknowledges this co-managed structure may result in increased risk of security incidents or Service outages. Client will work in good faith with Trustwave to remediate any such security incident and perform a root cause analysis. If Trustwave reasonably determines that the security incident or outage was caused by a change or activity performed by Client, Client will be solely responsible for the effects of the change and for completing and producing the full root cause analysis.
- Client representatives with co-managed access to the Managed Technology will be responsible for attaining reasonable competency and training in cybersecurity to make standard changes to the Managed Technology's rules and configurations. Client is responsible for validating such competency and training.

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- procure and maintain valid vendor software licenses and maintenance contracts applicable to the Managed Technology;
- provide, when requested by Trustwave, access to vendor portals to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of the Client for management and maintenance purposes;
- access the Trustwave Fusion platform to submit change request tickets, respond to tickets, and confirm scheduled change windows;
- consider risk factors related to change requests and promptly provide requested information to Trustwave;
- review and assess changes that Trustwave proposes and promptly provide Trustwave with approval or rejection of such proposals;
- at Trustwave's reasonable request, provide pre-determined change control windows during which change management functions can be executed;
- inform Trustwave of all maintenance activities and changes in Client's environment that may impact Trustwave's ability to provide the Service; and
- provide Trustwave with access to the Managed Technology according to the SOW or Order Confirmation between Client and Trustwave.

Trustwave Obligations

For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will

- provide product and security update recommendations and assistance with issues resulting from upgrades;
- provide Service-related remote assistance, support, and configuration within the managed environment;

- attempt to resolve any connectivity or application issues identified with regard to the Managed Technology to return it to a steady state of operation;
- perform assessment based on Trustwave's risk level and change categories and determine whether a change request is in-scope within the terms of the Service;
- source additional information as necessary to support the implementation of the change request;
- assess the potential risk that will result from implementation of the change request and advise Client of the outcome, as necessary;
- notify Client if a change request is outside the scope of the Service or if additional charges will apply to a change request;
- perform change management activities when requested and in compliance with Trustwave policies and inform Client of implemented changes;
- Trustwave will not be responsible for the design, implementation, effect, or any damages, direct or indirect, of any Client changes made to the Managed Technology; and
- Trustwave may audit any Client-directed change and confirm whether there are any errors or consequences resulting from the change. If Trustwave determines no additional action is required, Trustwave will close the relevant ticket. If Trustwave's review raises any questions or concerns, Trustwave will communicate such questions or concerns to Client and Client will work with Trustwave to resolution.

Client Success Manager

The Client Success Manager ("**CSM**") feature provides Client with an assigned Trustwave representative who meets with Client's representatives on a regular basis and manages Client's overall experience and satisfaction with the Service. This CSM feature includes the following elements:

- Point-of-contact between Client and Trustwave for
    - Client's questions pertaining to the Service;
    - escalation requests;
    - customer service requests; and
    - Client contact and representative information updates
- Regular meetings between the CSM and Client's representatives to review Client's statistics in the Trustwave Fusion platform, conduct status checks on open items, and receive updates from Client
- Maintains availability during regular, regional business hours for contact via email, phone, or other Trustwave communication mechanisms, as provided
- Supports continuous service improvement initiatives

CSM Service Tiers

This feature is offered at the following service tiers:

- **Monthly** – This is the default service tier. The Service automatically includes monthly meetings with a CSM.
- **Weekly** – Client may elect to additionally purchase the premium service tier, in which case, meetings with a CSM will occur weekly**.** This will be indicated in the applicable Order Confirmation or SOW.

Client Obligations

For Trustwave to provide this feature of the Service, Client will

- review documents provided by the CSM;
- establish and remain available for communications from Trustwave; and
- accurately provide Trustwave representatives with information and access to data as reasonably requested by Trustwave.

Client further acknowledges that the CSM feature is not a substitute for legal or regulatory advice and the quality and effectiveness of the feature is dependent upon Client's cooperation with and provision of information to Trustwave.

Trustwave Obligations

As a part of the CSM feature of the Service, Trustwave will

- review relevant documents with Client's representatives to manage administrative activities of the Service;
- work with Client's representatives to maintain communication throughout the Service Term;
- schedule and lead meetings according to the applicable service tier;
- generate and analyze standard service review reports and performance as relates to the Service;
- act as a point-of-contact between Trustwave and Client; and
- help respond to Service-related requests and escalate requests as applicable.

Core Trustwave Features

The Service includes the following core features which are standard to many of Trustwave services:

Onboarding

The Onboarding feature of the Service includes two phases: Client-side implementation and MSS Transition.

Client-side Implementation

Client will implement the necessary steps to connect the Managed Technology (including its management station (dependent on type) and sensors on each endpoint) to the Trustwave Fusion platform.

Client will ensure the Managed Technology is prepared to provide appropriate and consistent information about Client's environment in a manner that allows Trustwave to provide the Service. Trustwave may assist Client during this phase.

Trustwave will not continue with this feature of the Service until Trustwave has the necessary access to the Managed Technology.

MSS Transition

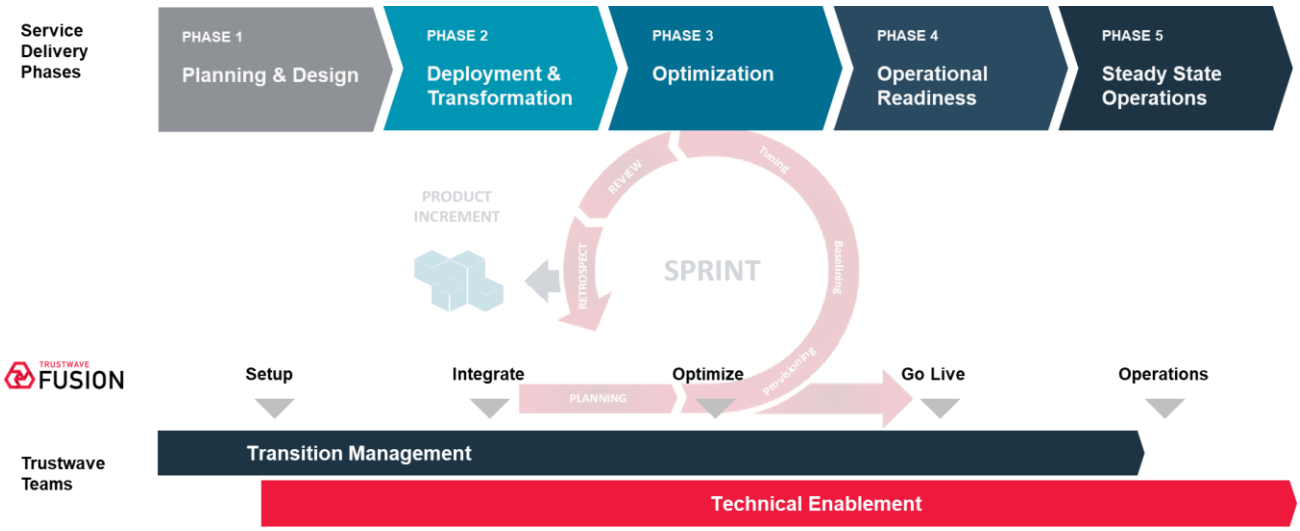
The Service includes a transition management feature to facilitate the integration of the Managed Technology with the Trustwave Fusion platform.

Trustwave will assign a transition manager and additional technical enablement resources, as needed, to work directly with Client in onboarding Client to the Service and the Trustwave Fusion platform.

Trustwave will advise Client through its five (5) phases of transition management. Client is deemed fully transitioned and at steady-state (beginning of the Service) following Trustwave's conclusion of the fifth (5th) phase ("**Steady State**"). Trustwave and Client may agree to additional scoping terms in an Order Confirmation or SOW for this onboarding feature to accommodate varying complexity, size, and project governance requirements for Client's security solution(s).

Transition Management Phases

The following chart summarizes the five (5) phases of transition management in this feature:



Trustwave Obligations

As a part of the onboarding feature of the Service, Trustwave will

- schedule and host a kick-off meeting with Client;
- provide new-user orientation materials and training;
- coordinate Trustwave technical delivery resources for
    - collection, review, and assessment of event data for the Service;
    - deployment of connectivity elements for the Trustwave Fusion platform;
    - initial configuration and baselining of data flow, quality, and analysis; according to the log source supportability and feature support underwritten by a statement of work;
    - Analysis and baseline of endpoint data individually and collectively to understand the current behavior vs expected behavior of each of the endpoints, developing recommendations based on the business significance/priority of the endpoint, and adjusting policy and configuration accordingly;
    - definition of the traffic light protocols (TLP) response and actions;
    - definition of authorized contacts for the Notification Procedures listed above; and
    - conducting final operational readiness assessment in preparation for steady-state status of the Service; and

- keep Client informed and up to date on transition progress and report on risks and issues relating to transition management.

Client Obligations

Client will

- ensure appropriate licensing is applied to the Managed Technology; and
- provide remote access to the Managed Technology to accommodate Trustwave's remote analysis and remediation as defined by this service description.

Trustwave Fusion Platform

The Trustwave Fusion platform is Trustwave's proprietary cloud-based cybersecurity platform. Client will be automatically enrolled in the Trustwave Fusion platform as a part of the Service. Client will have access to the following on the Trustwave Fusion platform:

- Event information, Threat Findings, and Incident tickets
- Client's reports and dashboards
- Request methods for change support and management
- Multiple methods for Client to securely communicate with Trustwave and the ability to upload documentation, security policies, and more

Trustwave Connectivity

The Service includes the following options to connect Client's log sources with the Trustwave Fusion platform. Trustwave will provide one or more of the following options in accordance with the SOW or Order Confirmation signed between Client and Trustwave.

Trustwave Connect

Trustwave Connect collects log data from Client's security solution(s). Trustwave Connect facilitates collection of log data via syslog, REST APIs, and other supported methods. It is hosted by Client or its designated cloud, virtualization, or data center.

The following deployment models are available for Trustwave Connect:

- Virtual Appliances (included in the Service): VMWare, Amazon Web Services, Microsoft Hyper-V, and Azure
- Physical appliances (additional fee)

Client may be required (i) to install a Trustwave Connect solution within its environment and establish the necessary network access for the Service or (ii) to set up event data so it is sent to Trustwave.

Direct Connectivity to the Trustwave Fusion platform

For certain supported cloud solutions, the Trustwave Fusion platform supports direct connectivity from Client's environment for log collections via an API. Trustwave and Client will work together to set up direct connectivity, as applicable. Client may have access to self-service options for onboarding Client's security solutions.

Trustwave Endpoint

Client may also select Trustwave-provided, dedicated endpoint solution ("**Trustwave Endpoint**") to support log collection of Windows security events. Trustwave Endpoint is provided and distributed

through the Trustwave Fusion platform and prepared by Trustwave with the applicable configuration set for Client's environment.

If utilized, Trustwave will be responsible keeping Trustwave Endpoint up-to-date and applying configuration changes according to any Trustwave change management procedures.

Problem Management

Trustwave will perform service failure analysis and suggest solutions designed to address the suspected causes of one or more Service interruptions in the form of an Incident post-mortem document. Trustwave will provide an Incident post-mortem document for P1 and P2 severity Incidents and Client may request similar reports for P3 and P4 severity Incidents and Trustwave will provide at its discretion.

Additional Information

Log Source Support Policy

Trustwave may deliver the Service by acquiring, parsing, or normalizing log data collected from commercially-available off the shelf products. Trustwave maintains support for a defined list of log sources supported under the Service. Any changes to monitoring and parsing activities are at Trustwave's sole discretion.

Correlation & Use Case Management

Trustwave maintains proprietary global processes to model high-fidelity attack scenarios and event sequences within the Trustwave Fusion platform from normalized, high-utility logs that may represent known or suspicious threats that need to be classified, analyzed, and actioned to minimize or to mitigate organizational risks. Trustwave's global correlation and use cases aim to reliably detect high-fidelity threats applicable to all Trustwave's subscribed clients. Trustwave retains sole discretion in determining if conditions are added, modified, or removed to the use case catalog.

Capacity Consumption Overages

The Service is provided with an initial data volume and any additional capacity Client may purchase (as set forth in the applicable SOW or Order Confirmation between Client and Trustwave) ("**Data Volume Cap**"). Trustwave may, from time to time, review the volume of data and events processed for Client in relation to the Service and recommend changes.

Where Client's data and event volumes are found to exceed the Data Volume Cap by twenty-five percent (25%) or more on average over any three (3) month-period, Trustwave may either

- request that Client agree to amend the current Order Confirmation or SOW to accommodate a higher threshold of data and event volumes and corresponding price change; or
- suppress, throttle, or filter excessive data and events from Client's systems.

Trustwave will notify Client of the overage and will select the method that is expected to limit impact to the Service.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable Statement of Work or Order Confirmation between Trustwave and Client.