SERVICE DESCRIPTION

DarkTrace Technology Implementation Service

Service Scope

Trustwave Technology Implementation Services provides a set of offerings focused on the plan, design, and implement phases of your DarkTrace network security solution. Trustwave implements the solutions vital to any successful security rollout and assists in effective maintenance.

The Services include specific pre-defined deliverables and will be completed at a time mutually agreed to between Client and Trustwave Holdings. The objective of the Services is to implement a solution which may or may not encompass the entire Client environment and health assessment for the deployed environment.

This Implementation Service does not manage the capabilities or execution of Carbon Black Response technology. Detection and Response services are available in MDR for Endpoints MSS; Carbon Black Response Technology Implementation Service is not required for MDR for Endpoints as it is integrated into the MSS.

The Trustwave project team will approach this engagement with the following goals:

- Provide a practical approach to project execution;
- Maintain discipline and structure without constraining the project effort;
- Frame the project within the strategies of Client's business requirements.

Trustwave has defined the effort into three (4) logical phases:

- Phase 1 – Project Initiation
- Phase 2 – Design and Architecture
- Phase 3 – Implementation/Migration
- Phase 4 – Knowledge Transfer
- Phase 5 – Maintenance (optional)

Assumptions

The following assumptions have been made in anticipation of this effort:

- Work under this SOW will be performed at Client's facilities located at **CLIENT'S PREFERRED ADDRESS (to be identified to Trustwave)** except for any project-related activities which Trustwave and Client agree be performed remotely or at Trustwave's premises in order to complete the obligations and responsibilities under this SOW.
- Any additional fees will be first agreed to in writing by Client.
- Trustwave will provide the Services under this SOW during normal business hours, 8:30 AM to 5:15 PM, local time, Monday through Friday, except holidays.

- Client provides sufficient access to the hardware and software environments being used for the project, including network connectivity and required authorizations.
- Client will provide resources with sufficient data security knowledge for this project.
- Client ensures sufficient security and compliance user participation.
- Client ensures sufficient access to Database administrators, Network and System Administrators as needed.
- Client will ensure that a proven backup and recovery strategy is in place for the systems being upgraded.
- Client will ensure that all hardware & software requirements have been met and configuration recommendations have been followed prior to the start of the Project. Client acknowledges that DarkTrace technology will not be installed without minimum specifications and may not perform optimally unless system sizing recommendations have been met. Any delays encountered as a result of system specifications or recommendations not being met are Client's responsibility.
- Client will test the DarkTrace technology solution according to the schedule and procedures outlined jointly with Trustwave.
- Client and Trustwave will ensure the steps outlined in the project plan are achieved in a timely manner.
- To complete certain Tasks and Deliverables under this SOW, Trustwave may request access to specific servers, network equipment, etc., as needed. Such access and related activities will only be performed with Client's explicit authorization, and always under direct Client supervision.
- Where used, "Duration" refers to man effort and not elapsed time.

Exclusions

- Trustwave will not provide Structure cabling, UPS, Patch Cords or Racks.
- Offering does not include performing Proof of Concept effort.
- Offering does not include customization or plug-in, e.g. report, API, alert, unless otherwise stated.
- Offering does not include whole network or infra redesigning effort.
- Offering does not include Load/Performance testing.
- Offering does not include Vulnerability Testing/Penetration Testing.
- Offering does not include external backup, logging and monitoring solution
- Support for operation tasks, e.g. change request, is not part of the scope. Username and password shall be handed over to customer operation team to perform operation tasks, e.g. check log, implementing Change Request, add/edit/remove policy.
- The Services do not include an assessment of the Customer's organization, personnel, or IT infrastructure compliance to existing policies, practices, standards, guidelines, processes, or procedures, and is not intended to provide assurance of compliance with any industry, regulatory, or legislative requirements.
- Any additional actions not defined in this SOW.
- Services in excess of the man-hours scoped in the order form.

Facilities

Client will provide Trustwave and its personnel with facilities that Trustwave may reasonably require to perform the Services, in particular: supplies, furniture, computer facilities, telephone/fax communications, and broadband access via network connectivity capability and other facilities. The Trustwave project team will be located in an area adjacent to your subject matter experts and technical personnel and all necessary security badges and clearance will be provided for access to this area. Client will be responsible for ensuring that Client has appropriate backup, security and virus-checking procedures in place for any computer facilities Client provides or which may be affected by the Services.

Completion Criteria

Trustwave will have fulfilled its obligations under this SOW when any one of the following occurs:

1. Trustwave accomplishes the activities defined in the scope, in accordance with the terms and conditions set forth in the agreement between the parties, including but not limited to the warranties contained therein, including delivery to Client of the Materials agreed to, if any; or
2. Trustwave provides a certain number of man-hours of Services as specified in the order form;

3. Client or Trustwave terminates the project in accordance with the provisions of the Agreement; or
4. The end of the term specified in the order form.

Project Phases & Timelines

This section defines the major tasks for the project. The appropriate estimate, based on Trustwave's knowledge of the date of signatures in the scoping document and/or order form, will likely outline man-hour initiative as follows:

Phase 1: Project Initiation

Estimated duration to be agreed by the parties.

The purpose for this activity is to kick off the project and set expectations with the client

Trustwave will work with Client to review the current infrastructure, change control, and other project processes and expectations. Trustwave will initiate data gathering process to receive initial information about the customer environment.

	Task	Participants
1	Set project expectation with Client	Client and Trustwave
2	Provide initial environment information	Client
3	Initial project plan creation	Trustwave

Data gathered from Client's environment:

a) Complete inventory of all networking devices, such as routers, switches, firewalls, wireless…
b) Device model, software version, firmware revision, IP addressing, MAC addressing
c) Current state network design

Note: For Clients that cannot provide the information above, assigned Network Engineer should be scoped.

Phase 1 Deliverables:

- Initial Project Plan
- Network topology documentation

Phase 2: Design & Architecture

Estimated duration to be agreed by the parties.

The purpose of this activity is to help the project team scope and design the implementation based on business needs and technical environment. The Trustwave project team will work with Client to gather necessary data from network administrators and designers.

Phase 2 Requirements

- Complete the pre-engagement Data gathering

Phase 2 Tasks:

	Task	Participants
1	Existing topology documentation	Client

2	Scoping of DarkTrace deployment functions and requirements	Client and Trustwave
3	Documentation of key functions/requirements and a test plan to ensure full validation during the deployment.	Client and Trustwave
3.1	Data flow mapping - Mapping data is a subset of the data ingested by Darktrace and enables Darktrace to track devices as they move around a network. This is especially important in the analysis of user devices, since these will typically have dynamically-assigned IP addresses. Mapping data usually takes the form of DHCP events seen in transactional data provided by legitimate corporate DHCP servers. These are automatically ingested and the tracking of devices is seamlessly handled by Darktrace. Other forms of mapping data may be used, depending on your specific environment.	
3.2	Ingestion Recommendation – The ingestion of network data into a Darktrace appliance is typically performed by one of three methods. (Depending on your infrastructure and environment, there may be other options. These options are not mutually exclusive and any combination of these methods may be used): • Layer 3 SPAN (VLAN mirroring); • Layer 2 SPAN (Port mirroring); • Network taps. In many situations it is preferable to configure multiple points of data capture. The aggregation of these data capture points may necessitate passing duplicate packets to the Darktrace appliance. However, the Darktrace platform is aware that some packets may be duplicates and methods are in place which mean that duplicate packets do not affect the behavioral models.	
4	Development and documentation of a network diagram that details what equipment will be deployed where.	Client and Trustwave
5	Creation of deployment design document.	Trustwave
6	Update of project plan with timelines and responsibilities.	Trustwave

The design document and accompanying network diagrams may cover the following elements.

- Network Topology
  - Current Topology
  - Future Topology
  - Migration Strategy
  - Global High-Level Topology

  - Any site-specific differences
  - Routing
  - Private Cloud
  - Public Cloud
- DarkTrace Technology
  - Data mapping
  - Data ingestion recommendations (VLAN mirroring, Port mirroring, network taps).
  - DarkTrace configuration recommendations
    - Appliance implementation
    - Log and/or SIEM configuration
    - Complex configurations (multiple physical and/or virtual appliances)

Phase 2 Deliverables:

- Project Plan for deployment
  - Roles and responsibilities
  - Timeline and milestones
- Overview and detailed network diagrams
- Use case/key requirements documentation and approach to resolve.

Phase 3: Implementation and Validation

Estimated duration to be agreed by the parties.

During the implementation phase Trustwave will, with Client assistance, implement the DarkTrace technology design and equipment scoped in Phase 2.

Guided by the agreed-on design documentation the implementation phase will follow the following high-level outline. Trustwave will validate implementation according to the design document and remain onsite for up to half day as well as provide remote standby where needed.

Phase 3 Requirements

The following must be completed prior to start of work:

- Client has agreed on the design documentation
- Hardware and software platforms prepared and available for implementation
- Designating a Project Technical Lead who will be the primary contact during the implementation
- Have appropriate change requests approved (if needed) and an agreement on change control windows.

Phase 3 Tasks

	Task	Participants
1	Technology Deployment - Depending on your network topology, a deployment may require more than one Darktrace appliance at more than one location. There are several types of Darktrace appliance which, depending on your network, may perform different functions. • Single appliance, single capture point • Single appliance, multiple capture points • Complex network deployment (master/probe configurations)	Client and Trustwave

2	Technology Configuration – Based on phase two design and architecture, DarkTrace will be configurated to support network monitoring (VLAN mirroring, Port mirroring, network taps) and can be configured to include device log and/or SIEM data to incorporate historical information in DarkTrace analysis.	Client and Trustwave
3	Post-Migration Threat Assessment – Trustwave will perform a post-migration Threat Assessment of live traffic. Based on the Analysis, Trustwave will provide additional documented changes to configurations to further secure the client network. The results of the Threat Analysis will be appended to the approved design documentation	Trustwave

Phase 3 Deliverables:

- Completed implementation as per design document (Phase 2)
- Updated design documentation with any agreed changes made during deployment.

Phase 4: Knowledge Transfer

Estimated duration to be agreed by the parties.

Trustwave will ensure that Client is familiar with the deployed solution. This will be achieved through a handover process. Knowledge transfer to the team occurs interactively during the engagement and covers the installation, configuration, and basic administration of the Firewall solution.

Phase 4 Tasks:

	Task	Participants
1	Review as-built document. This document consists of non-default setting/parameter configured during deployment, not a how-to guide.	Client and Trustwave
2	Knowledge Transfer Activities with reference to implementation solution	Client and Trustwave
3	Review the actions and decisions that were taken during the validation phase.	Client and Trustwave
4	Review the actions and remediation's taken during the different phases of the project to go over an operations knowledge transfer.	Client and Trustwave
5	Review Procedures for contacting Trustwave Maintenance Support where applicable	Client and Trustwave

Phase 5: Maintenance Health Check

Estimated duration to be agreed by the parties.

On a selected periodic basis, Trustwave staff will remotely access each of the security products deployed at the customer site to perform a system review.

Trustwave will verify the following as part of a health check service:

- Verify current patch levels.
- Audit log review
    - Identification of any performance issues
    - Identification of any potential security issues.
- Old or unused policies verification and recommendation.

Note: Additional checks are continuously added based on Trustwave's best practices for deployment and maintenance.

Phase 5 Deliverables:

- Health Status report.
- Recommended remediation activities (if applicable)

Project Staffing

Trustwave will coordinate the Trustwave resources and provide project management inputs to Client's project manager.

Roles and Responsibilities

Success of this project is dependent on our mutual understanding of roles and responsibilities. This section details Client and consultant participation and responsibilities.

Client Project Manager

Prior to the start of this engagement, Client will designate a person to be the Client Project Manager who will be the focal point for Trustwave communications relative to this project and will have the authority to act on behalf of Client in all matters regarding this project. Client's Project Manager's responsibilities include:

- Manage Client personnel and responsibilities for this project.
- Serve as the interface between Trustwave and all Client departments participating in the project.
- Administer the Project Change Control Procedure with the Trustwave Implementation Manager.
- Participate in project status meetings.
- Help resolve project issues and escalate issues within Client's organization, as necessary.
- Review with the Trustwave Implementation Manager any of Client's invoice or billing requirements. Requirements that deviate from Trustwave's standard invoice format or billing procedures may have an effect on price, and will be managed through an Addendum or additional order form.

Client IT Responsibilities

- Provide supervised access to hardware, software, database, and network, when needed.
- Validate deployed solution and assume maintenance of it at the end of implementation phase.

Client Network Administrator

- Provide appropriate subject matter experts to participate in the project.
- Provide policy and reporting requirements.
- Review and approve solution designs.
- Design and develop any new change control processes required to maintain DarkTrace technology solution.
- Approve the promotion of the system to production.

Trustwave Project Management

- Create project plan with timelines as well as roles and responsibilities based on Design Document.
- Align Trustwave resources with tasks and coordinate work schedule. Work with Client Project manager to ensure appropriate resources are booked as required while deployment work is in progress.
- Lead weekly project status meetings to ensure all parties are inline with progress and next steps.
- Track project progression and measured milestones to ensure timely delivery.

Trustwave Network Engineer

- Provide input in requirements gathering to tailor DarkTrace technology solution to client environment.
- Provide expertise in deployment and customization of deployed hardware and software.
- Provide product knowledge transfer to Client staff. This supplements formal DarkTrace technology training with specifics of how solution was customized for Client's network.
- Provide standard product documentation, as necessary.
- Provide all Trustwave deliverables for signoff.