SERVICE DESCRIPTION

Advanced Continual Threat Hunting

Overview

Trustwave's Advanced Continual Threat Hunting (ACTH) service ("**Service**") offers Trustwave's threat hunting capabilities specifically aimed at identifying and responding to undetected threat actors that may be in Client's environment. Trustwave uses behavioral indicator collection, analytics, and systematic enrichment to identify threats within Client's endpoint detection and response (EDR) security solutions which are included in the Service and indicated in the applicable SOW or Order Form ("**Managed Technology**"). The following description sets out the parameters of the Service.

Core Trustwave Features

Trustwave Fusion Platform & Fusion Mobile App

The Trustwave Fusion platform is Trustwave's proprietary cloud-based security operations platform. Client and Trustwave will cooperate to add the Managed Technology to one Client account in the Trustwave Fusion platform as part of the Onboarding feature (see below). Client will have access to the following capabilities on the Trustwave Fusion platform via web or mobile application:

- Security Incidents (as defined below)
- Device health and availability incident tickets
- Client's reports and dashboards
- Request methods for change support and management
- Methods of communication including tickets and chats

Such capabilities and related documentation are available to Client in the Trustwave Fusion platform, including allowing for ticketing integration. Client is responsible for any further connectivity, access, health, and advanced ticketing integrations between Client infrastructure, software, the Managed Technology and the Trustwave Fusion platform. Any changes to connectivity, services, and documentation for the Trustwave Fusion platform advanced integrations are at Trustwave's sole discretion.

Security Events Ingestion & Log Source Support

Trustwave maintains a defined list of log-based and system-monitoring-based event sources supported by the Trustwave Fusion platform and the Service ("**Security Events**"). The Service includes connectivity and collection of Security Events only for the total quantity of contracted, active endpoints in the endpoint detection and response (EDR) Managed Technology specifically set forth in the applicable SOW or Order Form between Client and Trustwave.

Trustwave reserves the right to query, tune, suppress, throttle, or stop ingestion of Security Events to maximize hunt fidelity, align to security best practices, protect platform health, meet licensed levels, or other reasons as needed.

If Trustwave gives Client the option to select the region in which it wants its Trustwave Fusion platform account to be hosted then Client understands it must select the region in its sole discretion. Client is responsible for all appropriate analysis to verify Client selects the region appropriate for its Trustwave Fusion platform account (including any legal or regulatory analysis). Client may only select one region for all Trustwave services it procures. The SOW or Order Form between Trustwave and Client will indicate which region Client selects. The country where Trustwave Fusion platform accounts are hosted for each region is as follows:

Region	Hosting Country
AMS	United States
EMEA	Germany
ASIA	Singapore
PAC	Australia

Systems Management

MDR Bundled Service Option

If Client has concurrently purchased the Service for the same Term with Managed Detection & Response services from Trustwave, Client and Trustwave agree to operate under the terms specified in the Managed Detection and Response applicable SOW or Order Form. Trustwave will solely provide the Service for the Managed Security Application (defined below) connected to Managed Technology under the terms of the Managed Detection and Response service (unless otherwise agreed between Client and Trustwave in writing).

Sole Service Option

When the Client does not concurrently purchase the Service and Managed Detection & Response services from Trustwave, the Service is a stand-alone service. In such case, Client will manage and monitor the security configuration of those Client security applications connecting to the Managed Technology which are included in the Service as indicated in the applicable SOW or Order Form ("**Managed Security Application**"). For the avoidance of doubt, Trustwave will solely provide the Service for Managed Security Application connected to Managed Technology (unless otherwise agreed between Client and Trustwave in writing) and Client is responsible for additional systems management terms below.

Connectivity

Client and Trustwave will work together to connect the Trustwave Fusion platform and the Managed Technology using one or more of the following connection methods (subject to the applicable SOW or Order Form between Client and Trustwave).

- **Trustwave Connect**: A physical or virtual appliance jump box hosted in Client's environment that allows Trustwave to remotely connect the Trustwave Fusion platform to the Managed

Technology. Trustwave will deploy Trustwave Connect based on the model of the Managed Technology indicated in the applicable SOW or Order Form. Trustwave Connect may be a virtual or physical appliance.

- **Direct Connectivity**: A direct connection between the Managed Technology and the Trustwave Fusion platform using either:
    - Trustwave-hosted managed console;
    - Client-hosted managed console; or
    - API connection to the Trustwave Fusion platform (available only with cloud-based Managed Technology via API)

Additional Information

Where Trustwave Connect is used, Trustwave will provide Client the applicable Trustwave Connect deployment model and the necessary perimeter network access configurations for the Service.

Where a Client-hosted managed console is used to connect the Managed Technology to the Trustwave Fusion platform, Client is responsible for implementation and creating Trustwave-user accounts as requested by Trustwave. This connection method is only available to the extent explicitly agreed to by Trustwave in the applicable SOW or Order Form. Client acknowledges certain access methods may require increases in the applicable Fees.

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 Security Application;
- monitor and maintain patches, health, and connectivity of Client's non-Trustwave managed systems, software, and EDR agents to any Managed Security Application, including security application on-premise appliance(s) and networking equipment and applications.
- provide, when requested by Trustwave, prompt and legally permitted 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;
- 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 Security Application.

Trustwave Obligations

- For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will provide Service-related remote assistance within the Managed Technology and Managed Security Application. For the avoidance of doubt assistance for on-premise appliances will be limited to the Managed Security Application software operating on the appliance;
- attempt to resolve connectivity or application issues identified regarding the Managed Security Application to return it to a steady state of operation. Assistance for on-premises appliances will be provided after the Client has provided sufficient evidence of no existing environmental issues or self-initiated changes to the infrastructure that may negatively impact the steady-state operation of the appliance;

- Trustwave will not be responsible for the design, implementation, effect, or any damages, direct or indirect, of any Client changes made to the Managed Security Application, Managed Technology, or Client-managed systems the Service relies upon.

Operations Features

The Service includes the following features:

Onboarding

Onboarding includes two components: Client-side implementation and MSS Transition.

Client-side Implementation

Client will take the necessary steps to connect Client's systems which generate security events to the Trustwave Fusion platform and the Managed Technology (including endpoints to management stations and sensor agents on each endpoint in scope) as agreed between Trustwave and Client in the applicable SOW or Order Form. 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.

If necessary for the Managed Technology to work with the Service, Client will create access groups and individual Trustwave-users in the Client environment that allow such users to deliver services. Client is responsible for providing initial and ongoing Trustwave user and system remote access to the Managed Technology to accommodate Trustwave's remote Threat Hunts.

Trustwave will provide Client with an initial list of users during Onboarding. After Onboarding (during Steady State as defined below), Trustwave will provide Client with ongoing user access, update requests, and use change management tickets to maintain updated user access to the Client's Managed Technology. If Client fails to perform changes and maintain Client-side implementation responsibilities for Trustwave user access to Managed Technology, then Trustwave has no responsibility for providing the Service and Trustwave will not continue with this feature of the Service until Trustwave has the necessary access to the Managed Technology.

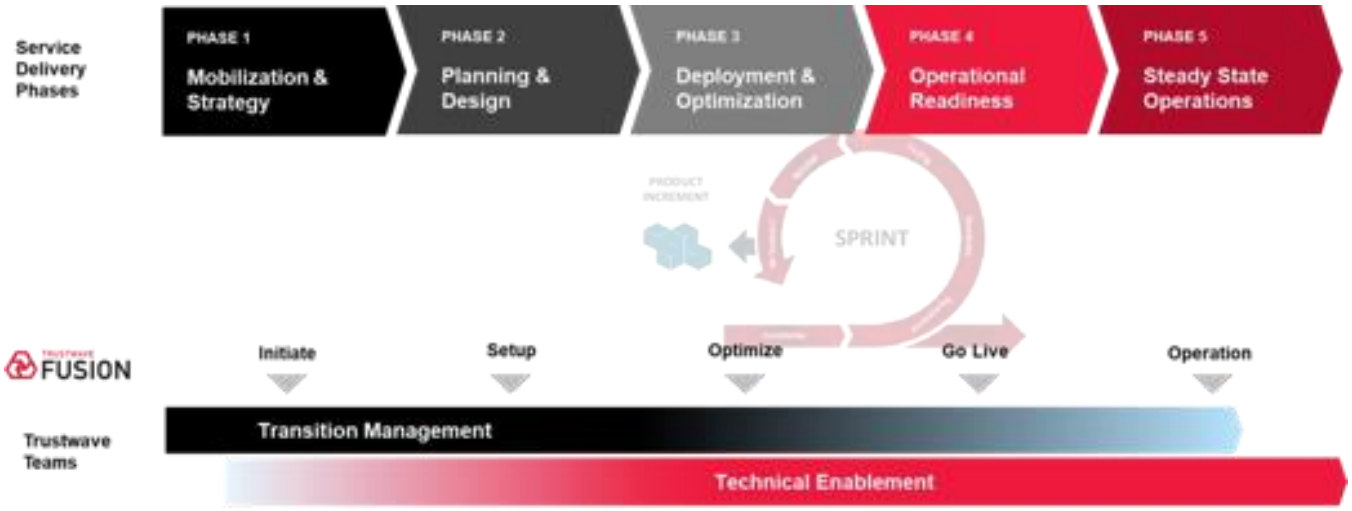
MSS Transition

MSS Transition is designed to facilitate the integration of the Managed Technology with the Trustwave Fusion platform. Trustwave will assign a transition manager and additional technical enablement resources (at Trustwave's discretion) to work with Client on onboarding the Service. Trustwave will advise Client through five (5) phases of transition management. Client is deemed fully transitioned and at steady-state (beginning of the Service features other than Onboarding) following Trustwave's conclusion of the fifth (5^{th}) phase ("**Steady State**").

Trustwave and Client may agree to additional scoping terms in an Order Form or SOW Onboarding to accommodate varying complexity, size, and project governance requirements for Client's security solution.

Transition Management Phases

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



Client Obligations

For Trustwave to provide Onboarding, Client will:

- be responsible for deploying the software necessary for Trustwave to provide the Service for the Managed Technology or related telemetry;
- configure initial and ongoing network connectivity from Client systems to Managed Technology utilizing the Trustwave address ranges and domains that allow Trustwave to provide the Service;
- upon Trustwave's request, confirm to Trustwave that Client systems are reporting to the Managed Technology in order to support log and alert collection;
- ensure Managed Technology has appropriate licensing and support contracts with third parties during the Term.

Trustwave Obligations

As a part of Onboarding, Trustwave will:

- schedule and host a kick-off meeting with Client;
- provide new-user orientation materials and training regarding the Service;
- keep Client informed of transition progress; and
- coordinate Trustwave technical delivery resources to
    - enroll Client and Client's indicated authorized user(s) in the Trustwave Fusion platform;
    - collect, review, and assess event data for tuning;
    - validate network connectivity from Client systems to Managed Technology utilizing the Trustwave address ranges and domains that allow Trustwave to provide the Service;
    - review data flow, quality, and analysis subject to the scope agreed between Trustwave and Client in the applicable SOW or Order Form;
    - validate Client has added authorized contacts to groups for the Notification Procedures listed for Security Incident Priority Levels table below; and
    - conduct an operational readiness assessment to determine if Client has reached Steady State.

Hunt Development

Trustwave will analyze Client's current threat landscape using open-source and other intelligence sources, and SpiderLabs proprietary threat intelligence. Then, Trustwave will build a profile of targeted threat actors' common tactics, techniques, and procedures (TTPs) and design custom, hypothesis-based hunts with the assumption a breach has already occurred on Client's network.

Threat Hunts

Trustwave will perform one of the threat hunts designed above by leveraging Client's Managed Technology and, when the Service is purchased in conjunction with Trustwave's Managed Detection & Response services, may use other telemetry inside Client's environment as Trustwave deems appropriate. Trustwave may use the following threat modeling variables and processes to perform such threat hunts:

- **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 intelligence sources 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 may help identify potential previous compromises and existing corporate vulnerabilities.

Methodology

To perform the hunts, Trustwave will use a proprietary library of hunt queries designed to identify behaviors exhibited by threat groups, actors, and malware campaigns. This library contains queries curated and routinely updated to map to the MITRE ATT&CK matrix. Trustwave will investigate identified and suspicious behaviors that fit into one of the MITRE ATT&CK tactics categories below:

- **Reconnaissance –** Adversary is trying to gather information for future operations.
- **Resource Development –** Adversary is trying to establish resources to support operations.
- **Initial Access –** Adversary is trying to get a foothold in the environment.
- **Execution –** Adversary is trying to run malicious code.
- **Persistence** – Adversary is trying to maintain foothold.
- **Privilege Escalation** – Adversary is trying to gain higher-level permissions.
- **Defense Evasion** – Adversary is trying to avoid detection.
- **Credential Access** – Adversary is trying to steal usernames / passwords.
- **Discovery** – Adversary is trying to conduct reconnaissance internally in the environment.
- **Lateral Movement** – Adversary is moving throughout the environment.
- **Collection** – Adversary is aggregating targeted data.
- **Command and Control** – Adversary is communicating to compromised systems internally or externally.

- **Exfiltration** – Adversary is exporting stolen data.
- **Impact** – Adversary is trying to manipulate, interrupt or destroy, systems, operations and data.

Triage

Trustwave will review the data resulting from each hunt for false positives and separate out suspicious elements for a deeper human-led investigation.

Deep Analysis

Once filtered, Trustwave will hunt through the newly discovered TTPs throughout Client's network to determine the severity of the associated incident. If Trustwave discovers a significant ongoing data breach or widespread infection, Trustwave may recommend Client escalate the incident to a digital forensics and incident response (DFIR) provider. Trustwave will provide information and support for ongoing security events within the Trustwave Fusion platform and the Managed Technology related to any such incident response engagement during the Term of the Service.

Security Incident Escalations

Trustwave will create and store the output of deep analysis where Trustwave identifies malicious findings, vulnerabilities, and network infrastructure deficiencies in Client's environment using security incident tickets within the Trustwave Fusion platform ("**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 incident
- Analysis
- Recommendations
- List of Trustwave actions taken
- Requests for Client to perform recommended actions

In addition, at its sole discretion, Trustwave may request Client collect and submit binary files and suspected malware within the Security Incident for SpiderLabs Malware Reverse Engineering. In such cases, Trustwave may add any further observations, findings, or recommendations developed by this process to the applicable Security Incident.

Client Obligations

For Trustwave to provide this feature, Client will

- retain exclusive responsibility for mitigating actual and potential threats to its environment;
- lead and execute Client processes for incident management and incident response;
- regularly update incident contacts and their respective accesses and information in the Trustwave Fusion platform including contact email, phone numbers, and contact order;
- utilize the Trustwave Fusion platform and mobile app to generate secure communications, notifications, and Service feedback;
- collaborate with Trustwave on security detection and response best practices, including Client deployed configurations, and policy definitions;
- provide initial and ongoing Trustwave user and system remote access to the Managed Technology to accommodate Trustwave's remote analysis as defined by this service description;

- review Security Incidents, notifications, and reports as made available in the Trustwave Fusion platform;
- notify Trustwave if Security Incidents, events or reports are not available in the Trustwave Fusion platform as reasonably expected;
- resolve each Security Incident by providing Security Incident feedback, 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;
- provide network documentation promptly upon request; and
- provide additional telemetry as required.

Trustwave Obligations

For this feature, Trustwave will

- allow authorized Client personnel (authorized by Client) access to the Trustwave Fusion platform to interact with Trustwave personnel and to monitor the Service and as a repository for Client communications for Security Incidents;
- create tickets within the Trustwave Fusion platform to notify of hunt iteration, findings, and required actions;
- collect and process events from the Managed Technology;
- analyze and raise Security Incidents, investigations, and reports identified by Trustwave from events collected from Client's environment;
- provide recommendations aimed to improve Client's overall security posture if a hunt yields actionable findings in Trustwave's sole discretion;
- periodically update the status of Security Incidents in the Trustwave Fusion platform and record communications between Client and Trustwave pertaining to such Security Incidents;
- review Client feedback; and
- conduct further analysis on binaries that are suspicious or require reversing to validate malicious intent and gather additional indicators of compromise.

Security Incident Priority Levels

Client incident contacts defined in the Trustwave Fusion platform will receive communications from Trustwave for Security Incidents via the Trustwave Fusion platform, the Fusion mobile app, email, or phone. Clients should continuously update notification groups in the Trustwave Fusion platform.

Trustwave assigns priority levels to Security Incidents based on factors from Trustwave's investigation, including attack classification, SpiderLabs threat intelligence, security outcome, derived risk, impact, and properties of the events related to the Security Incident. Trustwave will send Client notifications according to the Security Incident's assigned priority and using Trustwave integrated phone, app, and email systems (see table below). Client will document all communications, questions, clarifications, and feedback for the Security Incident in the Trustwave Fusion platform or Fusion mobile app.

Priority	Notification Procedure	Priority Description
Critical (P1)	Phone, App, Email	Security Incidents at this level potentially pose an immediate and 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, App, Email	Security Incidents at this level 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 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.

Problem Management

A problem is a cause or potential cause of one or more incidents impacting the health of the Service. Client agrees to report problems through the Trustwave Fusion platform. Client and Trustwave agree to collaborate on problem resolution subject to Trustwave policy.

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 Form between Trustwave and Client.