# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme
# Validation Report

# ForeScout
# ActiveScout v3.0.5 / CounterACT v4.1.0

**Report Number:** **CCEVS-VR-05-0108**
**Dated:** **2005-08-02**
**Version:** **1.2**

**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 6740**
**Fort George G. Meade, MD 20755-6740**

# Table of Contents

# 1. Executive Summary

The evaluation of the ForeScout ActiveScout v3.0.5 / CounterACT v4.1.0 Intrusion Detection and Prevention (IDP) software product was performed by CygnaCom Solutions, Inc. (an entrust Company) in the United States and was completed on 13 July, 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 2 (EAL2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.2.

CygnaCom Solutions, Inc. is an approved NIAP Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL2) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of ForeScout ActiveScout / CounterACT by any agency of the US Government and no warranty of the product is either expressed or implied.

## *1.1 ForeScout ActiveScout / CounterACT Functionality*

ForeScout ActiveScout / CounterACT is an IDP (Intrusion Detection and Prevention) software product that protects organizational networks from network-borne threats. The product identifies impending attacks against the protected network by identifying the reconnaissance activities (e.g., network probing) that precede them, and then neutralizes the attacks by blocking them before they penetrate the protected network.

The IDP performs the following 4 security functions, which are described in Section 3 of this report:

- Security Audit
- Identification and Authentication
- Security Management
- Attack Detection and Prevention

## *1.2 Evaluation Details*

Table 1-1 provides the required evaluation identification details.

**Table 1-1. Evaluation Details**

| Item | Identification |
|---|---|
| Evaluation Scheme | US Common Criteria Evaluation and Validation Scheme (CCEVS) |
| Target of Evaluation | ForeScout ActiveScout v3.0.5 / CounterACT v4.1.0 |
| EAL | EAL2 |
| Protection Profile | None |
| Security Target | ForeScout ActiveScout v3.0.5 / CounterACT v4.1.0<br>Security Target, Version 2.4, 26 June, 2005 |
| Developer | ForeScout Technologies, Inc. |

| | |
|---|---|
| | 10001 N. DeAnza Blvd.<br>Cupertino, CA 95014 |
| Evaluators | Jean Petty, Dragua Zenelaj<br>CygnaCom Solutions, Inc.<br>7925 Jones Branch Drive, McLean, VA 22102-3321 |
| Validator | Ralph Broom<br>Mitretek Systems, Inc., Falls Church, VA 22042 |
| Dates of Evaluation | 9 October 2003 to 13 July 2005 |
| Conformance Result | Part 2 conformant, Part 3 conformant, and EAL2 conformant |
| Common Criteria (CC) Version | CC, version 2.2, January 2004 |
| Common Evaluation Methodology (CEM) Version | CEM version 2.2, January 2004 |
| Evaluation Technical Report | ForeScout ActiveScout v3.0.5 / CounterACT v4.1.0<br>Evaluation Technical Report:<br>- Volume 1, Security Target Evaluation, version 1.4, 6 July 2005<br>- Volume 2, Evaluation of the TOE, version 1.4, 6 July 2005 |
| Key words | Network, hacker, attack, Intrusion Prevention, Scout, Site Manager, Mark, ForeScout, Scout Flow Policy |

## 1.3 Interpretations

The Evaluation Team performed an analysis of the international and national interpretations of the CC and the CEM and determined that the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below in Table 2.1 were applicable to this evaluation. The Validator determined that the Evaluation Team correctly applied the CCIMB interpretations that it determined to be applicable.

**Table 1-2. CCIMB Interpretations Applied to the Evaluation**

| Interp # | Interpretation Title |
|---|---|
| 137 | Rules governing binding should be specifiable |

As the product is sold internationally, the Evaluation Team determined that national interpretations do not apply.

# 2. Identification of the TOE

## *2.1 Software*

The ForeScout ActiveScout v3.0.05 / CounterACT v4.1.0 are, in essence, functionally identical, differing only in their placement on an external or internal network, respectively.

The TOE consists of two components:

- a “Scout” component that monitors traffic to the network;
- a management component by which administrators manage the TOE, define policies, review audit logs, etc.

The first component can be either:

- ForeScout ActiveScout Scout, or
- ForeScout CounterACT Scout,

which are different configurations of the same product. Both have the same capabilities, share the same code base, and can be considered essentially identical for the purpose of this evaluation.

The second component can be either:

- ForeScout ActiveScout Site Manager (which is used to manage ForeScout ActiveScout Scout), or
- ForeScout CounterACT Site Manager (which is used to manage ForeScout CounterACT),

which are different configurations of the same product. Both have the same capabilities, share the same code base, and can be considered essentially identical for the purpose of this evaluation.

In the remainder of this document:

- references to “Scout” should be understood as referring to both ForeScout ActiveScout Scout and ForeScout CounterACT Scout, and
- references to “Manager” should be understood as referring to both ForeScout ActiveScout Site Manager and ForeScout CounterACT Site Manager.

The product includes the Scout application, the Manager application and a Linux-based operating system for the Scout, but only the Scout and Manager applications comprise the TOE.

The TOE can be managed via the Manager GUI, and certain functions may be performed via a command-line interface on the Scout. The command-line interface is not part of the TOE.

The TOE consumer will need to provide the following:

- Appropriate hardware to run the Scout and Manager.
- A supported operating system to host the Manager.
- Appropriate network environment.
- Trained administrators; and
- Physical security of the Scout and Manager.

## *2.2 Documentation*

The following documents were used to validate the evaluation:

- ETR, Volume 1: Evaluation of the TOE, v1.4 dated 2005-07-06.
- ETR, Volume 2: Evaluation of the TOE, v1.4 dated 2005-07-06.
- Security Target v2.4 for ForeScout ActiveScout/CounterACT, dated 2005-05-24.
- ForeScout ActiveScout / CounterACT Functional Specification, v2.2 dated 2005-06-06.
- ForeScout ActiveScout / CounterACT High Level Design, v2.1 dated 2005-06-06.
- ForeScout ActiveScout / CounterACT Administrator and User Guidance (AGD) v1.3 dated 2005-07-05.
- ForeScout ActiveScout / CounterACT Vulnerability and Strength of Function Analysis v1.1 dated 2005-07-01.
- ForeScout ActiveScout / CounterACT Test Evidence (Reference ATE-EVIDENCE) v1.0, dated 2005-03-10.
- Test Report for ActiveScout v3.0 with Site Manager v3.0, CounterACT v4.1 with Site Manager v4.1 at EAL2, v0.3 dated 2005-05-25.
- ActiveScout Version 3.0 and Site Manager Version 3.0, CounterACT Version 4.1 and Site Manager Version 4.1 Vulnerability Analysis and Penetration Test v0.2 dated 2005-05-25.
- ForeScout ActiveScout Installation Guide v3.0, P.N. 3.0 – 06/04.
- ForeScout ActiveScout Site Manager User’s Guide v3.0, P.N. AS3-30/06/04.
- **ForeScout ActiveScout / CounterACT Administrator and User Guidance Reference AGD v1.3, dated 2005-07-05. Note that this document is sent to those customers who request an evaluated configuration of the TOE.**

# 3. Security Policy

The IDP performs the following 4 security functions:

- Security Audit
- Identification and Authentication
- Security Management
- Attack Detection and Prevention

## *3.1 Security Audit*

The TOE generates audit information for security-relevant events and enables authorized administrators to view the audit records.

The TOE generates audit records for the following events:

- start-up and shutdown of the audit function
- modifications to the policy enforcement function
- modifications to the TOE data

Each audit record includes the date and time as obtained from the IT environment (OS), user identity (when applicable), type of event, and its outcome (success or failure). The audit records can be viewed by authorized administrators. It is possible to filter the view according to various parameters. In addition, certain events (as specified in the TSP), can trigger alerts, which are sent to Manager for immediate attention.

## *3.2 Identification and Authentication*

The TOE allows only users who have been successfully identified and authenticated (authorized administrators) to access security-relevant functionality, including viewing audit records. The TOE maintains a list of user accounts and data about these accounts: name, credential data, and a list of privileges. The TOE identifies and authenticates users (based on user name and password) before allowing them to assume the administrative role defined by their privileges. No user may perform any administrative functions unless the identification and authentication are successful.

## *3.3 Security Management*

The TOE enables authorized administrators to define policies in which the parameters affecting the attack identification process and the response are specified, as well as defining other administrators and system-wide parameters.

## 3.4 Attack Detection and Prevention

The Scout protects networks from attack by identifying the reconnaissance activities that precede attacks, responding with false information and then identifying the false information embedded in the actual attack attempt, which is then blocked by the TOE and thus rendered harmless.
The detected reconnaissance activities and the subsequent attack attempts (if they materialize) are logged and administrators are alerted, in accordance with the policies defined by the TOE administrators.

The Scout is positioned outside the firewall and monitors Internet traffic for signs of pre-attack activity (see Figure 1 in Section 5). It is responsible for accurately identifying potential attackers, marking them as potential threats, and implementing a blocking policy that prevents the attackers from infiltrating the network. Scout identifies potential attackers by recognizing reconnaissance techniques that precede the attack itself, on the basis of known scanning methods.

The Scout assumes that reconnaissance activities ("scans") must be launched against a network prior to an attack, in order to gather information available network services and resources. The Scout identifies these reconnaissance activities, replies with false information (a "mark"), and implements a pre-defined policy that can block any subsequent activity that includes this mark.

The Scout identifies a scan request from an external network based upon concrete scan type and a minimum number of occurrences of scan events from the same source (threshold). The threshold enables Scout to define the level of sensitivity and to minimize false negative scenarios.

Additionally, the implemented policy allows Scout to block events, to monitor them, or to pass them through to the firewall. The block/monitor status is limited to a pre-defined amount of time, which can expire if no other mark-carrying activity is encountered. Scout is also responsible for: administrator identification and authentication, assigning user privileges, managing security aspects of the product, auditing, logging and Scout protection.

# 4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the Scout and Manager are expected to operate.

## 4.1 Usage Assumptions

The assumptions listed below are not addressed by any IT requirements but instead rely on the procedural or administrative measures applied to the operating environment. Users must consider these assumptions and whether they are valid for the intended use of the product.

| | |
|---|---|
| A.ADMIN | The administrators assigned to manage the TOE are competent, properly trained, not careless, not willfully negligent, not hostile, follow the guidance and instruction provided in the TOE documentation, and install and administer the TOE in a manner consistent with organizational policies. |
| A.LOCATE | The TOE components are located in a physically secure area, protected from unauthorized physical access. |
| A.BANDW | The volume of incoming traffic monitored by the TOE does not exceed the volume specified in the TOE administrator guidance documentation. |
| A.TIME | The operating environment provides a reliable time stamp for use by the TOE. |
| P.MANAGE | IT Systems are protected from unauthorized access and modification. |

## 4.2 Environmental Threats

| | |
|---|---|
| T.UA-ACCESS | An unauthorized user may gain access to or modify TOE data stored in the TOE database. |
| T.UA-ACTION | An authorized user may exceed his or her privileges and perform unauthorized modifications of TOE data which go undetected. For example, the user may:<br>• modify the Scout Flow Control Policy for a Scout which the user is not authorized to do so, or<br>• modify details of a Scout Flow Control Policy which the user is not allowed to modify. |
| T.UA-TRANSIT | An unauthorized user may gain access to or modify TOE data when it is in transit between distributed parts of the TOE. |
| T.ATTACK | An attacker may gain access to the protected network via the unprotected network (Internet) using any of a variety of attack methods and gain access to and/or modify user data. |
| T.DISABLE | An attacker may disable the TOE or modify its behavior and thus expose the protected network to attack. |

# 5. Evaluated Configuration

The evaluated configuration consists of two machines that meet the requirements specified in "TOE System Requirements"). One of the machines runs Scout and the other runs Manager.

The Scout, which monitors traffic entering the protected network, runs on an (unevaluated) customized Linux operating system and is located between the firewall and the router. The Scout machine has 2 interfaces:

- An interface with no IP address facing the Internet
- An interface with an IP address facing the internal (protected) network

The Manager machine is located inside the protected network. The Manager is a Java application that may run on Windows XP/2000/NT/98, Linux or Solaris; however it was only evaluated on Windows XP Professional. The Manager host operating system and Java environment were not evaluated.

The Manager and Scout communicate via SSL. The TOE consists of only the Scout and Manager software; the platforms (machines) and their operating systems are not included in the TOE.

Figure 1 illustrates the test configuration.

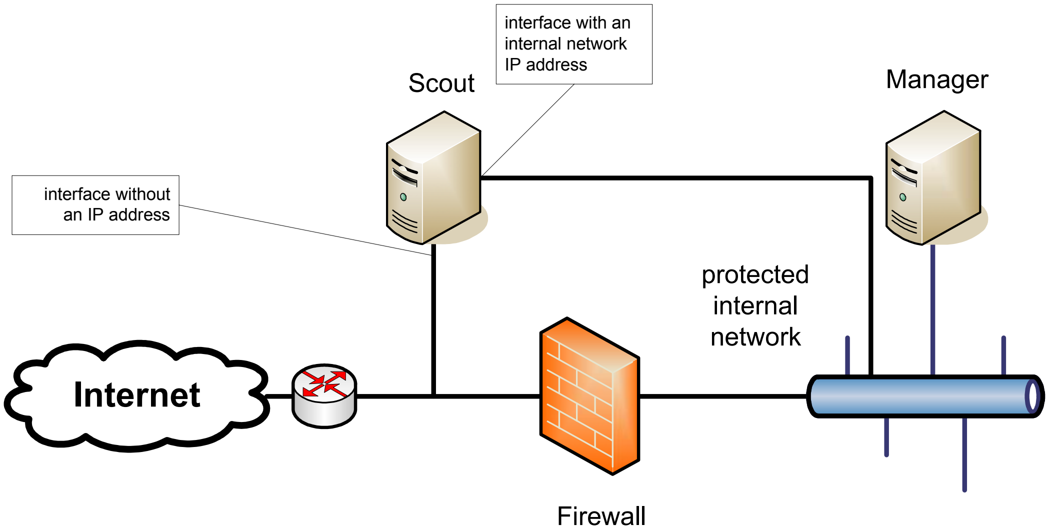
interface with an internal network IP address
Scout
Manager
interface without an IP address
protected internal network
Internet
Firewall

**Figure 1**

The hardware configuration is as follows:

- Scout
    - IBM X330 running a customized Linux (installed from the TOE distribution CD's) OS

    - Two Network Interface Cards (one connecting to the external threat network with no IP address assigned, the other for management and connecting to the protected network where the Manager is installed)
- Manager
    - IBM R31 running Windows XP Professional

### 5.1 Architectural Information

The TOE consists of two components with associated subsystems: the Scout and Manager.

The Scout contains the following subsystems:

- S.ACU – manages S.Database, writes audit records generated by other subsystems to S.Database, provides data for display by and accepts data from M.GUI
- S.Enforcement – enforces the current policy on the interface to unprotected network
- S.Firewall - allows only predefined communications on interfaces to protected and unprotected networks (note that this functionality is provided by the IT Environment)
- S.Communicator - controls and secures communication with Manager (via M.Communicator) (note that this functionality is provided by the IT Environment)
- S,Database – repository for administrative, policy and audit data

The Manager contains the following subsystems:

- M.Communicator - controls and secures communication with Scout (via S.Communicator) (note that this functionality is provided by the IT Environment)
- M.GUI – management interface for administrators

## 6. Evaluation and Validation Process and Conclusions

This section describes the evaluation process used by the team and the activities the Validator performed to gain confidence in the evaluation team's analysis.

The evaluation team conducted a review of the Scout and Manager components of the product based on functional requirements as specified in the Security Target and assurance requirements as required for EAL2.

The EAL2 assurance requirements include the following:

**Table 9-1. EAL2 Components**

| EAL2 Component | EAL2 Component Title |
|---|---|
| ACM_CAP.2 | Configuration items |
| ADO_DEL.1 | Delivery procedures |
| ADO_IGS.1 | Installation, generation, and start-up procedures |

| | |
|---|---|
| ADV_FSP.1 | Informal functional specification |
| ADV_HLD.1 | Descriptive high-level design |
| ADV_RCR.1 | Informal correspondence demonstration |
| AGD_ADM.1 | Administrator guidance |
| AGD_USR.1 | User guidance |
| ATE_COV.1 | Evidence of coverage |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing – sample |
| AVA_SOF.1 | Strength of TOE security function evaluation |
| AVA_VLA.1 | Developer vulnerability analysis |

## 6.1 Evaluation of the Security Target (ASE)

The evaluation team applied each EAL2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies. The team also confirmed that the ST contains a statement of security requirements claimed to be met by the ForeScout ActiveScout / CounterACT product that are consistent with the Common Criteria, and product security function descriptions that support those requirements.

The Validator reviewed the Evaluation team's work units and compared them with the Security Target to determine that the work units were performed correctly.

## 6.2 Evaluation of the Configuration Management Capabilities (ACM)

Configuration Management (CM) systems are put in place to provide a method of tracking changes to the portions of the TOE that they control. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; that the configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. The consumer must request the evaluated version of the product.

The evaluation team analyzed the CM process and determined that TOE components and documentation have unique references and that a system is in place to track release configurations of the TOE and changes to its components.

The Validator reviewed the Evaluations team's work units and evidence to determine that the work units were performed correctly.

## 6.3 Evaluation of Delivery and Operations Documents (ADO)

The evaluation team analyzed the documentation of the procedures used to ensure that the TOE is delivered, installed, generated and started in the same way that the developer intended it to be and that it was delivered without modification. The consumer must request the evaluated version of the product to receive the appropriate documentation.

The Validator reviewed the Evaluations team's work units, evidence and TOE documentation to determine that the work units were performed correctly.

## 6.4 Evaluation of the Development (ADV)

The evaluation team inspected the design documentation to determine that the TOE Security Functions (TSF) could be understood, were consistent and that they supported the claims in the ST. The design documentation consists of a functional specification describing the TOE in terms of internal subsystems and a high-level design which describes how those subsystems work together.

The Validator reviewed the Evaluations team's work units, the TOE functional specification and user and administrator guidance to determine that the work units were performed correctly.

## 6.5 Evaluation of the Guidance Documents (AGD)

The evaluation team analyzed the documentation that describes how to operate the TOE in a secure manner and compared it with the actual operation of the TOE. The TOE includes both a Graphical User Interface (GUI) and a command-line interface; only the GUI was evaluated.

The Validator reviewed the Evaluations team's work units, test results and user and administrator guidance to determine that the work units were performed correctly.

## 6.6 Evaluation of the Test Documentation and Testing Activity (ATE)

The evaluation team examined the developer tests to ensure that those tests would confirm that the TOE behaves as specified in the design documentation and in accordance with the TSF requirements as specified in the ST. In addition, the evaluation team independently performed all of the developer tests and compared them to the developer test results.

The Validator reviewed the Evaluations team's work units, test results and developer test results to determine that the work units were performed correctly.

## 6.7 Vulnerability Assessment Activity (AVA)

The evaluation team examined the TOE for flaws or weaknesses in its intended environment and conducted its own penetration testing. The team reviewed the developer's claims for the strength of specific security functions, performed searches for obvious vulnerabilities and conducted a sample penetration test.

The Validator reviewed the Evaluations team's work units, test results and penetration test to determine that the work units were performed correctly.

## 6.8 Summary of the 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 performance of the entire vendor test suite also demonstrates the veracity of the claims in the ST.

# 7. IT Product Testing

Testing was conducted from 12 April, 2005 to 15 April, 2005 at the ForeScout Technologies facility in Cupertino, CA. The testing was conducted by Dragua Zenelaj, representing the CCTL CygnaCom. Functional and vulnerability testing was conducted, including a full execution of the developer test suite. Delivery and installation procedures were also examined.

The test configuration was as described in section 5. Evaluated Configuration. The approach used was design-based functional testing.

# 8. Validator Comments/Recommendations

This is a software-only TOE. The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices.

The Validator agrees that the CCTL presented appropriate rationales to support the Evaluation Results presented in Section 4 of the ETR, volume 1, and the Conclusions presented in Section 5 of the ETR, volume 2.

The Validator, therefore, concludes that the evaluation and the Pass results for the TOE identified below is complete and correct:

ForeScout ActiveScout v3.0.5 / CounterACT v4.1.0

# 9. Security Target

The Security Target (ST) reference for this product is "ForeScout ActiveScout v3.0.5 / CounterACT v4.1.0, Security Target, Version 2.4, 26 June, 2005". The ST describes what the TOE does, defines the functional claims that the developer is making for the TOE and which standards / specifications the TOE is claimed to conform with.

The conformance claims for this product are:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004, CCIMB-2004-01-002.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, January 2004, CCIMB-2004-01-002.

# 10. List of Acronyms

| Acronym | Definition |
|---|---|
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCIMB | Common Criteria Interpretations Management Board |
| CCTL | Common Criteria Testing Laboratory |
| CEM | Common Evaluation Methodology for Information Technology Security Evaluation |
| CLI | Command Line Interface |
| EAL2 | Evaluation Assurance Level 2 |
| ETR | Evaluation Technical Report |
| GUI | Graphical User Interface |
| IDP | Intrusion Detection and Prevention System |
| NIAP | National Information Assurance Partnership |
| SSL | Secure Sockets Layer |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |

# 11. Bibliography

In addition to the documents specified in section 2.2 Documentation, the following documents were used in compiling this Validation Report:

- Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004:

  - Part 1: Introduction and General Model
  - Part 2: Security Functional Requirements
  - Part 2: Annexes
  - Part 3: Security Assurance Requirements
- Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004: