National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

AppDetective Pro v5.8.0

Report Number: CCEVS-VR-VID10257-2011
Dated: 31 March 2011
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
Nicole Carlson

The Aerospace Corporation
El Segundo, CA

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the AppDetective Pro v5.8.0 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 March 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 2.3. 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 and AVA_MSU.1. 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.

AppDetective Pro is a software application that runs in the context of a commercial operating system. AppDetective Pro discovers database applications within an organization's network infrastructure and scans them for potential vulnerabilities. Administrators can then take appropriate remedial actions. AppDetective Pro utilizes a library of known vulnerabilities and misconfiguration signatures. AppDetective Pro includes modules for the following database applications:

- Oracle 11g, Oracle 10g, Oracle9i, Oracle8i
- Microsoft SQL Server Versions 2000, 2005, and 2005 Express Edition. MSDE 2000 SP4
- Lotus Domino 6 and 7
- Sybase Adaptive Server Enterprise 11.9.2, 12.0, 12.5, 15
- IBM DB2 Version 8.1, IBM DB2 Version 8.2, IBM DB2 Version 9.1, IBM DB2 Version 9.5, IBM DB2 Version 7, 8 and 9 on z/OS and OS/390
- MySQL 4.0, 4.1, 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).

AppDetective Pro is designed to operate in the context of the following operating systems: Microsoft Windows XP Professional SP2 or greater; Microsoft Windows Server 2003 Standard Edition; Microsoft Windows Server 2003 Enterprise Edition; Microsoft Windows Server 2003 Enterprise; Microsoft Windows Vista (Business, Enterprise, and Ultimate editions); and Microsoft Windows 7 (Professional, Enterprise, and Ultimate editions).

AppDetective Pro can be configured to use Microsoft SQL Server Express, SQL Server 2000 SP4, Microsoft SQL Server 2005, Microsoft SQL Server 2008 or MSDE 2000 as its Backend Database. The Backend Database can be local or remote to the system hosting AppDetective Pro.

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 AppDetective Pro v5.8.0 Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	AppDetective Pro v5.8.0
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 March 2011
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.3, August 2005.
Evaluation Class:	EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1
Description:	AppDetective Pro 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 AppDetective Pro v5.8.0 product by any agency of the U.S. Government and no warranty of the AppDetective Pro 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 Jerome Myers Daniel Faigin Nicole Carlson

1.2 Interpretations

Not applicable.

1.3 Threats

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

- Unauthorized attempts to access TOE data or security functions may go undetected.
- An unauthorized user may attempt to remove or destroy data collected by the TOE.
- Improper security configuration settings may exist in the IT System the TOE monitors.
- Vulnerabilities may exist in the IT System the TOE monitors.

1.4 Organizational Security Policies

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

- The authorized administrator of the TOE shall be accountable for using the TOE management functions.
- Configuration and vulnerability information that might be indicative of the potential for a future intrusion of a targeted IT System (database) must be collected.
- The TOE shall provide management functions, which allow the authorized administrators to effectively manage the TOE.

2 Identification

The evaluated product is **AppDetective Pro v5.8.0**.

3 Security Policy

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

> ***Note:*** *Much of the description of the AppDetective Pro security policy has been extracted and reworked from the AppDetective Pro v5.8.0 ST and Final ETR.*

3.1 Database Discovery and Scanning

The TOE is a software application that runs in the context of a commercial operating system. AppDetective Pro is able to discover database applications within an organization's network infrastructure and scan them for potential vulnerabilities. AppDetective Pro utilizes a library of known vulnerabilities and misconfiguration signatures. AppDetective Pro performs the following operations:

- **Discovery**—systematically searches the network, inventorying applications and relevant application components by vendor and release.
- **Penetration Test (Pen Test)**—applies a series of detailed security tests. AppDetective Pro Pen Tests identify how an intruder or unauthorized user might gain access to application components. Pen Tests use various mechanisms to simulate how an intruder could exploit vulnerabilities to break into applications from the outside without possessing any authentication credentials.
- **Audit**—connects to the target database application and its underlying operating system to perform an assessment of its configuration, determining susceptibility to internal misuse. AppDetective Pro Audits require a valid user account on the target application in order to verify internal configuration settings.
- **Reporting**—provides a reporting capability that enables the administrator to generate and view various types of report that document the results of a Pen Test or Audit, identifying potential vulnerabilities, an assessment of the risk associated with a vulnerability, and recommending actions to address a vulnerability.

Pen Tests and Audits both consist of a series of security tests or checks that are grouped together in a Policy. Each security test or check targets a specific database application type and performs actions to determine if the application is susceptible to the vulnerability tested for by the check. Pen Test and Audit checks are categorized according to the type of vulnerability for which they test.

The Pen Test categories are:

- **Denial of Services**—these checks examine the target application for susceptibility to specific Denial of Service attacks.
- **Misconfigurations**—these checks examine the target application for possible misconfigurations that may leave the application susceptible to attack.
- **Password Attacks**—these checks examine the target application to determine if it is vulnerable to direct password attacks, including: accounts with blank passwords; accounts with default passwords; and susceptibility to dictionary and brute-force attacks.
- **Vulnerabilities**—these checks determine if the application is susceptible to a specific published vulnerability for that application.

The Audit categories are:

- **Access Control**—these checks examine the target application for potentially inappropriate or insecure access control or privilege settings on database objects.
- **Application Integrity**—these checks determine if specific security measures (such as enabling auditing of specific events or encrypting sensitive data) have been applied in the application.

- **Identification/Password Control**—these checks examine the target application configuration to determine if it might be vulnerable to password attacks or problems associated with user accounts (e.g., by allowing short or poorly constructed passwords).
- **OS Integrity**—these checks examine aspects of the OS supporting the database application to ensure they do not expose the application to attack (e.g., permissions on database files) and that the database configuration does not introduce vulnerabilities into the OS (e.g., application processes running with elevated privileges).

Note that 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.

3.2 Security Audit

The TOE has the ability to generate audit records for the TOE security-relevant events. 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 IT environment to protect and store the audit records, provide the ability to review the audit records, and to provide a reliable timestamp. The user ID is also obtained from the IT environment.

3.3 Security Management

The TOE provides a graphical user interface and a command line interface for managing the TOE's security functions and the TOE data. The notion of authorized administrator role, which has full control and privileges to manage the TOE and its security functions, is realized as any user that the IT environment allows to invoke the TOE application. Note also that the TOE relies on the IT environment to perform identification and authentication of the authorized administrator.

4 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 TOE can only be accessed by authorized users.

4.1 Clarification of Scope

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 and AVA_MSU.1 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 TOE relies on the IT 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 IT 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.

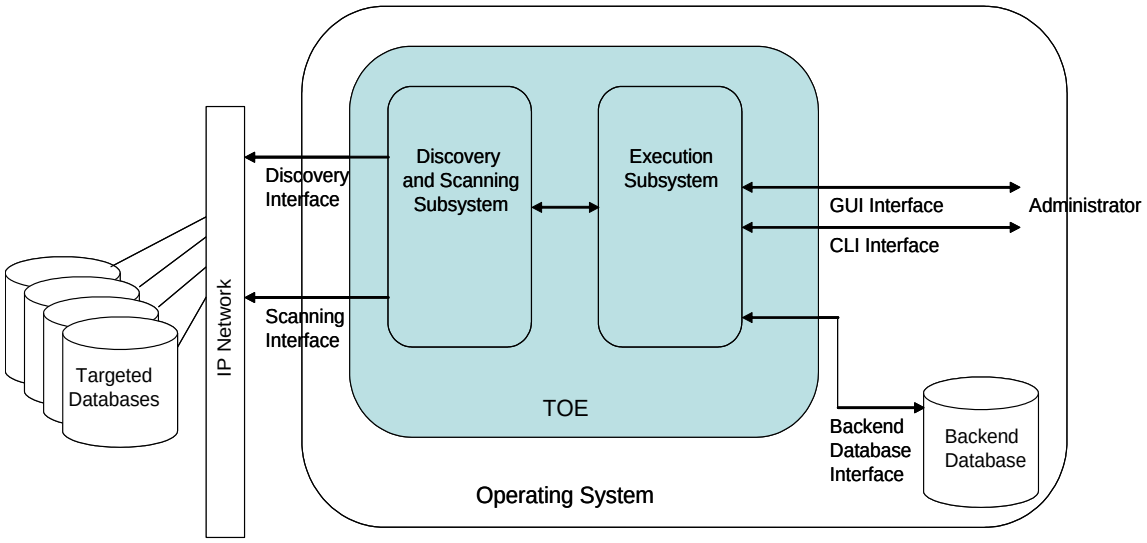
   Additionally, the TOE relies on its host to facilitate communication with target database applications and operating system products for the purposes of scanning and auditing.
6. The following product capabilities described in the guidance documentation were not included within the scope of the evaluation and no claims are made regarding them:
   - The ability of the TOE to generate fix scripts that the administrator can apply to correct problems identified by Pen Tests or Audits. The evaluation has not covered the efficacy of these fix scripts in actually correcting detected problems.
   - The ASAP Updater tool 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 would take the TOE out of its evaluated configuration, and so it is excluded from the evaluation.
   - 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. In addition, the effectiveness of policy exclusions has not been assessed.
   - 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.

5 Architectural Information

AppDetective Pro consists of the following core components:

- **Execution Subsystem**—this subsystem includes components interacting with the user and the backend database.
- **Discovery and Scanning Subsystem**—this subsystem includes components that discover targeted IT systems (databases) and performs scans against those targeted IT systems.

The TOE architecture is depicted in the following figure, which also identifies its external interfaces and the components of the IT environment with which it interacts.



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 incorporates 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.

- **Audit**—these tests communicate with the targeted IT system using a 3rd party vendor implementation of a database client or operating system communication protocol. Audit checks require valid user credentials for the targeted IT system.

Each check is part of a security policy that is managed by the Execution 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 provide report generation and review functionality.

The TOE depends on its operating environment to identify and authenticate users, store and protect TSF data and ensure that the TOE functions are not tampered with or bypassed.

6 Documentation

6.1 Product Guidance

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

- AppDetective Pro 5.8 Installation and User's Guide, Last Modified: May 8, 2009
- Installing and Using the Common Criteria Configuration of AppDetective Pro v5.8, Version 1.1, 29 March 2011.

6.2 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
Application Security AppDetective Pro V5.8.0 Functional Specification and High Level Design Document for Common Criteria Evaluation	1.2	15 Feb 2011

Configuration Management Documentation	Version	Date
DbProtect AppRadar, DbProtect AppDetective, AppDetective Pro Configuration Management Plan	0.4	11 May 2010
Shared Documents List for Configuration Management Document	0.2	10 Jan 2011

Delivery and Operation Documentation	Version	Date
DbProtect AppRadar DbProtect AppDetective AppDetective Pro Delivery Procedures	0.3	27 May 2009

Lifecycle Documentation	Version	Date
DbProtect AppRadar, DbProtect AppDetective, AppDetective Pro Life Cycle Document	0.3	27 May 2009

Test Documentation	Version	Date
AppDetective Pro 5.8.0 Test Plan & Vulnerability Assessment	0.7	10 May 2010
Requirement Component – Database Scan Data Collection	1.0	3 Aug 2010
Requirement Component – Database Scan Data Review	1.0	3 Aug 2010
Requirement Component – Audit data generation	1.0	3 Aug 2010
Requirement Component – Specification of Management Function	1.0	3 Aug 2010
Test Evidence for Audit Job using Sample-Test-Set Checks	0.1	
Test Evidence for Pen Test Job using Sample-Test-Set Checks	0.1	

Vulnerability Assessment Documentation	Version	Date
AppDetective Pro 5.8.0 Test Plan & Vulnerability Assessment	0.7	10 May 2010

Security Target	Version	Date
AppDetective Pro v5.8.0 Security Target	1.0	29 Mar 2011

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 AppDetective Pro v5.8.0.

Evaluation team testing was conducted at the vendor's development site May 18 through May 19, 2009. Re-testing of the TOE as a consequence of the results of the Final Validation Oversight Review occurred in May 2010, with further re-testing occurring in August 2010.

7.1 Developer Testing

The vendor's approach to testing for AppDetective Pro is based on manual testing of the AppDetective Pro features and security functions. AppDetective Pro is tested using a number of manual test suites by security function with varying numbers of test cases. The testing for each AppDetective Pro 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 AppDetective Pro, test cases were provided for Audit data generation; Database Scan Data Review; Database Scan Data Collection; and Specification of Management Functions.

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

Operating System:

- Microsoft Windows Server 2003 Enterprise Edition SP2

Backend Database (for storing TOE data):

- Microsoft SQL Server 2000 SP4

Targeted IT systems:

- Oracle 9i running on RedHat Linux 4
- Microsoft SQL Server 2000, 2000 SP4, both running on Windows 2003 Enterprise Edition (64 bit) SP2
- Lotus Domino 7.0.2, running on Windows 2003 Enterprise Edition (32 bit)
- Sybase ASE 12.5, running on Windows 2000 Advanced Server SP4
- IBM DB2 Version 8.2, Version 9.1, both running on RedHat Linux 5
- MySQL 4.1, 5.0, both running on Windows 2003 Enterprise Edition (32 bit)

The evaluation team devised a test subset based on coverage of the security functions described in the ST.

The evaluation team performed the following additional functional tests:

- **Testing via the Command Line Interface**—all of the developer's tests were performed using the TOE GUI. The TOE includes a Command Line Interface (CLI) from which a selection of TOE functions, including running Discovery, Audit, and Pen Test scans and generating reports, can be performed. The evaluation team confirmed the CLI behaved as described in the guidance documentation and appropriate audit records were generated.
- **Security Audit Behavior**—the evaluation team complemented the developer's testing of the Security Audit security function by confirming: that the TOE includes the user's identity from the underlying operating system as the subject identity in generated audit records; that the Security Audit security function can be disabled and enabled and both actions are audited; and that the Security Audit security function is disabled by default when the TOE is first installed.

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.

8 Evaluated Configuration

The evaluated version of the TOE is AppDetective Pro v5.8.0.

AppDetective Pro 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.

The TOE is designed to operate in the context of the following operating systems: Microsoft Windows XP Professional SP2 or greater; Microsoft Windows Server 2003 Standard Edition; Microsoft Windows Server 2003 Enterprise Edition; Microsoft Windows Server 2003 Enterprise x64; Windows Vista (Business, Enterprise, and Ultimate editions); and Windows 7 (Professional, Enterprise, and Ultimate editions).

The TOE can be configured to use Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Express, or MSDE 2000 as its Backed Database. **Note that although the *AppDetective Pro 5.8 Installation and User's Guide* identifies Microsoft Access as the default for the Backend Database, its use is not supported in the evaluated configuration.** This is stated clearly in *Installing and Using the Common Criteria Configuration of AppDetective Pro v5.8*, which also provides guidance on how to install the TOE and connect it to a supported database. The SQL Server or MSDE 2000 Backend Database can be local or remote to the system hosting the TOE.

Additionally, the TOE requires the following components in the IT 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
- SQL Server 2005 Backwards Compatibility (aka Feature Pack for Microsoft SQL Server 2005)

The TOE includes Crystal Reports 9.2.0 to support its report generation and viewing function, WinPcap Pro 4.0.2.1123 to support the Discovery operation, and WodSSH to support the TOE's ability to connect to target Linux/UNIX operating systems for the purpose of audits.

The TOE supports its Discovery, Pen Test and Audit operations on the following database applications:

- Oracle 11g, Oracle 10g, Oracle9i, Oracle8i
- Microsoft SQL Server Versions 2000, 2005, and 2005 Express Edition. MSDE 2000 SP4
- Lotus Domino 6 and 7
- Sybase Adaptive Server Enterprise (ASE) 11.9.2, 12.0, 12.5, 15
- IBM DB2 Version 8.1, IBM DB2 Version 8.2, IBM DB2 Version 9.1, IBM DB2 Version 9.5, IBM DB2 Version 7, 8 and 9 on z/OS and OS/390
- MySQL 4.0, 4.1, 5.0

However, in order to perform audits on some database applications, the administrator needs to ensure the following components are installed and accessible in the IT environment:

- IBM DB2 Server audits require the IBM DB2 runtime client
- IBM DB2 for Mainframe audits require IBM DB2 Connect
- Lotus Domino audits require the Lotus Notes client driver
- Sybase ASE audits require the Sybase ASE ODBC driver

9 Results of the Evaluation

The evaluation was conducted based upon version 2.3 of the CC and the CEM. 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.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.2 and AVA_MSU.1" certificate rating be issued for AppDetective Pro v5.8.0.

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.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_FLR.2	Flaw Reporting Process
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_MSU.1	Examination of guidance

Assurance Component ID	Assurance Component Name
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10 Validator Comments/Recommendations

1. The validators observe that tools such as AppDetective Pro can aid in meeting the continuous assessment requirements of 800-53r3 and 800-37r1. Note that this tool focuses on databases and other products must be used for OS and network component assessments.
2. The validators recommend that administrators of the TOE keep up to date with patches for the components in the operational environment.
3. The vendor asserts that AppDetective Pro can operate in environments where its underlying operating system and Backend Database are configured in accordance with applicable Security Technical Implementation Guides (STIGs). However, this assertion was not tested by the evaluation.
4. With respect to the use of telnet, users must clearly understand that telnet provides no protection for authentication credentials (and use creates a problem for those subject to DOD 8500.2's DCPP control). Secure shell (SSH) should be used whenever possible.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **AppDetective Pro v5.8.0 Security Target,** Version 1.0, dated March 29, 2011.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3, August 2005, CCIMB-2005-08-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.3, August 2005, CCIMB-2005-08-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.3, August 2005, CCIMB-2005-08-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 2.3, August 2005, CCIMB-2005-08-004.
5. AppDetective Pro v5.8.0 Security Target, Version 1.0, March 29, 2011.