National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

StillSecure VAM V5.5

Report Number: CCEVS-VR-06-0060
Dated: January 26, 2007
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 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of StillSecure VAM V5.5.

This VR is not an endorsement of the Information Technology (IT) product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

StillSecure VAM is a vulnerability management platform that identifies and manages the remediation of network security vulnerabilities. StillSecure VAM scans for vulnerabilities using the current vulnerability signatures that are updated hourly. There are scheduled and on-demand scans. StillSecure VAM allows an authorized administrator to manage the repair of vulnerabilities using VAM's Vulnerability Repair Workflow. StillSecure VAM tracks all scanning and remediation activities and delivers a range of reports for auditors, managers, and IT staff members.

The Target of Evaluation (TOE) includes four two main components: Server VAM safeguards the target network infrastructure,. Desktop VAM secures the target network's desktop environment Remote VAM locks down the exposed target network perimeter allowing the authorized administrator to focus on vulnerabilities that represent immediate threats to the organization. StillSecure VAM has a web-based User Console through which all StillSecure VAM functions are managed.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with IT environment:

- Vulnerability System including:
  - Map, Scan, Repair, and Report
- Identification and Authentication
- Security management
- Security Audit
- Partial protection of TOE security functions

The following are explicitly excluded from the TOE configuration, but are included in its IT environment:

- Hardware platform(s) for all product components
- Operating System platform(s) for all product components
- Cryptographic module(s): SSL implementation on all platforms
- Transport implementations (HTTP, HTTPS, and FTP)
- Network or other connectivity: (Ethernet network)
- Third party relational database (MySQL) and its interface
- Internet Browser (e.g., Internet Explorer, Netscape Communicator)
- Distributed Scanners

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during January 2007. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) is contained within the document Security Target for StillSecure VAM V5.5 [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	StillSecure VAM V5.5
Evaluated Software:	StillSecure VAM V5.5 with VAM5.5_NetPatch
Developer:	StillSecure Suite 200 100 Superior Plaza Way Superior, CO 80027
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Validation Body:	NIAP Common Criteria Evaluation and Validation Scheme
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in section 5.2 of the ST. A description of the principle security policies is as follows:

- **Vulnerability System** – The TOE provides several features that map, scan, manage remediation, and report on vulnerabilities of the devices on the target network.
  - **Map and Scan** –Autodiscovery uses onboard scanners to map the network. The TOE finds devices on the target network using ICMP pings with port and service scanners. Once the network is mapped, the onboard scanners scan for vulnerabilities of the devices on the target network.
  - **Repair** – Once the vulnerabilities have been mapped, the TOE provides a workflow process through its User Console to aid authorized users in managing the patches and software updates that are necessary in correcting the found vulnerabilities.
  - **Report** – The TOE provides reporting functionality to aid the authorized users in managing the found vulnerabilities and workflow process.
- **Identification / authentication and Security Management** – The TOE provides user identification and authentication through the use of user accounts and the enforcement of password policies. The TOE provides security management through the use of the User Console. The TOE provides multiple administrative roles.
- **Security audit** – The TOE provides its own internal auditing capabilities separate from those of the Operating System. The TOE provides the ability to search and view its own audit records.

A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_STG_EXP.1-1	Protected audit trail storage
Class FIA: Identification & Authentication	
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback

FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MTD.1	Management of TSF data
FMT_REV.1	Revocation
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_RVM_EXP.1-1	Non-bypassability of the TSP
FPT_SEP_EXP.1-1	TSF domain separation
Class VUL: Vulnerability System	
VUL_SDC_EXP.1	System data collection
VUL_ARP_EXP.1	Security alarms
VUL_DRS_EXP.1	Data reporting

IT Environment Security Functional Requirements

Class FAU: Security Audit	
FAU_STG_EXP.1-2	Protected audit trail storage
Class FPT: Protection of the TSF	
FPT_RVM_EXP.1-2	Non-bypassability of the TSP
FPT_SEP_EXP.1-2	TSF domain separation
FPT_STM.1	Reliable time stamps

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords. However, administrators and operators are capable of error.
- Administrators will ensure that the environment has adequate facility to provide disk storage and other capabilities for the TOE's protection.
- The attack potential on the TOE is assumed to be low.

- It is assumed that there will be no untrusted users and no untrusted software on the StillSecure VAM Server host which hosts the Server VAM, Desktop VAM, and Remote VAM modules.
- Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access.
- Those responsible for the TOE will ensure the communications between the User Console and StillSecure VAM Server host are secure.
- It is assumed that authorized users will protect their authentication data.

4.3 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. This evaluation does not verify all claims made in the product's end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5.2 and 6 respectively).
2. This evaluation only covers the evaluated configuration of the specific version identified in this document, and not any later versions released or in process.
3. As with all EAL2 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. StillSecure VAM depends on IT environment to provide trusted communication channel between the TOE and a remote trusted IT product.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

StillSecure VAM is software that executes on a RedHat Enterprise 3 Linux operating system platform and consists of the following modules: Server VAM, Desktop VAM, Remote VAM, and a User Console. Each VAM module targets a specialized scanning need. The User Console component provides the user interface which is accessed via an Internet browser over a Secure Sockets Layer (SSL) communication channel. The database is not part of the TOE.

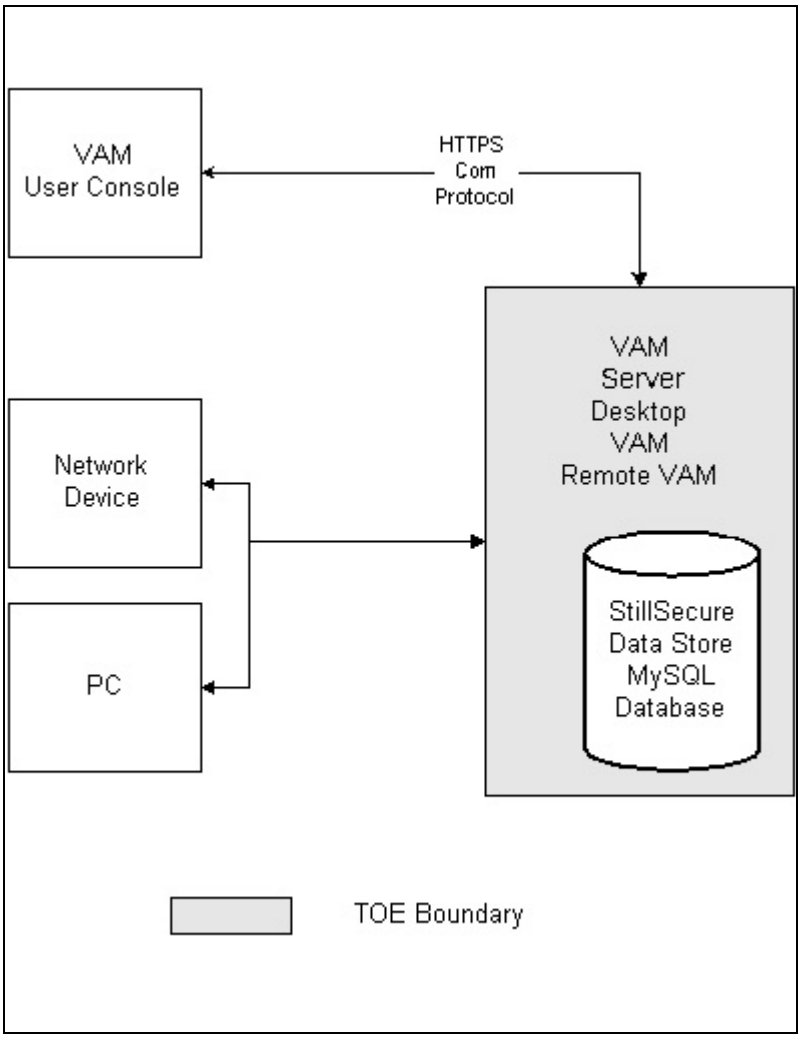

Figure 1. TOE Physical Boundary.

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

StillSecure VAM V5.5 Security Target V1.6
StillSecure VAM V5.5 Installation Guide
StillSecure VAM V5.5 Users' Guide
StillSecure VAM Quick-start card

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

7.1 Developer Testing

The vendor testing covered the security functions identified in Section 6.1 of the ST. These security functions were: Security audit, Identification and Authentication, Security Management, partial Protection of TSF and Vulnerability System.

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. In general, only those user interface functions that were directly related to SFRs were explicitly verified.

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests.

The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

The evaluation team reran part of the developer tests, modified input parameters to ensure full functionality of the interface and verified the results.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall minimum strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

The StillSecure SOF analysis assumes passwords length to be a minimum of 8 with at least one character has to be uppercase, a number, or a special character. It further assumes that common dictionary words are not used and that passwords expire in StillSecure recommended period of 30 days.

StillSecure is a software-only product and hence relies on the underlying Operating System for initial authentication. Users first must identify and authenticate themselves through the OS, and then the StillSecure console requires each user to be successfully identified and authenticated before using VAM.

7.4 Vulnerability Analysis

The developer searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of StillSecure VAM V5.5 were found. The following public domain sources were used to identify and search for relevant vulnerabilities:

- http://www.securityfocus.com
- http://securiteam.com
- http://www.nvd.nist.gov
- http://cve.mitre.org

Known vulnerabilities in the IT environment could also be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer will installed the latest security critical patches to the operating system and database software. Under unusual circumstances a patch to TOE may also be required to address compatibility issues with a specific operating system or database patch. The customer is advised check the StillSecure support web site for any restrictions on specific patches to components of the IT environment.

The assumed level of expertise of an attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2.1 of the ST.

8. Evaluated Configuration

The evaluated version of StillSecure VAM is version 5.5 internally identified as build VAM 5.5-887 with the VAM5.5_NetPatch.

StillSecure provides delivery of this software product by mail in an installation CD or via web by downloading and burning an ISO image to a CD. Anybody can download the software; however, the license key to operate the StillSecure software is provided to customers via email. The VAM installation CD automatically reformats the hard drive on the host machine erasing all existing data. The patch VAM5.5_NetPatch is available from StillSecure's web site (http://www.stillsecure.com/vam/support/instructions0911.php).

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 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 details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed 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
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10. Validator Comments/Recommendations

The effectiveness of StillSecure VAM's vulnerability detection functionality depends largely on the specific scan rules in its local database. As part of their product support for licensed users, StillSecure maintains scan rules on their web server that reflect newly discovered vulnerabilities. This evaluation was limited to the scan rules that were available on StillSecure's web server at the time that evaluation testing was performed. The product's scan rule update functionality primarily represents a service that StillSecure provides to its customers and is outside the scope of the evaluation.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 certificate rating be issued for the StillSecure VAM V5.5.

11. Security Target

The Security Target for StillSecure VAM V5.5 is contained within the document StillSecure VAM™ V5.5 Security Target version 1.6 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria [CC]
CCEVS	Common Criteria Evaluation and Validation Scheme

CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology [CEM]
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PP	Protection Profile
SFR	Security Functional Requirement
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.nsa.gov/ia/industry/niap.cfm).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- StillSecure (http://www.stillsecure.com).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology, January 2004.
- [CCEVS3] Guidance to Validators of IT Security Evaluations, Version 1.0, February 2000.
- [CCEVS4] Guidance to Common Criteria Testing Laboratories, Draft, Version 1.0, March 2001.

Other Documents

- [ST] Security Target for StillSecure VAM V5.5, version 1.6, December 13, 2006