SERVICE DESCRIPTION

Managed Database Security

Service Description Overview

DbProtect is a database security and compliance solution that helps organizations control their database security processes in a more streamlined way. Designed to scale from small to medium sized businesses, to large enterprises, DbProtect boosts operational efficiency and streamlines key database security activities while enabling organizations to help achieve database security, minimize risk, and achieve regulatory compliance.

Trustwave Managed Database Security utilizes the Trustwave DbProtect product, which is installed locally in a client's environment and remotely managed by Trustwave experts.

Trustwave will maintain and manage the Client's instance of DbProtect, which includes scan schedule, on-demand scans, and real-time monitoring. The Client's security process will define how Trustwave implements and configures the scan and monitor policy(ies) along with patching, updates, and upgrades.

- Trustwave Managed Database Security – Scanning will allow organizations to utilize DbProtect for their vulnerability scanning and user rights reviewing.
- Trustwave Managed Database Security – Monitoring will allow organizations to utilize DbProtect for their database activity monitoring requirements.

Features

Trustwave will provide the following services:

Scan Maintenance	On-demand Scans	Maintenance	Monitoring
• Scheduling • Policy • Validation • Reporting	• New database scans • Remediation Validation Scans	• Upgrades /Patches/Updates • Health Monitoring	• Alert Notification • Policy • Reporting

Service Operations

Scan Maintenance

Scheduling

- Clients may have a mix of scan schedules as long they have processes in place to utilize the results within their vulnerability or development lifecycles.

Policy

- Trustwave will define Client's policy(ies) to ensure that only applicable checks are enabled. Trustwave will create as many policies as needed to ensure that the scan(s) can complete in a reasonable timeframe.

Validation

- Trustwave will monitor scans as they start and complete. Trustwave will provide Client with a report identifying the targets that DbProtect was unable to scan and the reason that such scan was not possible. Trustwave will investigate and notify the Client if an error report is returned for any scan.

Reporting

- Trustwave will generate reports for Client using default report templates. Trustwave will not edit reports except in the event that makes it impossible to distribute the report because of its size or other factors.

On-Demand Scans

New Database Scans

- As Client deploys a new database, Client may request an on-demand vulnerability scan. Client is guaranteed two on-demand scans per quarter, subject to asset license availability within the Client's DbProtect license count.

Remediation Scans

- A remediation scan is a scheduled scan to test for previously known vulnerabilities. Clients are guaranteed one remediation scan per completed scan.

Maintenance

Upgrades

- Trustwave will apply upgrades, patches, and/or updates to DbProtect during scheduled maintenance windows of Client's choosing. Client will be responsible for any OS upgrades and patching, and or upgrading sensors on databases.

Health Monitoring

- Trustwave will provide health monitoring of DbProtect. Trustwave will notify Client if DbProtect becomes unreachable. Trustwave will monitor scan start and completion. If the issue is outside of DbProtect, Trustwave will notify Client and provide information. Client is solely responsible for any errors, bugs or other such issues that occur outside of DbProtect. Trustwave will assist in gathering any information needed to resolve the issue.

Monitoring

Alert Notification

- Client will receive automated alert notification from the Trustwave Fusion Platform. For additional information, please see the Incident Management Policy below.
- Trustwave will define Client's policy(ies) to ensure that only applicable rules are enabled. Trustwave will create as many policies as needed to ensure that there is limited to no impact on the databases being monitored.

Reporting

- Trustwave will generate reports for Client using the default report templates. Trustwave will not edit reports except in the event that makes it impossible to distribute the report because of its size or other factors.

Change Management

Change Management SLAs are valid for both Trustwave-initiated and customer-initiated change requests. Each type of change request categorization is attached to an appropriate SLA as described below.

Table 1: Change Management SLAs

Type of Request	Constructs	Completion time
Emergency Security Change Request	Immediate security threat mitigation • Change for mitigating security risk(s) identified by SOC or Client. • Involves security policy settings, not an upgrade of software or patch for the managed technology.	Within 4 Hours
Standard Change Request	Scheduled changes which can be planned for in advance and are proactive rather than reactive in nature. • Can be planned, not a significant impact on managed technology. • Does not alter architectural design or functions of managed technology.	Within 24 Hours
Normal Change Request	Large changes that are planned and scheduled appropriately. • Scheduled changes that could potentially have a major impact on the functions of the managed technology. • Could alter the architectural design of the managed technology. • Could require POC to be completed prior to scheduling. An error during this change could have significant outage consequences.	Lead Time 7 calendar days Governed by Trustwave's change board review process. Weekly maintenance window planned with the customer to take place during a client maintenance window as approved and collaborated with the client.

Trustwave will setup a change window to apply changes in the Client environment. Change window will be available per global geographic region twice a week (Americas, EMEA, APAC) and will be available for normal change requests and standard requests when SLA time frame falls within the change window.

Incident Management

The goal of Incident Management is to restore normal service operations as quickly as possible and minimize disruption to users' work while ensuring agreed levels of service quality are maintained.

Table 3: Incident Management SLAs

Type of Outage	Definition	Initial Notification	Notification Type
Total Outage (Critical)	Technology total outage affecting a majority of users on-site. This may include any technology service component, such as interface, software or hardware failure, and power or network failure.	30 min	Email generated from the ticket and defined client notification policy
Threat Detected	Trustwave detects and determines a potential threat in a Client environment based on available information.	15 min	Email generated from the ticket and defined client notification policy*

***** If Client provides a notification policy to Trustwave prior to such potential security compromise, Trustwave will provide such notification according to that notification policy.

Exclusions

Trustwave's Managed Services SLAs will only apply to the supported technologies. The following is excluded:

- Changes to structure cabling, UPS, patch cords or racks
- Any customization or plug-in, (e.g. report, API, alert) unless otherwise stated
- Networks and interconnected devices that are not monitored or managed by Trustwave
- Infrastructure redesign efforts
- Database Versions that are not supported by Trustwave

Trustwave will report its compliance to Client upon request.

Responsibilities and Assumptions

Client

- Remediate any failed scans due to credentials or database host connection issues.
- Review events and reports provided to Client.
- Notify Trustwave if events or relevant reports are not available as expected.
- Provide Trustwave with requested information and confirmations in a timely manner.
- Provide an accurate and validated account of supported databases.
- Render assistance when required to upgrade, update, or troubleshoot any host-based sensor as these are installed on Client Databases.
- Provide remote access to DbProtect and its components, as this is required to maintain the health and operation of the system.

Trustwave

- Create an exception rule or turn off the relevant rule for identified false positives of monitoring events.
- Ensure DbProtect is running and completing schedule scans.
- Ensure DbProtect is monitoring Client selected databases.
- Notify Client in case of suspected, actual, or potential threat.

Assumptions

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

- All implementation services to be performed in accordance with this Service Description will be at Client's facilities located at the Client Location except for any project-related activities which Trustwave and Client agree would be best performed remotely or at Trustwave's premises in order to complete its obligations and responsibilities under this Service Description. All work performed in Phase 5 will be provided remotely.
- Trustwave will provide the Implementation 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 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 analyzed. Client will ensure that all hardware & software requirements have been met and configuration recommendations have been followed, prior to implementation, as discussed above.. Any delays encountered as a result of system specifications or recommendations not being met are the Client's responsibility.
- Client and Trustwave will ensure the steps outlined in any project plans are achieved in a timely manner. To complete certain Tasks and Deliverables as part of this Service, Trustwave may request access to specific servers, network equipment, etc., as reasonably necessary to provide the Services. Such access and related activities will only be performed with Client's explicit authorization, and always under direct Client supervision.

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 this Service Description, in accordance with the terms and conditions set forth in an 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-days of Services as specified in the applicable order form or statement of work;
3. Client or Trustwave terminates the project in accordance with the provisions of the Agreement; or
4. The applicable Term, as defined in the applicable Order Form expires.

Provisioning and Implementation

Phase 0: Project Initiation

The purpose of this Phase is to finalize the project team members, develop a common understanding of the project objectives, roles and responsibilities and validate Client readiness to engage the Services by confirming the appropriate information is documented.

Trustwave will:

1. Project Initiation Call
    a. Prepare and distribute any data collection questionnaires; and
    b. Facilitate a project initiation conference call for up to two hours on a mutually agreed date and time to initiate the project
        i. Introduce the project participants
            1. Discuss project team's roles and responsibilities;
            2. Review the project objectives; and
            3. Provide an overview of the project methodology;
        ii. Discuss key business drivers and/or dependencies that could influence project delivery or timelines;
    c. Review format of weekly project status report; and
    d. Review high level project plan and schedule of activities.
2. Project Mobilization Meeting
    a. Conduct a project kickoff meeting to communicate the objectives of the project;
    b. Review and communicate requirements and project goals with key participants; and
    c. Finalize list of DB instances, including location and primary point contact.

Completion Criteria: This Phase will be complete when the project initiation and project kick-off meetings have concluded.

Note: Phase 2 is only optional if Activity Monitoring is not selected as a module

Phase 1: Installation and configuration of DbProtect Management Console and Scan Engine(s)

Deliverables:

1. Deployment Planning
    a. DbProtect Installation and Configuration
    b. Scan Engine installation
        i. Determine how to deploy based on Client's deployment methodology
    c. Account validation - ensure appropriate accounts have been created to run the scans
2. Provide assistance with scan engine installations
3. Validate that Vulnerability Assessment and Rights Management Scans are running as expected (Optional)

The purpose of this Phase is to install the DbProtect Console and components in the Client's production environment. During this Phase, the Client's project team will review the server configuration inventory to verify where DbProtect scan engines should be deployed. In addition to this all necessary firewall rules will be put in place for the operation of DbProtect and the Managed Services.

	Task	Participants
1	Review the Client's Database Server Configuration Inventory	Client & Trustwave

2	Validate appropriate accounts have been created for DbProtect deployment	Client & Trustwave
3	Identify all necessary firewall rules for DbProtect and Managed Services functionality and start process to implement rules	Client & Trustwave
4	Configure production hardware per Trustwave's recommendations	Client
5	Install Windows 2016 O/S for Console Server and Install Windows 2016 O/S for Scan Engine and MS SQL Server 2016 Server	Client
6	Install DbProtect Console on production server	Client & Trustwave
7	Install DbProtect Scan Engines, configure appropriate IP ranges and Register with console.	Client & Trustwave
8	Deploy and Configure Trustwave Connect box for Managed Services	Client & Trustwave
9	Deploy production vulnerability assessment policy, optional	Client & Trustwave
10	Run Vulnerability Assessment and/or Rights Management jobs to validate that scan engines and policies are operating as expected, optional.	Client & Trustwave

Phase 2: [Optional] Activity Monitoring policy development, sensor deployment and tuning

Deliverables:

1. Sensors installed, registered, and configured
2. Built-in activity monitoring policies created based on customer business requirements
3. Activity monitoring policies deployed to sensors
4. Tuning performed as needed

During this Phase, a policy to enforce Client's security requirements for Activity Monitoring will be generated. Sensors will be installed, registered, and tuned, as necessary, during this phase.

	Task	Participants
1	Conduct Policy development workshop for Activity Monitoring	Client & Trustwave
2	Install Sensors on Client selected databases	Client & Trustwave
3	Deploy Policy, verify and test monitoring activity through Analytics reporting capabilities	Client & Trustwave

4	Provide Sensor Tuning	Client & Trustwave

Phase 3: DbProtect User Training

Deliverables:

1. Training & Knowledge transfer completed
2. Assistance with new console configuration provided
3. Built-in reports that Client will use to meet their audit requirements reviewed

During this Phase, the Client will attend a training session on the use and reporting features of DbProtect.

	High-level Activities

1	Train Client's team on DbProtect
	• Analytics and Reporting
	  ○ Operations
	  ○ Security
	  ○ Compliance
	  ○ Vulnerability Assessment

2	Conduct best practices workshop • How other customers are using DbProtect • Vulnerability Severity/Importance Scoring • Reporting - get the right data, to the right people, at the right time

Phase 4: Transition to Steady State Services

Deliverables:

1. Services Mobilization and Planning
2. Updated monitoring plan
3. Complete readiness checklist
4. Finalize Service Manual

During this Phase, the DbProtect environment will be reviewed and recommendations made. This Phase involves preparation and integration with Trustwave.

	Task	**Participants**
1	Resource mobilization and scheduling	Client & Trustwave
2	Review SOW with Client POC	Client & Trustwave
3	Finalize communications plan	Client & Trustwave
4	Validate all firewall rules are in place and DbProtect components are accessible	Client & Trustwave
5	Integrate DbProtect with Trustwave supporting systems and validate connectivity, as needed	Client & Trustwave

6	Update Managed DbProtect Monitoring Plan document, as needed	Client & Trustwave
7	Finalize Day 1 monitoring plan with Client POC	Client & Trustwave
8	Complete Managed DbProtect Readiness Checklist	Client & Trustwave
9	Setup VPN's and remote access for Trustwave	Client & Trustwave
10	Perform go-live operations testing	Client & Trustwave
11	System and policy validation	Client & Trustwave
12	Finalize Service Manual with Client POC	Client & Trustwave

Phase 5: Managed DbProtect Run Services

Deliverables:

1. Alert Monitoring
2. Report generation and error investigations
3. Change and policy requests
4. Upgrades and patches
5. Vulnerability and Rights Management scanning

During this Phase, the DbProtect environment will be moved to steady state operations with Trustwave. Trustwave will require the assistance of the Client for any host-based Sensors that are installed on Database Hosts.

	Task	Participants
1	Alert Monitoring, if in scope with Database Activity Monitoring	Trustwave
2	Report generation	Trustwave
3	Missing and error report investigation	Trustwave
4	Change requests and policy change requests	Trustwave
5	DbProtect upgrades	Trustwave
6	Sensor upgrades	Client & Trustwave
7	DbProtect patches	Trustwave
8	Infrastructure and outage issues	Trustwave
9	Vulnerability Management Scanning, if in scope	Trustwave
10	Rights Management scanning, if in scope	Trustwave