



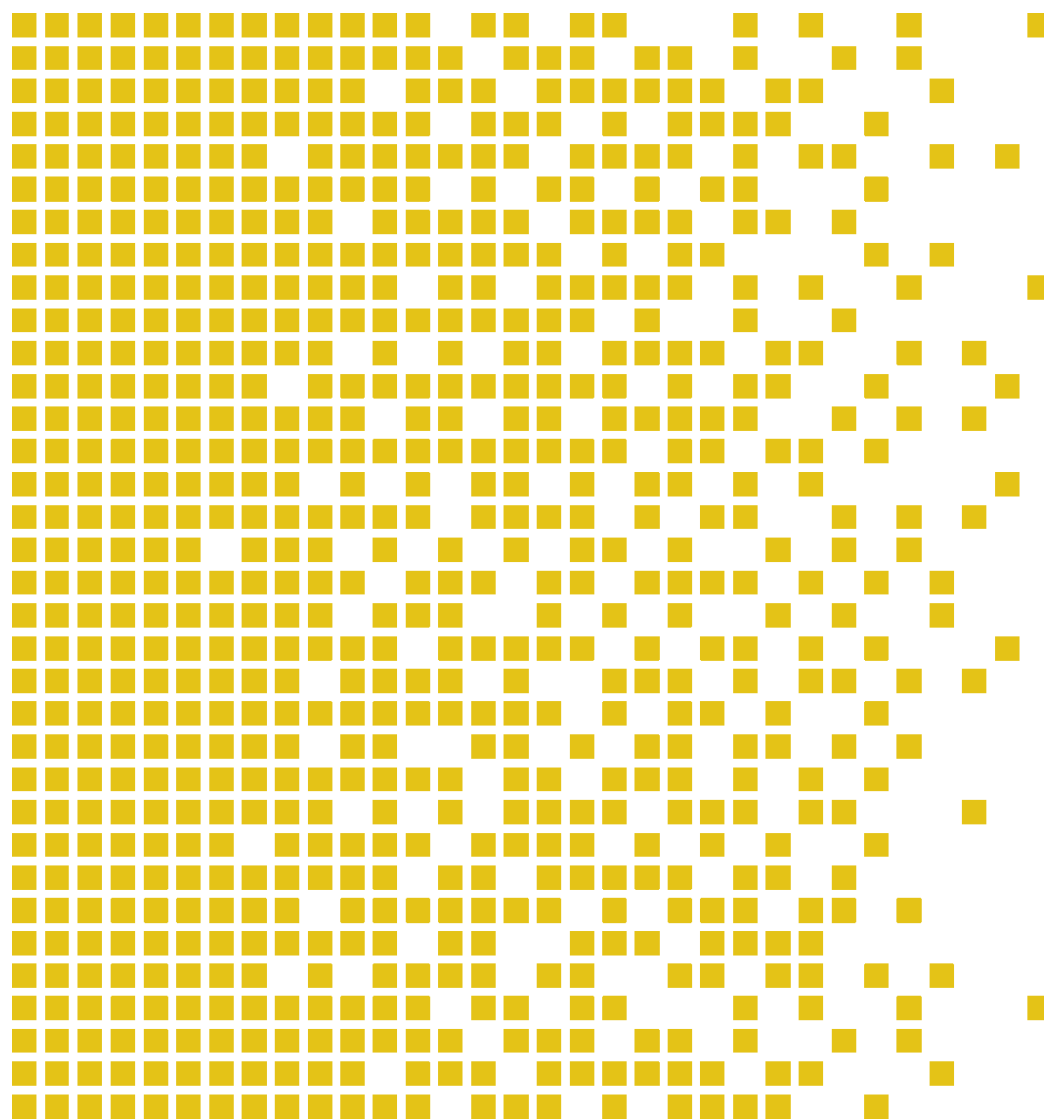
**SERTIT**

Sertifiseringsmyndigheten for IT-sikkerhet Norwegian Certification Authority for IT Security

# SERTIT-084 CR Certification Report

Issue 1.0 13 February 2017

Attivo BOTsink Solution



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011



**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN  
THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA July 2<sup>nd</sup> 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC\_FLR CC part 3 components.





## Contents

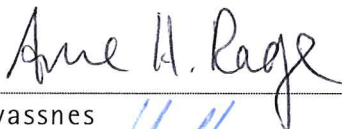


<b>1</b>	<b>Certification Statement</b>	<b>4</b>
<b>2</b>	<b>Abbreviations</b>	<b>5</b>
<b>3</b>	<b>References</b>	<b>6</b>
<b>4</b>	<b>Executive Summary</b>	<b>7</b>
4.1	Introduction	7
4.2	Evaluated Product	7
4.3	TOE scope	7
4.4	Protection Profile Conformance	7
4.5	Assurance Level	8
4.6	Security Policy	8
4.7	Security Claims	8
4.8	Threats Countered	8
4.9	Threats Countered by the TOE's environment	8
4.10	Threats and Attacks not Countered	8
4.11	Environmental Assumptions and Dependencies	8
4.12	IT Security Objectives	8
4.13	Non-IT Security Objectives	8
4.14	Security Functional Requirements	9
4.15	Evaluation Conduct	10
4.16	General Points	10
<b>5</b>	<b>Evaluation Findings</b>	<b>11</b>
5.1	Introduction	12
5.2	Delivery	12
5.3	Installation and Guidance Documentation	12
5.4	Misuse	12
5.5	Vulnerability Analysis	12
5.6	Developer's Tests	13
5.7	Evaluators' Tests	13
<b>6</b>	<b>Evaluation Outcome</b>	<b>14</b>
6.1	Certification Result	14
6.2	Recommendations	14
	<b>Annex A: Evaluated Configuration</b>	<b>15</b>
	TOE Identification	15
	TOE Documentation	15
	TOE Configuration	16



## 1 Certification Statement

Attivo BOTsink Solution intends to close security infrastructure gaps. Attivo BOTsink is an advanced decoy and deception solution, which detects network breaches and can stop threats that have bypassed prevention security systems from further propagation in the network. Additionally, this solution can be configured for analyzing suspect content submitted by users and partner security devices. Both virtualized and physical instances of Attivo BOTsink are available. This means that the Attivo BOTsink Solution can be deployed in networks, datacenters and on the cloud.

Attivo BOTsink Solution (For version, See chapter 4.2) has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC\_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality.

Author	Arne Høye Rage Certifier 
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance 
Approved	Kristian Bae Head of SERTIT 
Date approved	13 February 2017



## 2 Abbreviations

APT	Advanced Persistent Threat
BOT	Software application that runs automated tasks (scripts) over the Internet.
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
OSP	Organisational Security Policy
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy



### 3 References

- [1] Attivo BOTsink Solution Security Target Version: 1.3, February 3 2017.
- [2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.
- [3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.
- [4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.
- [5] The Norwegian Certification Scheme, SD001E, Version 9.0, 20 April 2013.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.
- [7] ICAO. Doc 9303 - Machine Readable Travel Documents, version 6, 2006
- [8] ETR for the evaluation project SERTIT-084 Common Criteria EAL2 Augmented with ALC\_FLR.1 Evaluation of Attivo BOTsink Solution A-ATTIVO-1-SOL-ETR-1.1, February 6 2017.
- [9] Attivo Lifecycle Documentation, Version 1.0



## 4 Executive Summary

### 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Attivo BOTsink Solution (For version See chapter 4.2) to the Sponsor, Attivo Networks, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

### 4.2 Evaluated Product

The version of the product evaluated was Attivo BOTsink Solution including

- BOTsink appliances:
  - Model 3200
  - Model 5100
- vBOTsink for Vmware Version 3.3
- ACM appliance Version 200
- Software – ACM Version 3.3
- Software – BOTsink and Endpoint Version 3.3.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Attivo Networks, Inc.

The BOTsink solution consists of a network of self-sustaining virtual machines running on various operating systems. A set of configurable network services run on these virtual machines. The user can deploy these virtual machines on the required subnets.

BOTsink lures BOTs and APTs scanning for valuable corporate assets to target its virtual machines. Thus, Attivo BOTsink leaves a wide footprint across the enterprise to detect, engage, and defend against BOTs and APTs.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

### 4.3 TOE scope

The TOE scope is described in the Security Target[1], chapter 1.

### 4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.



#### **4.5 Assurance Level**

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 2 augmented with ALC\_FLR.1. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

#### **4.6 Security Policy**

The TOE security policies are detailed in ST[1] section 3.

#### **4.7 Security Claims**

The Security Target[1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet and security functional requirements and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[3] except one extended component described in the Security Target[1] section 5.1. Use of this standard facilitates comparison with other evaluated products.

#### **4.8 Threats Countered**

All threats that are countered are described in the Security Target[1], section 3.1.3.1

#### **4.9 Threats Countered by the TOE's environment**

Threats that are covered by the TOE's environment are identified in the Security Target[1], section 3.1.3.2

#### **4.10 Threats and Attacks not Countered**

No threats or attacks are described that are not countered

#### **4.11 Environmental Assumptions and Dependencies**

The assumptions that apply to this TOE are described in the Security Target[1], section 3.3

#### **4.12 IT Security Objectives**

The security objectives that apply to this TOE are described in the Security Target[1], section 4.1

#### **4.13 Non-IT Security Objectives**

The security objectives that apply to this TOE's operational environment are described in the Security Target[1], section 4.2



#### 4.14 Security Functional Requirements

The SFRs that apply to this TOE are described in the Security Target[1], section 6.1

Functional Class	Functional Component	
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
FIA: Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
FMT: Security management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on security roles
FPT: Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PHP.1	Passive detection of physical attack
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
FRU: Resource utilisation	FRU_RSA_EXT.1	Maximum quotas
FTA: TOE access	FTA_SSL.3	TSF-initiated termination

Functional Class	Functional Component	
	FTA_TAB.1	Default TOE access banners
FTP: Trusted path/channels	FTP_TRP.1	Trusted path

#### 4.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Advanced Data Security. The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[8]. to SERTIT on 6 February 2017. SERTIT then produced this Certification Report.

#### 4.16 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.



## 5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC part 3[4]. These classes comprise the EAL2 assurance package augmented with ACL\_FLR.1

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Basic Flaw Remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.



## 5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR [8] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

## 5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery procedure is described in the Lifecycle Documentation [9].

## 5.3 Installation and Guidance Documentation

Installation procedures are described in detail in supporting documents listed in Annex A.

## 5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Users shall follow the guidance documentation listed in Annex A for the TOE in order to ensure that the TOE is operated in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

## 5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluators have conducted a search of ST, guidance documentation, functional specification, TOE design and security architecture description evidence to identify possible potential vulnerabilities in the TOE.

For each binary that is present in the TOE the evaluators have performed a vulnerability search using publicly available vulnerability database.

Upon completing penetration tests based on independent vulnerability analysis, the evaluator's overall conclusion is that the TOE is resistant to attackers possessing Basic attack potential, per requirements of EAL2.



## 5.6 Developer's Tests

The vendor's tests concentrate on critical functionality of the TOE. The test results were integrated into the description of the tests, or provided separately.

The TOE configuration that was used by the vendor was consistent with the test configurations that are described in the ST.

The developer's test documentation includes test plans, expected results, and actual results. The test coverage evidence shows that the correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification is accurate.

## 5.7 Evaluators' Tests

The evaluators have tested a subset of the developer's tests selected using a random sampling method and a method based on an intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. The evaluators took into consideration the potential security impact of the tests, as well as the number of subsystems that contribute to successful completion of the tests. The subset covers about 1/3 of the developer's tests.

The evaluators have also developed and performed a number of independent testing. The tests cover the TSFI, Security Functions, and subsystems to the maximum extent possible. It is also taken into consideration the potential security impact of the tests, as well as the number of subsystems that contribute to successful completion of the tests.

To devise a test subset, the evaluators used augmentation of developer testing for interfaces and supplementation of developer testing strategy for interfaces.

The independent tests concentrated on critical functionality of the TOE.



## **6 Evaluation Outcome**

### **6.1 Certification Result**

After due consideration of the ETR[8], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Attivo BOTsink Solution (For version See chapter 4.2) meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC\_FLR.1 for the specified Common Criteria Part 2 extended functionality, in the specified environment described in the Security target[1].

### **6.2 Recommendations**

Prospective consumers of Attivo BOTsink Solution (For version See chapter 4.2) should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

These guidance documents include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

## Annex A: Evaluated Configuration

### TOE Identification

The version of the product evaluated was Attivo BOTsink Solution including

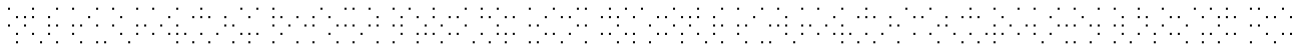
- BOTsink appliances:
  - Model 3200
  - Model 5100
- vBOTsink for Vmware Version 3.3
- ACM appliance Version 200
- Software – ACM Version 3.3

Software – BOTsink and Endpoint Version 3.3

### TOE Documentation

The supporting guidance documents evaluated were:

1. Attivo BOTsink Solution Security Target, Version: 1.3
2. Attivo Guidance Documentation, v. 1.5
3. Administrator Guide for FIPS and Common Criteria Certification, v. 1.0
4. Attivo BOTsink® Software version 3.1.1, Deployment Scenarios Guide Revision A
5. Attivo BOTsink® Software version 3.1.1, Installation Guide for VMware Revision A
6. Attivo BOTsink® Software version 3.3.3, IRES Cheat Sheet Revision A
7. Attivo BOTsink® Software version 3.3.3, Central Manager User Guide Revision A
8. Attivo BOTsink® Software version 3.3.3, User Guide Revision D
9. Attivo vBOTsink-AWS Software version 3.2.1, User Guide Revision A
10. Attivo vBOTsink-VMware Requirement details
11. ACM Alerts Design Document, v.0.3
12. ACM Integrated Help document
13. BOTsink Integrated Help document
14. VMware Integrated Help document



### TOE Configuration

The following configuration, consistent with the ST, was used for testing:

