Australian Government
Department of Defence

# Australasian Information Security Evaluation Program

## Skybox Security
## Skybox Security Suite Version 9.0.201

**Certification Report**
**2018/117**

**30-08-2018**
**Version 1.0**

# Amendment Record

| Version | Date | Description |
|---|---|---|
| 0.1 | 19 - 07 - 2018 | Internal |
| 1.0 | 30 - 08 - 2018 | Public Release |
|  |  |  |

# Executive Summary

This report describes the findings of the IT security evaluation of Skybox Security Suite against Common Criteria at the level of EAL2.

The TOE is Skybox™ Security Suite 9.0.201, a Security Operations, Analytics and Reporting Solution providing attack surface visualisation and a suite of security analytics solutions for vulnerability, threat and security policy management.

Skybox™ Security provides security professionals with a suite of solutions for security operations, analytics and reporting. Skybox integrates over a hundred networking and security technology organisations, and merges the data into a dynamic network model of an organisation's attack surface, giving comprehensive visibility of public, private and hybrid IT environments. Skybox provides the context needed for informed action, combining attack vector analytics and threat-centric vulnerability intelligence to continuously assess vulnerabilities in the environment and correlate them with exploits in the wild. This makes the accurate prioritisation and mitigation of imminent threats a systematic process, decreasing the attack surface and enabling swift response to exposures that truly put an organization at risk.  Skybox supports both FIPS and non-FIPS modes, and either is allowed in the evaluated configuration.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- Network data collection and discovery—Skybox Security Suite collects information about all the elements comprising the network: security control devices such as firewalls, IPS, and VPNs; network infrastructure devices such as routers, switches and load balancers; and network assets such as servers and workstations.
- Modelling—Skybox Security Suite uses the information gathered through the data collection and discovery process to create a normalised model of the network that supports attack surface visualisation.
- Analysis—Skybox Security Suite uses the network model to perform and support a range of analyses, including: firewall rule and configuration checks; access path analysis; and firewall rule optimisation.
- Compliance monitoring—Skybox Security Suite is able to perform audits of the network and monitor the compliance of the network and its elements to various published standards, including: PCI; FISMA; and NIST.

The report concludes the TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5, April 2017.
    - Part 2 Extended

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017.
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2 Augmented (ALC_FLR.1).

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Applied Intelligence and was completed on 6 July 2018.

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

b) Configure and Operate the TOE according to the vendor's product administrator guidance

c) 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 and

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.

# Contents

# Chapter 1 – Introduction

## 1.1 Overview

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

## 1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria (CC).

b) 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.

## 1.3 Identification

The TOE is Skybox Security Suite 9.0.201.

**Table 1 Identification Information**

| Description | Version |
|---|---|
| Evaluation Scheme | Australasian Information Security Evaluation Program. |
| TOE | Skybox Security Suite |
| Software Version | 9.0.201 |
| Hardware Platforms | - |
| Security Target | Security Target Skybox Security Skybox Security Suite, version 1.0, dated 20-08-2018 |
| Evaluation Technical Report | Evaluation Technical Report, version 1.0, dated 21-August-18,<br>Document reference EFS-T053-ETR |

| | |
|---|---|
| Criteria | Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1.Rev3 |
| Methodology | Common Methodology for Information Technology Security,  April 2017 Version 3.1 Rev 5 |
| Conformance | No Protection Profile Conformance Claimed |
| Developer | Skybox Security, Inc<br>2077 Gateway Pl #200<br>San Jose CA 95110 United States |
| Evaluation Facility | BAE Applied Intelligence<br>Level 1<br>14 Childers Street<br>2600 |

# Chapter 2 – Target of Evaluation

## 2.1 Overview

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

## 2.2 Description of the TOE

The TOE is Skybox™ Security Suite 9.0.201, a Security Operations, Analytics and Reporting Solution providing attack surface visualisation and a suite of security analytics solutions for vulnerability, threat and security policy management.

Skybox™ Security provides security professionals with a suite of solutions for security operations, analytics and reporting. Skybox integrates over a hundred networking and security technology organisations, and merges the data into a dynamic network model of an organisation's attack surface, giving comprehensive visibility of public, private and hybrid IT environments. Skybox provides the context needed for informed action, combining attack vector analytics and threat-centric vulnerability intelligence to continuously assess vulnerabilities in the environment and correlate them with exploits in the wild. This makes the accurate prioritisation and mitigation of imminent threats a systematic process, decreasing the attack surface and enabling swift response to exposures that truly put an organization at risk.  Skybox supports both FIPS and non-FIPS modes, and either is allowed in the evaluated configuration.

## 2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- Network data collection and discovery—Skybox Security Suite collects information about all the elements comprising the network: security control devices such as firewalls, IPS, and VPNs; network infrastructure devices such as routers, switches and load balancers; and network assets such as servers and workstations.
- Modelling—Skybox Security Suite uses the information gathered through the data collection and discovery process to create a normalized model of the network that supports attack surface visualisation.
- Analysis—Skybox Security Suite uses the network model to perform and support a range of analyses, including: firewall rule and configuration checks; access path analysis; and firewall rule optimisation.
- Compliance monitoring—Skybox Security Suite is able to perform audits of the network and monitor the compliance of the network and its elements to various published standards, including: PCI; FISMA; and NIST.

## 2.4 TOE Architecture

The Skybox Security Suite comprises three main components:

- Skybox Server—the core component of the product, providing most of the functionality to support network data collection, modelling, analysis and compliance monitoring. It is built on J2EE and incorporates a MySQL database and InetSoft reporting engine. InetSoft's software is based on open standards technology that incorporates XML, SOAP, Java language, and JavaScript.
- Skybox Manager—the client component of Skybox, which provides a Graphical User Interface (GUI) to manage and use the capabilities of the Skybox Security Suite. Each of the Skybox components has its own client. Four components (Firewall Assurance, Network Assurance, Vulnerability Control, and Threat Manager) use a thick client implemented in Java Swing, while Change Manager and Horizon use a browser-based web client.
- Skybox Collector—the Collector is similar to the Server component, without the MySQL database. Multiple Collectors can be installed throughout the network to support network data collection and discovery.

## 2.5 Clarification of Scope

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

The evaluated configuration is based on default installation of the TOE with additional configuration taken from the Operational User Guidance documents [6].

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

### 2.5.1 Evaluated Functionality

The evaluators have examined the provided developer test documentation and found that it shows the correspondence between the tests present in the test documentation and the TSFIs identified within the functional specification.

The evaluators examined the TOE prior to testing and determined that the test configuration was consistent with the configuration under evaluation as specified in the ST. The evaluators followed the user installation and configuration guidance to ensure that the TOE had been installed correctly and was in a known state prior to conducting testing.

The evaluators performed all tests adapted from the developer test plan.

## 2.6 Security

### 2.6.1 Security Policy

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

## 2.7 Usage

### 2.7.1 Evaluated Configuration

The evaluated configuration is based on default installation of the TOE with additional configuration taken from the Operational User Guidance documents [6].

### 2.7.2 Secure Delivery

This section outlines the delivery process and steps required for secure acceptance of the TOE. The administrator should check the version of the TOE and the integrity of the delivered materiel in accordance with the guidance provided by the developer [6], which are reproduced below.
The verification of the TOE was undertaken by following the instructions in the provided guidance material to check the version of the TOE components.

Inspect the shipping carton to ensure that the packaging has not been damaged, and verify that all tamper evident seals are intact. Verify that the appliance serial number, purchase order number, and FedEx tracking number match the information provided by Skybox Customer Support.

### 2.7.3 Installation of the TOE

The Guidance Documentation [6] contains all relevant information for the secure configuration of the TOE.

## 2.8 Version Verification

The Guidance Documentation [6] contains all relevant information for validation of the TOE software version.

## 2.9 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. All guidance material is available for download at **www.skyboxsecurity.com.**

- Skybox Installation and Administration Guide 9.0.200 Revision: 11, 2018
- Skybox Reference Guide 9.0.200 Revision: 11, 2018
- Skybox Virtual Appliance VMware Quick Start Guide 9.0.200, Revision: 11, 2018
- Skybox Appliance 7000 Quick Start Guide 9.0.200, Revision: 11, 2018
- Skybox Appliance 8000 Quick Start Guide 9.0.200, Revision: 11, 2018
- Skybox Change Manager User's Guide 9.0.200 Revision: 11, 2018
- Skybox Horizon User's Guide 9.0.200 Revision: 11, 2018
- Skybox Change Manager Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Change Manager Help 9.0.200 Revision: 11, 2018
- Skybox Threat Manager Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Threat Manager User's Guide 9.0.200 Revision: 11, 2018
- Skybox Firewall Assurance Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Firewall Assurance User's Guide 9.0.200 Revision: 11, 2018
- Skybox Network Assurance Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Network Assurance User's Guide 9.0.200 Revision: 11, 2018
- Skybox Vulnerability Control User's Guide 9.0.200 Revision: 11, 2018
- Skybox Vulnerability Control Getting Started Guide 9.0.200 Revision: 11, 2018

All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au [4]**. The NZISM is available at **www.gcsb.govt.nz** [5].

## 2.10 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 software component will protect the component and its configuration from unauthorized access.

- The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

# Chapter 3 – Evaluation

## 3.1 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.

## 3.2 Evaluation Procedures

The evaluation was conducted in accordance with the Common Criteria and associated methodology, [1], [2], [3] and [4].

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

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

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.

## 3.3 Functional Testing

### 3.3.1 Testing Coverage

To gain confidence that the developers 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: 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. The testing provides a full coverage of all security functions claimed by the TOE.

## 3.5 Penetration Testing

The evaluators’ penetration tests are based on an independent vulnerability analysis of the TOE using the guidance documentation and available public information. The evaluators used these tests to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. 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 exploitation.

The developers search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables.

# Chapter 4 – Certification

## 4.1 Overview

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

## 4.2 Assurance

This certification is focused on the evaluation of product compliance with EAL 2. Agencies can have confidence that the scope of an evaluation against an EAL 2 covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

EAL2 provide assurance by a full security target and an analysis of the SFR in that ST, 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 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. Compliance also provides assurance through evidence of secure delivery procedures.

## 4.3 Certification Result

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 (ACA) **certifies** the evaluation of the Skybox™ Security Suite 9.0.201 performed by the Australasian Information Security Evaluation Facility, BAE Applied Intelligence.

BAE Applied Intelligence **has determined** that the TOE upholds the claims made in the Security Target [7] to the assurance level EAL2 augmented with ALC_FLR.1.

Certification is not a guarantee of freedom from security vulnerabilities.

## 4.4 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 ISM [4] and New Zealand Government users should consult the GCSB NZISM [5].

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

b) Configure and operate the TOE according to the vendor's product administrator guidance

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.

d) The evaluators also recommend that the administrator verify the integrity of downloaded software, as present on the **www.skyboxsecurity.com** website.

# Annex A – References and Abbreviations

## A.1 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 2107, Version 3.1, Revision 5

4. 2017 Australian Government Information Security Manual (ISM), Australian Signals Directorate

5. NZ Information Security Manual (NZISM): https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

6. Guidance Documentation:

    - Skybox Installation and Administration Guide 9.0.200 Revision: 11, 2018
    - Skybox Reference Guide 9.0.200 Revision: 11, 2018
    - Skybox Virtual Appliance VMware Quick Start Guide 9.0.200, Revision: 11, 2018
    - Skybox Appliance 7000 Quick Start Guide 9.0.200, Revision: 11, 2018
    - Skybox Appliance 8000 Quick Start Guide 9.0.200, Revision: 11, 2018
    - Skybox Change Manager User's Guide 9.0.200 Revision: 11, 2018
    - Skybox Horizon User's Guide 9.0.200 Revision: 11, 2018
    - Skybox Change Manager Getting Started Guide 9.0.200 Revision: 11, 2018
    - Skybox Change Manager Help 9.0.200 Revision: 11, 2018
    - Skybox Threat Manager Getting Started Guide 9.0.200 Revision: 11, 2018
    - Skybox Threat Manager User's Guide 9.0.200 Revision: 11, 2018

- Skybox Firewall Assurance Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Firewall Assurance User's Guide 9.0.200 Revision: 11, 2018
- Skybox Network Assurance Getting Started Guide 9.0.200 Revision: 11, 2018
- Skybox Network Assurance User's Guide 9.0.200 Revision: 11, 2018
- Skybox Vulnerability Control User's Guide 9.0.200 Revision: 11, 2018
- Skybox Vulnerability Control Getting Started Guide 9.0.200 Revision: 11, 2018

7. Security Target Skybox Security Suite 9.0.201, Version 1.0, 20-August-2018

8. Evaluation Technical Report, Skybox Security Suite 9.0.201, Version 1.0, 21-August-2018

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

## A.2 Abbreviations

| | |
|---|---|
| ACA | Australasian Certification Authority |
| AISEF | Australasian Information Security Evaluation Facility |
| AISEP | Australasian Information Security Evaluation Program |
| ASD | Australian Signals Directorate |
| CA | Certification Authority |
| CC | Common Criteria |
| CEM | Common Evaluation Methodology |
| ETR | Evaluation Technical Report |
| FTP | File Transfer Protocol |
| GCSB | Government Communications Security Bureau |
| NTP | Network Time Protocol |
| PP | Protection Profile |
| SFP | Security Function Policy |
| SFR | Security Functional Requirements |
| SNMP | Secure Network Management Protocol |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |