SERVICE DESCRIPTION

Cybereason Technology (EDR and NGAV) Implementation Service

Service Scope

Trustwave Technology Implementation Services provides a set of offerings focused on the plan, design, and implement phases of your Cybereason Technology (Endpoint Detection & Response or EDR; Next Generation Anti-Virus or NGAV) endpoint security solution. Trustwave implements best practices for a successful security rollout and assists in effective maintenance.

The Services include 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 an endpoint security solution which may or may not encompass the entire Client environment and health assessment for the deployed environment.

The Trustwave project team will approach this engagement with the following perspectives in mind:

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

Trustwave has defined the effort into the following phased approach:

- Phase 1 – Project Initiation
- Phase 2 – Design & 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:

- Services will be performed at Client's facilities specified in advance except for any mutually agreed activities that may be performed remotely or from a Trustwave location.
- 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 will provide sufficient access to the hardware and software environments being used for the project, including network connectivity and required authorizations.
- Client will provide resources and personnel with sufficient data security knowledge for this project.

- Client will ensure sufficient security and compliance user participation.
- Client will ensure 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 and software requirements have been met and configuration recommendations have been followed, prior to the start of the Project. Client acknowledges that Cybereason Technology (EDR and NGAV) technology will not be installed until and unless Trustwave's provided system sizing recommendations have been met. Any delays encountered as a result of system specifications or recommendations not being met are the Client's responsibility.
- Client will test the Cybereason Technology (EDR and NGAV) technology solution according to the schedule and procedures outlined jointly with Trustwave.
- Client and Trustwave will make commercially reasonable efforts to complete tasks in a timely manner as mutually agreed.
- 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

- This Service does not manage the capabilities or execution of Cybereason Technology (EDR and NGAV) technology. (This type of service is available in an MDR for Endpoints MSS. Cybereason Technology Implementation Service is not required for MDR for Endpoints as it is integrated into the MSS.)
- 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 network or infrastructure redesign services.
- Offering does not include load or performance testing.
- Offering does not include vulnerability testing or 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 submitted to Client 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 Client'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 are excluded.
- Services days beyond [number] ([##]) man-hours are excluded.

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 while Trustwave is working on the project. The Trustwave project team will be 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:

- Trustwave accomplishes the activities defined in this SOW, in accordance with the terms and conditions set forth in the Agreement, including but not limited to the warranties contained therein, including delivery to Client of the Materials agreed to, if any;
- Trustwave provides [number] ([##]) man-hours of Services as specified in Phases 1 - 5;
- Client or Trustwave terminates the project in accordance with the provisions of the Agreement; or
- The end of the one-year term of this SOW.

Project Phases & Timelines

This section defines the major tasks for the project. Trustwave's current estimate, based on Trustwave's present knowledge, outlines the 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 a data gathering process to receive initial information about the Client 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:

- Complete inventory of all endpoint devices, such as servers, desktops, and laptops managed by either Windows, Linux, or MAC OS.
- Device model, software version, firmware revision, IP addressing, MAC addressing.
- Current state network design.

Note: If client cannot provide the information above, assigned additional time will be required for discovery engagement that will collect and document complete scope.

Phase 1 Deliverables:

- Initial Project Plan
- Endpoint topology documentation

Phase 2: Design & Architecture

Estimated duration to be agreed by the parties.

The purpose of this activity is to help the Trustwave 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 endpoint topology documentation	Client
2	Scoping of Cybereason 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
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 project plan with timelines and responsibilities	Trustwave

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

- Endpoint Topology
  - Current (to include High/Med/Low prioritization)
  - Future (to include High/Med/Low prioritization)
  - Global High-Level Topology
  - Any site-specific differences
- Cybereason Technology (EDR and NGAV) Technology
  - On-premise or cloud-based analysis server
  - Deployment and validation of Cybereason sensors (light agents)

Phase 2 Deliverables:

- Project Plan for deployment
  - Roles and responsibilities
  - Timeline and milestones
- Use case/key requirements documentation and approach to resolve.
- Recommendations for Cybereason technology configuration

Phase 3: Implementation and Validation

Estimated duration to be agreed by the parties.

During the implementation phase Trustwave will, with Client assistance, implement the Cybereason 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:

- Accepted the design documentation
- Prepared hardware and software platforms and made available for implementation
- Assigned Project Technical Lead who will be the primary contact during the implementation
- Approved all necessary change requests and, if needed, agreed on change control windows.

Phase 3 Tasks

	Task	Participants
1	Technology Deployment - Depending on your network topology, Trustwave may require differing Cybereason Technology (EDR and NGAV) server types. There are several types of Cybereason Technology (EDR and NGAV) implementation, depending on your endpoint protection strategy, may perform different functions. • Cybereason Analysis Server Application (Cloud-based). • Cybereason Analysis Server Application (On-premises).	Client and Trustwave
2	Technology Deployment (Sensors) – Preconfigured endpoint sensors (light agents) are to be deployed through Client’s standard software deployment tools (unless otherwise noted).	Client and Trustwave
2	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 Phase 2 design document.
- As-built “run book”: updated design documentation with any agreed changes made during deployment.

Phase 4: Knowledge Transfer

Estimated duration to be agreed by the parties.

Trustwave will help ensure that Client understands the deployed solution. This will be achieved through a handover process. Knowledge transfer to Client occurs interactively during the engagement and covers the installation, configuration, and basic administration of the Endpoint 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 to Client on implemented 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 will remotely access each of the security products deployed at the Client 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

Client Project Manager

Prior to the start of this SOW, Client will designate a person to be the Client Project Manager who will be the focal point for Trustwave communications related to this project and will have the authority to act on behalf of Client in all matters regarding this project. Client 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 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 influence price and will be managed through an Addendum.

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 the implementation phase.

Client Security Consultant

- 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 Cybereason Technology (EDR and NGAV) 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 the 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 aligned with progress and next steps.

Trustwave Security Consultant

- Provide input in requirements gathering to tailor Cybereason Technology (EDR and NGAV) technology solution to Client environment.
- Provide expertise in deployment and customization of deployed hardware and software.
- Provide product knowledge transfer to Client. This supplements formal Cybereason Technology (EDR and NGAV) 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.