Trustwave DbProtect

SECURE DATABASES. PROTECT SENSITIVE DATA. GO BEYOND COMPLIANCE.

Enterprise Database Security Platform

DbProtect is a database security platform designed for consistent monitoring and management of enterprise databases within the data center. Built on a centrally managed and distributed architecture, DbProtect uncovers database weaknesses. This includes configuration mistakes, identification and access control issues, missing patches, or any toxic combination of settings that could lead to escalation of privileges attacks, data leakage, denial-of-service (DoS), or unauthorized modification of data held within data stores – both relational databases and big data stores

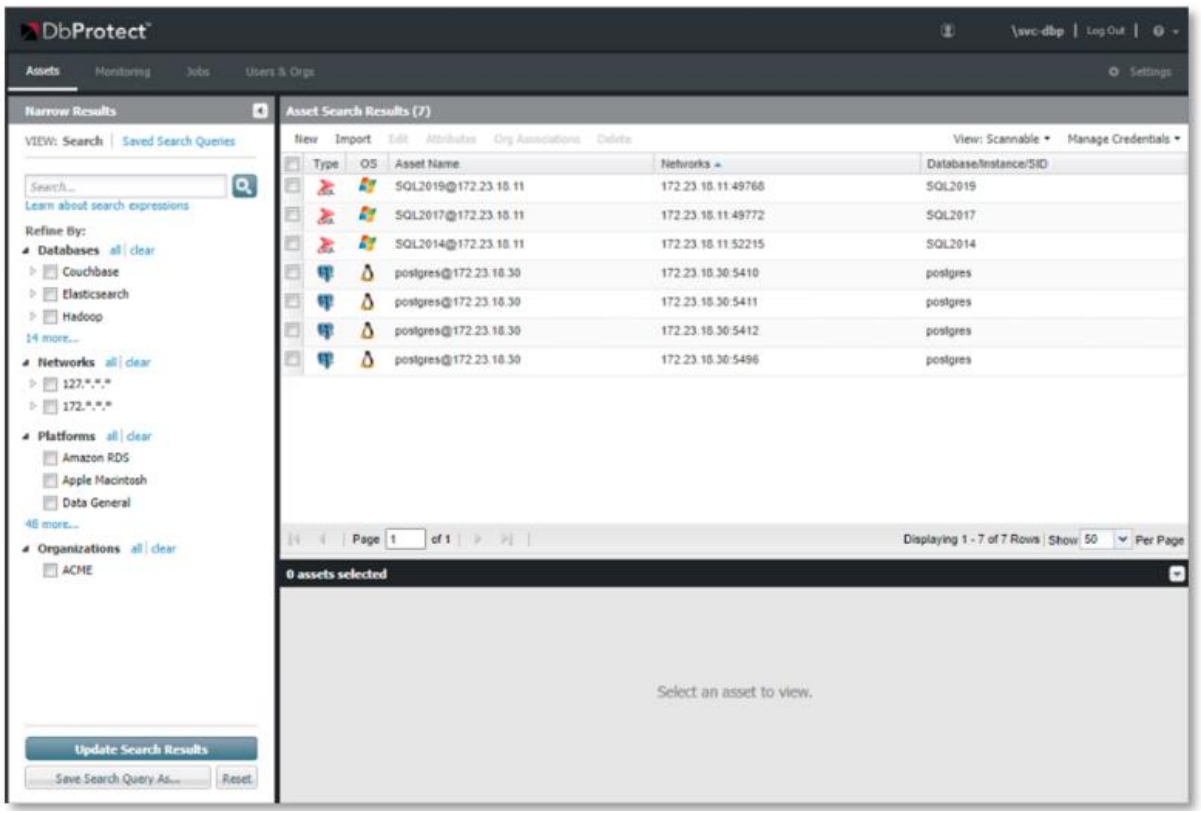
DBPROTECT COMPONENTS, MODULES AND DEPLOYMENT ARCHITECTURE

DbProtect Components

A DbProtect installation includes a Console server and one or more scan engines.

DbProtect Core Console

The Core Console is the Web browser-based, graphical component of DbProtect that allows you to navigate to the various features of DbProtect. The Console Server also provides several central services to control scanning, provide reporting, and manage the warehousing of data.



Scan Engines

DbProtect agentless and network-based vulnerability management scan engines discover database applications within your infrastructure and assesses their security strength. Backed by a proven security methodology and extensive knowledge of application-level vulnerabilities, DbProtect locates, examines, reports, and helps users operationalize security holes and misconfigurations. Scan engines scan your database instances for vulnerabilities and allow you to perform Pen Tests and Audits against them.

Sensors

Sensors deliver database-specific monitoring and alerting for best-in-class protection of enterprise organizations. You can fine-tune your event detection parameters and customize which audit and security events are monitored by DbProtect. This helps you focus security efforts on relevant information, while bypassing false positives and irrelevant events.

DbProtect Explorer Console is a new user interface and visualization tools that DbProtect uses for all reporting capabilities. The Explorer Console sits on top of all your existing and ongoing DbProtect data and settings.

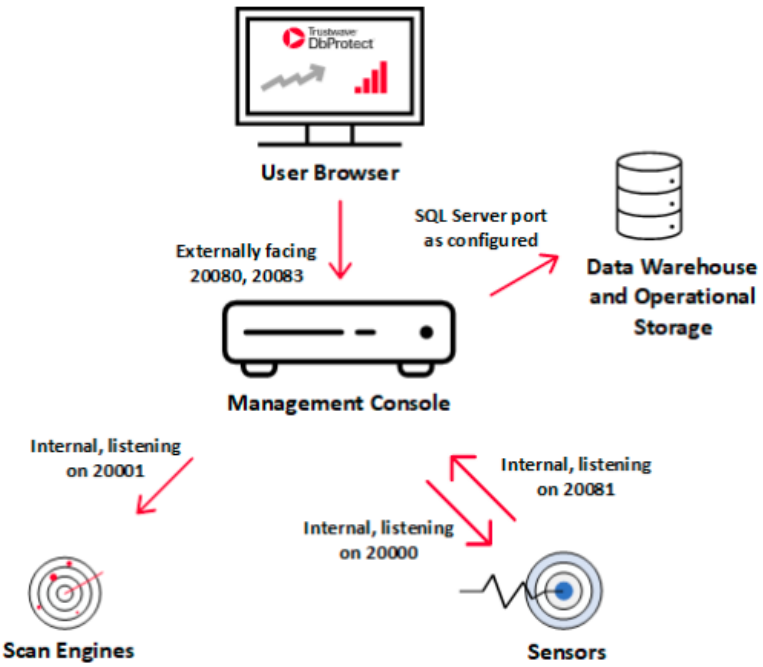
DbProtect is comprised of three feature modules:

Vulnerability Management: capability to locate, examine, and report on database security vulnerabilities and misconfigurations in any database.

Rights Management: capability to examine and report on an organization's database user and object privileges, ownership, and access controls.

Activity Monitoring: capability to track, identify, and alert on all database activities, suspicious behavior, and threats.

The following diagram illustrates how DbProtect components interact and shows which standard listening ports must be open for DbProtect to work.



It is possible to scale each of these components to achieve the goals necessary for your intended scope.

The databases supported at this time are:

Supported Database Types

Microsoft SQL Server
Oracle
MySQL
PostgreSQL

Monitoring Sensor Supported Platforms

- Linux RedHat versions 7, 8 on Intel x64
- Windows Server 2012, 2012R2, 2016, 2019

Supported Databases

- Oracle 12.2, 18, 19.9
- Microsoft SQL Server 2012 (SP3), 2014 (SP2), 2016 (SP1), 2017, 2019.
- IBM DB2 LUW 10.5, 11.1, 11.5
- Sybase ASE 15.7, 16.0 is available on Linux only

Minimum system requirements

DbProtect Suite system requirements

Data repository

DbProtect requires a Microsoft SQL Server 2016 or 2017 Data Repository to operate. This data repository
stores all alerts and audit data, as well as its system configuration information.
Acceptable data repositories for DbProtect include:
Microsoft SQL Server 2016, or 2017 (Windows only) 64-bit Standard Editions or higher

Memory

24 -128 GB (24 GB+ recommended)

Processor

x64 Processor 2.0 GHz+
8+ cores (Standard)

Disk Space

Each Product Use Profile requires 100 GB for the application in addition to
Standard: 500+ GB for temp/output/data repository
Note: Our benchmarking has shown that disks (whether physical or virtual) having sequential read and write speeds more than 100 MB/s yield acceptable performance.

Operating Systems

Windows Server 2016 or Windows Server 2019
64-bit Standard Editions or higher

Browser - Using DbProtect requires a modern Chromium-based browser.

Account Rights and Privileges

A Local or Domain Administrative account is required for installation

Required Microsoft.NET Version .NET Framework 3.5 and 4.7.2

Port considerations

Network Access for DbProtect Components

DbProtect components communicate on the network ports listed in the table below. For full details of required access, see the *DbProtect Installation Guide and Getting Started Guide*.

DbProtect Network Connectivity Requirements

Component	Default Listening Port	Type	Purpose
Console	20080 20081	TCP TCP	Console browser connections Receives Activity Monitoring Alerts/Events from Sensors. Used by Message Collector
Explorer	20082 20083	TCP TCP	Explorer Authentication Service Explorer Interface
SQL Service Repository	as configured	TCP	Verify this port assignment with the SQL Server Administrator
Scan Engine	20001	TCP	Console communication with the scan engine
Sensor	20000	TCP	Console communication with sensor