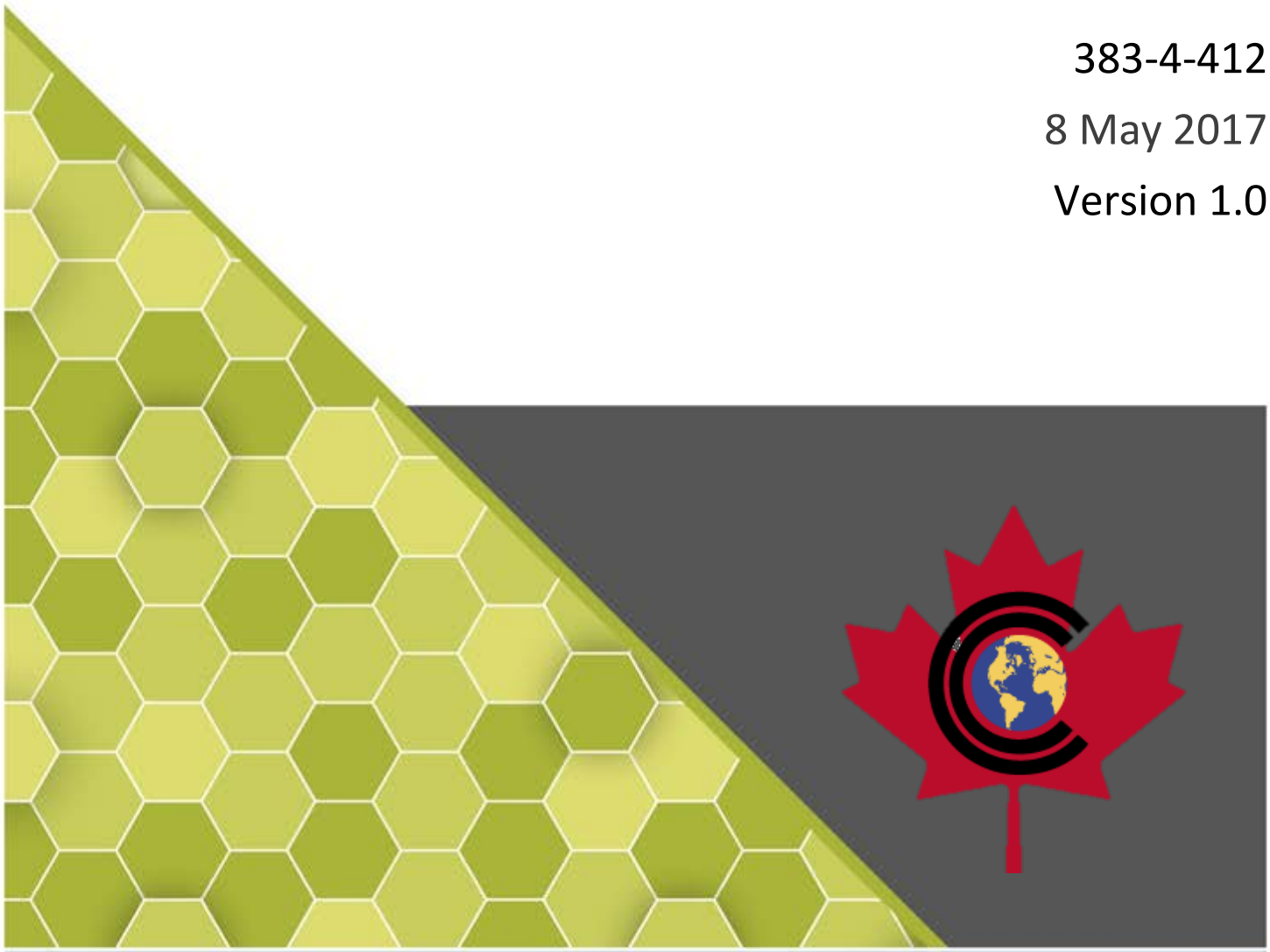
COMMON CRITERIA CERTIFICATION REPORT

BeyondTrust Software, Inc. IT Risk Management Framework v6.0

383-4-412

8 May 2017

Version 1.0



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. 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 Canadian CC Scheme, 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, 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 Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration 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 DXC Security Testing and Certification Laboratories .

By awarding a Common Criteria certificate, the 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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

BeyondTrust Software, Inc. IT Risk Management Framework v6.0 (hereafter referred to as the Target of Evaluation, or TOE), from BeyondTrust Software, Inc., was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a unified hardware and software suite of privileged account management, vulnerability management, and audit management components. The TOE delivers a view of the vulnerabilities that could provide doors into an environment, as well as the privileges that could present corridors to sensitive assets.

DXC Security Testing and Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 08 May 2017 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	BeyondTrust Software, Inc. IT Risk Management Framework v6.0
Developer	BeyondTrust Software, Inc.
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.2 TOE DESCRIPTION

The TOE is a unified hardware and software suite for privileged account management, vulnerability management and auditing. The TOE delivers a view of the vulnerabilities that could provide doors into an environment, as well as the privileges that could present corridors to sensitive assets.

The TOE contains the following components:

- BeyondInsight (BI) which provides a set of tools to help administrators organize assets for scanning;
- PowerBroker for Windows (PBW) which enables administrators to create privileged identity, risk and compliance, event monitoring, and file integrity rules;
- Retina which provides vulnerability testing for multiple platforms and automatic fixes of vulnerabilities;
- PowerBroker Management Suite (PBMS) which includes the following Power Broker Auditor (PBA) modules:
    - PBA for File Systems,
    - PBA for Exchange,
    - PBA for SQL Server, and
    - PBA for Active Directory (AD) including PowerBroker (PB) Recovery for AD.
- UVM50 Security Management Appliance which delivers pre-installed and pre-configured vulnerability and privileged account management capabilities, combining BeyondTrust's Retina and PBW under the BI centralized management, reporting and analytics console.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

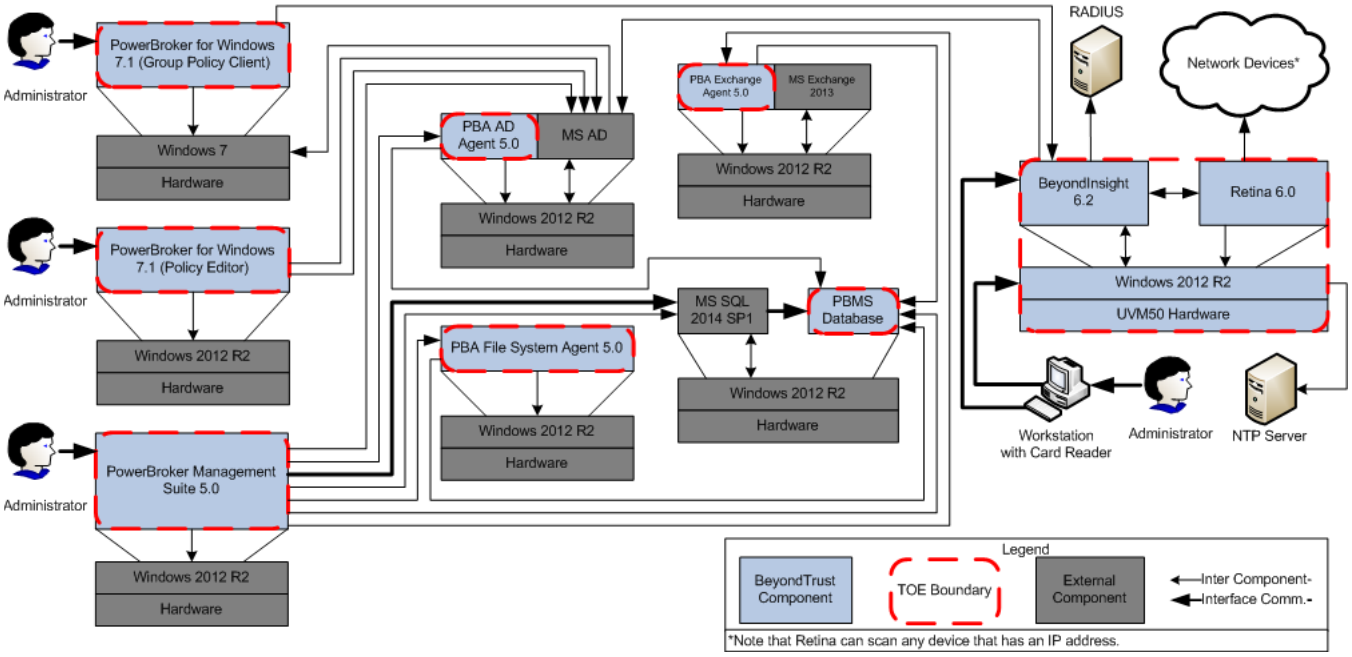


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Scanning and Reporting

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

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

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE environment will provide authentication servers for the identification and authentication of administrators attempting to access the TOE. The TOE environment will also protect communications between the TOE and authentication servers. The authentication servers will support AD, RADIUS and Smart Card authentication.
- The TOE environment will provide secure communications for the PBW, PBA, and PBMS components.
- The TOE is installed on the appropriate hardware, OS, and runtime environment.
- The TOE and all components of the TOE environment (including the authentication servers, database server, Exchange server, and administrator workstations) are located within a controlled access facility and appropriately located within the network to perform their functions.
- There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration, and management of the TOE in a secure and trusted manner.
- The TOE environment will provide the identification and authentication of administrators attempting to manage and use the TOE from the Microsoft Management Console.
- The TOE software will be protected from unauthorized modification.
- The TOE and TOE environment will provide the TOE with the necessary reliable timestamps.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- PowerBroker for Windows Policy Editor v7.1.0.32 running on Windows Server 2012
- PowerBroker for Windows Group Policy client v7.1.0.32 running on Windows 7
- BeyondTrust UVM50 hardware appliance running UVM50 software v2.0.3, Retina v6.0.0.6071 and BeyondInsight v6.2.0.1092
- PowerBroker Management Suite v5.0.138.0 running on Windows Server 2012 R2 using the below modules:
    - PowerBroker Auditor for AD v5.0.138.0
    - PowerBroker Recovery for AD v5.0.138.0
    - PowerBroker Auditor for File System v5.0.138.0
    - PowerBroker Auditor for Exchange v5.0.138.0
    - PowerBroker Auditor for SQL Server v5.0.138.0

An AD server, MS SQL server, MS Exchange Server, Radius Server, and a NTP server are required components in the operational environment.

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. BeyondTrust Software, Inc. IT Risk Management Framework v6.0 Guidance Supplement, Version 0.7
b. BeyondInsight Installation Guide, Revision Number 0, September 2016
c. BeyondInsight User Guide, Revision Number 0, November 2016
d. BeyondInsight Analytics and Reporting User Guide, Revision Number 0, November 2016
e. PowerBroker for Windows Installation Guide, Revision Number 0, August 2016
f. PowerBroker for Windows User Guide, Revision Number 1, August 2016
g. PowerBroker Management Suite Installation Guide, Revision Number 1, September 2016
h. PowerBroker Auditor for SQL Server User Guide, Revision Number 0, July 2016
i. PowerBroker Auditor for Exchange User Guide, Revision Number 0, July 2016
j. PowerBroker Auditor for File System User Guide, Revision Number 1, July 2016
k. PowerBroker Auditor for Active Directory User Guide, Revision Number 2, August 2016
l. PowerBroker Recovery for Active Directory User Guide, Revision Number 0, July 2016
m. UVM Appliance Getting Started Guide, Revision Number 0, July 2016

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the TOE functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the TOE security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.

6 TESTING ACTIVITIES

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

6.1 ASSESSMENT OF 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.

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

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Console User Interface: The objective of this test case is to demonstrate that the TOE can scan a target machine and return the domain name of the target and that a scan will report when a desktop target is not in regulatory compliance, using the HIPAA compliance scan template;

c. Compliance Events: The objective to this test case is to demonstrate that the TOE will identify compliance events in the PBA for Active Directory;

d. PBA for File systems: The objective of this test case is to demonstrate that the TOE will identify system events for deleted/restored files from the recycle bin;

e. Audit: The objective of this test case is to demonstrate that the TOE generates audit records for PBA management and PBA deployment events and for the start up and shut down of audit functions; and

f. Authentication Failure: The objective of this test case is to demonstrate that authentication failure handling can be configured by an authorized administrator of the TOE and that this management function is restricted to the BI administrator.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

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

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST;

b. User Account Harvesting: The evaluator attempted to compromise the security of the TOE by guessing user account names and passwords to determine if user account and/or password errors would provide information which could be exploited;

c. Unauthorized Access: The objective of this test is to determine whether a non-adminstrative user can access the TOE management console; and

d. Secure Communication: The objective of this test is to determine whether TSF data is vulnerable while in transit.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
AD	Active Directory
BI	Beyond Insight
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
NTP	Network Time Protocol
PALCAN	Program for the Accreditation of Laboratories – Canada
PBA	PowerBroker Auditor
PBMS	PowerBroker Management Suite
PBW	PowerBroker for Windows
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

Term	Definition
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
BeyondTrust Software, Inc. IT Risk Management Framework v6.0 Security Target, Version 1.0, May 8, 2017.
Evaluation Technical Report For BeyondTrust Software, Inc. IT Risk Management Framework, v6.0, Version 1.1, May 8, 2017.