Certification Report

EAL 3+ Evaluation of Third Brigade, Inc.

Deep Security Version 5.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-68
Version:	0.9
Date:	07 April 2008
Pagination:	i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3,* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada (CSEC), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSEC, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada (CSEC).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is DOMUS IT Security Laboratory, a division of NUVO Network Management, located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated ***April 08, 2008***, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html
This certification report makes reference to the following trademarked names:

- Third Brigade is a registered trademark of Third Brigade, Inc.
- Microsoft and Windows are registered trademarks of Microsoft Corporation.
- Solaris is registered trademark of Sun Microsystems, Inc.
- RedHat and RedHat Enterprise Linux are registered trademarks of Red Hat, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Third Brigade® Deep Security 5.0 (hereafter referred to as Deep Security 5), from Third Brigade, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Deep Security 5 is an advanced intrusion prevention system (IPS). It provides the last line of defence against attacks that exploit vulnerabilities in commercial and custom software, including web applications. It enables its users to create and enforce comprehensive IT security policies that proactively protect sensitive data, applications, hosts or network segments.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on March 20 2008, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Deep Security 5, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of Deep Security 5 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 3 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.3*. The following augmentations are claimed:

ALC_FLR.1 – Basic flaw remediation

The Communications Security Establishment Canada, as the CCS Certification Body, declares that Deep Security 5 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Third Brigade® Deep Security 5.0 (hereafter referred to as Deep Security 5), from Third Brigade, Inc.

2 TOE Description

Deep Security 5 is an advanced intrusion prevention system (IPS). It provides the last line of defence against attacks that exploit vulnerabilities in commercial and custom software, including web applications. It enables its users to create and enforce comprehensive IT security policies that proactively protect sensitive data, applications, hosts or network segments.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Deep Security 5 is identified in Section 5 of the ST.

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: Third Brigade Deep Security 5.0 Security Target (EAL3+)
Version: Version 1.4
Date: 22 May 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3,* for conformance to the *Common Criteria for IT Security Evaluation, version 2.3,* incorporating all final CC interpretations. Deep Security 5 is:

a) Common Criteria Part 2 extended with security functional requirements based upon functional requirements in Part 2, except for the following explicitly stated requirements defined in the ST as well as in the Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006:

• IDS_SDC.1	System Data Collection
• IDS_ANL.1	Analyzer analysis
• IDS_RCT.1	Analyzer react
• IDS_RDR.1	Restricted Data Review
• IDS_STG.1	Guarantee of System Data Availability

- IDS_STG.2 Prevention of System data loss

b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c) Common Criteria EAL 3 augmented, containing all security assurance requirements in the EAL 3 package, as well as the following:

- ALC_FLR.1 – Basic flaw remediation.

6 Security Policy

Deep Security 5 implements:

- Identification and Authentication Security Policy

  The Identification and Authentication function only allows authorized administrator to carry out administrative tasks through the administrative interface.

- Role-base Access Control Security Policy

  The Role-based Access Control function restricts authorized TOE administrators' access to the system using role based access control.

- Auditing Security Policy

  The Audit function generates audit logs for system events. The audit logs are only accessible to authorized administrator, and are protected against unauthorized deletion, modification, and audit data loss when audit trail is full.

- Intrusion Detection and Prevention Security Policy

  The Intrusion Detection and Prevention function provides capabilities for Deep Security Manager to configure security profiles and assign them to Deep Security Agents. Deep Security Agents collect and analyze the traffic data, react to specified events according to security profiles, and pass events to Deep Security Manager for review and storage.

- Secure Communication Security Policy

  All communications between Deep Security Agents and Deep Security Manager are protected from disclosure or modification.

Further details on these security policies may be found in Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Deep Security 5 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of Deep Security 5.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

The TOE has access to all the IT System data it needs to perform its functions, is managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors, and is appropriately scalable to 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.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

For more information about the TOE security environment, refer to section 3 of the ST.

7.3 Clarification of Scope

The TOE was designed and intended for use in a structured corporate environment. In this type of environment, users will not typically be allowed to install programs on their machines or change system settings. Administrators will set policy controlling what users are and are not allowed to do and rely on different mechanisms for enforcement.

8 Architectural Information

The TOE is separated into subsystems that provide the TOE Security Functions. These subsystems are:

- Manager

The Manager is a centralized web-based management system that allows administrators to create and manage comprehensive security policies, to track threats and take preventive actions in response to them.

- Agent (User Mode)

  The User Mode Agent subsystem is responsible for communication with Deep Security Manager, Configuration Management, Audit Analysis and Storage, and SSL Decryption.

- Agent (Kernel Mode)

  The Kernel Mode Agent subsystem is responsible for implementation of the Stateful Firewall and IDS/IPS system.

9 Evaluated Configuration

9.1 Deep Security 5 Components under Evaluation

Deep Security 5 Components under Evaluation	**Versions**
Deep Security Manager (for Microsoft® Windows®)	Manager-5.0.3025.exe
Deep Security Agent (for Solaris™ 10 SPARC)	Agent-Solaris_5.10_sparc-5.0.0-3372.sparc.pkg.gz
Deep Security Agent (for RedHat® Enterprise Linux® 5)	Agent-RedHat_2.6.18_8.el5_i686-5.0.0-3373.i386.rpm
Deep Security Agent (for Microsoft® Windows®)	Agent-Windows-5.0.0-3376.i386.msi

Deep Security 5 evaluated configuration requires:

- Deep Security Manager

  i. Memory: Minimum RAM 512 MB (1 GB recommended)

  ii. Disk Space: Minimum 100 MB (2 GB recommended)

  iii. Operating System: Windows 2003 Server SP1

  iv. Oracle Database 10g Express Edition

v. Tomcat Embedded 5.5.17

- Deep Security Agent

  i. Memory: Minimum RAM 128 MB

  ii. Disk Space: Minimum 5 MB (15 MB recommended, primarily for logging)

  iii. Windows 2003 Server SP1

  iv. Solaris 10

  v. Linux Red Hat Enterprise Edition 5

10 Documentation

Deep Security 5 user and administrator guidance documentation provided to the consumer includes:

- Deep Security 5.0 User's Guide

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Deep Security 5, including the following areas:

Configuration management: An analysis of Deep Security 5 CM system and associated documentation was performed. The evaluators found that Deep Security 5 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed**.**

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Deep Security 5 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed Deep Security 5 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined Deep Security 5 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of Deep Security 5 design and implementation. The evaluators reviewed the flaw remediation procedures used for Deep Security 5. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: Deep Security 5 ST’s strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer’s vulnerability analysis for Deep Security 5 and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL3 augmented consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer’s test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation,

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

executing a subset of developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Testing focused on the following areas:

- Audit;
- Role Based Access Control;
- Identification and Authentication;
- Secure intra-TOE communication; and
- Intrusion detection and prevention.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Port Scanning;
- Monitoring the network traffic;
- Denial-of-service attack; and
- SQL injection.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

Deep Security 5 was subjected to a comprehensive suite of formally-documented, independent functional and penetration tests. The testing took place at the Third Brigade’s facility in Ottawa, Ontario, Canada, and at the ITSET facility at DOMUS IT Security Laboratory located in Ottawa, Ontario, Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer’s tests and independent functional tests yielded the expected results, giving assurance that Deep Security 5 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3 augmented level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

Consumers of Deep Security 5 should consider assumptions about usage and environmental settings, defined in the Section 3 of ST, and the TOE protection scope, clarified in the Section 7.3 of this document, as requirements for the product's installation and its operating environment.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CC	Common Criteria for Information Technology Security Evaluation
CCS	Common Criteria Evaluation and Certification Scheme
CR	Certification Report
CSEC	Communications Security Establishment Canada
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection System
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MB	Megabyte
PALCAN	Program for the Accreditation of Laboratories Canada
RAM	Random Access Memory
ST	Security Target
TOE	Target of Evaluation

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2005-08-002, Version 2.3, August 2005.

b) Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2005-08-003, Version 2.3, August 2005.

c) Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2005-08-004, Version 2.3, August 2005.

d) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

e) Third Brigade Deep Security 5.0 Security Target (EAL3+), Version 1.4, May 22 2007

f) Evaluation Technical Report for EAL3+ Evaluation of Deep Security 5.0, Version 0.8, March 20 2008