

SERVICE DESCRIPTION

DbProtect

Service Description Overview

DbProtect is a database security, risk and compliance solution that helps organizations control their database security processes in a more streamlined way. Designed to scale to support the needs of any size organization, DbProtect boosts operational efficiency and streamlines key database security activities while enabling organizations to help achieve database security, minimize risk, and achieve regulatory compliance. DbProtect is installed locally.

The DbProtect suite is comprised of a Web application server, data repository and distributed components for scanning (scan engines) and monitoring (sensors). The credentials users log on to DbProtect with (using a Web browser) are authenticated against a Windows domain or accounts created locally on the Web application server. Once logged on, users are authorized to use DbProtect with the privileges granted to them through their role memberships.

The browser and distributed components communicate with one another using secure protocols. For certain types of scans the scan engines communicate with targets using vendor-supported ODBC and .Net database drivers.

DbProtect Core Features Overview

The DbProtect product suite offers a set of software components that are used for scanning and monitoring databases. DbProtect is comprised of three feature modules:

- **Vulnerability Management (VM)** - Capability to help locate, examine and report on database security vulnerabilities and misconfigurations in databases, cloud and big data stores.
- **Rights Management (RM)** - Capability to examine and report on an organization's database user and object privileges, ownership, and access controls.
- **Database Activity Monitoring (DAM)** - Capability to help track, identify, and alert on all database user activities, suspicious behaviour and other threats.

Provisioning and Implementation

Required DbProtect implementation services will be scoped as appropriate to complete full implementation and knowledge transfer. Trustwave will ensure that appropriately trained and knowledgeable personnel are deployed for all implementation services. During that time, a Trustwave consultant works with Client to implement the product and provide knowledge transfer to customer staff.

Phases 1 & 2 Design/Architecture & Install/Configuration of DbProtect Task	Participants
Review the Client's Database Server Configuration Inventory	CLIENT & Trustwave
Validate appropriate accounts have been created with necessary permissions for DbProtect deployment and configuration	CLIENT & Trustwave
Validate that production hardware meets Trustwave's requirements	CLIENT & Trustwave
Install DbProtect Console	CLIENT & Trustwave
Install DbProtect Scan Engines and/or Sensors and Register with console.	CLIENT & Trustwave
Tune DbProtect repository database growth parameters	CLIENT & Trustwave
Run Scans and/or reports to validate that DbProtect is operating as expected.	CLIENT & Trustwave
Phase 3 Creation of DbProtect Operation Run Book	Participants
Gather data on Client's operational, processes, procedures and requirements	CLIENT & Trustwave
Develop documents that incorporate Client's operational processes, procedures and requirements into DbProtect operational best practices	CLIENT & Trustwave
Run Book reviewed and adjusted as needed.	CLIENT & Trustwave

Trustwave Responsibilities

Trustwave consultants work directly with Client throughout initial implementation and training based on Implementation and tuning (up to 2 database instances) including Installation, Component setup, Building Policy, DbProtect tuning and 3 or 4 days of training (depending on implemented DbProtect Modules).

- Configuration, installation and tuning of vulnerability assessment policies and/or DAM host sensors requires careful planning. Trustwave can provide the expert knowledge to properly define and scope such an implementation. Where scope or complexity of desired services vary from this Service Description, Trustwave will recommend adding the appropriate amount of required professional services resources to properly support the successful implementation of your project.

Client Responsibilities

Trustwave requires Client to verify the address, building, office location for the implementation where appropriate. During the first day it is required to physically access the DbProtect allocated servers to get them online. Client is expected to pre-arrange any necessary access requirements, so that the Trustwave consultant and appropriate Client personnel will be able to physically access the servers.

Reporting

- DbProtect provides detailed Reporting on the results of tests and monitoring. One or more Reports can be run as part of a test or audit Job. Reports can also be run as stand-alone jobs or created on demand. Reports can be delivered by email to users.
- The DbProtect Dashboard gives quick access to an overview of assets, monitoring, and testing status.
- The Report section of the Console has three sub-sections; the Dashboard, On Demand Reports, and Report History.
- Dashboard graphs, pie charts and tables are drillable, thus providing drill down functionality, allowing DbProtect administrator to click links of interest and receive more in-depth information of the link/subject of choice.

Support

Includes options for Standard Support and Maintenance or Premium Support and Maintenance. Telephone and electronic mail support include the following:

- Clarification of functions and features of the Supported Program;
- Clarification of the Documentation;
- Guidance in operation of the Supported Program;
- Assistance in identifying and verifying the causes of suspected Errors in the Supported Program; and
- Advice on bypassing identified Errors in the Supported Program, if reasonably possible.

Optional Product Features - Training

There are two (2) training courses depending on the required/implemented DbProtect Module:

Certified DbProtect Administrator (CDPA) – Admin 2

For customers with DbProtect vulnerability assessment and/or rights management modules. Trustwave is committed to the success of its DbProtect customers. We are pleased to offer the Certified DbProtect Administrator (CDPA) training course, which is designed to provide you with the fundamental knowledge to configure and administer the DbProtect solution. The Certified DbProtect Administrator (CDPA) designation provides evidence of your ability to design, implement, and manage the DbProtect database security and compliance platform.

Certified DbProtect Administrator (CDPA) – Admin 3

For customers with the full suite of DbProtect software, including Vulnerability Management, Rights Management, and Activity Monitoring modules. Trustwave is committed to the success of its DbProtect customers. We are pleased to offer the Certified DbProtect Administrator (CDPA) training course, which is designed to provide you with the fundamental knowledge to configure and administer the DbProtect solution. The Certified DbProtect Administrator (CDPA) designation provides evidence of your ability to design, implement, and manage the DbProtect database security and compliance platform.

Certified DbProtect Administrator Training

1. Train the Client's DbProtect Administrators on the use and administration of DbProtect technology and all its components
2. Training provided in a three (3) or four (4) day session depending on CDPA-2 or CDPA-3, training days must be consecutive and cannot be split up.

During this phase the Administrator teams will go through extensive training on the DbProtect platform.

High-level Activities

Train Client's team on DbProtect the platform

- **Review**
 - **DbProtect components**
- **Review**
 - **Policies**
 - **User defined checks**
 - **Exceptions**
 - **Org. structure**
 - **Users**
- **Job Management**
 - **Creating jobs**
 - **Scheduling jobs**
 - **Report Jobs**
- **Analytics and Reporting**
 - **Operations**
 - **Security**
 - **Compliance**
 - **Report Filters**
 - **Dash Boards**
- **Administration**
 - **Backend database**
 - **Upgrades**
 - **Shatter Knowledgebase**
 - **Backup, Purge and restore**
 - **Troubleshooting**
- **Multi Tenancy**

Activity Monitoring (CDPA-3 ONLY)

- **Monitoring**
- **Policies**
- **Filters/Exceptions**

- **Upgrades**
- **Management**

Conduct best practices workshop

- **How other customers are using DbProtect**
- **Vulnerability Severity / Importance Scoring**
- **What to scan for Vulnerability Assessments & Rights Management**
- **Reporting - get the right data, to the right people, at the right time**
- **Automation**

Activity Monitoring (CDPA-3 ONLY)

- **Monitoring Tuning**
- **What to monitor**
- **Defining False Positives and how to alleviate them**

Optional Maintenance Health Check

As part of this highly recommended Health Check service, the configuration and performance of each of the DbProtect components will be reviewed. Performance tuning recommendations will be discussed with Client. DbProtect Knowledgebase and Analytics content will be upgraded as necessary.

Task	Participants
Environment review: <ul style="list-style-type: none"> • DbProtect installation and configuration • Scan engines • Databases • Policies • User defined checks • Reports • Asset Organization structure 	Client & Trustwave
Install Shatter Knowledgebase Update	Client & Trustwave
Install Analytics Update	Client & Trustwave
Create & Present recommendation report	Client & Trustwave
Perform fine tuning of DbProtect components and policies where applicable.	Client & Trustwave