Trustwave®

SERVICE DESCRIPTION

Managed Database Security

Overview

Trustwave's managed database security service ("**Service**") provides remote maintenance and management of Client's locally installed instance of Trustwave's database security and compliance software ("**DbProtect**"). Client's security process guides Trustwave's implementation and configuration of specific DbProtect scanning and automated database monitoring policies, patching, updates, and upgrades. 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

This Service includes the following features:

General Components

Scan Maintenance

Trustwave will review and define Client's policies to ensure that only Client-selected and Trustwave-implemented database checks are enabled ("**Ongoing Scans**") and scans complete within a reasonable timeframe. Trustwave will also monitor scans as they start and complete. Trustwave will provide Client with a report identifying the targets that DbProtect was unable to scan along with supportive reasoning. Trustwave will investigate and notify the Client if an error report is returned for any scan.

Trustwave will generate reports for Client using Trustwave's DbProtect reporting templates. Trustwave will not edit reports unless their size inhibits distribution.

On-Demand Scans

In addition to the Ongoing Scans, Trustwave will provide upon Client's prior request up to two (2) on-demand scans per quarter for each new database deployed, subject to Client's DbProtect license availability. Client may also request a remediation scan, which tests previously known vulnerabilities. Client is guaranteed one remediation scan per completed scan.

Maintenance

Trustwave will apply DbProtect upgrades, patches, and updates to DbProtect during Client's scheduled maintenance windows. However, Client will apply any operating system (OS) upgrades or patching and database sensor upgrades. Trustwave will also provide DbProtect health monitoring including 1) notifying Client if DbProtect becomes unreachable, and 2) monitoring DbProtect scan success. If Trustwave determines any issue falls outside of DbProtect, Trustwave will notify Client and provide

information; however, Client is solely responsible for any errors, bugs or other such issues. Trustwave will provide Client assistance with gathering information to solve the issue.

Monitoring

Trustwave will provide Client automated alert notifications within the Trustwave Fusion platform as further detailed in the Incident Management feature. Trustwave will define Client's policies to ensure only applicable rules are enabled. Trustwave will create as many policies as needed to ensure that there is limited performance impact on the databases Trustwave monitors. Automated alert data will be received in Fusion and have automatic rule processing applied for the automated alert notifications.

Trustwave will generate reports for Client using Trustwave's DbProtect reporting templates. Trustwave will not edit reports unless their size inhibits distribution. These reports are available in the DbProtect console report history page.

Provisioning and Implementation

Trustwave will provide provisioning and implementation in five (5) phases. Phase 2 is optional as it is only applicable if Client has purchased the DbProtect database activity monitoring (DAM) module and the Service monitoring option.

Phase 0: Project Initiation

Trustwave and Client will finalize project team members and develop a common understanding of the project objectives, roles and responsibilities. Trustwave will validate Client readiness by confirming the appropriate information is documented. Specific tasks include but are not limited to preparing and distributing any data collection questionnaires, agreeing on a start date and timeline for execution, conducting project kickoff meeting(s), and finalizing a list of Client database instances within the scope of the Service.

Phase 1: Installation and Configuration

Client's project team will review the server configuration inventory to verify where DbProtect scan engines should be deployed. Trustwave will enable all necessary firewall rules for the operation of DbProtect and the Service. Specific tasks include:

	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 Service functionality and start implementing 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 Client's 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 Service	Client & Trustwave
9	Deploy production vulnerability assessment policy (optional)	Client & Trustwave

10	Run Vulnerability Management (VM) or Rights Management (RM) module jobs to validate that scan engines and policies are operating as expected (optional)	Client & Trustwave

Phase 2: Policy Development, Sensor Deployment and Tuning

Trustwave will generate and deploy a policy to enforce Client's security requirements for the DAM module and install, register, and tune sensors as necessary.

Phase 3: Training

Trustwave will schedule and Client will attend a DbProtect best practices training session, including a review of DbProtect built in reports.

Phase 4: Transition

Trustwave will review Client's DbProtect environment and make any final recommendations. Specific tasks include:

	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 Service 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: Steady State

Trustwave will move the DbProtect environment to steady state operations. Trustwave will require the assistance of the Client for any host-based sensors that are installed on database hosts.

	Task	Participants
1	Setup automated alert monitoring, if in scope with DAM module	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	VM scanning, if in scope	Trustwave
10	RM scanning, if in scope	Trustwave

Client Obligations

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

- 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; and
- provide remote access to DbProtect and its components.

Trustwave Obligations

For this Feature, Trustwave will

- 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; and
- notify Client through automated alert notification from the Trustwave Fusion platform of any suspected, actual, or potential threat to Client's database environment.

Change Management

Change management SLAs apply to both Trustwave-initiated and Client-initiated change requests and are categorized as follows:

Type of Request	Constructs	Completion time
Emergency Security Policy or Configuration Change Request	• Change for mitigating security risk(s) identified by either automated database monitoring or Client • Involves security policy settings, and is not an upgrade of software or patch for the managed technology	Within four (4) hours
Standard Policy or Configuration 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 twenty-four (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	• Seven (7) calendar days' lead time • Governed by Trustwave's change board review process • Occurs during Client's weekly maintenance window

	• Could require POC to be completed prior to scheduling. An error during this change could have significant outage consequences.	

Trustwave will set up a twice weekly change window to apply changes in Client's environment based on Client's geographic region. Further details are available in Trustwave's Threat Protection Support Manual.

Incident Management

Incident management SLAs endeavor to restore normal service operations as quickly as possible and minimize disruption to users' work while ensuring agreed levels of service quality are maintained. Trustwave's incident management SLAs are set forth as follows:

Type of Outage	Definition	Initial Notification	Notification Type
Total Outage (Critical)	Technology total outage affecting a majority of Client onsite users. This may include any technology service component, such as interface, software or hardware failure, and power or network failure.	30 minutes	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

Service SLAs will only apply to supported technologies. The following is specifically excluded:

- Changes to structure cabling, UPS, patch cords or racks
- Any customization or plug-in (e.g. report, API, alert) unless otherwise stated in the Threat Protection Support Manual
- Networks and interconnected devices that are not monitored or managed by Trustwave
- Infrastructure redesign efforts
- Unsupported database versions

Trustwave will report its compliance electronically upon Client's prior request.

Core Trustwave Features

The Service includes the following core features which are standard to many of Trustwave services:

Trustwave Fusion Platform

The Trustwave Fusion platform is Trustwave's proprietary cloud-based cybersecurity platform. Client will be automatically enrolled in the Trustwave Fusion platform as a part of the Service. Client will have access to the following on the Trustwave Fusion platform:

- Event information, Threat Findings, and 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 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 (additional fee)

Client may be required (i) to install a Trustwave Connect solution within its environment and establish the necessary network access for the Service or (ii) to set up event data so it is sent to Trustwave.

Additional Information

Trustwave's delivery of the Service is dependent on the following assumptions:

- All implementation services to be performed in accordance with this Service will be at Client's facilities unless agreed otherwise. All work performed in Phase 5 will be provided remotely.
- Trustwave will provide provisioning and implementation services 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 sufficient access to its database, 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 and 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. Trustwave may request access to specific servers, network equipment or other Client technology as reasonably necessary to provide the Services. Such access and related activities will only be performed with Client's explicit authorization and under direct Client supervision.

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.