Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australalasian Information Security Evaluation Program

Certification Report

Symantec Data Center Security: Server Advanced version 6.7

Version 1.0, 28 May 2019

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Symantec Data Center Security: Server Advanced (Symantec DCS) version 6.7 against Common Criteria EAL2+ALC_FLR.1.

The Target of Evaluation (TOE) is Symantec Data Center Security: Server Advanced (Symantec DCS) version 6.7. The TOE provides a policy-based approach to endpoint security and compliance, as well as delivering agentless malware protection for VMware infrastructures. Its intrusion prevention and intrusion detection features operate across a range of platforms and applications. Data Center Security: Server Advanced features a policy-based host security agent for monitoring and protection, proactive attack prevention using the least privilege containment approach, a policy-based mechanism to secure guest virtual machines against malware attacks and network threats and a centralized management environment for enterprise systems that contain Windows, UNIX and Linux computers.

This report concludes that the TOE has complied to the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP).

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program. The evaluation was performed by BAE Applied Intelligence and was completed on 6 February 2019.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- configure and operate the TOE according to the vendor's product administrator guidance
- Ensure that the TOE's ISO is downloaded from the secure Symantec file transfer platform. Once downloaded, verify that the file downloaded is correct by performing a comparison against the provided MD5 hash and byte count.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [7] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Symantec Data Center Security: Server Advanced (Symantec DCS) version 6.7.

Description	Version
Evaluation scheme	Australasian Information Security Evaluation Program
TOE	Symantec Data Center Security: Server Advanced (Symantec DCS)
Software version	6.7
Security Target	*Symantec™ Data Center Security: Server Advanced Security Target,* *v1.0, dated June 7, 2019*
Evaluation Technical Report	*Evaluation Technical Report v1.0, dated 02 May 2019* Document reference EFS-T048 ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	EAL 2 Augmented with ALC_FLR.1
Developer	Symantec Corporation 350 Ellis Street, Mountain View, CA 94043

	United States of America
Evaluation facility	BAE Applied Intelligence, Level 1, 14 Childers Street, Canberra, ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Symantec Data Center Security: Server Advanced (Symantec DCS) version 6.7.

The TOE provides capabilities to monitor and protect physical and virtual network endpoints and data centres using a combination of host-based intrusion detection, intrusion prevention, least privilege access control, and antivirus and network security policies to secure guest virtual machines against malware attacks and network threats. It uses a policy-based approach to endpoint security and compliance to provide intrusion prevention and intrusion detection capabilities for a range of platforms and applications. The TOE supports:

- policy-based host security agents for protection and monitoring
- proactive attack prevention using the least privilege containment approach
- policy-based agentless malware protection for VMware infrastructures
- a centralised management environment for enterprise systems that contain Windows, UNIX and Linux computers.

TOE Functionality

The TOE functionality that was evaluated is described in section 2.5 of the Security Target [7].

TOE physical boundary

The TOE physical boundary is described in section 2.4 of the Security Target [7].

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [7].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the *New Zealand Information Security Manual* [5].

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [7] contains a summary of the functionality that are evaluated.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per operational guidance documentation [6].

Secure delivery

Software delivery procedures

TOE software is provided to licensed customers via a secure Symantec administered download support site (Flexnet).

The customer is provided a Flexnet username and password information by the Symantec Product Client Management team licensing department.

The download link is secured utilising HTTPS encryption.

Integrity of the download is verified utilising the following two attributes:

- MD5 Hash
- Byte Count

Updates are provided to customers via the Flexnet publishing site.

Product documentation is provided to the users via the Flexnet publishing site.

Customers are informed of available product updates by the Symantec Product Client Management team.

Installation of the TOE

The operational guidance documentation [6] contains all relevant information for the secure configuration of the TOE.

Version verification

Log on to the Management Console. To view the Management Server registration status, go to **Settings > Product Setup** and ensure that the status is configured and the version is 6.7. Further instruction on the verification of version can be obtained in the operational guidance documentation [6].

Documentation and guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased and on the Flexnet publishing site:

- Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 Administrator's Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 Agent Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server, Server Advanced, and Monitoring Edition REST API Reference Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 Detection Policy Reference Guide, Version 2.0, 18/05/2017

- Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 FIPS 140-2 Compliance Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Operations Director Reference Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Overview Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Planning and Deployment Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server Advanced 6.7 Platform and Feature Matrix, Version 4.0, 18/05/2017
- Symantec™ Data Center Security: Server Advanced 6.7 Prevention Policy Reference Guide, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Release Notes, Version 2.0, 18/05/2017
- Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Release Notes, Version 1.0, 18/05/2017
- Symantec™ Data Center Security: Server Advanced 6.7 VMware vSphere Support Guide, Version 2.0, 18/05/2017

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4]. The *New Zealand Information Security Manual* is available at https://www.gcsb.govt.nz/ [5].

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The underlying operating system of each TOE component will protect the component and its configuration from unauthorised access.
- The TOE software critical to security policy enforcement will be protected from unauthorised physical modification.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program [10].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [9].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All Security Functional Requirements listed in the Security Target were exercised during testing.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The developer performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for the exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

BAE Applied Intelligence **has determined** that the TOE upholds the claims made in the Security Target [7] and **has met** the requirements of Common Criteria EAL2+ALC_FLR.1.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australasian Certification Authority **certifies** the evaluation of the Symantec Data Center Security: Server Advanced (Symantec DCS) version 6.7 performed by the Australasian Information Security Evaluation Facility, BAE Applied Intelligence.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4] and New Zealand Government users should consult the *New Zealand Information Security Manual* [5].

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australasian Certification Authority also recommends that users and administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
- configure and operate the TOE according to the vendor's product administrator guidance
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved

- Ensure that the TOE's ISO is downloaded from the secure Symantec file transfer platform. Once downloaded, verify that the file downloaded is correct by performing a comparison against the provided MD5 hash and byte count.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

5. *New Zealand Information Security Manual:* https://www.nzism.gcsb.govt.nz/ism-document/

6. Guidance documentation:

   - *Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 Administrator's Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 Agent Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server, Server Advanced, and Monitoring Edition REST API Reference Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 Detection Policy Reference Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server Advanced and Monitoring Edition 6.7 FIPS 140-2 Compliance Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Operations Director Reference Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Overview Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Planning and Deployment Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server Advanced 6.7 Platform and Feature Matrix, Version 4.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server Advanced 6.7 Prevention Policy Reference Guide, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Release Notes, Version 2.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Release Notes, Version 1.0, 18/05/2017*
   - *Symantec™ Data Center Security: Server Advanced 6.7 VMware vSphere Support Guide, Version 2.0, 18/05/2017*

7. *Symantec™ Data Center Security: Server Advanced Security Target,v1.0, dated June 7, 2019*

8. Evaluation Technical Report - *EFS-T048 ETR v1.0, dated 02 May 2019*

9. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014

10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/publications/aisep-policy-manual

Abbreviations

AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
TOE	Target of Evaluation