National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

DbProtect AppRadar 2009.1 R2

Report Number: CCEVS-VR-VID10258-2011
Dated: 04 June 2012
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
The Aerospace Corporation
Columbia, MD

Daniel Faigin
The Aerospace Corporation
El Segundo, CA

Common Criteria Testing Laboratory

Shukrat Abbas
Anthony J. Apted
Lisa Vincent
SAIC, Inc.
Columbia, MD

Table of Contents

List of Figures

List of Tables

1 EXECUTIVE SUMMARY

The evaluation of the DbProtect AppRadar 2009.1 R2 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in May 2012. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, Revision 3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

DbProtect AppRadar 2009.1 R2, hereafter called AppRadar, is a software application that runs in the context of an operating system. AppRadar provides real-time database intrusion detection and security auditing. It provides database-specific monitoring and auditing of commercially available database servers. The key features of the product are event monitoring and auditing.

Note: The DbProtect Console may also be used to administer AppDetective, a sibling application to AppRadar. AppDetective has been evaluated separately (see CCEVS-VR-VID10256-2012) and may be installed on the same system with AppRadar.

The DbProtect AppRadar 2009.1 R2 is supported in the following environments:

The AppRadar Console runs on Microsoft Windows Server 2003 or 2008 Enterprise Edition or Microsoft Windows Server 2003 or 2008 Enterprise x64, each with the latest patches. It is accessible via Microsoft Internet Explorer 7.0 or higher with JavaScript enabled. Sun Microsystems Java Runtime Environment (JRE) 1.6 is required for DbProtect Console applet to load into the web browser.. Network connectivity is required for the AppRadar Console to communicate with AppRadar Sensors. AppRadar can use Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005, or Microsoft SQL Server 2008 as a backend database to store data collected by the sensors and consolidated by the Console (MSDE 2000 SP3, which is bundled with AppRadar, is not included in the evaluated configuration).

The AppRadar Sensors run on versions of Microsoft Windows, AIX, Sun/Oracle Solaris or Red Hat Enterprise Linux. The AppRadar Host-based Sensor requirements are detailed in Section 3.3.

The TOE is dependent on the correct operation of the environment and on its underlying OS, neither of which are included within the scope of the evaluation.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the DbProtect AppRadar 2009.1 R2 Security Target (ST).

2 IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation granted by the National Institute of Standards and Technology (NIST).

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile (PP) to which the product is conformant (if any);
- The organizations and individuals participating in the evaluation.

Table 1. Evaluation Details

Evaluated Product:	DbProtect AppRadar 2009.1 R2
Sponsor:	Application Security, Inc 350 Madison Avenue, 6th Floor New York, NY 10017
Developer:	Application Security, Inc 350 Madison Avenue, 6th Floor New York, NY 10017
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	2 May 2007
Completion Date:	31 May 2012
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3

Evaluation Class:	EAL 2 augmented with ALC_FLR.2
Description:	DbProtect AppRadar 2009.1 R2 is a software application that provides real-time database intrusion detection and security auditing. AppRadar provides database-specific monitoring and auditing of the commercially available database servers. The key features of the product are database event monitoring and auditing.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the DbProtect AppRadar 2009.1 R2 product by any agency of the U.S. Government and no warranty of the AppRadar product is either expressed or implied.
PP:	None
Evaluation Personnel:	Science Applications International Corporation: Shukrat Abbas Anthony J. Apted Lisa Vincent
Validation Body:	National Information Assurance Partnership CCEVS

2.1 Interpretations

Not applicable.

3 SCOPE OF EVALUATION

3.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- Data transmitted between TOE components may be captured and read by an attacker, thereby compromising sensitive TOE data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- Inadvertent activity and access by unauthorized or authorized users may be undetected on a database the TOE monitors thereby compromising the data maintained in the database.
- Malicious activity by attackers may be undetected on a database the TOE monitors, thereby compromising the data maintained in the database.
- Unauthorized accesses and activity indicative of misuse by unauthorized or authorized users may be undetected on a database the TOE monitors, thereby compromising the data maintained in the database.
- An unauthorized user may gain undetected access to the TOE and exploit system privileges to gain access to TOE security functions and data.

- An attacker may access and modify TOE data assets and configuration data, causing the TOE functions to work incorrectly and causing loss of TOE data and database monitoring functions.

3.2 Organizational Security Policies

The ST does not identify any organizational security policies that the TOE and its operational environment are intended to fulfill.

3.3 Physical Scope

The evaluated product is **DbProtect AppRadar 2009.1 R2**.

The TOE consists of the following components, which are described in Section 6:

- DbProtect Console v2009.1R2
- DbProtect Message Collector v2009.1R2
- DbProtect Sensor v2009.1R2
- WinPcap Pro 4.0.2.1123

DbProtect AppRadar 2009.1 R2 can perform host-based monitoring of the following database applications:

- Microsoft SQL Server 2000 (all editions), 2005 (all editions), and 2008 (all editions)
- Oracle 9iR2, 10g, and 10gR2
- IBM DB2 UDB version 8 and 9.

DbProtect AppRadar 2009.1 R2 can perform network-based monitoring of the following database applications:

- Oracle 7.x, Oracle 8, 8i, 9i, 9iR2, 10g, 10gR2
- Sybase Adaptive Server Enterprise (ASE) 11.x through 15
- IBM DB2 UDB version 8 and 9
- IBM DB2 for zSeries v7 and v8.

Note that the monitoring functions were evaluated solely for their alerting capabilities and not for their suitability to task for specific external criteria (for example, the correctness or completeness of the signature library).

The following software components are not included in the TOE. They are part of the TOE operational environment for the AppRadar Console in the evaluated configuration:

- **Operating system**: Microsoft Windows Server 2003 or 2008 Enterprise Edition, Microsoft Windows Server 2003 or 2008 Enterprise x64 each with the latest patches.

  Note that the Windows Data Protection API (DPAPI) is required to encrypt backend database credentials if Windows authentication is not used.

- **Browser**: Internet Explorer 7.0 or higher with JavaScript enabled. Sun Microsystems Java Runtime Environment (JRE) 1.6 is required for DbProtect Console applet to load into the web browser. Refer to the DbProtect User Guide for troubleshooting JRE security settings on Internet Explorer.

  Note the browser requirement applies to any host from which the AppRadar Console might be accessed, including the local host.

- **Networking**: Network connectivity is required for the AppRadar Console to communicate with AppRadar Sensors. Also, OpenSSL is required to encrypt that communication using SSL.

  Note that OpenSSL is also used to encrypt (and thereby protect) database credentials used by the host-based sensors. Note also that Tomcat 5.5.20, distributed with the TOE, is required to enable the web-based management front end of the TOE.

- **Backend Database**: Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005, Microsoft SQL Server 2008, used to store data collected by the sensors and consolidated by the Console (MSDE 2000 SP3, which is bundled with AppRadar, is not included in the evaluated configuration).
- **Supporting Components**:
    - **Tomcat Engine**. The TOE is distributed with the 3rd party Tomcat Engine 5.5.20 to facilitate the web-based management interface.
    - **Database Communication Support**. The TOE relies on its host to facilitate communication with target database applications and operating system products for the purposes of scanning and auditing. The TOE uses the ODBC, Oracle Instant client, DB2 client, Lotus Notes Domino C++, or TCP/IP socket APIs.
- **Support for Optional Services**:
    - **SMTP Server.** AppRadar Console can optionally be configured to email alerts using a configured SMTP server.
    - **SNMP Server.** AppRadar Console can optionally be configured to send SNMP traps to a configured SNMP server (i.e., trap receiver).

The AppRadar Host-based Sensors run on various operating systems, depending on the type of database to be monitored. The operational environment requirements for the AppRadar Host-based Sensor requirements are as follows:

- **Operating system**:
    - For Microsoft SQL Server:
        - Microsoft Windows Server 2003 or 2008 Enterprise Edition, Microsoft Windows Server 2003 or 2008 Enterprise x64
    - For Oracle
        - Sun/Oracle Solaris 8, 9, 10 (32 and 64 bit SPARC)
        - Red Hat Enterprise Linux 3, 4 and 5 (32 bit x86 and 64 bit x64)
        - IBM AIX 5.2 Technology Level 5 and greater
        - HP-UX 11i v1 or later on the PA-RISC processor and HPUX 11i v2 or later on the Itanium (IA64) processor
        - Windows Server 2003 (including Enterprise Edition), 32-bit
    - For DB2
        - Red Hat Enterprise Linux 3, 4, or 5 (32-bit x86 and 64-bit x64)
        - Solaris 8, 9, and 10 (64-bit SPARC)
        - AIX 5.2 Technology Level 5 and greater (32-bit and 64-bit)
        - Windows Server 2003 or 2008 (including Enterprise Edition), 32-bit
- **Networking**: Network connection to the AppRadar Console. Also, OpenSSL is required to encrypt that communication using SSL.

The operational environment requirements for the AppRadar Network-based Sensors are as follows:

- **Operating system**: Microsoft Windows Server 2003 or 2008 Enterprise Edition, Microsoft Windows Server 2003 or 2008 Enterprise x64
- **Networking**: Network connection to the AppRadar Console. Also, OpenSSL is required to encrypt that communication using SSL.

Note that the TOE must be configured in accordance with the set of evaluated Guidance documentation specified in Section 8.1.

3.4 Logical Scope

The security features of the product are described in detail in Section 4. In summary, these functions are:

- Security Audit.
- Security Management.
- Database Data Collection and Monitoring.

3.5 Excluded Features

The product provides a tool, ASAP Updater, which can be used to update the TOE and its knowledge base of application problems. However, the developer's deployment methodology is to make only complete releases of the TOE software available to customers. Use of ASAP Updater would take the TOE out of its evaluated configuration, and so it is excluded from the evaluation.

Similarly, the product includes a Configuration Manager tool. The Configuration Manager tool provides a means for modifying various configuration parameters on the Console's host machine. This tool is not necessary for the normal use of the TOE and has been excluded from the evaluated configuration as a result.

Additionally, the following capabilities have been excluded from the scope of analysis during the evaluation:

- Use of the report customization (e.g., to exclude specific data) capabilities available in the product.

4 SECURITY POLICY

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the DbProtect AppRadar 2009.1 R2 security policy has been extracted and reworked from the DbProtect AppRadar 2009.1 R2 ST and Final ETR.*

4.1 Security Audit

The TOE generates audit records for administrator operations, including attempts to access the TOE and its data and any configuration changes made to the TOE. The audit records are stored in the backend database and can be queried by the TOE to facilitate review of those records.

4.2 Security Management

The TOE provides security management functions to allow installation of TOE sensor components, modifications to TOE policies and filters, and loading of database login IDs and Passwords. The functions are accessible via an SSL-enabled web-browser. Each user is required to be identified an authenticated, using services of the host operating system (OS), and must be in one of the two pre-defined OS groups associated with the TOE in order to get access to the corresponding functions. Once a user is identified, authenticated and found to be associated with only one of the applicable groups, the corresponding functions are presented to the user so they can be used.

4.3 Database Data Collection and Monitoring

The TOE monitors database functions based on policies and filters defined in the TOE by the AppRadar Administrator. Both normal database usage and security events are monitored and records are generated. Security events, as defined by TOE policies, cause the TOE to generate an alert that is sent to the Console.

In general, the database monitoring is performed by AppRadar Sensor components that are configured to monitor associated databases in accordance with their individual configurations. The AppRadar Sensor components are centrally managed via the AppRadar Console component and report the results of monitoring to the AppRadar Console so that they can be centrally accessed.

Note that AppRadar includes both host-based and network-based sensors. Host-based sensors reside on the same host as the database they monitor while network-based sensors reside on the same network as the database they monitor. Host-based sensors use database credentials in order to monitor database activities while network-based sensors monitor network traffic to discern database activities. Both types of sensors perform similar monitoring functions, though given the differences in mechanics there are some differences in their functions.

- Network-based Sensors fire Alerts for all remote connections, e.g., from a web server communicating to its remote back-end database. However, they do not detect activity originating from the database host.
- Host-based Sensors detect both local and remote activity. However, they detect only successfully executed commands.

The TOE relies on SSL in the operational environment to protect stored host-based database credentials. The TOE also relies on the Windows Data Protection API (DPAPI) to protect credentials for its backend database when Windows authentication is not being used.

5 CLARIFICATION OF SCOPE

5.1 Assumptions

The ST identifies the following assumptions about the use of the product:

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The processing resources of the TOE, i.e., the sensors and console will be located within controlled access facilities, which will prevent unauthorized physical access. Remote

access to the console component of the TOE is possible outside the controlled access facilities.

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.
- The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

5.2 Limitations and Exclusions

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The evaluation did not assess any of the TOE's built-in policies for conformance to identified regulatory standards.
5. The TOE relies on the TOE environment in which it operates for the following security and other functionality:
   - Protect the TOE's stored executable image and its execution environment.
   - Protect TOE stored data, including audit records and scan results.
   - Provide a means to audit attempts to access the TOE stored executable image and stored data from the operational environment (i.e., not through the TOE's own interfaces).
   - Provide a reliable time stamp for use in audit records and scan results.
   - Identify and authenticate authorized administrators.
   - Provide encryption services used to encrypt database credentials and also to encrypt communication channels between the TOE components and also between the TOE Console and web browsers used to access it.

   Additionally, the TOE relies on its host to facilitate communication with target database applications and operating system products for the purposes of scanning and auditing.

6. The following product capabilities described in the guidance documentation were not included within the scope of the evaluation and no claims are made regarding them:
    - The software install from CD is not part of the evaluated configuration.
    - Software upgrades are not supported.
    - The ASAP update is a function allowing software updates to be downloaded and installed from the Application Security Inc. website. Most enterprise deployments of the TOE are in restricted areas and cannot directly access vendor websites. Therefore, ASAP updates are excluded from the evaluated configuration.
    - The TOE uses a SQL Server during its operational use, having network access using TCP/IP and addressed with an IPv4 network address. However, the setup and security of the SQL server is outside the scope of the TOE.
    - The customization of reports that allow users to exclude specific data for functional reporting. This configuration is not part of the evaluated configuration, which only permits built-in reports.
    - The use of the configuration manager tool is not part of the evaluated configuration.
    - The use of email transmissions for transferring reports. Since the TOE depends on the operational environment for email services, which cannot be assured to be secure, the use of email transmissions are excluded from the evaluated configuration.
    - Vendor services on the host server (e.g., Microsoft Services) are outside the scope of the evaluation.

6 ARCHITECTURAL INFORMATION

AppRadar comprises two main components: 1) the Console, which serves as a data collector and provides a web-based front end and 2) a number of sensors that monitor databases on a host or on the network and send collected data back to the Console. An example deployment of the TOE is depicted in Figure 1, below.

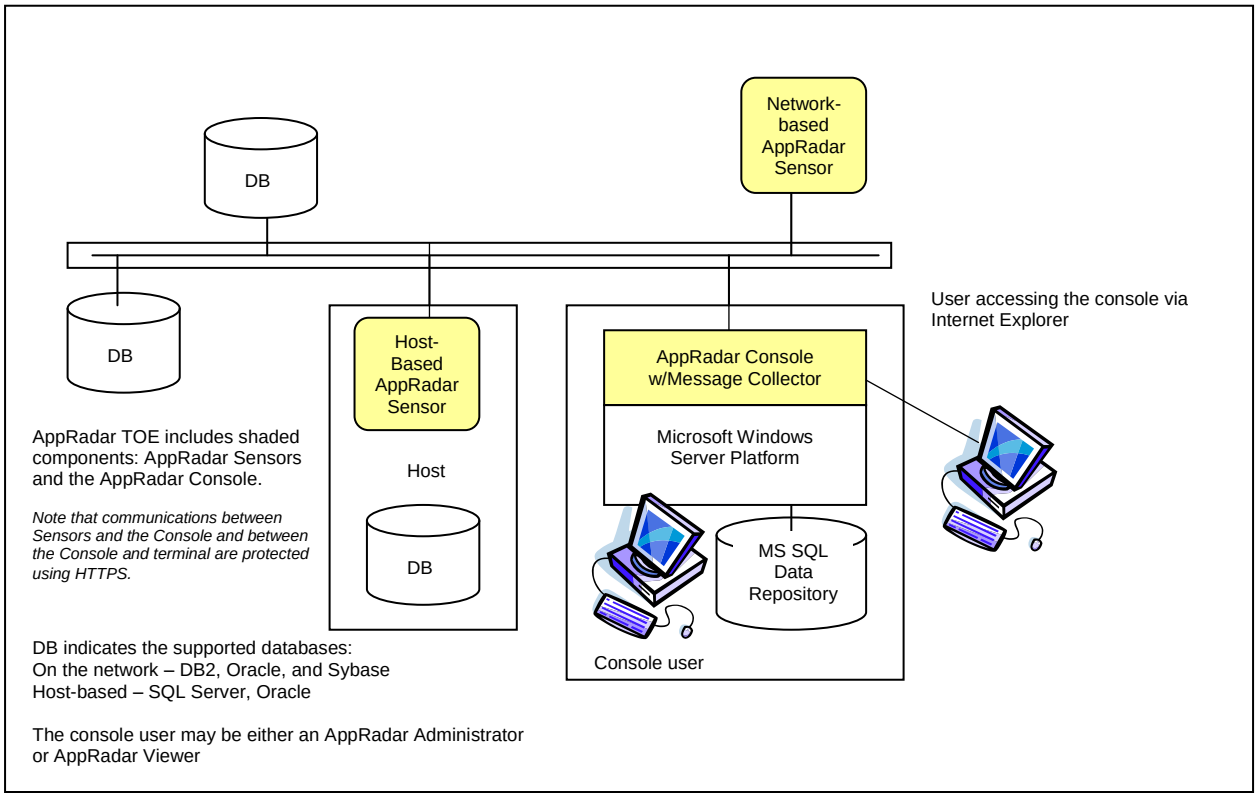

Figure 1. Example TOE Deployment

The AppRadar Console runs on a Microsoft Windows Server and it is accessible via Microsoft Internet Explorer.

The AppRadar Host-based Sensor runs on various operating systems, depending on the type of database to be monitored. The AppRadar Network-based Sensors run on Microsoft Windows Server.

The AppRadar Console provides capabilities to initialize and manage the TOE and to view alerts and audit data collected by the Sensors. The TOE relies on the operational environment to ensure all communication between the Console and Sensors uses HyperText Transfer Protocol Secure (HTTPS) or SOAP over HTTPS.

The AppRadar Console allows users to:

- Initialize and configure sensors
- Load database identification and authentication information (i.e., login and password) required for querying Sensors during the initialization of the sensors
- View alerts on the AppRadar Console and on a Syslog server, an SNMP Trap Receiver, or through configurable email forwarding
- Initialize and configure policies
- Initialize and configure filters
- View reports and define report templates

When a user connects to the AppRadar Console via their browser (using SSL), they are prompted for a username and password. The AppRadar Console uses the username and password to attempt to log the user into the host Microsoft Windows operating system (OS). All user definitions and authentication credentials are controlled by the OS in the operational environment. The AppRadar Console is accessed by two types of users: AppRadar Administrators and AppRadar Viewers. However, those roles are not defined by AppRadar; but rather are distinct, product-specific Windows groups that must be administered (e.g., user assigned) by the Windows administrator as part of the operational environment. Using Windows Groups (determined in the processing of logging the user into the Windows host platform), the TOE permits AppRadar Administrators to perform all AppRadar functions, including configuring the system, modifying existing policies and filters and creating new policies and filters, and assigning additional destinations for alerts in addition to the Console. AppRadar Viewers are allowed to only view the AppRadar configuration, policies, filters, and reports and create, edit and delete report templates. AppRadar Viewers may not initialize any TOE components or configure any policies or filters. AppRadar Viewers have no access to the monitored databases' identification and authentication information, which is entered by the AppRadar Administrator at sensor install and is maintained by the administrator as required by the specific database. Note that users that are not assigned to either the AppRadar Administrator or AppRadar Viewer role will be denied access during the log in process. AppRadar Console is accessible to users via Internet Explorer.

AppRadar Sensors monitor database activity; there is a sensor associated with each database monitored. There are two types of AppRadar sensors:

- Host-based sensors monitor Microsoft SQL Server or Oracle databases. Host-based sensors are located on the same machine as the monitored database. The Sensor captures SQL commands and reports activity back to the AppRadar Console, which stores information in its backend database.
- Network-based sensors monitor Oracle, DB2, or Sybase ASE databases on the network. The network-based sensors may be located anywhere on the network where database traffic is flowing to and from the monitored database; the network-based sensor is similar to a sniffer. The database traffic is analyzed and information on the activity is reported back to the AppRadar Console, which stores the information in its backend database.

AppRadar Sensors monitor for a variety of events such as intrusion attempts or auditing of normal usage as defined by TOE policies and filters. Audit records and Alerts are created by the sensors based on database events. An

An alert is a notification of a monitored event detected on the database host or network and an audit is a record of standard database activity. AppRadar Sensors generates alerts for activities defined as security events by the TOE policies. The alerts and audit records are sent via a network connection to the AppRadar Console (actually its Message Collector component) and are stored in the Microsoft SQL[1] Data Repository (i.e., backend database), which is outside the TOE boundary.

[1] Note that the AppRadar Console can be configured to utilize a Microsoft SQL server that is running either on the same host server or on another server that is continuously accessible via a network connection. Note also that the TOE can be configured to either use Windows authentication for database access or alternately to use database authentication. In the latter case, the TOE stored the applicable database credentials using Windows Data protection API (DPAPI) to protect them and recall them when needed.

Databases monitored:

AppRadar monitors the following databases and versions:

Table 2. Databases Monitored by AppRadar

AppRadar Sensor Type	Database Platform	Versions
Network-based Sensor	Oracle	Oracle 7.x, Oracle 8, 8i, 9i, 9iR2, 10g, 10gR2
	Sybase	Sybase ASE 11.x through 15
	IBM DB2	IBM DB2 UDB version 8 and 9 IBM DB2 for zSeries v7 and v8
Host-based Sensor	Microsoft SQL Server	Microsoft SQL Server 2008 (all editions) Microsoft SQL Server 2005 (all editions) Microsoft SQL Server 2000 (all editions)
	Oracle	Oracle 9iR2, 10g, and 10gR2
	IBM DB2	IBM DB2 UDB version 8 and 9

7 PRODUCT TESTING

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for DbProtect AppRadar 2009.1 R2.

Evaluation team testing on version 2008.1 of the product was conducted at the vendor's development site May 19 through May 22, 2009. Subsequently the TOE was moved to version 2009.1 R2, which appears to be a major change based on number alone, but is in reality a minor change. The evaluation team reviewed the differences between v2008.1 and v209.1 R2, which were as follows:

- Fixes to alert forwarding when multiple addresses specified
- Performance and reliability improvements to the Installer
- Improvements to the user interface for host-based Oracle sensor configuration
- Improvements to the user interface for specifying network addresses when configuring sesnsors (default to physical IP address, add description).

In July 2011, the vendor retested v2009.1 R2 of the TOE and provided the results to the evaluation team. The evaluation team witnessed the retesting. The evaluation team also analyzed the original team tests, and concluded that they were unaffected by any of the areas updated by the v2008.1 to v2009.1R2 transition, and thus did not require rerunning. Analysis of the updated test evidence indicated that all tests passed.

7.1 Developer Testing

The vendor's approach to testing for DbProtect AppRadar is based on manual testing of the DbProtect AppRadar features and security functions. DbProtect AppRadar is tested using a number of manual test suites by security function with varying numbers of test cases. The testing for each AppRadar release is tracked in Microsoft Word test cases that are stored in a project with separate folders for each release.

The Microsoft Word test cases are separated by security function to address that specific requirement component. For DbProtect AppRadar, test cases were provided for Audit data generation and Review; Management of TSF Data and Specification of Management Function; and Database Data Collection and Database Data React.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the operating systems supported and the application environment. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed the vendor test suite for DbProtect AppRadar per the evaluated configuration as described in the developer's test documentation. This document describes the testing environment for DbProtect AppRadar as follows:

- Console Operating System (OS) – Microsoft Windows 2000 Advanced Server SP4
- Backend database – Microsoft SQL Server 2000 Enterprise Edition SP4
- Host-based sensor – Microsoft Windows 2000 Advanced Server SP4
- Network-based sensor – Microsoft Windows 2000 Advanced Server SP4
- Browser – Microsoft Internet Explorer 6.0
- Targeted databases in the IT environment – SQL Server 2000 and Oracle 9i R2.

The evaluation team conducted testing of DbProtect AppRadar on the environment as described above.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The test environment described above was used with team generated test procedures and team analysis to determine the expected results.

The evaluation team performed the following additional functional tests:

- **Security Management**—the evaluation team complemented the developer's testing of the Security Management security function by testing that capabilities were allowed or restricted were consistent with the specification of management restrictions in the ST. This included: verifying both the capabilities and restrictions of the 'View' user role; confirming that users must be defined in Active Directory groups in order to login to the TOE; and determining the behavior when a user changes groups while logged in or belongs to both groups.
- **Database Credentials Protection**—the evaluation team tested the protection of database credentials, since the ST indicates that the TOE uses Windows Data Protection API (DPAPI) or OpenSSL to protect database credentials it stores. For the following two

cases, the evaluation team created credentials and determined if they were stored in the clear or in an apparently encrypted form:

- When the Backend Database is configured for SQL authentication, the database credentials used by the TOE are encrypted and stored in the Windows registry (this is not necessary when the Backend Database is configured for Windows authentication)
- Host-based sensors are configured with database credentials for direct access to the database being monitored. The TOE uses OpenSSL (AES-256) to encrypt/decrypt applicable credentials with Sensor-specific keys which are stored in the Backend Database. The individual database credentials are stored locally (in the host filesystem) in encrypted form by each host-based Sensor and sent to the AppRadar Console to be decrypted when needed.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product that extended the vulnerability repositories and search parameters used by the developer. Neither the developer nor the evaluation team identified vulnerabilities in the TOE. The developer's search included searching for vulnerabilities in third party products or components bundled with or used by the TOE. The developer's analysis demonstrated none of the identified vulnerabilities were applicable to the TOE in its evaluated configuration. The evaluation team extended this search and also found no vulnerabilities that were applicable to the TOE in its evaluated configuration. In addition, the developer performed an NMAP scan of the TOE in its test environment and provided an analysis of the results to the evaluation team. The list of open ports shows that the services running are minimal, and do not belong to the TOE process. This signifies that the TOE does not expose a network interface that opens it up for network based attacks. Finally, since the Console is accessed via a web browser, the TOE was tested to see if a View user could navigate to Administrator pages and perform administrative functions by caching and reusing URLs. However, the evaluation team found that based on the specific web page, either an error was returned, or the page was rendered correctly, but the user restricted to their normal capabilities (e.g., buttons were not enabled).

8 DOCUMENTATION

8.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- DbProtect 2009.1 R2 Installation Guide, 7 April 2009
- DbProtect 2009.1R2 Administrators' Guide, 6 April 2012
- DbProtect 2009.1R2 Users' Guide, 6 April 2012.
- DbProtect AppRadar 2009.1R2 Evaluated Configuration, Version 1.0, 11 May 2012

Note that these are the only documents provided with the TOE.

8.2 Evaluation Evidence

The following tables identify the additional documentation submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents are proprietary and not available to the general public.

Design Documentation	Version	Date
DbProtect AppRadar 2009.1 R2 Functional Specification and High Level Design Document	2.1	11 May 2012

Lifecycle Documentation	Version	Date
DbProtect AppRadar 2009.1R2, DbProtect AppDetective 2009.1R2 Life Cycle Document	0.4	6 Apr 2012
DbProtect AppRadar 2009.1R2, DbProtect AppDetective 2009.1R2 Configuration Management Plan	0.5	6 Apr 2012
DbProtect AppRadar 2009.1R2, DbProtect AppDetective 2009.1R2 Delivery Procedures	0.4	6 Apr 2012

Test Documentation	Version	Date
DbProtect AppRadar 2009.1 R2 Test Plan	1.3	8 May 2012
Requirement Component – Audit data generation and Review	0.1	10 Apr 2012
Requirement Component – Management of TSF Data and Specification of Management Function	1.0	10 Apr 2012
Requirement Component – Database Data Collection and Database Data React	1.0	10 Apr 2012

Vulnerability Assessment Documentation	Version	Date
DbProtect AppDetective 2009.1R2, DbProtect AppRadar 2009.1R2 Vulnerability Assessment	0.1	6 Apr 2012

Security Target	Version	Date
DbProtect AppRadar 2009.1 R2 Security Target	1.0	21 May 2012

9 RESULTS OF THE EVALUATION[2]

The evaluation team determined the product to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of EAL 2 augmented by ALC_FLR.2. In short, the product satisfies the security technical requirements specified in "DbProtect AppRadar 2009.1 R2 Security Target" on platforms specified in Section 3.3, "Physical Scope".

The evaluation results confirmed that the work units defined in Version 3.1, Revision 3 of the CC and the CEM were satisfied. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or

[2] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

Note: When this evaluation started, work was performed using the version of the CEM that corresponded to Common Criteria Version 2.3. When the Security Target was moved to Common Criteria Version 3.1 Revision 3, the evaluation work performed was reviewed in light of the Version 3 work units. Where work units were identical, the evaluation work was reused. Where there were slight differences addressed by the overall body of evaluation evidence, an argument was provided (including pointers within the body of evidence) that the Version 3 work units were satisified. Where there were new work units, the work dictated by the CEM was performed and reported in the Evaluation Technical Report. All of these mappings, as well as the updated Evaluation Technical Reports, were reviewed by the validation team, who concluded that the Version 3.1 work units were satisfied.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.2" certificate rating be issued for DbProtect AppRadar 2009.1 R2.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

Table 3. TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures
ACL_FLR.2	Flaw reporting procedures
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.2	Vulnerability analysis

10 VALIDATOR COMMENTS/RECOMMENDATIONS

1. The DbProtect 2009.1R2 Users' Guide contains a number of claims that the TOE does not ensure current patches and does not ensure current compliance, etc. The validators recommend that administrators of the TOE keep up to date with patches for the components in the operational environment.
2. The evaluation did not verify any claims regarding suitability of legislative-based policies, described in the DbProtect 2009.1R2 Users' Guide.
3. Note that DbProtect AppRadar 2009.1 R2 does not support IPv6.
4. There is no automatic backup of the SQL database. Instead, the AppRadar Administrator is instructed to periodically backup the database and to monitor its size and manage it outside of the TOE.
5. It should be noted the evaluated TOE is not the current version of this product and must be specially ordered from the vendor.

11 ANNEXES

11.1 List of Acronyms

AIX	Advanced Interactive eXecutive
API	Application Program Interface
ASAP	As Soon As Possible
ASCII	American Standard Code for Information Interchange
ASE	Adaptive Server Enterprise
CA	California
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Methodology for IT Security Evaluation
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
DB2	Database 2 (IBM Product)
DPAPI	Data Protection API
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HPUX	HP Unix

HTML	Hypertext Markup Language
IBM	International Business Machines
ID	Identification
IT	Information Technology
JRE	Java Runtime Environment
MD	Maryland
MSDE	Microsoft SQL Server Desktop Engine
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
Nmap	Network Mapper
Not applicable.TOE	Target of Evaluation
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
NY	New York
ODBC	Open Database Connectivity
OS	Operating System
PP	Protection Profile
RISC	Reduced Instruction Set Computer
SAIC	Science Applications International Corporation
SCAP	Security Content Automation Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	Special Publication
SP1	Service Patch 1
SP2	Service Patch 2
SPARC	Scalable Processor Architecture
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TSP	TOE Security Policy
UDB	Universal Database
VPL	Validated Products List

VR	Validation Report
WinPCap	Packet library for Windows. WinPcap is the standard tool for link-layer network access in the Windows environments.
WMI	Windows Management Instrumentation
XML	Extended Markup Language

12 SECURITY TARGET

The ST for this product's evaluation is **DbProtect AppRadar 2009.1 R2 Security Target,** Version 1.0, dated 21 May 2012.

13 BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009, CCMB-2009-07-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003.
4. Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004.
5. DbProtect AppRadar 2009.1 R2 Security Target, Version 1.0, 21 May 2012.