National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

DbProtect AppDetective 2009.1 R2

Report Number: CCEVS-VR-VID10256-2012
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 AppDetective 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 AppDetective 2009.1 R2 discovers database applications within an organization's network infrastructure and scans them for potential vulnerabilities. Administrators can then take appropriate remedial actions. It utilizes a library of known vulnerabilities and misconfiguration signatures. DbProtect AppDetective 2009.1 R2 provides a GUI front-end (the Console) that centralizes the management of multiple scanning engines and access to the data collected by the scanning engines. The Console enables access to set up and run AppDetective jobs. Access to AppDetective functions is role-based and can be limited to specific users based on role assignments within the Console component.

Note: The DbProtect Console may also be used to administer AppRadar, a sibling application to AppDectective. AppRadar has been evaluated separately (see CCEVS-VR-VID10258-2012) and may be installed on the same system with AppDetective.

DbProtect AppDetective 2009.1 R2 is designed to operate in the context of the following operating systems: Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Server 2003 Enterprise x64 each with the latest patches.

The TOE can be configured to use Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005, or Microsoft SQL Server 2008 to store and retrieve scan results. Microsoft Access and Microsoft SQL Express are not supported in the evaluated configuration.

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 TOE, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the DbProtect AppDetective 2009.1 R2 Security Target.

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 AppDetective 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:	8 March 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 AppDetective 2009.1 R2 is a network-based vulnerability assessment application that reports on the security strength of database applications within the network. It assists in identifying vulnerable databases residing within the network by scanning for potential vulnerabilities within those databases. Administrators can then take appropriate remedial actions.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the DbProtect AppDetective 2009.1 R2 product by any agency of the U.S. Government and no warranty of the DbProtect AppDetective 2009.1 R2 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.

- An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a TOE security mechanism.
- An unauthorized user may attempt to compromise the integrity of the data collected by the TOE by bypassing a security mechanism.
- Unauthorized attempts to access TOE data or security functions may go undetected.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential vulnerability to go undetected.
- An unauthorized user may attempt to remove or destroy data collected by the TOE.
- An unauthorized user may attempt to compromise the continuity of the collection functionality by halting execution of the TOE.
- A user may gain access unauthorized to TOE security functions and data.
- Improper security configuration settings may exist in the IT System the TOE monitors.

- Vulnerabilities may exist in the targeted IT System the TOE monitors.

3.2 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operating environment are intended to fulfill:

- Users of the TOE shall be accountable for their actions.

  This policy effectively support the implementation of an audit and accountability policy, as specified by NIST SP 800-53 Revision 3 controls AU-1 and AU-2.

- Configuration and vulnerability information that might be indicative of the potential for a future intrusion of a targeted IT System (database) must be collected.

  This policy effectively supports the implementation of a system monitoring policy, as specified by NIST SP 800-53 Revision 3 control SI-4.

- The TOE shall only be managed by authorized users.

  This policy effectively supports both account management (AC-2) and access control (AC-3) controls in NIST SP 800-53 Revision 3. It does this by enforcing the requirements that external authorization is required to perform management functions, and that the system restricts use of those management functions to only authorized individuals

3.3 Physical Scope

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

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

- DbProtect Console v2009.1R2
- AppDetective Scan Engines v2009.1R2
- Crystal Reports 9.2.0
- WinPcap Pro 4.0.2.1123

DbProtect AppDetective 2009.1 R2 includes modules for the following database applications:

- Oracle 11g, Oracle 10g , Oracle9i, and Oracle8i (note that while Oracle 8 and Oracle 7 are also supported, Audit-type tests[1] do not work for those versions)
- Oracle Application Server 9i and 9i Release 2
- Microsoft SQL Server Versions 6.x, 7.0, 2000, 2005, 2005 Express Edition, 2008, and MSDE versions 1.0 and 2000 SP4
- Lotus Domino v4.5 through 7.0
- Sybase ASE 11.0, 11.5, 11.9.2, 12.0, 12.5, 15

[1] Note that "audit" is an overloaded term in this VR. Not only does it refer to traditional Common Criteria audit (as in monitoring of administrative actions), it also refers to a type of testing that the product may perform against a database. Audit tests make use of privileged accounts on the target database application and its underlying operating system host to determine susceptibility to internal misuse; this is contrasted with PenTests. For more information, see Section 4.1, page 4.

- IBM DB2 Versions 6.1, 7.1, 8.1 and 8.2
- IBM DB2 zSeries Versions 7 and 8
- MySQL 3.20, 3.21, 3.22, 3.23, 4.0, 4.1, and 5.0.

Note that the assessment functions were evaluated solely for their testing 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 in the evaluated configuration:

- **Operating System**. The TOE is designed to operate in the context of the following operating systems: Microsoft Windows Server 2003 and 2008 Enterprise Edition, Microsoft Windows Server 2003 and 2008 Enterprise x64 each with the latest patches.
- **Backend Database**. The TOE can be configured to use Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005, or Microsoft SQL Server 2008 to store and retrieve scan results. Microsoft Access and Microsoft SQL Express are not supported in the evaluated configuration.
- **Supporting Components**. Additionally, the TOE requires the following components in the operational environment (and will install them if not already present upon installation of the TOE):
    - Microsoft XML Core Services 4.0 SP2
    - Microsoft .NET Framework 2.0 SP1
    - Microsoft Visual Studio 2005 C++ Redistributable
    - Tomcat Engine 5.5.20
    - WodSSH v2.4.1
- **Database Access Supporting Components**. In order to perform audit-type tests on some database applications, the administrator needs to ensure the following components are installed and accessible in the operational environment:
    - IBM DB2 Server audit-type tests require the IBM DB2 runtime client
    - IBM DB2 for Mainframe audit-type tests require IBM DB2 Connect
    - Lotus Domino audit-type tests require the Lotus Notes client driver
    - Sybase ASE audit-type tests require the Sybase ASE ODBC driver.

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 description of the security features of the product are described in further details in Section 4. In summary, these functions are:

- Database Discovery and Scanning
- Security Audit
- Identification and Authentication

- Security Management

3.5 Excluded Features

The TOE can generate fix scripts that the administrator can apply to correct problems identified by Pen Tests or Audit-type Tests. The evaluation has not covered the efficacy of these fix scripts in actually correcting detected problems.

The product provides a tool, ASAP Updater, that 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 has the potential to change the TOE software, and thus would take the TOE out of its evaluated configuration. Use of ASAP Updated is excluded from the evaluation.

Similarly, the product includes Configuration Manager and DbProtect Migration tools. The Configuration Manager tool provides a means for modifying various configuration parameters on the Console's host machine. The DbProtect Migration tool provides a means to migrate data from AppDetective Pro to DbProtect AppDetective. These tools are not necessary for the normal use of the TOE and have been excluded from the evaluated configuration as a result.

The product also provides a Policy Editor that offers an interface for managing policies that define the checks to be performed by Audit and Pen Test jobs. Access to the Policy Editor cannot be controlled or monitored by the TOE and as such its use has not been included in the scope of evaluation, but should have no affect on the TOE itself. Rather the evaluation addresses the use of primitives found in policies however they may have been created (built-in, user created, or otherwise obtained).

The TOE provides the capability for users to create their own tests and checks for Pen Tests and Audits. However, the evaluation is unable to make any comment on the efficacy of those tests and checks not provided as part of the TOE.

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

- The ability to log to a Check Point event logging server.
- Support for the Security Content Automation Protocol (SCAP).
- Use of Network Mapper (Nmap) files in performing Discoveries.
- Claims regarding Common Vulnerabilities and Exposures (CVE) compatibility.

4 SECURITY POLICY

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

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

4.1 Database Discovery and Scanning

The TOE is a network-based vulnerability assessment scanner that discovers database applications within the network infrastructure and assesses their security strength. Without requiring any agents on the target systems, the TOE can perform audit-type tests and simulate attacks against discovered and targeted applications to uncover security vulnerabilities and misconfigurations. The TOE performs the following operations on database applications:

- **Discovery** — This operation systematically searches the network, inventorying applications and relevant application components by vendor and release.
- **Pen Test** — Through a series of detailed security tests and Pen Tests, the TOE identifies how an intruder or unauthorized user might gain access to application components. Pen Tests use a black-box approach to simulate how an intruder would exploit vulnerabilities to break into a database application from the outside (this is termed "outside-in" in the product documentation). The TOE can perform the following types of security checks (i.e., includes applicable signatures) as part of a Pen Test:
    - *Denial of Services* — These checks examine the database application for susceptibility to specific Denial of Service attacks.
    - *Misconfigurations* — These checks examine the database application for possible misconfigurations that may leave the database application susceptible to attack.
    - *Password attacks* — These checks examine the database application to determine if it is vulnerable to password attacks, such as accounts with blank passwords, accounts with default passwords still set, and susceptibility to dictionary and brute-force attacks.
    - *Vulnerabilities* — Each of these checks determines if the database is susceptible to any specific published vulnerabilities for that database application.
- **Audit-type Tests** (also known as just "Audits") — In contrast to Pen-Tests, an Audit-type test makes use of privileged accounts on the target database application and its underlying operating system host to determine susceptibility to internal misuse (this is termed "inside-out" in the product documentation). Audit-type tests require a valid user account in order to verify internal configuration settings. The TOE can perform the following types of security checks as part of an Audit-type test:
    - *Access Control* — These checks examine the database application access control configuration for potentially inappropriate or insecure access control or privilege settings on database objects.
    - *Accountability* — These checks examine the database application accountability configuration to determine if specific security measures, such as enabling auditing of specific events, have been applied.
    - *Authentication* — These checks examine the database application authentication-related configuration to determine if it is vulnerable to password attacks or problems associated with user authentication.
- **Report** — The TOE can generate reports in various formats (HTML, XML, ASCII text) that identify specific potential vulnerabilities, provide an assessment of the risk associated with a vulnerability, and recommend actions to address a vulnerability. The TOE internally uses Crystal Reports for generating reports.

The TOE can access targeted IT systems using privileged accounts in order to gather specific internal configuration data. Applicable security credentials can be configured into the TOE and the TOE will store and protect those credentials using capabilities provided by its host operating system. Specifically, the TOE calls upon the Windows Data Protection API (DPAPI) to encrypt and store the credentials in its registry so that they can be recalled by the TOE when needed.

4.2 Security Audit

The TOE has the ability to generate audit records for the following TOE security-relevant events: initiation of Discovery, Pen Test, or Audit-type tests scans, scheduling Discovery, Pen test, or Audit-type test scans, creation and review of DB Scan reports based on DB scan data. The TOE records within each audit record at least the following information: Date, Time, Event Type, Success or Failure, User ID of the user. The TOE relies on the operational environment to protect and store the audit records, provide the ability to review the audit records, and to provide a reliable timestamp.

4.3 Identification and Authentication

The Console maintains four different roles (super user, admin user, basic user and view user). The Console requires each user to provide a username and password before gaining access to any other Console security functions. The Console will pass the provided username and password to the underlying operating system and will deny the user session if the operating system does not indicate successful authentication of the username.

Note that the TOE does not authenticate users, but rather relies on its host operating system to protect it from inappropriate user access. The TOE depends upon Windows Active Directory for user information, including User ID and Windows Group. The TOE maintains User ID, Role, and Organization assignments for each user.

4.4 Security Management

The Console provides security management functions that are accessible via an SSL-enabled web-browser. Each user is required to be identified and authenticated, using services of the host operating system.

The Console implements role-based security management to control user access to the management functions. The Console partitions access in two ways: by Organization and by role. Organizations are created by super users. The admin user defines the users, policy access rights, and data partitioning within each Organization. The main principle is to restrict data stored, collected, and associated with an Organization to users in that Organization. This applies to all jobs, reports, and discovery results. Organizations are hierarchically organized, which affects the visibility of one Organization to another. The admin users can create new Organizations or delete Organizations within the Organization to which they have access. However, they are restricted from creating or deleting Organizations above the Organization to which they have access.

An authorized user who has administrator access to the DbProtect Console host is able to use the Policy Editor tool in the operational environment to view, create and manage policies.

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.
- 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 processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.

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 analyze the signatures, templates, and other mechanisms used in the Penetration Test and Audit operations for suitability to task or completeness.
5. The evaluation did not assess any of the TOE's built-in policies for conformance to identified regulatory standards.
6. The TOE relies on the operational 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 and restrict the ability to manage and operate the TOE to authorized administrative users.
    - Provide a means for authorized administrators to review the audit records in the audit trail.
    - 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.

- For database applications, the TOE uses the ODBC, Oracle Instant client, DB2 client, Lotus Notes Domino C++, or TCP/IP socket APIs.
- For Windows operating systems, the TOE uses the remote registry APIs, SMB file share APIs, and Windows Management Instrumentation (WMI) APIs.
- For Linux/Unix operating systems, the TOE uses telnet and SSH (via a third party WodSSH component).

7. The product capabilities described in Section 3.5 were not included within the scope of the evaluation and no claims are made regarding them

6 ARCHITECTURAL INFORMATION

The TOE allows the authorized administrator to perform the tasks explained above (Discovery, Pen Tests, Audit-type tests) as well as examining scan results, based on administrative privileges that control access to functions.

Logically, the Scan Engine operates as a single application though it is instantiated in a series of processes utilizing inter-process communication mechanisms provided by the underlying operating system to communicate with one another. Within the host, the Scan Engine executes using the host user credentials it is configured to use.

The Console provides a means of centrally managing multiple Scan Engine instances. It implements a Graphical User Interface for the users to manage the TOE. Users can access the console remotely via a web browser. Sun Microsystems Java Runtime Environment (JRE) 1.6 is required for DbProtect Console applet to load into the web browser. Through the Console, users can access the functions and scan results of the Scan Engine instances to which they have been granted access.

The Console is an SSL-enabled web-browser accessible GUI tool that provides access to functions based on user roles and configured organizations. Roles within the console include super user, admin user, basic user, and view user; different functions are available from the console based on the user role. Super and admin users can define organizations, in terms of an IPv4 address range or set of IPv4 addresses on the network, that are hierarchically organized. The super and admin users can then assign test policies and users and/or groups to applicable organizations. The test policies are sets of Pen Tests or Audit Tests grouped for convenience and associated to appropriate organizations. The users and groups are defined in the associated Active Directory, every Console user must always be assigned to at least one organization, and serve to identify which users can access each organization.

The organization hierarchy supports the definition of exclusive/isolated organizations as well as organizations that inherit IP ranges and test Policies in the “parent” Organization. Users that are assigned to an organization, either directly or via a group, can access that organization and its children organizations in accordance with their assigned role.

A Windows Administrator is assigned the Console super user role at system install and the super user can assign other Console roles to Active Directory Users, create Organizations and assign Users to Organizations. Organization assignments may also be made by Windows Groups within Active Directory, which are recognized by the Console. The Console depends upon the Operating System (OS) in the operational environment to authenticate users. The Console provides a login screen that captures the UserID and Password. It sends the UserID and Password to the OS for authentication. If the OS authenticates the user, then the Console GUI is

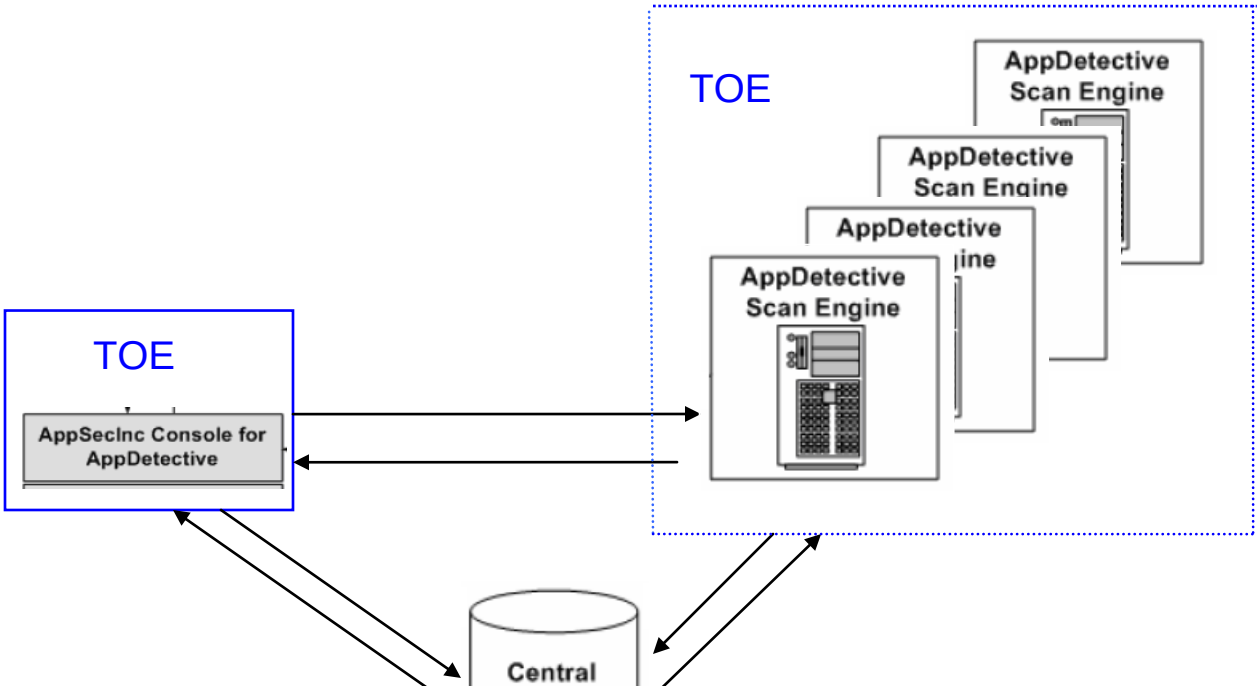

Figure 1. TOE Architecture

displayed. The user is granted access to specific Console functions based on the role assigned to that UserID within the Console. The user is allowed to run vulnerability scans on specific IPv4 addresses and to access data from those scans based on the Organization to which that userID is assigned. Groups are a convenient means of assigning one or more users to the same Organization. A user may be assigned to multiple groups and may be assigned to multiple Organizations. When the user runs a vulnerability scan, that scan is run only against the IPv4 addresses in the "active" Organization for that user, i.e., the Organization displayed on the console screen at the time. The active Organization also limits the user from accessing data except that data generated by the specific IPv4 addresses assigned to that Organization. The Console allows the user to switch from one Organization to another within the same user session.

Figure 1 depicts the association between the Console and the Scan Engine instances in their operating environment:

The TOE relies on an external Backend Database (in the operational environment) to store the scan results from AppDetective instances as well as scan policies established via the Console. The AppDetective scan results are stored in the Backend Database, which is accessed by the Console when reporting the results. The Backend Database is in the operational Environment and is not a part of the TOE. Note that the Console and the Scan Engine depend on the underlying operating system to protect their executables and stored data images (e.g., files and registry keys), all communications between components (via an implementation of,SSL supporting HTTP and SOAP used by the TOE components), and their executing environments. The TOE also depends on the environment to ensure the Backend Database is secure.

DbProtect AppDetective 2009.1 R2 is comprised of the following subsystems:

- **AppDetective User Interface Subsystem**. This subsystem includes the Console and the interface to the Backend Database, including components for interacting users, managing

user access, managing the TOE and user data, and interacting with other TOE components.

- **Execution Subsystem**. This subsystem includes components interacting with the AppDetective User Interface subsystem, the Backend Database, and the Discovery and Scanning Subsystem.
- **Discovery and Scanning Subsystem**. This subsystem includes components that discover targeted IT systems (databases) and performs scans against those targeted IT systems.

The AppDetective User Interface subsystem implements the Console, which provides the GUI for managing the TOE and its functions. This subsystem implements the TOE's role-based security management function. The TOE defines four user roles: super admin; admin; basic; and view. The TOE identifies users and associates them with assigned roles, but relies on the underlying operating system to authenticate user identity, based on the password the user enters at login.

The AppDetective User Interface subsystem generates audit records of the security management functions performed via the Console.

The Execution subsystem invokes and manages the Discovery and Scanning subsystem to identify targeted IT systems on the network and to perform Audit-type Tests and Pen Tests as requested by the AppDetective User Interface subsystem. When the user chooses to perform a Discovery, Pen Test or Audit-type Test, the Execution subsystem launches the Discovery and Scanning Subsystem for a discovery and scanning tasks. The Execution subsystem maintains a pool of threads and makes Dynamic Link Library calls to invoke the Discovery and Scanning subsystem.

The Discovery and Scanning Subsystem provides information about targeted IT systems and performs scanning tasks as directed by the Execution subsystem. The Discovery function comprises two phases: Port Scanning; and Application Detection. The Port Scanning phase locates live TCP/IP ports on network hosts using TCP Connect and Half-Open Port Scanning methods. The TOE includes WinPCAP by CACE Technologies for this purpose. The Application Detection phase involves using a collection of detectors, which can identify database application vendors, versions, and operating system platforms, to identify the database applications on discovered ports. This is done through protocol simulation. Each detector has a native implementation of a client protocol that the target database application understands.

The Discovery function records the IPv4 addresses and ports it discovers, performs application detection tasks, and outputs information about the targeted IT system. This information is passed to the Execution Subsystem and is stored in the Backend Database.

The Scanning function performs checks against discovered targeted IT systems. Checks are classified as one of two types:

- **Penetration Test**—These tests communicate with the targeted IT system via the TCP/IP network interface of the TOE's underlying operating system, using either a partially implemented protocol or bare TCP/IP. Penetration tests do not require credentials.
- **Audit-type Tests**—These tests communicate with the targeted IT system using a 3rd party vendor implementation of a database client or operating system communication protocol. Audit–type tests require valid user credentials for the targeted IT system, which are specified by the administrator within the AppDetective User Interface subsystem.

Each check is part of a security policy, which is managed by the AppDetective User Interface subsystem. A security policy consists of one or more checks, configurable by the authorized

administrator. The Scanning process will perform all checks in a specified policy against each targeted IT system. The results of each check are passed back to the Execution subsystem and stored in the Backend Database for reporting as requested by the administrator. The TOE includes Crystal Reports to support report generation and review functionality.

The TOE is delivered with a number of predefined policies; users can also create their own policies. Policies are edited with the Policy Editor tool, which is in the operational environment. This tool provides the capability to create and edit Audit-type Test and Pen Test policies, based on the built-in policies provided with the TOE. The tool interacts directly with the Backend Database. It is invoked directly from the underlying operating system and does not require the user to be identified or authenticated. Note that this evaluation did not look at the effectiveness of any given policy; rather, it simply confirmed that the primatives included in a policy work as claimed. The TOE depends on its operating environment to authenticate users, store and protect TSF data and ensure that the TOE functions are not tampered with or bypassed.

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 AppDetective 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 2009.1R2, 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 v2009.1R2, which were as follows:

- Ability to test Audit-type Test credentials from Console
- Advanced scheduling options
- Sybase 15 support
- Bug fixes for following issues related to job scheduling:
    - A job that was scheduled with a yearly frequency and in the future ran immediately when DbProtect restarted
    - When a Scheduled Job was run using the 'Run Once' option, its schedule was lost
- Performance and reliability improvements to the Console, Dashboard and Installer
- Support for Fix Scripts.

In July 2011, the vendor retested v2009.1R2 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. The team also ran some additional updated tests identified by the validation panel in May 2012. Analysis of the updated test evidence indicated that all tests passed.

7.1 Developer Testing

The vendor's approach to testing for DbProtect AppDetective is based on manual testing of the DbProtect AppDetective features and security functions. DbProtect AppDetective is tested using

a number of manual test suites by security function with varying numbers of test cases. The testing for each DbProtect AppDetective 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 AppDetective, test cases were provided for: Audit data generation; Database Scan Data Review; Database Scan Data Collection; User attribute definition; Timing of identification; Management of security function behavior; Specification of Management Functions; Security roles; and Non-bypassability of the TSP.

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 AppDetective per the evaluated configuration as described in the developer's test documentation. This document describes the testing environment for DbProtect AppDetective as follows:

- Console Operating System (OS)—Windows Server 2003 Standard Edition
- Backend database—Microsoft SQL Server 2005 Standard Edition
- Scan Engine 5.7—Windows Server 2003 Standard Edition
- Browser—Microsoft Internet Explorer 6.0
- Targeted databases in the operational environment—SQL Server 2005 and Oracle 9i R2.

The evaluation team conducted testing of DbProtect AppDetective in 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:

- **Auditing security related events**—The evaluation team conducted testing to determine if all auditable events claimed in the ST were in fact generated by the TOE. Testing identified that some events being claimed for the evaluated version of the TOE were not actually generated by the TOE. The ST was updated to correctly represent the auditing capability of the TOE.
- **Security Function Behavior**—The evaluation team complemented the developer's testing of the Security Management security function by testing that capabilities were allowed or restricted consistent with the specification of management restrictions in the ST—the developer's testing was not complete in this area. The evaluator testing confirmed all security management functions were restricted consistent with information in the ST and guidance documentation.

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 any findings that indicated 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 evaluation team conducted tests confirming that unauthorized users in the operational environment of the TOE (i.e., not in any Active Directory users or groups granted access to the TOE, or granted administrative privileges on the operating system on which the Console component is installed) could not successfully login to the Console or access the TOE executables.

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 Apr 2009
- DbProtect 2009.1 R2 Administrator's Guide, last updated 6 Apr 2012
- DbProtect 2009.1 R2 User's Guide, last updated 6 Apr 2012
- DbProtect AppDetective 2009.1 R2 Evaluated Configuration, 6 Apr 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 AppDetective 2009.1 R2 Functional Specification and High Level Design	2.1	11 May 2012

Guidance Documentation	Version	Date
DbProtect 2009.1 R2 Administrator's Guide		6 Apr 2012
DbProtect 2009.1 R2 User's Guide		6 Apr 2012
DbProtect 2009.1 R2 Installation Guide		7 Apr 2009
DbProtect AppDetective 2009.1 R2 Evaluated Configuration	0.9	6 Apr 2012

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

Test Documentation	Version	Date
DbProtect AppDetective 2009.1 R2 Test Plan	1.6	11 May 2012
Requirement Component – Database Scan Data Collection	1.1	6 Apr 2012
Requirement Component – Database Scan Data Review	1.1	6 Apr 2012
Requirement Component – Audit data generation	1.1	6 Apr 2012
Requirement Component – User Attribute Definition	1.2	8 May 2012
Requirement Component – Timing of Identification	1.1	6 Apr 2012
Requirement Component – Management of Security function behavior	1.2	8 May 2012
Requirement Component – Specification of Management Function	1.1	6 Apr 2012
Requirement Component – Security Roles	1.2	8 May 2012
Requirement Component – Non-bypassability of the TSP	1.1	6 Apr 2012

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

Security Target	Version	Date
DbProtect AppDetective 2009.1 R2 Security Target	1.0	16 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 AppDetective 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 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

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

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 AppDetective 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 2. 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
ALC_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 AppDetective 2009.1 R2 does not support IPv6.
4. 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

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
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
SAIC	Science Applications International Corporation
SCAP	Security Content Automation Protocol
SOAP	Simple Object Access Protocol
SP	Special Publication
SP1	Service Patch 1
SP2	Service Patch 2
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
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 AppDetective 2009.1 R2 Security Target,** Version 1.0, dated 16 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, CCIMB-2009-07-004.
5. DbProtect AppDetective 2009.1 R2 Security Target, Version 1.0, 16 May 2012.