Trustwave®

SERVICE DESCRIPTION

Managed Detection & Response

Overview

Trustwave's Managed Detection and Response (MDR) service ("**Service**") provides (i) 24x7x365 threat monitoring, (ii) threat hunting, and (iii) 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 Client's high-fidelity security telemetry that enables the potential detection of intrusions ("**High Fidelity Alerts**"), SpiderLabs threat intelligence, and the Trustwave Fusion platform to identify potential indicators of attack in or compromise of Client's environment. The Service includes (i) threat-focused detection analytics; (ii) human-led threat investigation; (iii) human-led threat hunting; and (iv) threat response containment guided by Client's pre-approved preferences (see Response Runbook below).

Threat Analysis and Investigation

The Trustwave Fusion platform ingests alert and event data from supported data sources (see Security Telemetry Ingestion & Log Source Support Policy below for supported sources), reviews SpiderLabs threat intelligence, and applies threat-focused detection analytics to seek out suspicious patterns and events ("**Threat Findings**").

Trustwave may classify Threat Findings as "critical" if Trustwave determines such Threat Findings to be critical confidence and critical severity intelligence. Trustwave will indicate a Threat Finding's priority level in the Trustwave Fusion platform.

Then, such Threat Findings are either

(i) deemed non-threatening by additional system or human analysis;

(ii) automatically added to a new or existing security incident ticket ("**Security Incident**"). Trustwave may recommend next steps for Client action, in Trustwave's sole discretion; or

(iii) manually added to a new or existing Security Incident with details on Trustwave's investigation, determination, and threat containment response actions if deemed appropriate by Trustwave and according to Client's Response Runbook.

Alerts and events that are not classified as Threat Findings and Threat Findings that are not added as Security Incidents are still available for review by Client in the Trustwave Fusion platform.
Security Incidents are created and stored in the Trustwave Fusion platform and reference the related Threat Findings and security telemetry relevant to that Security Incident. Trustwave will send Client notifications according to the Security Incident's assigned priority (see below). Security Incidents may include any of the following information:

- Summary of the findings
- Analysis
- Recommendations
- List of Trustwave actions taken
- Requests for Client to authorize recommended actions

Trustwave may add additional Threat Findings and logged telemetry to an existing Security Incident for related follow-up activity. Trustwave may, at its sole discretion, collect and submit binary files and suspected malware from the Managed Technology to its SpiderLabs Malware Reverse Engineering team for analysis. In such cases, Trustwave will add any further observations, findings, or recommendations developed by this team to the applicable Security Incident(s).

Threat Findings which are not added to a Security Incident are deemed non-actionable. This means Trustwave has reviewed associated threat indicators and determined such indicator to be non-threatening due to context, threat intelligence, or other factors.

Client may review Trustwave's closure notes relating to such non-actionable Threat Findings in the Trustwave Fusion platform. These closure notes (provided at Trustwave's discretion) may document

- intelligence resources reviewed;
- details available within logs;
- factors that appeared as a threat but that can be attributed to testing, problem management, or change management processes;
- items that can be implemented or recommended as tuning measures for the Service or policy updates for managed technologies; or
- recommendations for unmanaged security technology configuration or policy updates.

Incident Priority Levels

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

Client-designated point(s)-of-contact defined by Client in the Trustwave Fusion platform for each Security Incident and according to the notification procedure and its assigned priority (see table below).

Priority	Notification Procedure	Priority Description
Critical (P1)	Phone, Email	Security Incidents at this level are actionable, potentially pose an immediate 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 Security Incident.
High (P2)	Phone, Email	Security 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 Security Incident.
Medium (P3)	Email	Security 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	Security 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 response pre-authorizations for EDR/XDR agent response actions on Trustwave managed endpoints (as defined in the applicable SOW or Order Confirmation) which will make up Client's "**Response Runbook**" and which must contain:

- 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 to be defined in the Trustwave Fusion platform for Security Incidents which Trustwave will use when following the notification procedures above.

The TLP designations for each asset will indicate whether Trustwave

- may contain a direct threat to a Client asset; or
- may notify Client that Trustwave recommends a response and will not act unless Trustwave receives separate approval from Client via the Trustwave Fusion platform.

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 within the Trustwave Fusion platform and follow the Fusion policy change request procedures set out in Trustwave's SLA documentation.

Where Trustwave recommends a containment action following analysis of files and suspected malware, Trustwave will include such recommendations in the applicable Security Incidents according to the details in the Threat Analysis & Investigation section above. Threat containment actions will vary based on the Managed Technology (see definition below) and Trustwave's ability to perform such containment actions.

Client Obligations

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

- provide an initial Response Runbook and periodically review TLPs to keep response actions Trustwave is allowed to take up to date within the Trustwave Fusion platform;
- collaborate with Trustwave on security detection and response best practices, including access, configurations, policy definitions, and settings that allow high fidelity and timely threat containment;
- review Threat Findings, Security 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 Security 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 policy and configuration modifications using change tickets ("**Change Tickets**") in the Trustwave Fusion platform and 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
- 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 telemetry 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 Security Incidents identified by Trustwave in Client's environment (to the extent pre-approved by the Response Runbook);
- periodically update the status of Security Incidents in the Trustwave Fusion platform and record all communications between Client and Trustwave pertaining to such Security Incidents;
- manage the process of developing a Response Runbook in the Trustwave Fusion platform;
- allow authorized Client personnel access to the Trustwave Fusion platform to interact with Trustwave personnel and to monitor the Service. The Trustwave Fusion platform will also be used as a repository for Client-approved policies and change management activities;
- confirm that Change Ticket requests are submitted by authorized Client contacts 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.

Threat Hunts

Trustwave will perform regular cybersecurity threat hunts for artifacts on Client telemetry (derived from the Managed Technology only) that are likely to indicate an intrusion based on (i) threat intelligence qualified by Trustwave's SpiderLabs for emerging global cybersecurity threats and (ii) additional and high security impact Trustwave proprietary indicators of compromise.
Trustwave will perform threat hunts on telemetry available to Trustwave from Client's environment. Trustwave will generate a Security Incident ticket if it identifies any matches between Client's telemetry and such threat intelligence noted in the preceding paragraph. Then, Trustwave will provide documentation of Trustwave's investigation. The Security Incident will describe (i) the threat Trustwave identified, (ii) response actions Trustwave may have performed, (iii) remediations Trustwave may recommend, and (iv) if Trustwave discovered any materially new tactics, techniques, or procedures (TTP).
Trustwave will

- determine what threats, indicators, and TTPs are subjected to hunts
- assess the impact of any discovered and material threats discovered in a given threat hunt;
- inform Client of identified potentially impactful threats to Client's security environment via a Security Incident ticket in the Trustwave Fusion platform;
- follow incident response protocols to the extent Trustwave identifies Security Incidents and to the extent such protocols are agreed between Client and Trustwave in the Response Runbook; and
- reasonably coordinate with and transition supporting Security Incident activities with the Client lead investigator or Client's approved delegate.

Advanced Continual Threat Hunts

Trustwave offers Advance Continual Threat Hunts as an add-on service to the Service ("**Add-On Service**"). Client's SOW or Order Confirmation for the Service will indicate if such Add-on Service is included.

Trustwave begins the Add-On Service by researching common threat actor TTPs and devising custom hypothesis-based hunts with the assumption a breach has already occurred on Client's network. To accomplish this, Trustwave searches for any indication of anomalous behavior, TTPs, and indicators of compromise (IOCs). Trustwave analyzes Client's current threat landscape (as determined by Trustwave based on open source intelligence, internal references provided by Client, and Client's technology stack). Further, Trustwave examines (i) which specific threat actors may be motivated to target Client's current threat landscape and (ii) the TTPs that such threat actors are known to use. This results in a list of potential threats to Client ("**Potential Threats**").

Hunts

Trustwave will then perform a threat hunt on Client's network for a group of Potential Threats. Trustwave uses the following threat modeling variables and process to perform such threat hunts.

Variables

- **Threat Actors** - Trustwave tracks active threat actor groups operating around the world, including nation-state sponsored threat groups, hacktivists, and cybercrime syndicates.
- **Industry Historical Breach Analysis** - Trustwave examines historical data breaches from Client's industry to identify previously successful TTPs.
- **Data Leakage & Credential Compromise** - Trustwave reviews dark web and credential harvesting sites to identify leaked corporate data, employee personally identifiable information (as determined by provided username and domain name credentials from Client), or user credentials. This can help identify potential previous compromises and existing corporate vulnerabilities.

Scripted Hunting

Trustwave uses a proprietary library of hunt scripts designed to identify suspect behavior exhibited by advanced persistent threat (APT) and cybercrime groups. Trustwave regularly updates its library and has mapped it to the MITRE ATT&CK framework. Suspect behavior identified in the library includes but is not limited to the following:

- **Unsigned or Unauthorized Persistence** – processes that start automatically on reboot
- **Privilege Escalation** – processes or users that have elevated privilege to SYSTEM / ADMIN
- **Lateral Movement** – processes or users that have moved throughout Client's network in an unusual manner or have conducted unusual network reconnaissance activities
- **Data Theft** – processes or users transmitting unusually high volumes of data
- **Suspect Process Execution** – hidden or obfuscated file execution, execution from TEMP or suspect directories, downloaded file execution, Powershell and PSEXEC execution, etc.
- **Remote Admin** – RDP and other remote administrative tool usage

- **SpiderLabs IFP Threat Intelligence IOC Search** – contextualized IOCs attributed to known threat actors will be automatically identified

Analysis

Initial Findings Analysis

Each scripted hunt tends to produce voluminous results which then require analysis. Trustwave will review the data for false positives and to separate out suspicious elements for manual analysis.

Manual Analysis

Trustwave will conduct a manual, human-led analysis of all the data collected thus far. If Trustwave determines malicious behavior to exist on Client's network, Trustwave will then review Client's network for further instances of such malicious behavior. If Trustwave determines there is significant ongoing data breach or a widespread cyber infection, Trustwave will work with the Trustwave's Digital Forensic & Incident Response (DFIR) team (if Client has purchased such a retainer or emergency services) or may work with Client's alternative DFIR provider (at Trustwave's sole discretion).

Reporting

Where Trustwave identifies malicious findings, vulnerabilities, and network infrastructure deficiencies, Trustwave will generate a Security Incident ticket in the Trustwave Fusion platform.

Trustwave Obligations

For this Service, Trustwave will:

- create Security Incident tickets within the Trustwave Fusion platform to notify Client a hunt is underway. Information and results of the hunt will be attached to the ticket to notify Client where action is taken or required;
- if a hunt yields actionable findings, provide recommendations aimed to improve Client's overall security posture; and
- if a hunt yields actionable findings, conduct further analysis on binaries that are suspicious or require reversing to validate malicious intent and gather additional indicators of compromise.

Client Obligations

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

- respond timely to email or Security Incident ticket or Change Ticket communications from Trustwave; and
- provide network documentation promptly upon request.

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 sections. For the avoidance of doubt, Trustwave will not provide the Service for any Client security solution other than what is specifically set forth in the SOW or Order Confirmation unless otherwise agreed between Client and Trustwave in writing.

Policy and Configuration Management

Client and Trustwave will collaborate on initial configuration of a policy and settings of the Managed Technology for the Service and work together during the Term to maintain that configuration. This must be completed in order to achieve Steady State (defined below).

If the Managed Technology has no existing configuration or policies, Trustwave will assist Client in developing and applying a base policy.

Trustwave may modify the configuration policy and settings of the Managed Technology further with the aim of protecting against threats to Client.
Trustwave and Client 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 Trustwave-approved communication methods. Trustwave evaluates such requests against industry best practices and the change's potential cybersecurity impact on Client's security environment. Trustwave will propose a schedule and notify Client of changes Trustwave expects (in its sole discretion) may disrupt Client's environment, and Client will approve or deny these scheduled change windows. Client acknowledges that denying a scheduled change window may impact Trustwave's ability to provide the Service and service level agreements (SLAs) may not apply until Trustwave is able to implement the change

Trustwave will also notify Client if a change request is (i) so significant in scope that it would require a separate engagement between Trustwave and Client or (ii) outside the scope of the Service and, therefore, will only be performed at Trustwave's discretion.

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 the change's potential impact on Client's environment.

Client may review each proposed change. Trustwave will perform the change according to the change window schedule agreed between Client and Trustwave.

Trustwave-Initiated Maintenance and Endpoint Management

Trustwave will, at its discretion, recommend version updates for the Managed Technology. Client will be responsible for implementing such updates and understands failure to implement may result in Trustwave's inability to provide the Service.

Trustwave will monitor the health and availability of the alert and event data from Managed Technology that is connected to the Fusion platform. The health and availability of endpoints that connect to the Managed Technology, and not directly to the Trustwave Fusion platform, are Client's sole responsibility to manage and monitor.

Co-Managed Access Change Management

Trustwave maintains access to the Managed Technology and may provide Client with access permissions to the Managed Technology if Client requires co-management of the Managed Technology's feature sets. Such additional access permissions may include:

- **Read Only:** Default option. Trustwave fully manages the Managed Technology. Client can monitor Managed Technology, but not directly alter without contacting Trustwave.
- **Role Based:** Co-managed option (as permitted by Trustwave). Trustwave grants Client partial access to manage the Managed Technology. See below for related restrictions.
- **Full Admin:** Co-managed option (as permitted by Trustwave). Trustwave grants Client full access to manage the Managed Technology. See below for related restrictions.

If granted Role Based or Full Admin access permissions, Client agrees to the following shared change and change audit process

- Restrictions: Before implementing any changes to the Managed Technology, Client will create a Change 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 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 for Client owned Managed Technology;
- monitor and maintain patches, health, and connectivity of Client's non-Trustwave managed systems, software, and EDR agents to any Managed Technology;
- provide, when requested by Trustwave, prompt access to third-party 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 Ticket requests, 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 and maintain access 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 Change 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 (see service tiers below) 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:

- **Quarterly** – This is the default service tier. The Service automatically includes quarterly 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.

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.

Data Access & Retrieval

Client will have access to parsed logs ("**Events**") and raw logs for a rolling period of at most ninety (90) consecutive days during the Term and beginning on the first day of the Term. Client may access Events via the self-service feature from the Fusion Event Explorer in the Trustwave Fusion platform.

Client may purchase up to nine (9) additional months of rolling access to raw logs only, which will extend the default access period for up to a maximum of three hundred and sixty-five (365) consecutive days during the Term. Such additional months must be purchased at the time of execution of the applicable SOW or Order Confirmation. To access raw logs during any additionally purchased months, Client will submit a ticket in the Trustwave Fusion platform ("**Access Request**"). Any Access Requests (i) requesting a download of two (2) gigabytes or more, or (ii) totaling more than one (1) per calendar month are subject to additional Fees and agreement by Trustwave.

Security Colony Subscription

The Service includes limited access to Security Colony. Security Colony is available at https://www.securitycolony.com/.

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 components: 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

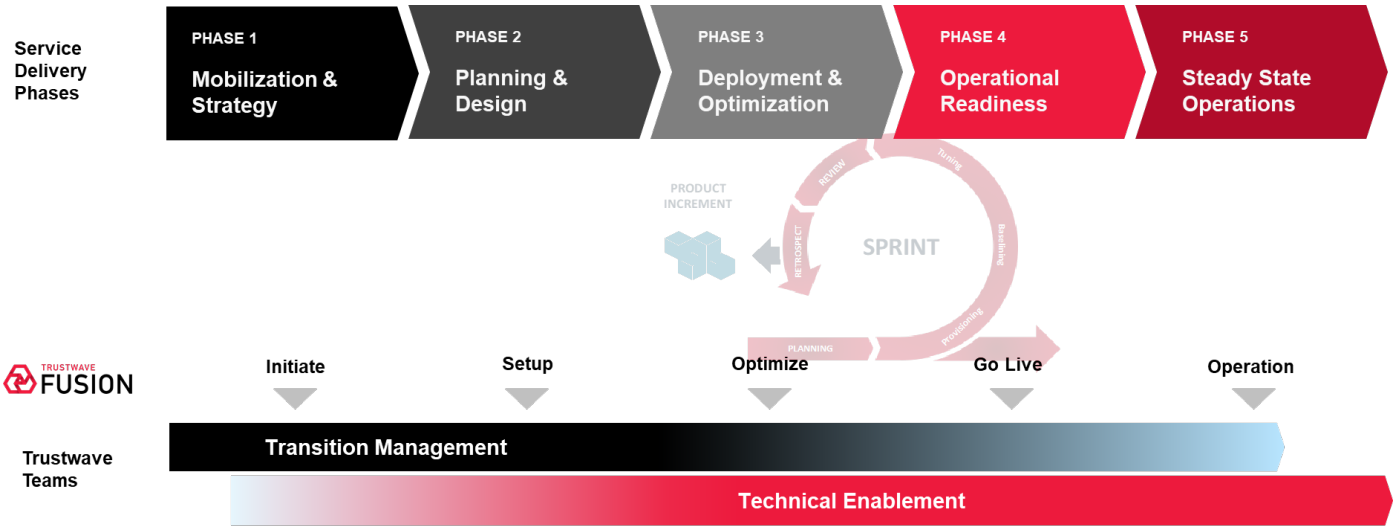
The Service includes a transition management feature to facilitate the integration of the Managed Technology with the Trustwave Fusion platform.

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 regarding the Service;
- coordinate Trustwave technical delivery resources for
    - enrollment of Client and Client's indicated authorized user(s) to the Trustwave Fusion platform
    - collection, review, and assessment of event data for the Service;
    - deployment of connectivity elements for the Trustwave Fusion platform;
    - review of data flow, quality, and analysis; according to the log source supportability and feature support underwritten by a statement of work;
    - analysis and review of endpoint data individually, and collectively for logical groupings, 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 Response Runbook and actions;
    - definition of authorized contacts to groups for the Notification Procedures listed above in Incident Priority Levels; 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

- be responsible for deploying required software for any Client-owned Managed Technology or related endpoints;
- confirm to Trustwave that endpoints are reporting to the Managed Technology in order to support log and alert collection;
- 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 security operations platform. Client is enrolled in the Trustwave Fusion platform as a part of the Service. Client and Trustwave will cooperate to add the Managed Technology to a single Client account within Fusion as part Onboarding (described above) (addition to multiple accounts is not included in the Service). Trustwave and Client may agree to additional scoping terms for the Trustwave Fusion platform (multi-tenancy, hierarchical,

etc.) in an Order Confirmation or SOW to accommodate varying complexity, size, and requirements for Client's Managed Technologies. Client will have access to the following on the Trustwave Fusion platform via web or mobile application:

- Event information, Threat Findings, and Security Incidents
- Device health and availability 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 (provided for an additional fee)

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 for keeping Trustwave Endpoint up-to-date and applying configuration changes according to any Trustwave change management procedures. The events collected by the Trustwave Endpoint will reduce the total number of events remaining under Client's purchased level of million-events-per-day allowance.

Client Obligations

Client will implement Client's managed IT changes and create user accounts for Trustwave in the Managed Technology (as applicable) and pursuant to any Trustwave direction. Trustwave will not provide the Service relying on any access method to Client's managed IT systems except to the extent explicitly agreed to by Trustwave in the SOW or Order Confirmation. Client acknowledges certain access methods may require increases in the applicable Fees.

Trustwave Obligations

Client is responsible for installing the applicable Trustwave Connect deployment model. If separately agreed that Trustwave will install the applicable Trustwave Connect deployment model in Client's environment, Trustwave will also provide Client with the necessary perimeter network access configurations for the Service.

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

Security Telemetry Ingestion & Log Source Support Policy

The Service only supports security telemetry ingestion from Trustwave supported endpoint detection and response (EDR) platforms and specific data sources (see table below). Trustwave may support additional sources, such as firewalls, if agreed in the applicable SOW or Order Confirmation between Client and Trustwave. Trustwave may deliver the Service by acquiring, parsing, or normalizing log, alert, and incident data collected from supported EDR platforms and cloud security platforms (see table below). Trustwave may agree to changes to monitoring and parsing activities at Trustwave's sole discretion.

Supported Data Sources

Trustwave will support the following data sources for the Service. Trustwave may agree to support additional data sources at Trustwave's sole discretion and only to the extent agreed in an Order Confirmation or SOW.

Data Sources Included with the Service and have unlimited ingestion of High Fidelity Alerts

Vendor	Device
Carbon Black	CB Response
CrowdStrike	CrowdStrike Falcon
Cybereason Inc.	Cybereason EDR
Microsoft Corporation	Microsoft Defender for Endpoint
Palo Alto Networks	Palo Alto Cortex XDR

Data Sources Included with the MDR Service and will Count Towards the Events Per Day Events per Day (EPD)

Vendor	Device
Amazon.com	AWS Guard Duty via API
Microsoft Corporation	Microsoft Azure AD Identity Protection
Microsoft Corporation	Microsoft Azure AD Sign In
Microsoft Corporation	Microsoft Azure Security Center
Microsoft Corporation	Microsoft Cloud App Security

Netskope	Netskope SWG
Google	Google Alert Center via API
Microsoft Corporation	Microsoft Azure Activity Logs
Microsoft Corporation	Microsoft Graph
Microsoft Corporation	Microsoft Graph - Azure AD Identity Protection (IPC)
Microsoft Corporation	Microsoft Graph - Azure Advanced Threat Protection (ATP)
Microsoft Corporation	Microsoft Graph - Azure Cloud App Security (MCAS)
Microsoft Corporation	Microsoft Graph - Azure Security Center (ASC)
Microsoft Corporation	Office365 Audit
Palo Alto Networks	Palo Alto Prisma Cloud
Microsoft Corporation	Microsoft Azure Advanced Threat Protection
Microsoft Corporation	Microsoft Azure Defender for IoT via API
Microsoft Corporation	Microsoft Azure Directory Audit
Microsoft Corporation	Microsoft Defender Incidents
Microsoft Corporation	Microsoft Office 365 Security and Compliance
Palo Alto Networks	Palo Alto Prisma Cloud CWPP via API

Correlation & Use Case Management

Trustwave maintains a global use case catalog using 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 detect high- fidelity threats applicable to any of Trustwave's clients. Trustwave's use cases aim to detect threats to the Managed Technology and high fidelity extended detection and response (XDR) alerts using Trustwave intelligence. Trustwave retains sole discretion in determining if conditions are added, modified, or removed to the use case catalog.

Initial Data Ingestion Capacity

The Service includes unlimited collection of security telemetry from supported EDR platforms plus up to five (5) million events per day (MEPD) of additional telemetry from supported data sources (see Security Telemetry Ingestion & Log Source Support Policy for supported data sources). The Service may include additional data volume and sources (such as firewalls) to the extent indicated in the applicable SOW or Order Confirmation between Client and Trustwave.

Capacity Consumption Overages

The Service is provided with an initial data volume and may include additional capacity to the extent indicated in the applicable SOW or Order Confirmation between Client and Trustwave ("**Data Volume Cap**"). Trustwave will periodically review the volume of data and events processed for Client in relation to the Service and may recommend changes. Client may monitor its data volumes in the Trustwave Fusion platform and take actions, including tuning and configuration changes, to maintain volumes within its purchased allotments.

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 two (2) month period, Trustwave may 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.

Trustwave will notify Client of any sustained overage during a two (2) month period and will prescribe actions to limit impact to the Service. Client's failure to take such prescribed actions may result in additional fees payable to Trustwave to accommodate higher ingestion volumes.

If Client data and event volumes exceed the Data Volume Cap such that it impacts Trustwave's ability to perform the Service, Trustwave may immediately suppress, throttle, or filter such excessive data and events. Client acknowledges the Service may not perform as agreed while the Service ingests such excessive volumes of data.

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.