National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

ForeScout CounterACT

Report Number: CCEVS-VR-VID10728-2018
Version 1.0
April 2, 2018

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Marybeth Panock
Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
David Cornwell
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Annapolis Junction, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of ForeScout CounterACT provided by ForeScout Technologies, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in March 2018. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen and as summarized in the available Assurance Activities Report (AAR) for the ForeScout CounterACT. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device collaborative Protection Profile, version 1.0 (NDcPP).

The Target of Evaluation (TOE) is the ForeScout CounterACT that runs the CounterACT software version 7.0. CounterACT's primary functionality is a network device that enables network access control, threat protection, and compliance of the entire enterprise based on network security policies. The TOE type is justified because the TOE provides an infrastructure role in internetworking of different network environments across an enterprise. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *ForeScout CounterACT Security Target v1.0*, dated February 14, 2018 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	ForeScout CounterACT that runs the CounterACT software version 7.0. Refer to Table 2 for Model Specifications
Protection Profile	Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	ForeScout CounterACT Security Target v1.0, dated February 14, 2018
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "ForeScout CounterACT" Evaluation Technical Report v1.0 dated February 23, 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	ForeScout Technologies, Inc.
Developer	ForeScout Technologies, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Marybeth Panock, The Aerospace Corporation Kenneth Stutterheim, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain administrator access to the TOE's management functionality through nefarious means such as replay, impersonation, or man-in-the-middle attacks.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak keys or cryptographic algorithms to gain unauthorized access to protected data at rest or in transit.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may exploit unencrypted communications channels to access sensitive data or manipulate data in transit.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols to access a remote endpoint used by the TOE using shared, static, plaintext, or default credentials.
- **T.UPDATE_COMPROMISE –** Threat agents may exploit an unpatched system or provide a malicious update to the TOE in order to cause a known failure.
- **T.UNDETECTED_ACTIVITY** – A malicious administrator may perform improper activities on the TOE and have the ability to prevent audit records of the activity from being generated or to remove all traces of their activities.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** A self-protection mechanism of the TOE may fail or be improperly implemented, allowing a threat agent to access functions or data that were meant to be protected.
- **T.PASSWORD_CRACKING –** A weak administrator password may allow a malicious actor to access administrative functionality through password guessing or brute force exhaustion.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** A component of the TOE responsible for implementing security functionality may fail without administrator awareness.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 1.1, 27 February 2015, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. The network access control, threat protection, and compliance of the entire enterprise based on network security policies functionality included in the product and described in Section 1.4 of the Security Target was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated configuration of the TOE is the ForeScout CounterACT described in Table 2 running the CounterACT software version 7.0. In the evaluated configuration, the TOE uses TLS to secure remote GUI-based administration, SSH to secure remote command-line administration, and TLS to secure transmissions of security-relevant data from the TOE to external entities such as authentication server and syslog. The TOE includes administrative guidance to instruct Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

ForeScout CounterACT is a network device as defined in the NDcPP which states: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network… Examples of network devices that are covered by requirements in this cPP include routers, firewalls, VPN gateways, IDSs, and switches". The TOE consists of the ForeScout CounterACT that runs the CounterACT software version 7.0. Thus, the TOE is a network device composed of hardware and software.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
ForeScout CounterACT: Appliance (CT-) & Enterprise Manager (CEM-)	ForeScout CounterACT v7.0 operating on CentOS 6.6	CT-Remote	1U Desktop
			2 USB 2.0
			1 CPU Intel Celeron
			4x Intel-based 10/100/1000 NIC Ports
		CT-100	1U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			1 CPU Intel Xeon E5
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-1000; CEM-05, and CEM-10	1U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			1 CPU Intel Xeon E5
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-2000; CEM-25, and CEM-50	2U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			1 CPU Intel Xeon E5
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-4000; and CEM-100	2U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			2 CPU Intel Xeon E5

System Name		Equipment	
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-10000; and CEM-150, CEM-200	2U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			2 CPU Intel Xeon E5
			4 (up to 8)x Intel-based NIC Ethernet Ports

Table 2 – Hardware Specifications

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Component	Definition
Active Directory Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory. In the evaluated configuration, the TOE connects to a server with Active Directory for its remote authentication store.
Management Workstation	Any general-purpose computer that is used by a Security Administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or the CounterACT Console to access the remote GUI.
Syslog Server	The TOE connects to a Syslog Server to send Syslog messages for remote storage via TLS connection where the TOE is the TLS client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Update Server	A general-purpose computer controlled by the vendor that includes a web server and is used to store software update packages that can be retrieved by product customers using HTTPS/TLS enabled browser or Console. The host of the CounterACT Console provides the secure channel and not the TOE. The TOE does not directly communicate with the update server. The TOE receives the update from the CounterACT Console.
Certificate Authority (CA) Server/Online Certificate Status Protocol (OCSP) Responder	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.
Network Infrastructure	The network infrastructure contains components such as routers, switches, DNS server, etc.

Table 3 – IT Environment Components

5 Security Policy

5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. The audit logs are stored in an internal database on the TOE's local hard drive. An authorized administrator has the ability to enable/disable the forwarding of events to a syslog server. When enabled, the audit data is also securely transmitted to the syslog server using a TLS v1.1 or 1.2 communication channel.

5.2 Cryptographic Support

The TOE provides cryptography in support of SSH, and TLS (v1.1 and 1.2) trusted communications. RSA key generation is implemented in accordance with FIPS 186-4 and RSA key establishment is implemented in accordance with NIST SP 800-56B. Diffie-Hellman group 14 (FFC) key generation is implemented in accordance with RFC 3526, Section 3 and Diffie-Hellman group 14 key establishment is implemented in accordance with RFC 3526, Section 3. Keys are destroyed when no longer used. AES, SHA, HMAC, RSA are all used by the TOE for encryption, hashing, message authentication and digital signatures, respectively. The TOE uses a hash DRBG to provide the random bit generation services with 256 bits of entropy. The cryptographic implementation has been validated to ensure that the algorithms are appropriately strong for use in trusted communications.

The following tables contain the CAVP algorithm certificates for the two cryptographic modules implemented in the TOE:

SFR	Algorithm/Protocol	OpenSSL CAVP Cert #
FCS_CKM.1	RSA FIPS 186-4 Key Generation	#1584
FCS_CKM.2	RSA Key Establishment SP 800-56B	Vendor affirmed
FCS_COP.1(1)	AES, CBC Mode, 128, 192, and 256 bits	#3113
FCS_COP.1(2)	RSA FIPS 186-4 Signature Generation and Signature Verification	#1584
FCS_COP.1(3)	SHS: SHA-1, SHA-256, SHA-512	#2569
FCS_COP.1(4)	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512	#1950
FCS_RBG_EXT.1	DRBG	#625

Table 4: Cryptographic Algorithm Table for OpenSSL

SFR	Algorithm/Protocol	Bouncy Castle CAVP Cert #	ForeScout CAVP Cert #
FCS_CKM.1	RSA FIPS 186-4 Key Generation	#1932	#2551
FCS_CKM.2	RSA Key Establishment SP 800-56B	Vendor Affirmed	Vendor Affirmed
FCS_COP.1(1)	AES, CBC Mode, 128, 192, and 256 bits	#3756	#4671
FCS_COP.1(2)	RSA FIPS 186-4 Signature Generation and Signature Verification	#1932	#2551
FCS_COP.1(3)	SHS: SHA-1, SHA-256	#3126	#3827
FCS_COP.1(4)	HMAC-SHA-1, HMAC-SHA-256	#2458	#3094
FCS_RBG_EXT.1	DRBG	#1031	#1580

Table 5: Cryptographic Algorithm Table for Bouncy Castle

OE Component	Definition of Communication (protocol, client/server, crypto module)
Management Workstation	Communications are secured using TLS where the TOE is the Server. TOE crypto required to support interfaces 3 as defined in Figure 1 above. Crypto Module: Bouncy Castle
	Communications are secured using SSH where the TOE is the Server TOE crypto required to support interfaces 2 as defined in Figure 1 above. Crypto Module: OpenSSL
Active Directory Server	Communications are secured using TLS where the TOE is the client. TOE crypto required to support interface 6 as defined in Figure 1 above. Crypto Module: OpenSSL
Syslog Server	Communications are secured using TLS where the TOE is the client. TOE crypto required to support interface 7 as defined in Figure 1 above. Crypto Module: OpenSSL

Table 6: Identification of Crypto Module Supporting Secured Communication Channel

5.3 Identification and Authentication

The TOE provides local password authentication as well as providing the ability to securely connect to an Active Directory server for the authentication of users. Communications over this interface is secured using TLS in which the TOE is acting as a client. The TOE enforces X.509 certificates to support authentication for TLS connections. The only available function available to an unauthenticated user is the ability to acknowledge a warning banner.

5.4 Security Management

The TOE can be administered locally and remotely and uses role based access control to prevent unauthorized management. The TOE enforces role based access control (RBAC) to prevent/allow access to TSF data and functionality. The NDcPP scopes the management capabilities to: manually download an update, manually initiate an update which verifies the digital signature before installation, configure inactivity time, and configuring the access banner.
A pre-defined set of permissions is called a role. The TOE has one pre-defined role: “Admin”. The user permissions for the “Admin” role cannot be modified or customized. A user assigned the “Admin” role is the TOE administrator (Security Administrator) and has access to all Console tools and features. All other users that do not have the full set of administrative permissions are categorized as a “Console User”. A Console User’s set of permissions are set during creation and can be customized by adding and subtracting specific permissions to allow/disallow the user TOE functionality.

5.5 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. Passwords are not stored in plaintext. The cryptographic module prevents the unauthorized disclosure of cryptographic data. The TOE does not support automatic updates. An administrator has the ability to query the TOE for the currently executing version the TOE software and is required to manually initiate the update process from the Console. The TOE automatically verifies the digital signature of the software update prior to installation. If the digital signature is found to be invalid for any reason the update is not installed. If the signature is deemed invalid, the administrator will be provided a warning banner and allow an administrator to continue with the installation or abort. There is no means for an administrative override to continue the installation if the signature is completely missing. The TOE implements a self-testing mechanism that is automatically executed during the initial start-up and can be manually

initiated by an administrator after authentication, to verify the correct operation of product and cryptographic modules. The TOE provides its own time via its internal clock.

5.6 TOE Access

The TOE displays a configurable warning banner prior to its use. Inactive sessions will be terminated after an administrator-configurable time period. Users are allowed to terminate their own interactive session. Once a remote session has been terminated the TOE requires the user to re-authenticate to establish a new session. Local and remote sessions are terminated after the administrator configured inactivity time limit is reached.

5.7 Trusted Path/Channels

Users can access a CLI for administration functions remotely via SSH (remote console) or a local physical connection (local console) to the TOE. The TOE provides the SSH server functionality. The main administrator interface is the Console which is running on a separate Windows PC. The Console initiates a TLS connection to the TOE appliance, which is acting as a TLS server, for this connection.

The TOE acts as a TLS client to initiate the following secure paths to:

- User Authentication (Active Directory)
- Auditing (Syslog)

The TOE acts as a TLS server and receives requests to establish the following secure paths from:

- CounterACT Console

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- ForeScout CounterACT Supplemental Administrative Guidance for Common Criteria version 1.0, February 16, 2018
- CounterACT® Installation Guide Version 7.0.0
- CounterACT® Console User Manual Version 7.0.0
- CounterACT® Certificate Interface Configuration Guide Version 1.0.0
- CounterACT® Syslog Plugin Configuration Guide Version 3.3.0 and Above
- CounterACT™ User Directory Plugin Configuration Guide Version 6.1.0 and Above

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is ForeScout CounterACT that runs the CounterACT software version 7.0. Section 4 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to directly communicate with the following environment components:

- Management Workstation for local and remote administration
- Active Directory Server for remote authentication
- Syslog Server for recording of syslog data
- Certificate Authority/Online Certificate Status Protocol (OCSP) Responder
- Network infrastructure containing components such as routers, switches, DNS server, etc.

To use the product in the evaluated configuration, the product must be configured as specified in the *ForeScout CounterACT Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Evaluation Technical Report for a Target of Evaluation "ForeScout CounterACT" Evaluation Technical Report v1.0 dated February 23, 2018*, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "ForeScout CounterACT" Assurance Activities Report v1.0 dated February 23, 2018*.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *ForeScout CounterACT Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all three management interfaces defined in the ST (local CLI, remote CLI, and remote GUI).

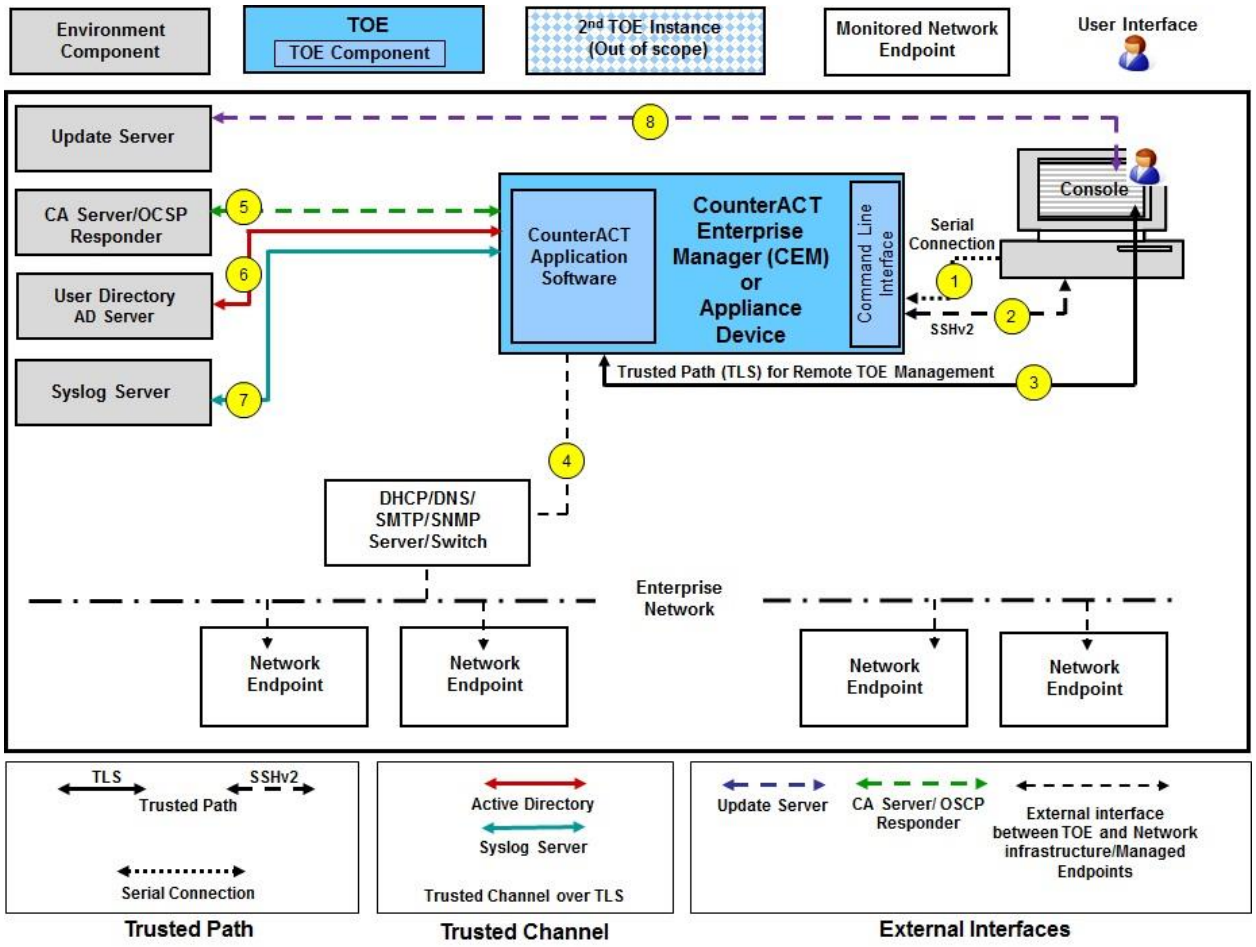
The TOE was configured to communicate with the following environment components:

- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- Active Directory Server for remote authentication
- Certificate Authority/Online Certificate Status Protocol (OCSP) Responder

The following test tools were installed on a separate workstation (management workstation)

- WireShark: version 2.4.2
- Bitvise SSH Client: version 7.15

Only the test tools utilized for functional testing have been listed.



Test Configuration

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research and initially discovering no known vulnerabilities, the team identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- CLI Privilege Escalation
  Access to the TOE's underlying shell should be limited to the CounterACT CLI shell. This test attempted to find ways to access the underlying OS shell.
- Vulnerability Scan (Nessus)
  Nessus is an automated vulnerability scanner and assessment tool. It looks for major vulnerabilities including vulnerable applications and services, as well as less critical vulnerabilities such as unnecessary information disclosure.
- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.
- Force SSHv1
  This attack determines if the SSH server on the TOE will accept an SSHv1 connection when the TOE claims to only support SSHv2

The TOE successfully prevented any attempts of subverting its security.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the CounterACT product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *ForeScout CounterACT Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the routers and switches network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *ForeScout CounterACT Security Target v1.0,* dated February 14, 2018.

13 List of Acronyms

Acronym	Definition
CA	Certificate Authority
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVL	Component Validation List
DN	Distinguished Name
DNS	Domain Name Server
DRBG	Deterministic Random Bit Generator
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
KAS	Key Agreement Scheme
KDF	Key Derivation Function
LDAP/AD	Lightweight Directory Access Protocol / Active Directory
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
RBG	Random Bit Generator
RU	Rack Unit
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

14 Terminology

Term	Definition
Administrator, System Administrator, Security Administrator	The class of TOE administrators that are tasked with managing the TOE's functional and security configuration. Embodies those administrators that have access to the CLI and Console.
Connection	One to One simple flows between a network port and a tool port.
Console or Console application	The CounterACT Console is a GUI application used for creating NAC, firewall and IPS policies, generating reports, viewing and managing detection information, and managing CounterACT Appliances.
Endpoint	A Network Host discovered by CounterACT, for example desktop, laptop, server, etc.
Enterprise Manager	A CounterACT Appliance configured to manage multiple Appliances distributed across the network.
Local console	When the TOE's command line interface (CLI) is accessed locally with a physical connection to the TOE using the serial port and a terminal emulator that is compatible with serial communications is referred to as the local console.
Plugins	Functionality enhancement modules that can be incorporated into CounterACT. Plugins enable deeper inspection as well as broader control over network endpoints. Bundled plugins are pre-packaged with CounterACT. Other plugins may be available from ForeScout or from a third party.
Network Port	Where data arrives into the TOE. The ports which receive copied network data for the TOE.
Remote console	When the TOE's CLI is accessed remotely using SSH is referred to as the remote console

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Collaborative Protection Profile for Network Devices, Version 1.0, 27 Feb, 2015
6. Supporting Document Mandatory Technical Document, Evaluation Activities for Network Device cPP, Version 1.0, February 2015
7. ForeScout CounterACT Security Target v1.0, dated February 14, 2018
8. ForeScout CounterACT Supplemental Administrative Guidance for Common Criteria Version 1.0
9. CounterACT® Console User Manual Version 7.0.0
10. CounterACT® Certificate Interface Configuration Guide
11. CounterACT® Installation Guide
12. CounterACT® Syslog Plugin Configuration Guide
13. CounterACT™ User Directory Plugin Configuration Guide
14. Assurance Activities Report for a Target of Evaluation ForeScout CounterACT Security Target, Version 1.0