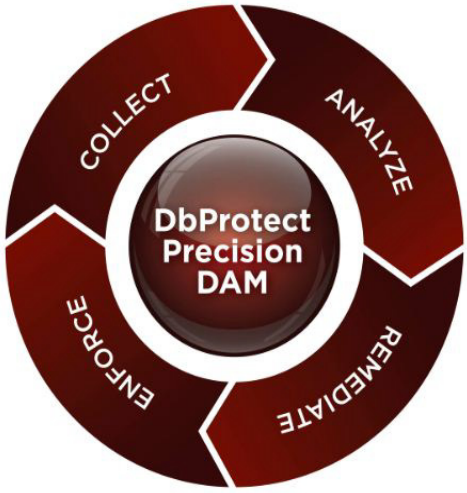
Chapter 1

Introduction

DbProtect is a database security, risk and compliance application designed to meet the needs of companies with large heterogeneous database environments. DbProtect's IT risk management framework, security controls, monitoring features, and governance for databases make it the leading solution on the market today.

DbProtect is a centrally-managed enterprise solution that uses a proven methodology for information assurance. It is built on the industry's most comprehensive database security knowledgebase—called SHATTER—which accurately identifies vulnerabilities, risks, and actual threats. DbProtect accomplishes DAM—Database Activity Monitoring—using a strategy of **Collect**, **Analyze**, **Remediate**, **Enforce**:



COLLECT – DbProtect Precision Database Activity Monitoring begins by collecting all data relevant to database security processes. DbProtect provides organizations with the most comprehensive profile of their database ecosystem. It collects data on:

- The inventory of databases deployed across the enterprise
- The location of all sensitive data
- The vulnerabilities exposing sensitive data
- User rights and entitlements
- All unauthorized and abnormal database activity

ANALYZE – DbProtect Precision Datababase Activity Monitoring simplifies the analysis process with field-proven analytics and reporting. DbProtect features dashboards, trend reports and drill-down reports. It provides over 50 standard reports, including reports on:

- Rights Management
- Risk Management
- Assessment
- Monitoring
- Risk Comparison
- Policy Management
- Compliance
- Operations

DbProtect also offer easy to use tools to generate customized reports.

REMEDIATE – DbProtect Precision Database Activity Monitoring provides tools to prioritize and facilitate rapid remediation of database vulnerabilities. DbProtect provides maps of database vulnerabilities, organized by their level of risk and business impact. Therefore the vulnerabilities that pose the greatest threats to your database and business can receive the highest priority. DbProtect's industry-leading vulnerability knowledgebase provides detailed remediation instructions to ensure rapid resolution of any identified vulnerabilities.

ENFORCE – DbProtect Precision Datababase Activity Monitoring enforces organizational database security policies by streamlining monitoring operations and focusing on unauthorized and abnormal database activity. DbProtect validates remediated vulnerabilities, monitors unremediated vulnerabilities and privileged user activity, and looks for any new avenues of attack. DbProtect's Active Response can be configured to take automatic action whenever an unauthorized activity is detected. This can include sending alerts and blocking the activity.

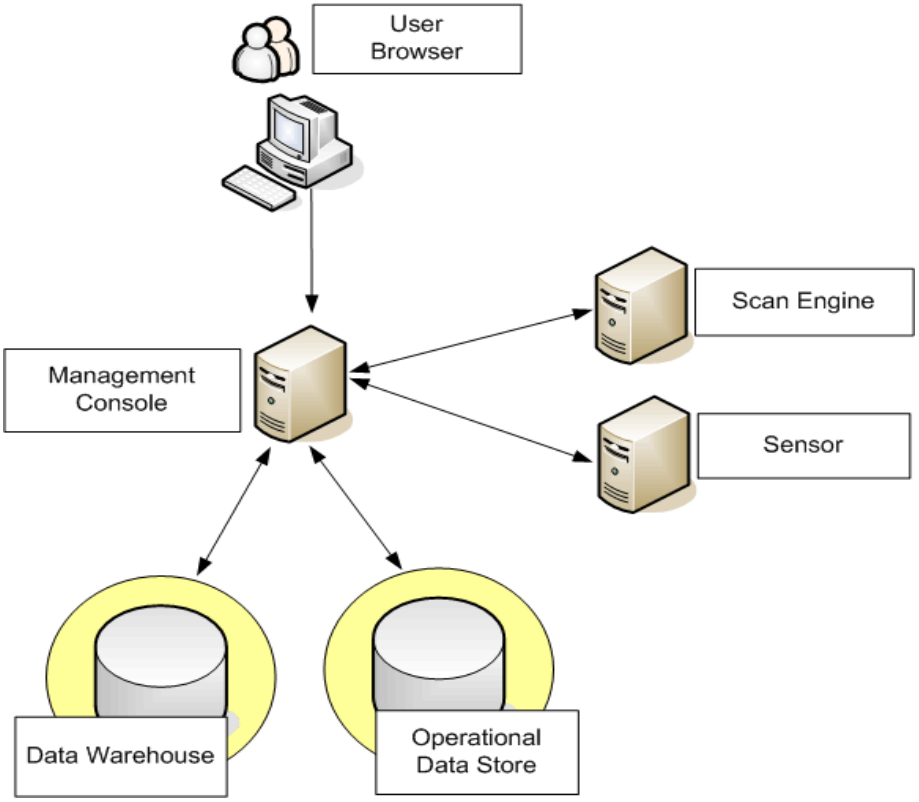
Intended Audience

This guide is intended for persons responsible for day-to-day usage of DbProtect. Typically, those responsible for installing DbProtect have the following (sometimes overlapping) job roles:

- System Administrators
- Network Administrators
- Database Administrators

DbProtect Components

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



Console

The Console is the web browser-based, graphical component of DbProtect that allows you to navigate to the various features of DbProtect.

For information on minimum system requirements and installation instructions for the Console, see the *DbProtect Installation Guide*.

Scan Engines

DbProtect's 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 fixes security holes and mis-configurations. Scan engines scan your databases for vulnerabilities, and allow you to perform penetration (pen) tests and audits against them.

Target databases (on Windows) include:

- Oracle
- Oracle Application Server
- SQL Server
- Lotus Notes/Domino
- Sybase
- DB2
- DB2 on the Mainframe
- MySQL

Sensors

Sensors deliver database-specific protection 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's ASAP Updates ensure that protection remains up-to-date as new vulnerabilities are identified and patches are released. Comprehensive policies and rules definitions, informed by industry best practices, enable security auditing and documentation specific for enterprise environments.

Logging In to the DbProtect Console

Some older versions of Google Desktop (5.1 and earlier) may cause problems when loading the DbProtect Console applet in Internet Explorer. Before installation, turn off Google Desktop, or re-install a newer version (5.2 or higher).

Note:	You must have the Java Runtime Environment (JRE) SE 6 Update 11 installed in order to connect to the DbProtect Console via a web browser.

Logging In to the Console

To use a browser to connect to the DbProtect Console:

1. Enter `https://ConsoleServer:Port` in the Address line, where:

   • `ConsoleServer` is the hostname or IP Address of the Console server

   • `Port` is the port number that the Console Management Server has been configured to provide service on. Typical DbProtect Console installations do not run on the default web server ports for security reasons.

   -example: https://dbprotect_server:20080

   -example: https://192.168.1.5:20080

A Security Alert message appears, prompting you to accept a security certificate from Application Security, Inc. DbProtect uses this certificate to communicate with users over a secure channel.

Note:	If you experience difficulty logging into the DbProtect Console and connecting to DbProtect, you may need to troubleshoot the Java Runtime Environment (JRE) security settings on your Internet Explorer 6 or greater web browser. For more information on a workaround, see Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 6 or Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 7.

2. Click **OK** to display the DbProtect Console login page.



3. In the Username field, enter your DbProtect user name. Use any of the following formats:

```
username: local user
<computername>\username
<netbios domain name>\username
<dns domain name>\username
username@<dns domain name>
```

4. In the Password field, enter your DbProtect password.

5. Use the Domain drop-down menu to select your domain, or manually enter a domain in the Domain field.

Note:	DbProtect is designed to use only Secure Sockets Layer (SSL) communication, which encrypts your user name and credentials prior to transmission to DbProtect. DbProtect then uses the Windows Authentication subsystem to verify the credentials.

6. Click **Login** to display the DbProtect Console.