ForeScout CounterACT v7.0.0

Security Target

Version 2.2

February 18, 2013

Prepared For

ForeScout Technologies, Inc.
10001 N. De Anza Blvd., Suite 220
Cupertino, CA 95014, USA
Tel: 1.866.377.8771 Fax: 1.408.213.2283
Online: www.forescout.com

Prepared By

TABLE OF CONTENTS

Section **Page**

Table of Tables and Figures

Table / Figure **Page**

1 Security Target Introduction

1.1 Security Target Reference

ST Title: ForeScout CounterACT v7.0.0 Security Target

ST Version: Version 2.2

ST Date: February 18, 2013

ST Author: Corsec Security, Inc.

1.1.1 References

Table 1-1: References provides the references used to develop this Security Target.

Table 1-1: References

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3	[CC]
CounterACT Glossary, Version 6.3.3, June 2009	[GLOSSARY]
CounterACT 6.3.3 Hotfix 6.0 Release notes; July 2012	[HF-RN]
CounterACT Release Notes, Version 6.3.3.2	[RELEASE1]
CounterACT Release Notes, Version 6.3.4.0, September 2010	[RELEASE2]
CounterACT Release Notes, Version 6.3.4.1, July 27, 2011	[REALESE3]
CounterACT Installation Guide, Version 7.0.0, November 13, 2012	[INSTALL]
CounterACT Release Notes, Version 7.0, August 2012	[RELEASE4]
CounterACT Console User Manual, Version 7.0.0, September 04, 2012	[USER]

1.2 TOE Reference

TOE Identification: ForeScout CounterACT v7.0.0-513

TOE Vendor: ForeScout Technologies, Inc.

1.3 TOE Overview

ForeScout CounterACT v7.0.0 (CounterACT) combines Network Access Control (NAC) and threat protection to ensure all connecting devices are in compliance with network security policies and are free of self-propagating malware (worms). CounterACT integrates into a network environment and enables enterprises to tailor enforcement and remediation actions to match the level of policy violations through network appliances that interrogates and controls access to the network devices.

The ForeScout CounterACT evaluated configuration consists of the following components: two CounterACT Appliances, the CounterACT Enterprise Manager, SecureConnector and the CounterACT Console used for managing the product.

CounterACT protects data through network access control policies, scanning of network devices for compliance to defined vulnerability management policies, user identification and authentication, role-based management functions, secure transmission of data between TOE components and auditing of security relevant events.

This Security Target (ST) defines the Information Technology (IT) security requirements for ForeScout CounterACT v7.0.0. The TOE is being evaluated at assurance level EAL4+.

1.3.1 TOE Type

ForeScout CounterACT v7.0.0 (CounterACT) is a Network Access Control System.

1.3.2 Hardware/Firmware/Software Required by the TOE

- External Domain Controller
- External DHCP Server
- External NTP Server
- Network Authentication Services
- Network Switches
- Host Platform for CounterACT Console application with the following minimum requirements:
    - Non-dedicated machine, running Windows XP/98/NT/2003/2000/Vista or Linux
    - Pentium 3, 1Ghz
    - 512MB RAM memory (1GB is recommended for more than 10,000 devices)
    - Disk Space - 100 MB
    - CD ROM drive

Please see Section 1.4.3.3 for a description of the CounterACT Console TOE component.

1.4 TOE Description

1.4.1 Acronyms

Table 1-2 and Table 1-3 define product specific and CC specific acronyms respectively.

Table 1-2: Product Specific Acronyms

Acronym	Definition
ARP	Address Resolution Protocol
CLI	Command Line Interface
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control

Acronym	Definition
MIB	Management Information Base
NAC	Network Access Control
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System.
NIC	Network Interface Controller
NTP	Network Time Protocol
OID	Object ID
P2P	Peer-to-Peer
PCI	Payment Card Industry
PDF	Portable Document Format
RADIUS	Remote Authentication Dial In User Service
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell Network Protocol
SSL	Secure Sockets Layer,
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Table 1-3: CC Specific Acronyms

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

1.4.2 Terminology

Table 1-4 and Table 1-5 define product-specific and CC-specific terminology respectively.

Table 1-4: Product-Specific Terminology

Term	Definition
Action	Measures taken at network endpoints; ranging from notices, warnings and alerts to remediation, access restrictions and complete blocking. Actions can be incorporated into NAC policies or applied manually on selected network endpoints.

Term	Definition
ActiveResponse	A patented technology created by ForeScout Technologies that effectively mitigates human attackers, worms and other self-propagating malware. ActiveResponse technology pinpoints and halts threats at the earliest stages of the infection process.
ActiveResponse range	The range of addresses protected by ActiveResponse technology.
Admission event	Network events that indicate the admission of an endpoint into the network. For example when it physically connects to a switch port; when its IP address changes or when it sends out a DHCP request.
Appliance	A CounterACT component, consisting of dedicated hardware and software that executes inspection and policy enforcement. The Appliance monitors traffic going through the enterprise network and, as needed, generates response traffic into the network in order to provide IPS, NAC and firewall functionality.
ARP request	Address Resolution Protocol Request: A request sent by a host on an IP network in order to find the hardware (MAC) address of another host whose network address (IP address) is known. ARP requests are monitored and used by CounterACT to detect hosts in the network.
Bite Event	An event in which a malicious host tries to gain access to the protected network using CounterACT bait (part of the ActiveResponse technology). When a network device (endpoint) tries to gain access to the protected network using a system mark.
Cell	A group of endpoints (hosts) that are monitored and protected by a single Appliance.
Channel	A set of input and output interfaces used by a CounterACT Appliance. A channel consists of: • a monitor interface that examines traffic going through the network • a response interface that generates traffic back into the network • a mapping of VLAN tagging between them
Condition	In NAC policies, a pre-defined set of host properties, logical conditions and Boolean relations connecting them.
Console	The CounterACT 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 Lockdown	A TOE feature of host/port block, where all CounterACT appliances in a multi-appliance configuration participate in the blocking actions.
Enterprise Manager	A CounterACT component that manages multiple Appliances distributed across the network.
Firewall policy	A CounterACT policy that lets the user create network security zones, giving more control over network traffic. The CounterACT firewall is virtual — providing (out-of-band) firewall protection, without being located inline.
Fstool	A command line toolset used at the Appliance and Enterprise Manager for extended configuration and troubleshooting.
Hijack	Actions that let CounterACT intercept and replace endpoint Web (HTTP) sessions with customized Web pages to realize a NAC function. For example, replace a Web session with a notification page indicating that the host does not comply with network policies. Endpoints can be prevented from using the network until they comply, or until they acknowledge an informatory message, etc.
Host	An endpoint; a network machine handled by CounterACT.
Host block	An IPS blocking option that prevents a host from communicating with the enterprise network for a specified time period.
Host inspection	Examination of network hosts by CounterACT. The purpose of inspection is to retrieve host properties and to verify compliance with NAC policies. Hosts that are defined within the CounterACT Internal Range are inspected.
HTTP local host login	A NAC action that lets CounterACT interrogate unmanageable guest hosts. It allows guests to provide CounterACT with credentials which in turn can be used to remotely inspect the host for compliance with the policy.

Term	Definition
Internal network range	The range of network hosts in an organization that CounterACT is configured to inspect.
IPS policy	Same as Threat Protection Policy. A policy that allows the user to define how CounterACT should handle hosts that attempt to attack or infect the network.
Irresolvable host	A Host that could not be properly inspected, and as a result not all properties required by the NAC policy were resolved.
Legitimate e-mail servers	Mail servers/hosts from which mail traffic is expected and should be allowed. Some hosts in the network may generate excessive or suspicious mail traffic that will be detected as a mail infection. For mail servers, this traffic actually qualifies as legitimate activity.
Legitimate traffic rules	Rules for allowing specific network activity. Activity defined in these rules will be ignored by CounterACT when it detects malicious network traffic.
Malicious Host	A machine at which self-propagating malware is detected, or operated by a malicious operator (attacker).
Malware	Software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse. Malware includes both viruses and spyware.
Manageable hosts	Hosts that are accessible for deep inspection by CounterACT.
Management Interface	An Appliance network interface through which the CounterACT Appliance is managed. The management interface is typically also used to perform queries, deep inspection and HTTP hijacking based on CounterACT policies. The interface needs be connected to a switch port and/or VLAN that has access to all network endpoints that it needs to interact with.
Manual action	NAC actions applied manually to endpoints from the Console
Manually added host	Hosts that users manually introduce into CounterACT for IPS related activities — for example adding an endpoint IP that should be ignored by CounterACT.
Mark	Virtual resource information generated by the TOE that is sent to suspected malware programs that are probing the network for information.
Mark naming rules	Instructions that CounterACT uses to create customized marks as part of the ActiveResponse technology. These rules should reflect the naming conventions used for host and user names in your network — for example host names that always begin with a fixed text string.
Monitor interface	The Appliance interface used to monitor network traffic. Typically, network traffic would be mirrored to a port on a switch, to which the monitoring interface would in turn be connected.
NAC policy	A set of rules instructing CounterACT how to detect and handle network endpoints for the purpose of maintaining Network Access Control, compliance and security.
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.
Response interface	An Appliance interface through which CounterACT sends generated traffic into the network. Response traffic is used to: • Protect against self propagating malware, worms and hackers. • Carry out firewall blocking. • Perform NAC Policy actions — for example hijacking Web browsers.
SecureConnector	A lightweight, small-footprint executable that runs at the endpoint so that CounterACT can inspect it. SecureConnector opens an encrypted tunnel to CounterACT allowing it to remotely inspect it, similar to how domain member host would be inspected. SecureConnector can be used when CounterACT cannot otherwise manage the endpoint (unmanageable). SecureConnector can be deployed via a NAC action or using other methods.
Segment	An option that lets the user organize and display the enterprise network into logical groups, which can then be used in NAC policy, reports etc.
Service attack	Concurrent attacks by a multitude of sources against a specific network service.

Term	Definition
Unmanageable host	A host that CounterACT cannot inspect. In general, Windows hosts are unmanageable if they cannot be accessed by CounterACT via ports 139 or 445 or do not allow remote inspection (e.g. registry, file system). This is typical, for example, when endpoints are guests or in cases where domain credentials are not available.
Virtual firewall policy	A CounterACT policy used to create traffic rules for both protecting and making available network services, resources and segments.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes (hosts on the network) and it may do so without any user intervention.

Table 1-5: CC-Specific Terminology

Term	Definition
Authorized User	A user who may, in accordance with the TSP, perform an operation.
External IT Entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

1.4.3 Product Description

The ForeScout CounterACT v7.0.0 (CounterACT) product components are shown in Figure 1 below.

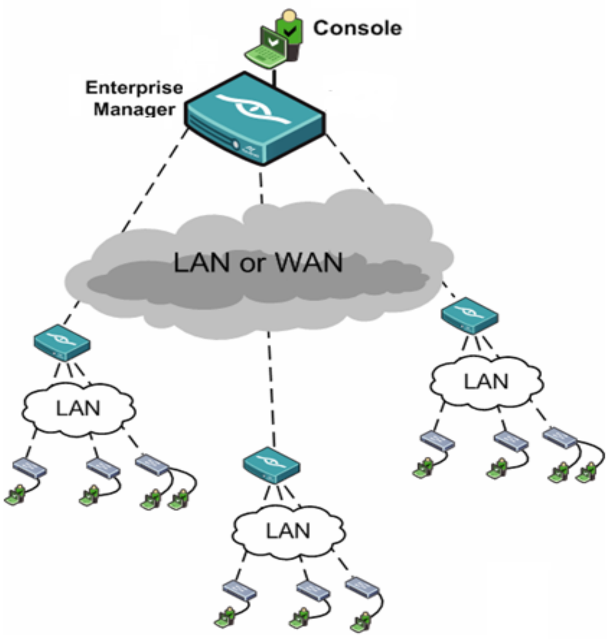

Figure 1: ForeScout CounterACT Product Diagram

CounterACT combines clientless Network Access Control (NAC) and threat protection to ensure all devices connecting to the network are in compliance with network security and access policies, and are free of self-propagating malware. CounterACT integrates into a network environment and enables enterprises to tailor enforcement actions to match the level of policy violations, while avoiding disruptions during device interrogation.

CounterACT provides enterprise-wide network policy enforcement across all devices connected to a network by ensuring that all endpoints are for example up-to-date with necessary patches, (e.g. Microsoft Security Updates or anti-virus definition files), are free of unauthorized programs and malware, and contain mandatory programs or components. While detecting and blocking critical threats (fast spreading worms and malware) upon connection, CounterACT allows users to connect to the network without disruptions while their device is undergoing interrogation. CounterACT includes a Threat Protection component, specifically tuned against fast propagating malware. Once propagation attempts are detected, the attempts can be automatically blocked, and the end-point can, for example, be placed in a quarantine VLAN.

CounterACT enforces the policies across all managed and unmanaged network devices, including desktops and laptops as well as non-OS devices such as VoIP phones, handhelds and network printers, without the need for a software agent. Hosts are unmanageable, if they cannot be accessed via ports 139/445 or do not allow remote inspection (e.g. registry, file system). This is typical of machines that are guests; cases where domain credentials do not work or are not available; where hosts are not part of the domain; and for VPN users and wireless networks. Unmanageable hosts can be automatically placed in a quarantine VLAN, depending on network policy.

Network administrators follow a step-by-step process to define security and access policies and associated enforcement actions that CounterACT will take when violations occur. Through a variety of detection mechanisms, including listening to network traffic, CounterACT is triggered as devices attempt to join the network, and determines whether the connecting endpoints are managed (typically, employee) or unmanaged (guest, contractor or an unauthorized user). The Appliance immediately scans the device for policy compliance and malicious behavior, and can block the device if it presents a threat.

Based on the policy in place, CounterACT can, for example, assign guest endpoints or non-OS devices into suitably designated VLANs. Managed devices can be placed in their corresponding segment of the LAN and granted role-based access to pre-determined network resources. CounterACT initiates an interrogation of the endpoint to determine its compliance status with defined network security policies, while the device gains access to the network.

In case a device is found to be non-compliant, CounterACT takes appropriate action associated with the specific policy violation. CounterACT continues to monitor devices for compliance throughout their connection to the network.

The ForeScout CounterACT Product is comprised of the following components:

- CounterACT Appliance
- CounterACT Enterprise Manager
- CounterACT Console
- SecureConnector
- CounterACT Assets Portal
- CounterACT Command Line Tools

1.4.3.1 CounterACT Appliance (Appliance)

The CounterACT Appliance component of the TOE includes both the hardware of the CounterACT appliance and the software installed on it, including: the ForeScout application software, Plugins and proprietary protocols; and the third-party software which includes the DBMS and operating system. The CounterACT Appliance performs compliance testing and enforcement, and provides protection against self-propagating threats. It automatically identifies and manages suspicious network activity, handles vulnerabilities and Network Access Control (NAC) compliance issues, and lets administrators create network security zones via a virtual firewall. CounterACT also stores and manages information about network threats and activity, as well as the action taken at hosts in the network. Multiple CounterACT Appliances can be deployed to ensure maximum protection of an organization.

The CounterACT Appliance provides administrators the ability to protect their network by the following:

- **NAC Policy Compliance**

  NAC policies allow administrators to define instructions for automatically identifying, analyzing and responding to a broad range of endpoint posture and network activity – for the purpose of bringing network hosts to policy compliance. Specifically, policies are used to initiate host inspection; specify conditions under which CounterACT should respond to hosts, and define actions to take at hosts that match or do not match the policy requirements. Policies can be defined as simply as identifying missing laptops or more complex policies that control network access and VLAN assignment based on organizational structure can be defined.

  For example, Administrator defined NAC Policies can automatically:

  - Pinpoint and quarantine hosts that are working without security software such as Anti-Virus software or patch-level installations, and provide self-remediation tools.
  - Verify that all mission critical servers are hardened by a server hardening procedure.
  - Run (scheduled) vulnerability checks and automatic repair/protection mechanisms.
  - Discover and quarantine rogue Wireless Access Points.
  - Create admission control policies to determine who accesses the network and under what conditions.
  - Monitor compliance progress across the enterprise.

- **Virtual Firewall Policy Compliance**

  Virtual Firewall protection allows administrators to create network security zones, giving more control over network traffic. Specifically, by defining a Virtual Firewall policy administrators can:

  - Create network zones or segments that should be closed off entirely as a result of new threats or newly detected vulnerabilities.
  - Create network zones or segments to close off to specific sources.
  - Prevent unwanted protocols from being transmitted within the network or between specific network segments. For example, to prevent RPC traffic, which should not be transmitted between various departments in an organization.
  - Designate business critical services that should always remain open.

- **Threat Protection Policy Compliance**

  Threat Protection policies allow administrators to define how CounterACT should handle hosts that attempt to infect the network. CounterACT Threat Protection is a component of Network Access Control that performs signatureless Threat Protection. Hosts can be blocked entirely, or prevented from accessing the service they targeted. Administrators can also choose to monitor hosts. When monitored, the hosts can communicate with the network, but CounterACT continues to record their activity.

  Machines at which self-propagating malware is detected are referred to as malicious hosts.

  CounterACT prevents infection attempts by identifying and suppressing malware code before it propagates within a customer's network, and to organizations outside the network. CounterACT monitors traffic directed toward the network for signs of reconnaissance, and identifies the techniques used to launch the scan, for example port scans or NetBIOS probes. In response to this activity, the CounterACT generates virtual resource information sought by malware programs and forwards the information back to them. This information is referred to as a mark. For example, if CounterACT identifies a request for a service at the network, it responds by creating and returning a mark in the form of the service requested. Marks are designed with the intent that malware programs cannot distinguish between the mark and a legitimate network response. When traffic attempts to access the network using the mark, CounterACT immediately recognizes it, and indicates the attacking host as malicious. Now CounterACT either continues to monitor the traffic, or prevents it from establishing communication with the network and external domains, or with the service at which the infection attempt took place.

- **Vulnerability Scanning**

  CounterACT's Vulnerability Scanning tools allow administrators to design vulnerability testing and protection procedures that comply with an organization's vulnerability assessment policy. These tools help protect an organization against an extensive range of vulnerabilities known to the security community. In addition, a wide range of tools is available to help manage vulnerable hosts and communicate with users at vulnerable machines. Two methods can be used for detecting and handling vulnerable hosts:

  - **Automated Protection and Notification**

    Enables automatic protection and remediation at vulnerable hosts by incorporating vulnerability scanning through a defined NAC Policy.

  - **Vulnerability Scanning Wizard**

    Used to plan scheduled vulnerability testing, or to carry out on-the-spot vulnerability testing. Vulnerable hosts are displayed in the Vulnerability Assessment Scans section of the Console Control Center, where administrators can enforce remediation and other actions. Hosts detected by the Vulnerability Scanning Wizard are referred to as vulnerable hosts.

NAC Policies, Virtual Firewall Policies, and Threat Protection Policies are all methods of Network Access Control. All three types of policies may be in force at the same time at one customer installation. Of the three types of policies, NAC Policies are the most flexible and significant to the user. Vulnerability Scanning can be integrated within the NAC Policies defined at a site. The following hierarchies, from highest to lowest, are applied when an endpoint is detected as a result of different policies:

- Threat Protection SFP Manual Ignore state (Allow access)
- Virtual Firewall SFP Allow
- Threat Protection SFP Block
- Virtual Firewall SFP Block
- NAC SFP Authentication Servers Allow
- NAC SFP Manual Allow
- NAC SFP Allow
- NAC SFP Manual Block
- NAC SFP Block

Plugins are additional software modules that can be integrated into the CounterACT Appliance to expand the scope of endpoint inspections and enforcement capabilities. Information gleaned from Plugins is incorporated into CounterACT NAC tools used for creating policies; in the Information Panel and events table as well as in existing reports or in newly designed reports designed to support the Plugin. Tools are available to install/uninstall, configure, test as well as start and stop Plugins at any time. The following set of Plugins is bundled with the product and included in the TOE:

- **Host Property Scanner (HPS-Inspection Engine):** This Plugin enables endpoint NAC Policy inspection mechanisms and the vulnerability scanning tools.

- **HPS-Vulnerability DB:** This Plugin pushes Microsoft vulnerability update information to the Host Property Scanner Plugin. This data is used when working with Vulnerability Policies. The HPS-Vulnerability DB Plugin consists solely of data files. This Plugin may be updated by the user to obtain the latest Microsoft vulnerability information.

  Warning: *All other Plugins contain executable code and cannot be updated without taking the TOE out of the evaluated configuration.*
- **NBT Scanner:** The NBT Scanner Plugin will obtain the user that is logged onto a given host, the host-name and the MAC address of that host.
- **User Directory:** The User Directory Plugin resolves user details via an external User Directory server. This Plugin can also be used to implement external authentication of TOE users (administrators), and of users attempting to access the network.
- **Switch:** This Plugin allows
  - The display of information about hosts connected to specific switch ports, as well as information about those switches and ports.
  - Assigning an endpoint into a designated VLAN, based on NAC Policy
  - Blocking of the host from the network by either:
    - Turning off the host's switch port.
    - Isolating a specific port, by assigning it to a specially defined VLAN that is isolated from the rest of the network.
  - Blocking in VoIP environments.
- **Macintosh/Linux Inspection:** This Plugin enables comprehensive, deep inspection of Macintosh/Linux endpoints.
- **DNS Client:** The DNS Client Plugin resolves IP addresses to Domain Names.
- **Reports:** This Plugin provides reports that are accessible by Web browsers.
- **Syslog:** The Syslog Plugin enables communications with an external Syslog Server.

Additional Plugins and updates to the Plugins listed above are available for download on the Internet. Download, installation and update of Plugins are by administrator command, and are not performed automatically. However, because these actions would change the TOE software, installation of Plugins not bundled with the product and updates to existing Plugins are not allowed in the evaluated configuration of the TOE.

The TOE includes Hotfix v1.2. ForeScout hotfixes apply current fixes to the TOE without requiring an entire TOE upgrade. Hotfixes are downloaded from the CounterACT Product Downloads website and are installed via the Plugins management functionality of the CounterACT Console. The status and version of the Hotfix are listed with the installed Plugins. Hotfix v1.2 is the only hotfix version allowed in the TOE.

The following proprietary protocols that run on top of SSL used for internal communications between TOE components are also included in the CounterACT Appliance TOE component:

- SecureConnector Service - allows a SecureConnector tunnel between endpoints and the Appliance. The SecureConnector Service protocol enables access to unmanageable endpoints via a secure executable file (the SecureConnector) while the endpoint is connected to the network. (See Section 1.4.3.4).
- CounterACT Management - used for installations with only one Appliance for communications from the Console to the Appliance; for systems with more than one CounterACT Appliance, this protocol is used for communications from the Enterprise Manager to the Appliance – (inbound to CounterACT)

All CounterACT Appliances (Models: CT-R, CT-100, CT-1000, CT-2000, and CT-4000) are installed with the same ForeScout software and provide the same security functionality. The following table is a comparison of the hardware appliance models (including the CounterACT Enterprise Manager hardware):

Table 1-6: CounterACT Appliance Hardware Comparison

EMS Models			CEM-05	CEM-10	CEM-25	CEM-50	CEM-100
Managed Appliances			5	10	25	50	100
Appliance Model	CT-R	CT-100	CT-1000		CT-2000		CT-4000
Managed Devices	100	500	1000		2500		4000
Hardware Specs:							
Chassis	1U desktop (steel slim line case)	1U 19″ rack mount	1U 19″ rack mount		2U 19″ rack mount		2U 19″ rack mount
	Height: 42mm	Height: 43.25mm	Height: 43.2mm		Height: 87.30mm		Height: 87.30mm
	(1.65 inches)	(1.703 inches)	(1.7 inches)		(3.44 inches)		(3.44 inches)
	Width: 180mm	Width: 430mm	Width: 430mm		Width: 430mm		Width: 430mm
	(7.48 inches)	(16.93 inches)	(16.93 inches)		(16.93 inches)		(16.93 inches)
	Depth: 150mm	Depth: 692mm	Depth: 654.4mm		Depth: 704.8mm		Depth: 704.8mm
	(5.91 inches)	(27.25 inches)	(25.76 inches)		(25.75 inches)		(25.75 inches)
I/O support	serial port (DB9)	serial port (DB9)	serial port (RJ45)		serial port (RJ45)		serial port (RJ45)
		PS/2 Keyboard and Mouse	PS/2 Keyboard and Mouse		PS/2 Keyboard and Mouse		PS/2 Keyboard and Mouse
USB ports	2	3	3		5		5
VGA	1 (DB15)	1 (DB15)	1 (DB15)		1 (DB15)		1 (DB15)
CD-ROM	N/a	1	1		1		1
Hard Drive	1 HDD	2 HDD (RAID-1)	2 HDD (RAID-1)		2 HDD (RAID-1)		2 HDD (RAID-1)
Bandwidth	100Mbps	500 Mbps	1 Gbps		2 Gbps		Multi-Gbps
Network Ports	4	6	8		8		8
Network Ports Fiber	N/A	optional*	optional*		optional*		optional*

* Not tested

CT-1000 = CEM-05 & CEM-10

CT-2000 = CEM-25 & CEM-50

CT-4000 = CEM-100

In addition to the ForeScout software that performs the functions described above, the following third-party and supporting software components are installed on the CounterACT Appliance:

- Linux Operating System
- PostgreSQL Database
- Nmap
- OpenSSL
- Java: Sun JRE
- Tomcat/Apache
- Network Communication Services:
    - TCP/IP
    - UDP
    - SSH
    - HTTP
    - HTTPS (over SSL or TLS)
    - SMTP
    - SNMP
    - DNS
    - NTP
    - LDAP, RADIUS, TACACS

1.4.3.2 CounterACT Enterprise Manager (Enterprise Manager)

When multiple CounterACT Appliances are present (up to 100 Appliances), these devices can be managed as one through a central CounterACT Enterprise Manager.

The CounterACT Enterprise Manager component of the TOE includes both the hardware of the Enterprise Manager appliance and the software installed on it, including: the ForeScout application software; and the third-party software which includes the DBMS and operating system. The Enterprise Manager appliance model numbers are designated: CEM-XX, where the XX reflects the number of managed appliances, either 5, 10, 25, 50, or 100.

The Enterprise Manager is an aggregation device that communicates with multiple CounterACT Appliances distributed across an enterprise. It manages the CounterACT Appliance activity and policies and collects information about malicious activity that was detected by each Appliance, including infection attempts, identification, and suppression actions taken. Administrators use the Enterprise Manager to define and distribute network policies throughout the LAN to all CounterACT Appliances. The Enterprise Manager collects security event data for reporting, and shares relevant security information gathered from individual Appliances with the rest of the CounterACT Appliances on the network.

The connection between multiple CounterACT Appliances and the Enterprise Manager is authenticated and encrypted using SSL on port 13000 using TCP.

The following proprietary protocol that runs on top of SSL used for internal communications between TOE components is also included in the CounterACT Enterprise Manager TOE component:

- CounterACT Management - used for systems with more than one CounterACT Appliance for communications from the Enterprise Manager to the Appliance from the Console to the Enterprise Manager– (inbound to CounterACT)

Note: The cryptographic functionality of the SSL connection is not being claimed by the vendor and will not be part of the evaluation of the TOE.

The Enterprise Manager also contains the Hotfix and set of Plugins that is bundled with the product as described in the previous section.

In addition to the ForeScout software that performs the functions described above, the following third-party and supporting software components are installed on the CounterACT Enterprise Manager:

- Linux Operating System
- PostgreSQL Database
- Nmap
- OpenSSL
- Java: Sun
- Tomcat/Apache
- Network Communication Services:
  - TCP/IP
  - UDP
  - SSH
  - HTTP
  - HTTPS (over SSL or TLS)
  - SMTP
  - SNMP
  - DNS
  - NTP
  - LDAP, RADIUS, TACACS

1.4.3.3 CounterACT Console (Console)

The CounterACT Console is the CounterACT management application GUI used for viewing and managing important information about Network Access Control policies, malicious activities, vulnerable network hosts, and more. The Console lets administrators define the conditions under which hosts are identified and handled by CounterACT. The Console provides the following management functionality:

- Policy tools allow administrators to define a policy for handling NAC, security and compliance issues, as well as a policy for Virtual Firewall and handling of malicious sources.

- Reporting tools that generate a range of reports about NAC activity, compliance levels, malicious activity and vulnerability scanning, as well as CounterACT's response to this activity.
- Control and Configuration Management tools to start and stop Appliances and Plugins and update the configuration defined during installation — for example the network range CounterACT is protecting or the time zone setting.
- The Executive Dashboard that can be accessed from the Console toolbar provides an at-a-glance view of trend and real-time information regarding endpoint compliance, remediation events, network guests, malicious threats and CounterACT network coverage. It is automatically updated as hosts are monitored and controlled by CounterACT. The dashboard was designed primarily for executives to quickly access and understand the information from CounterACT.

Access to the Enterprise Manager or an Appliance via the Console is authenticated by verifying an Enterprise Manager or Appliance IP address, user ID and password or by authenticating the user via an external User Directory server.

The CounterACT Console connections are encrypted using SSL on port 13000 using TCP. The CounterACT Management proprietary protocol that runs on top of SSL is also included in the CounterACT Console TOE component. It is used for installations with only one Appliance for communications from the Console to the Appliance and for installations with more than one CounterACT Appliance for communications from the Console to the Enterprise Manager– (inbound to CounterACT)

Note: The cryptographic functionality of the SSL connection is not being claimed by the vendor and will not be part of the evaluation of the TOE.

1.4.3.4 SecureConnector

SecureConnector is a lightweight, small-footprint executable that runs at the endpoint so that CounterACT can inspect it. SecureConnector can be used to access to otherwise unmanageable hosts on the network. The SecureConnector executable is signed by ForeScout's private key at build time, and never changes thereafter. Its customization is done by changing its name. When the SecureConnector installs at an endpoint, it uses its name to customize its working environment. The working environment includes:

- Managing Appliance (the appliance to which it connects)
- Mode of installation (Dissolvable or Permanent)
- Run as a service or as an application on the endpoint
- Show SecureConnector icon on the endpoint systray

SecureConnector creates a tunnel from the host to the Appliance through port 10003. The tunnel created is used to remotely inspect the host, as if it was a domain member. The port closes when network users reboot or disconnect from the network, and reopens at reconnection. During operation, the host does not listen to incoming connections as it establishes the encrypted SSL connection with the Appliance. SecureConnector can be configured to dissolve at reboot or disconnection from the network, leaving no footprints. Alternatively, it can be configured to install normally so that it remains upon reboot or disconnection; in this case it can be removed via the uninstall option in the Start > Programs menu.

A SecureConnector is required for VLAN quarantine in a VoIP environment. The SecureConnector must be installed on the host for VLAN assignment to work. A SecureConnector is also needed in order to inspect hosts which are not part of the domain.

The following methods are available for installing the SecureConnector executable:

- Install using NAC Web redirection actions. Once the SecureConnector configuration parameters are set by the administrator, a link to the SecureConnector.exe file is created. This link is available for download and installation by end users. The link is presented to end users by HTTP redirection. (i.e. Network users are prompted to download SecureConnector when attempting to browse the Internet.) The desktop notification and button labels can be customized.
- Install remotely using domain credentials.
- Distribute using standard file distribution methods. SecureConnector is distributed to network hosts by downloading an installation file from an Appliance, and then distributing the file via login script, e-mail, USB stick, or other methods. Alternately the link to the SecureConnector executable can be obtained from an Appliance and sent via e-mail or other method to specific hosts; when a user clicks the link, a SecureConnector installation file is automatically downloaded to the host.

After distribution, it is recommended to setup a NAC policy to verify that SecureConnector installation was successful at the intended hosts.

SecureConnector may be installed permanently on the host, or it can be configured to dissolve at reboot or disconnection from the network, leaving no footprints (Dissolvable Client). An un-installation password is set when the SecureConnector connects to its assigned Appliance.

A SecureConnector is activated via the Host Property Scanner Plugin.

The SecureConnector is supported on the following systems:

- Microsoft Windows (Both 32-bit and 64-bit machines are supported.)
    - Windows NT® 4.0 SP4 and above
    - Windows 2000
    - Windows XP (all service packs)
    - Windows Server 2000 (SP3 and above)
    - Vista
    - Windows 7
    - Windows Server 2003 (all service packs)
    - Windows Server 2008
- Linux
    - Linux Red Hat (version 7.2 and up)
    - Linux Fedora
    - Linux CentOS
    - Ubuntu 8
- Macintosh
    - Macintosh Operating System from 10.4 to 10.6
    - Macintosh Operating System 10.3 (only dissolvable mode)
    - Intel and PowerPC platforms.

Internal communications between the SecureConnector and the CounterACT appliance uses the SecureConnector Service proprietary protocol which runs on top of SSL

A host which cannot be inspected (either because it is not part of the Windows Domain or because it does not run the SecureConnector) can be restricted depending on policy.

1.4.3.5 CounterACT Assets Portal

The Assets Portal is a web-based search/discovery tool that allows authorized users to view network information collected and correlated by CounterACT. This includes not only host information, but also NAC Policy violations, login information, User Directory account details, organizational mapping details, and end-point device connections. The Asset Portal was not included as part of the evaluation.

1.4.3.6 CounterACT Command Line Tools

The CounterACT Appliance and Enterprise Manager also provide a Command Line Interface (CLI). These Command Line Tools provide the administrators with installation and maintenance functions such as: updating the Admin password, updating SSH access, and handling clock malfunctions.

During installation an access list is created specifying the IP address from which SSH should be allowed. (Remotely control the CounterACT Appliances and Enterprise Manager) If this list is empty, an administrator needs physical access to the appliances in order to use the Command Line Tools. An administrator must have root access to the OS of an appliance (be able to login to the OS with the root uid and password) in order to access the CLI.

Note: The Command Line Tools are only used for initial configuration of the product and for off-line maintenance purposes. They are not used during the normal operation of the TOE and will NOT be included in the scope of the evaluation.

1.4.4 Data

The data managed by the TOE can be categorized as:

- Data used to configure, manage, and operate the TOE such as: user accounts, TOE configuration settings and access control policies
- Audit data recorded by the TOE for security significant events produced by the system or by the use of administrative functions
- Data collected from the network devices to aid in the access control decisions

All of the above data is classified as TSF Data.

1.4.5 Users

The TOE has two defined user roles: Admin and Console User. The Admin role has access to all TSF data and management functions. The Console User may be assigned one or more permissions, each with its own set of privileges to the TSF data and functions. When a new user account is created, it must be assigned a role. No access is allowed to the system until a user has been authenticated and access to TSF data and functions is controlled by the providing interfaces only to those data and functions allowed to the authenticated user's role and permissions.

All users of the TOE have access to TSF data and management functions and therefore all are considered administrators for the purposes of this evaluation. The terms “TOE user”, “TOE administrator” and “authorized administrator” are used in this ST to refer collectively to all authorized TOE users.

1.4.6 Product Guidance

The following product guidance documents are provided with the TOE. The documents are available in PDF format on the installation media.

Table 1-7: User Guidance Documents

CounterACT Installation Guide, Version 7.0.0, November 13, 2012
CounterACT Release Notes, Version 7.0.0, August 2012
CounterACT Console User Manual, Version 7.0.0, September 4, 2012
CounterACT v7.0.0 Common Criteria Supplement to the Administrative Guidance, Version 1.2, February 18, 2013

User guidance is also available on:

- The CounterACT support page (http://www.forescout.com/support/index.php?url=counteract)
- The ForeScout documentation portal (www.forescout.com/kb)
- The CounterACT Console online Help tools

1.4.7 Physical Scope of the TOE

The TOE consists of the components described in Section **Error! Reference source not found.**. The TOE Boundary is depicted in Figure 2 below.

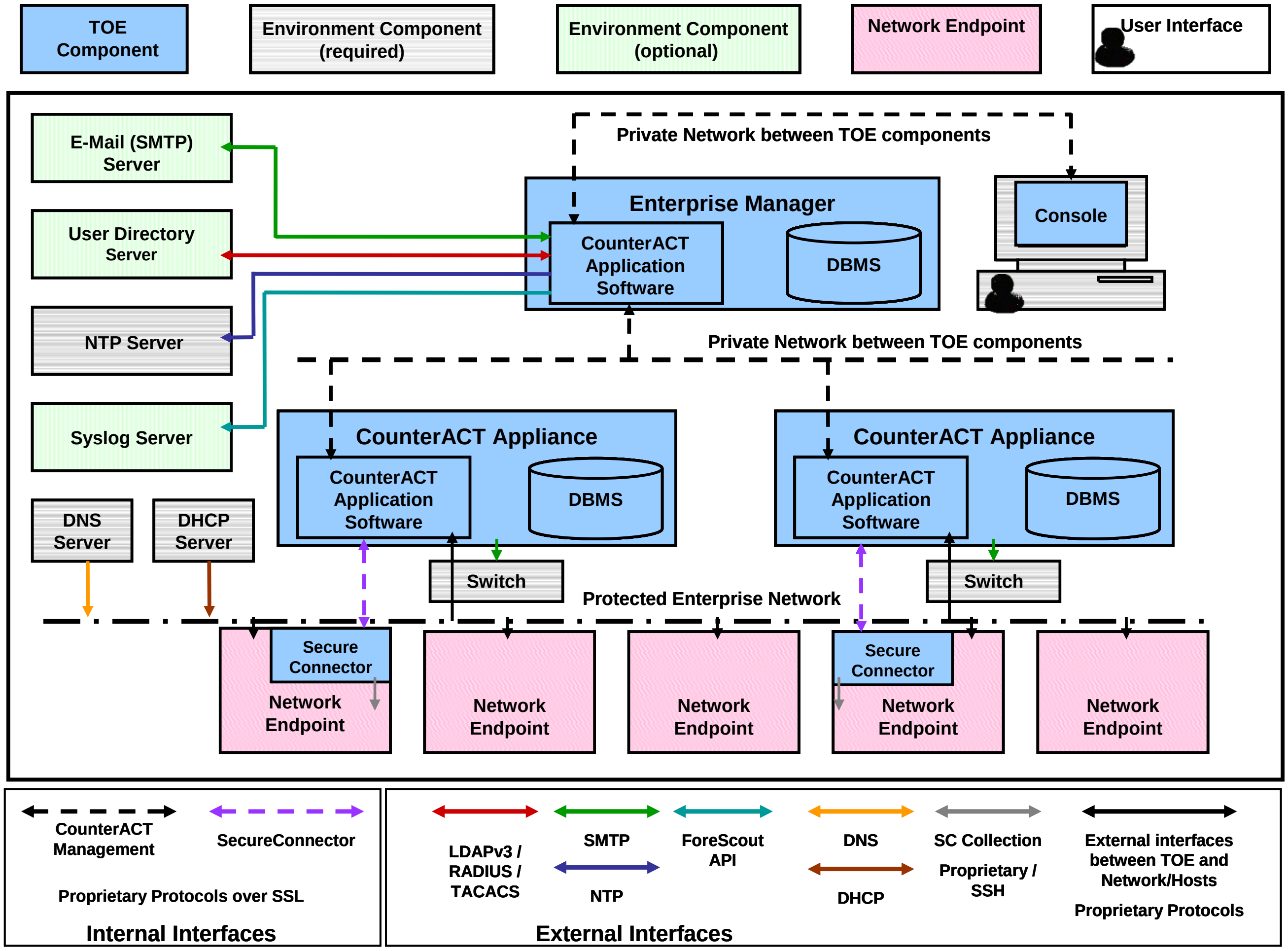

Figure 2: TOE Physical Boundary

The following table summarizes the ports and services needed by the TOE for protected communications between TOE components and between the TOE and services in the Operational Environment.

Table 1-8: ForeScout CounterACT Communication Interfaces

Port	Interface	Comments
13000/TCP	Console Interface	GUI management application installed on an administrative platform
13000/TCP	CounterACT Management Interface	For systems with more than one CounterACT Appliance - from the Console to the Enterprise Manager and from the Enterprise Manager to the Appliance (inbound to CounterACT)
67/UDP	DHCP Server Interface	Allows CounterACT access to communications between the network hosts and the DHCP Server (outbound from CounterACT)
68/UDP		Allows CounterACT access to communications between the network hosts and the DHCP Server (inbound to CounterACT)
53/UDP	DNS Server Interface	Allows CounterACT access to resolve internal IP addresses (outbound from CounterACT)
445/TCP 139/TCP	Host Scanning Interface (Windows)	Allows CounterACT to directly gather information from managed network (Windows) endpoints. (outbound to CounterACT)
22/TCP	Host Scanning Interface (Mac/Linux)	Allows CounterACT to directly gather information from managed network (Macintosh or Linux) endpoints. (outbound to CounterACT)
80/TCP 443/TCP	HTTP Redirection Interface	Allows HTTP redirection (inbound to CounterACT)
User Defined Ethernet Interface	Network Monitor Interface	Allows CounterACT to monitor network traffic (inbound to CounterACT
User Defined Ethernet Interface	Network Response Interface	Allows CounterACT to communicate with network endpoints (outbound from CounterACT)
123/UDP	NTP Server Interface	Allows CounterACT access to an External Time Server (outbound from CounterACT)
10003/TCP	SecureConnector Interface (Windows)	Allows a SecureConnector tunnel between Windows endpoints and the CounterACT Appliance. Port 10003 is the default but can be changed by the administrator. (inbound to CounterACT).
2200/TCP	SecureConnector Interface (Mac/Linux)	Allows a SecureConnector tunnel between Mac/Linux endpoints and the CounterACT Appliance. Port 2200 is the default but can be changed by the administrator. (inbound to CounterACT).
N/A	SC Collection Interface (Windows)	Allows the SecureConnector installed on a network Windows endpoint to inspect it (gather information about the endpoint that is used by the TOE used to enforce the access control policies)
N/A	SC Collection Interface (Mac/Linux)	Allows the SecureConnector installed on a network Macintosh/Linux endpoint to inspect it (gather information about the endpoint that is used by the TOE used to enforce the access control policies)
25/TCP	SMTP Interface	Allows CounterACT access to the enterprise mail relay or optional External E-mail Server (outbound from CounterACT)

Port	Interface	Comments
161/UDP	SNMP Interface	Allows CounterACT to communicate with network switches and routers (outbound from CounterACT)
		Allows SNMP management systems to inspect the TOE (inbound to CounterACT)
162/UDP		Allows CounterACT to receive SNMP traps from network switches and routers (inbound to CounterACT)
		Allows the TOE to send SNMP traps to SNMP management systems (outbound from CounterACT)
22/TCP	SSH Interface	Allows users to access the CounterACT command line interface (CLI) (inbound to CounterACT) Provides the administrators with installation, initial configuration and off-line maintenance functions. This interface is not used during the normal operation of the TOE and is not included in the scope of the evaluation.
514/UDP	Syslog Server Interface	Allows CounterACT to forward and receive events messages to an External Syslog Server (outbound from CounterACT)
User Configured	User Directory Server Interface	Allows CounterACT access to an External User Directory Server. Port 389 is the default but can be changed by the administrator. (outbound from CounterACT)
N/A	Web Reports Interface	Web-based GUI to provide management functionality for CounterACT reports. Accessed through the Console GUI.

1.4.7.1 Included in the TOE:

The evaluated configuration includes the following components of the ForeScout CounterACT v7.0.0-513 with Hotfix v1.2 product:

- **CounterACT Appliance**:
  - All appliance hardware (Models: CT-R, CT-100, CT-1000, CT-2000, and CT-4000),
  - All ForeScout software installed on the appliance including proprietary protocols and the following Hotfix and Plugins:
    - Hotfix (version 1.2)
    - Host Property Scanner (version 9.5.5)
    - HPS-Vulnerability DB (1.13010; may be updated by the user)
    - NBT Scanner (version 3.0.0)
    - User Directory (version 5.4.5)
    - Switch (version 8.5.2)
    - Macintosh/Linux (version 6.1.1)
    - DNS Client (version 2.11080)
    - Reports (version 4.1.0)

        - Syslog (version 3.0.2)
    - All 3rd party software installed on the appliance including:
        - Operating System: 2.6.32-220.4.2.el6
        - Database: Postgresql-8.4.9-1.el6_1.1
        - Nmap: nmap-5.21
        - SSL: OpenSSL 1.0.0-25
        - Java: Sun JRE 1.7.0_05
        - Tomcat: jakarta-tomcat-7.0.28; Apache (2.2.23)
- **CounterACT Enterprise Manager**:
    - All appliance hardware (Models: CEM-5, CEM-10, CEM-25, CEM-50 and CEM-100)
    - All ForeScout software installed on the appliance including proprietary protocols and the following Hotfix and Plugins:
        - Hotfix (version 1.2)
        - Host Property Scanner (version 9.5.5)
        - HPS-Vulnerability DB (1.13010)
        - NBT Scanner (version 3.0.0)
        - User Directory (version 5.4.5)
        - Switch (version 8.5.2)
        - Macintosh/Linux (version 6.1.1)
        - DNS Client (version 2.11080)
        - Reports (version 4.1.0)
        - Syslog (version 3.0.2)
    - All 3rd party software installed on the appliance including:
        - Operating System: 2.6.32-220.4.2.el6
        - Database: Postgresql- 8.4.9-1
        - Nmap: nmap-5.21
        - SSL: Open-SSL 1.0.0-25
        - Java: Sun JRE 1.7.0_05
        - Tomcat: jakarta-tomcat-7.0.28; Apache (2.2.23)
- **CounterACT Console**: software only component
- **SecureConnector (version 3.51)**: software only component

1.4.7.2 Excluded from the TOE:

The following product components and functionality will not be included in the TOE or the evaluation:

- The CounterACT Assets Portal Product Component and its Functionality (does not have a secure connection to the TOE components)
- Command Line Tools (CLI Functionality) (not used during run-time operation of the TOE)
- Plugins not bundled with CounterACT Appliance
- Updates to CounterACT Appliance Plugins, except for the HPS-Vulnerability DB Plugin
- High Availability Option (requires separate license)
- Payment Card Industry (PCI) Kit (requires PCI Plugin)
- Cryptographic Functionality of the SSL interfaces between TOE components
- User Permissions used only for updates to Plugins and other TOE software
- TOE reception of syslog messages from the external Syslog Server (requires installation of NTsyslog on Domain Controller)
- Remote Management Module 2 (RMM2) integration (requires an external Intel RMM2 server system solution)

The following are in the Operational Environment and therefore are excluded from the TOE:

- Host Platform for CounterACT Console application
- External Domain Controller
- External DHCP Server
- External NTP Server
- Network Authentication Services
- Network Switches
- Optional E-mail Server
- Optional Syslog Server
- Optional User Directory Servers:
    - Microsoft Active Directory
    - Sun Java System Directory Server
    - Novell eDirectory
    - IBM Lotus Notes
    - Radius
    - TACACS

1.4.8 Logical Scope of the TOE

The TOE provides the following security functionality:

- **Security Audit**

The TOE's auditing capabilities include the generation of information about system processing, use of the administrative functions and attempted access to the protected network. The TOE provides authorized personnel access to the audit data and the ability to interpret and sort the data. The TOE protects the audit data from modification and unauthorized deletion.

Security Audit relies on the Operational Environment to provide reliable timestamps for the audit records. This functionality may optionally rely on an external syslog server in the Operational Environment to archive audit records. It also relies on the Environment to provide a secure channel between the TOE and the external time server and the optional Syslog server.

- **Network Access Control**

  The TOE provides its own Network Access Control separate from that of the Operational Environment between subjects and objects covered by the TOE's access control policies. The TOE supports three types of Network Access Control policies: NAC, Virtual Firewall, and Threat Protection. All three types of policies may be used simultaneously for network protection. The TOE provides administrative functions for authorized administrators to define these policies.

  Network Access Control depends on the Operational Environment to provide secure communications between the TOE and the network endpoints. User data protection may rely on an external e-mail server in the Operational Environment if e-mail notifications are configured in a policy. It also depends on the Environment to provide a secure channel between the TOE and the e-mail server if it is present.

- **User Identification and Authentication**

  Each TOE user must be successfully identified and authenticated by the TSF or an external authentication service invoked by the TSF before access is allowed to the TOE. The TSF maintains security attributes for each individual TOE user for the duration of the user's login session. The TOE also supports a password policy, authentication failure handling and masks the user's authentication data upon input.

  User Identification and Authentication may rely on the Operational Environment to provide an optional external authentication service if that method of authentication of TOE users is configured for the system. It also depends on the Environment to provide a secure channel between the TOE and the authentication server if it is present.

- **Security Management**

  The TOE provides role-based security management functions through the use of the administrative GUI. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role and permissions.

  Security Management relies on a management console in the Operational Environment to host the CounterACT console application. Security management also depends on the Operational Environment to provide secure communications between the TOE and the DNS Server, Network Switch(es), optional User Directory Server, optional E-mail Server and between the TOE and network endpoints.

- **Protection of Security Functions**

  The TOE protects data being transferred between the distributed TOE components from disclosure and modification by the implementation of secure internal interfaces.

- **Vulnerability Scanning**

  The TOE further protects the targeted network through the ability to conduct vulnerability scans. The TOE has the ability to collect configuration and posture data from endpoints attempting network access, analyze the collected data and perform administrator configured remediation actions if a potential vulnerability is detected.

  Vulnerability Scanning depends on the Operational Environment for secure communications between the TOE and the network endpoints. Vulnerability scanning may rely on an external e-mail server in the Operational Environment if e-mail notifications are configured to be sent when a vulnerability is detected. It also depends on the Environment to provide a secure channel between the TOE and the e-mail server if it is present.

The following functionality is not included in the TOE:

- The web-based search/discovery functionality provided by the Assets Portal Product Component
- Initial configuration and non-run time configuration provided by the Command Line Tools (CLI functionality)
- Functionality provided by Plugins that are not bundled with the CounterACT Appliance
- Updates to the CounterACT Appliance Plugins, except for the HPS-Vulnerability DB Plugin
- High Availability configuration of the system
- PCI functionality provided by the Payment Card Industry (PCI) Kit
- The Cryptographic functionality of the SSL used for protection of data transferred between TOE components
- TOE reception of syslog messages from the external Syslog Server

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2 from the Common Criteria Version 3.1 R3.

This document conforms to the Common Criteria (CC) for Information Technology (IT) Security Evaluation, Version 3.1, Revision 3, CCMB-2009-07-002.

2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2.

3 Security Problem Definition

3.1 Threats

The TOE must counter the threats to security listed in Table 3-1. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

Table 3-1: TOE Threats

Item	Threat ID	Threat Description
1	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
2	T.NetAttack	An attacker may gain access to the protected network and gain access to and/or modify user, TOE, or system data.
3	T.Privilege	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
4	T.Tamper	An attacker may attempt to modify TSF programs and data.
5	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.
6	T.Vulnerable	A non-compliant or vulnerable endpoint may connect to the protected network and infect it with malware.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for the TOE.

3.3 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are listed in Table 3-2.

Table 3-2: Assumptions

Item	Assumption ID	Assumption Description
1	A.Manage	The TOE assumes there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
2	A.Physical	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
3	A.ProtectComm	Those responsible for the TOE will ensure the communications between the TOE components and external IT Entities are via secure channels.
4	A.Users	The TOE assumes that its users will protect their authentication data.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

Table 4-1: TOE Security Objectives

Item	TOE Objective	Description
1	O.Admin	The TOE must include a set of functions that allow effective management of its functions and data.
2	O.Audit	The TOE must record audit records for data accesses and use of the system functions.
3	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
4	O.IDProtect	The TOE must provide mechanisms to protect user identification and authentication
5	O.Integrity	The TOE must ensure the integrity of all audit and system data.
6	O.NetworkAccess	The TOE must control access to the protected network based on security policies and the attributes of the endpoints attempting access to the protected network.
7	O.Scanning	The TOE must support the detection and remediation of potential vulnerabilities on the endpoints attempting access to the protected network by collecting and analyzing configuration data from those devices.
8	O.TOEAccess	The TOE must allow authorized users to access only appropriate TOE functions and data.

4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

Table 4-2: Security Objectives for the Operational Environment

Item	Environment Objective	Description
1E	OE.Creden	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
2E	OE.Install	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
3E	OE.Person	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the System.
4E	OE.Physical	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
5E	OE.ProtectComm	The Operational Environment must provide a mechanism to establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.
6E	OE.Time	The Operational Environment must provide reliable time for the use of the TOE.
7E	OE.XAuth*	The Operational Environment must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user’s logical access to the TOE.

**Note: OE.XAuth is only applicable when the TOE is configured to use an external authentication service.*

4.3 Security Objectives Rationale

Table 4-3: Mapping of TOE Security Objectives to Threats/Policies

Item	TOE Objective	Threat
1	O.Admin The TOE must include a set of functions that allow effective management of its functions and data.	T.Mismanage
2	O.Audit The TOE must record audit records for data accesses and use of the system functions.	T.Undetect
3	O.IDAuth The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	T.Privilege
4	O.IDProtect The TOE must provide mechanisms to protect user identification and authentication	T.Privilege
5	O.Integrity The TOE must ensure the integrity of all audit and system data.	T.Tamper
6	O.NetworkAccess The TOE must control access to the protected network based on security policies and the attributes of the endpoints attempting access to the protected network.	T.NetAttack
7	O.Scanning The TOE must support the detection and remediation of potential vulnerabilities on the endpoints attempting access to the protected network by collecting and analyzing configuration data from those devices.	T.Vulnerable
8	O.TOEAccess The TOE must allow authorized users to access only appropriate TOE functions and data.	T.Privilege

Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions

Item	Environment Objective	Threat/Policy/Assumption
1E	OE.Creden Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	A.Users
2E	OE.Install Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	A.Manage
3E	OE.Person Personnel working as authorized administrators must be carefully selected and trained for proper operation of the System.	A.Manage
4E	OE.Physical Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	A.Physical

Item	Environment Objective	Threat/Policy/Assumption
5E	OE.ProtectComm The Operational Environment must provide a mechanism to establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.	T.Tamper A.ProtectComm
6E	OE.Time The Operational Environment must provide reliable time for the use of the TOE.	T.Undetect
7E	OE.XAuth The Operational Environment must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.	T.Privilege

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

Table 4-5: All Threats to Security Countered

Item	Threat ID	Objective	Rationale
1	T.Mismanage Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	O.Admin The TOE must include a set of functions that allow effective management of its functions and data.	The objective counters this threat by providing a set of effective administrative functions via the Console GUI.
2	T.NetAttack An attacker may gain access to the protected network and gain access to and/or modify user, TOE, or system data.	O.NetworkAccess The TOE must control access to the protected network based on security policies and the attributes of the endpoints attempting access to the protected network.	The objective counters this threat by protecting the network through administrator defined Network Access Control policies based on endpoint attributes.
3	T.Privilege An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.IDAuth The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	This threat is countered through a number of objectives. This objective requires that all TOE users to be identified and authenticated before allowing access to its functions and data. The TOE itself supports user id / password authentication.
		O.IDProtect The TOE must provide mechanisms to protect user identification and authentication	This objective supports strong user authentication via a password policy, masking the user password on input and supporting an authentication failure policy.

Item	Threat ID	Objective	Rationale
		O.TOEAccess The TOE must allow authorized users to access only appropriate TOE functions and data.	This objective provides that access to the TSF data and administrative functions is restricted by the TOE through administrative roles and privileges.
		OE.XAuth The Operational Environment must provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.	This objective allows for the TOE to invoke an external authentication service in the Operational Environment for user authentication before allowing access to its functions and data.
4	T.Tamper An attacker may attempt to modify TSF programs and data.	O.Integrity The TOE must ensure the integrity of all audit and system data.	The TOE objective counters this threat by protecting the audit data and preventing the modification or disclosure of data when it is transmitted between TOE components.
		OE.ProtectComm The Operational Environment must provide a mechanism to establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.	The Operational Environment objective contributes to the protection of the TOE data by providing protection of data transmitted between the TOE and any external entity such as an LDAP server.
5	T.Undetect Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.	O.Audit The TOE must record audit records for data accesses and use of the system functions.	The objective counters this threat by generating audit data that records security relevant events and the use of the administrative functions.
		OE.Time The Operational Environment must provide reliable time for the use of the TOE.	The objective supports the recording of the security audit data by providing reliable timestamps.
6	T.Vulnerable A non-compliant or vulnerable endpoint may connect to the protected network and infect it with malware.	O.Scanning The TOE must support the detection and remediation of potential vulnerabilities on the endpoints attempting access to the protected network by collecting and analyzing configuration data from those devices.	The objective counters the threat by stating that the TOE is able to collect configuration data from endpoints attempting network access, analyze the collected data and perform administrator configured remediation actions if a potential vulnerability is detected.

Table 4-6 shows that the security objectives for the operational environment uphold all assumptions. Rationale is provided for each Assumption in the table.

Table 4-6: All Assumptions Upheld

Item	Assumption ID	Objective	Rationale
1	A.Manage The TOE assumes there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.Install Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	This objective provides for the secure installation and operation of the TOE
		OE.Person Personnel working as authorized administrators must be carefully selected and trained for proper operation of the System.	This objective provides for trustworthy and well-trained administrators of the TOE
2	A.Physical The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	OE.Physical Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	This objective provides for the physical protection of the TOE hardware and software.
3	A.ProtectComm Those responsible for the TOE will ensure the communications between the TOE components and external IT Entities are via secure channels.	OE.ProtectComm The Operational Environment must provide a mechanism to establish a trusted communications path which provides for the protection of the data from modification or disclosure while being exchanged between TOE components and external entities.	The objective provides that those installing and maintaining the TOE will ensure that all connections between TOE components and any external IT Entities will be secure.
4	A.Users The TOE assumes that its users will protect their authentication data.	OE.Creden Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The objective provides that the TOE users will protect their authentication data.

5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding "_EXT" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FIA_UAU_EXT.2	User authentication before any action
2	SSC_ACT_EXT.1	Vulnerability scans remediation actions
3	SSC_ANL_EXT.1	Vulnerability scans analysis
4	SSC_SCN_EXT.1	Vulnerability scanning

5.1 FIA_UAU_EXT.2 User authentication before any action

5.1.1 Class FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.2 Family: User authentication (FIA_UAU)

5.1.3 Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.1.4 Management

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

5.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism
- Basic: All use of the authentication mechanism

5.1.6 Definition

FIA_UAU_EXT.2 Timing of authentication

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

5.1.7 Rationale

FIA_UAU_EXT.2 is modeled closely on the standard component FIA_UAU.2: User authentication before any action. FIA_UAU_EXT.2 needed to be defined as an extended component because the standard component was broadened by adding the text *"either by the TSF or by an authentication service in the Operational Environment invoked by the TSF".*

Note: The definition and use of the wording in FIA_UAU_EXT.2.1 was approved by the validation team for FAU_UAU_EXT.2 in a previous CygnaCom evaluation.

5.2 SSC_ACT_EXT.1 Vulnerability scans remediation actions

5.2.1 Class SSC: Vulnerability scans management

This class was explicitly created to describe the security functionality provided by the vulnerability scanning performed by the TOE to detect vulnerabilities and non-compliance to security policies of the endpoints attempting access to the protected network.

5.2.2 Family: Vulnerability scans actions (SSC_ACT)

5.2.3 Family Behaviour

This family defines the actions taken by the TSF when a potential vulnerability is detected by a vulnerability scan.

5.2.4 Management

The following actions could be considered for the management functions in FMT:

- Management (addition, removal, or modification) of actions.

5.2.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Actions taken due to detected potential vulnerabilities

5.2.6 Definition

SSC_ACT_EXT.1 Vulnerability scans remediation actions

Hierarchical to: No other components

Dependencies: SSC_ANL_EXT.1 Vulnerability scans analysis

SSC_ACT_EXT.1.1 The TSF shall take ***[assignment: list of actions]*** upon detection of a vulnerability in a network device that has been scanned.

5.2.7 Rationale

SSC_ACT_EXT.1 is modeled closely on the standard component FAU_ARP.1: Security audit automatic response. SSC_ACT_EXT.1 needed to be defined as an extended component because the actions taken by the TSF are a result of the analysis of the data collected by the vulnerability scans, rather than the analysis of audit event data.

5.3 SSC_ANL_EXT.1 Vulnerability scans analysis

5.3.1 Class SSC: Vulnerability scans management

This class was explicitly created to describe the security functionality provided by the vulnerability scanning performed by the TOE to detect vulnerabilities and non-compliance to security policies of the endpoints attempting access to the protected network.

5.3.2 Family: Vulnerability scans analysis (SSC_ANL)

5.3.3 Family Behaviour

This family defines the analysis performed by the TSF on the data collected by the vulnerability scans to detect a potential vulnerability.

5.3.4 Management

The following actions could be considered for the management functions in FMT:

- Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.

5.3.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Enabling and disabling of any of the analysis mechanisms.

5.3.6 Definition

SSC_ANL_EXT.1 Vulnerability scans analysis

Hierarchical to: No other components.

Dependencies: SSC_SCN_EXT.1 Vulnerability scanning

SSC_ANL_EXT.1.1 The TSF shall be able to apply a set of rules in analyzing the data collected from the endpoints during vulnerability scanning and based upon these rules indicate a vulnerability in those devices.

SSC_ANL_EXT.1.2 The TSF shall enforce the following rules for [assignment: subset of the collected compliance data] known to indicate a device vulnerability: ***[assignment: rules].***

5.3.7 Rationale

SSC_ANL_EXT.1 is modeled closely on the standard component FAU_SAA.1: Security audit analysis. SSC_ANL_EXT.1 needed to be defined as an extended component because the TSF performs the analysis on the data collected by the vulnerability scans, rather than the audit event data.

5.4 SSC_SCN_EXT.1 Vulnerability scanning

5.4.1 Class SSC: Vulnerability scans management

This class was explicitly created to describe the security functionality provided by the vulnerability scanning performed by the TOE to detect vulnerabilities and non-compliance to security policies of the endpoints attempting access to the protected network.

5.4.2 Family: Vulnerability scanning (SSC_SCN)

5.4.3 Family Behaviour

This family defines the scanning performed by the TSF to collect data from the endpoints that may indicate a potential vulnerability in those devices.

5.4.4 Management

The following actions could be considered for the management functions in FMT:

- Management (addition, removal, or modification) of specific information that will be obtained from targeted endpoints (network devices).
- Management (addition, removal, or modification) of specific targeted endpoints (network devices).

5.4.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- There are no auditable events foreseen.

5.4.6 Definition

SSC_SCN_EXT.1 Vulnerability scanning

Hierarchical to: No other components

Dependencies: No dependencies

SSC_SCN_EXT.1.1 The TSF shall be able to perform scans to collect the following information from the endpoints on the protected network ***[assignment: collected data]*** that may indicate a vulnerability in those devices.

5.4.7 Rationale

SSC_SCN_EXT.1 is modeled closely on IDS_SDC_EXT.1 taken from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007. SSC_SCN_EXT.1 needed to be defined as an extended component since the CC does not provide a standard component for the collection of data from network resources. It was modified from the Protection Profile component because the TOE only collects configuration data, not event data from the endpoints (network devices).

6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

6.1 Security Functional Requirements for the TOE

Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

iteration:	allows a component to be used more than once with varying operations;
assignment:	allows the specification of parameters;
selection:	allows the specification of one or more items from a list; and
refinement:	allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- Assignments and Selections specified by the ST author are in ***[italicized bold text].***
- Refinements are identified with "Refinement:" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.
- Iterations are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. “*” refers to all iterations of a component.
- Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- Extended components defined in Section *Error! Reference source not found.* have been denoted with the suffix “_EXT” following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section 5, and summarized in Table 6-1 below.

Table 6-1: Functional Components

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_SAR.1	Audit Review
3	FAU_SAR.2	Restricted audit review
4	FAU_SAR.3	Selectable audit review
5	FAU_STG.1	Protected audit trail storage
6	FDP_ACC.1-1	Subset access control (NAC)
7	FDP_ACC.1-2	Subset access control (Virtual Firewall)
8	FDP_ACC.1-3	Subset access control (Threat Protection)
9	FDP_ACF.1-1	Security attribute based access control (NAC)
10	FDP_ACF.1-2	Security attribute based access control (Virtual Firewall)

Item	SFR ID	SFR Title
11	FDP_ACF.1-3	Security attribute based access control (Threat Protection)
12	FIA_AFL.1	Authentication failure handling
13	FIA_ATD.1	User attribute definition
14	FIA_SOS.1	Verification of secrets
15	FIA_UAU_EXT.2	User authentication before any action
16	FIA_UAU.7	Protected authentication feedback
17	FIA_UID.2	User identification before any action
18	FMT_MSA.1-1	Management of security attributes (NAC)
19	FMT_MSA.1-2	Management of security attributes (Virtual Firewall)
20	FMT_MSA.1-3	Management of security attributes (Threat Protection)
21	FMT_MSA.3-1	Static attribute initialization (NAC)
22	FMT_MSA.3-2	Static attribute initialization (Virtual Firewall)
23	FMT_MSA.3-3	Static attribute initialization (Threat Protection)
24	FMT_MTD.1	Management of TSF data
25	FMT_SMF.1	Specification of Management Functions
26	FMT_SMR.1	Security roles
27	FPT_ITT.1	Basic internal TSF data transfer protection
28	SSC_ACT_EXT.1	Vulnerability scans remediation actions
29	SSC_ANL_EXT.1	Vulnerability scans analysis
30	SSC_SCN_EXT.1	Vulnerability scanning

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the ***[not specified]*** level of audit; and
c) ***[the following auditable events: events listed in column 3 of*** Table 6-2***].***

Table 6-2: Auditable Events

Item	SFR ID	Auditable Event
1	FAU_GEN.1	None
2	FAU_SAR.1	None
3	FAU_SAR.2	None
4	FAU_SAR.3	None
5	FAU_STG.1	None
6	FDP_ACC.1-1	None
7	FDP_ACC.1-2	None
8	FDP_ACC.1-3	None
9	FDP_ACF.1-1	All requests to perform an operation on an object covered by the SFP.
10	FDP_ACF.1-2	All requests to perform an operation on an object covered by the SFP.
11	FDP_ACF.1-3	All requests to perform an operation on an object covered by the SFP.

Item	SFR ID	Auditable Event
12	FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
13	FIA_ATD.1	None
14	FIA_SOS.1	Identification of any changes to the defined quality metrics.
15	FIA_UAU_EXT.2	All use of the authentication mechanism.
16	FIA_UAU.7	None
17	FIA_UID.2	All use of the user identification mechanism, including the user identity provided.
18	FMT_MSA.1-1	All modifications of the values of security attributes.
19	FMT_MSA.1-2	All modifications of the values of security attributes.
20	FMT_MSA.1-3	All modifications of the values of security attributes.
21	FMT_MSA.3-1	All modifications of the values of security attributes.
22	FMT_MSA.3-2	All modifications of the values of security attributes.
23	FMT_MSA.3-3	All modifications of the values of security attributes.
24	FMT_MTD.1	All modifications to the values of TSF data.
25	FMT_SMF.1	Use of the management functions.
26	FMT_SMR.1	Modifications to the group of users that are part of a role.
27	FPT_ITT.1	None
28	SSC_ACT_EXT.1	Actions taken due to detected potential vulnerabilities.
29	SSC_ANL_EXT.1	Enabling and disabling of any of the analysis mechanisms.
30	SSC_SCN_EXT.1	None

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[the additional information identified in Table 6-3].***

Table 6-3: Audit Record Information

Audit File	Field	Description
Host Log	Time	The date and time the event occurred.
	Source	The IP address of the source detected.
	Type/Name	The type of the event. The name is basic information about the type.
	Details	The details of the event.
	Status	The status of the operations taken place.
	MAC Address	The MAC address of the detected host.
	Origin	The CounterACT Appliance or Management Server that detected the event.
System Event Log	Event Name	The name of the event that occurred. (includes any subject identity)
	Event Group	The type of event that occurred.
	Date	The date and time that the event occurred.
	Severity	The severity level of a system event, indicated by a colored icon: Error, Warning, or Information.
User Audit Trail	Operation	Type of user operation indicated by a colored icon: Add, Edit, or Remove.
	User Name	The user who performed the operation.
	Host	The IP address of the machine from which the operation was made.
	Date	The date and time that the operation was made.

Audit File	Field	Description
	Resource	The resource the operation was performed upon.
	Operation Data	The changed information.

6.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[users listed in column 2 of Table 6-4]*** with the capability to read ***[all audit information in the audit files listed in column 1 of* Error! Not a valid bookmark self-reference. *]*** from the audit records.

Table 6-4: Audit Record Access

Audit File	Users with Access to the Records in the Audit File
Host Log	Admin
	All Console Users
System Event Log	Admin
	Console Users with ‘Event Log’ Permission
User Audit Trail	Admin
	Console Users with ‘Audit Trail User’ Permission

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users who have been granted explicit read-access.

6.1.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply ***[sorting]*** of audit data based on ***[date and time, subject identity, type of event, and success or failure of related event].***

6.1.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to ***[prevent]*** unauthorised modifications to the stored audit records in the audit trail.

6.1.2 Class FDP: User Data Protection

6.1.2.1 FDP_ACC.1-1 Subset access control (NAC)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1-1.1 The TSF shall enforce the ***[CounterACT NAC SFP]*** on ***[***

subjects: endpoints,

objects: network domain

operations: Authentication Actions, Management Actions, Notification Actions, Remediation Actions, Restriction Actions as listed in Section 6.1.4.1 ***FMT_MSA.1-1 Management of security attributes (NAC)***

]**.**

6.1.2.2 FDP_ACC.1-2 Subset access control (Virtual Firewall)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1-2.1 The TSF shall enforce the ***[CounterACT Virtual Firewall SFP]*** on ***[***

subjects: endpoints

objects: network domain

operations: block, allow

]**.**

6.1.2.3 FDP_ACC.1-3 Subset access control (Threat Protection)

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1-3.1 The TSF shall enforce the ***[CounterACT Threat Protection SFP]*** on ***[***

subjects: endpoints

objects: network domain

operations: host block, port block, monitor, ignore, notify

]**.**

6.1.2.4 FDP_ACF.1-1 Security attribute based access control (NAC)

Hierarchical to:	No other components
Dependencies:	FMT_MSA.3 Static attribute initialisation
	FDP_ACC.1 Subset access control

FDP_ACF.1-1.1 The TSF shall enforce the ***[CounterACT NAC SFP]*** to objects based on the following:

[

subjects: endpoints

subject security attributes: as defined in FMT_MSA.1-1.1 (see Section 6.1.4.1 FMT_MSA.1-1 Management of security attributes (NAC))

objects: network domain

object security attributes: policy scope

].

FDP_ACF.1-1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[***

- ***The Appliance inspects the endpoints requesting access to the protected network for compliance with the rules defined by an Admin or Console User with 'NAC Policy' Permission. A Rule consists of:***
    - ***A Scope: A subset of the network domain.***
    - ***A Condition: One set of properties (subject attributes) that is queried when evaluating endpoints.***
    - ***Actions: CounterACT measures taken at the network endpoints as defined in FMT_MSA.1-1.1 (see Section 6.1.4.1 FMT_MSA.1-1 Management of security attributes (NAC))***
- ***Each condition in a rule may consist of several criteria which must be met in order for the endpoint to match the policy. The administrator defines the Main and Sub Rules so that an endpoint is considered to match the policy when:***
    - ***When all criteria are met.***
    - ***When none of the criteria are met.***
    - ***When any criterion is met.***
    - ***When at least one criterion is not met.***
- ***A criterion can specify whether unresolved values should be treated as a match or as unmatched. If this is not specified, and if, as a result, the condition cannot be evaluated, then the evaluation is stopped and the corresponding action(s) are not applied. If the rule does not specify what to do in case of an unresolvable property, then the action(s) are not applied, and access is allowed.***
- ***Endpoints that match the Main Rule are included in the policy inspection; endpoints that do not match the Main Rule are not inspected for the policy.***

- ***Endpoints are inspected against any defined Sub Rules, in order, until a match is found. If the endpoint does not match the requirements of Sub Rule, it is checked against the next Sub Rule. Once a match is found, the corresponding action(s) are applied to the endpoint and evaluation of the policy against the endpoint stops.***

].

FDP_ACF.1-1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***[***

- ***Allow access to specific endpoints if they have been defined as excluded from inspection in administrator defined Rule or Sub Rule Exceptions.***
- ***Allow access to endpoints defined in the Authentication Servers group. (NAC SFP Authentication Servers Allow).***
- ***Threat Protection SFP Manual Ignore state (Allow access) has precedence over:***
  - ***NAC SFP Manual Block***
  - ***NAC SFP Block***
- ***Virtual Firewall SFP Allow has precedence over:***
  - ***NAC SFP Manual Block***
  - ***NAC SFP Block***
- ***NAC SFP Authentication Server Allow has precedence over:***
  - ***NAC SFP Manual Block***
  - ***NAC SFP Block***
- ***NAC SFP Manual Allow has precedence over:***
  - ***NAC SFP Manual Block***
  - ***NAC SFP Block***

]***.***

FDP_ACF.1-1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules:

[

- ***Threat Protection SFP Block has precedence over:***
  - ***NAC SFP Authentication Servers Allow***
  - ***NAC SFP Manual Allow***
  - ***NAC SFP Allow***

- ***Virtual Firewall SFP Block has precedence over:***
  - ***NAC SFP Authentication Servers Allow***
  - ***NAC SFP Manual Allow***
  - ***NAC SFP Allow***

].

6.1.2.5 FDP_ACF.1-2 Security attribute based access control (Virtual Firewall)

Hierarchical to: No other components

Dependencies: FMT_MSA.3 Static attribute initialisation
FDP_ACC.1 Subset access control

FDP_ACF.1-2.1 The TSF shall enforce the ***[CounterACT Virtual Firewall SFP]*** to objects based on the following:

[

- ***subjects: endpoints***
- ***subject security attributes: Target IP, Target Service***
- ***objects: network domain***
- ***object security attributes: Source IP***

].

FDP_ACF.1-2.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

- ***The Appliance inspects the endpoints requesting access to the protected network for matches with the subject and object attributes defined by an Admin or Console User with 'Virtual Firewall' Permission. (see FMT_MSA.1-2.1 in Section 6.1.4.2 FMT_MSA.1-2 Management of security attributes (Virtual Firewall)).***
- ***If the Action attribute value has been defined as "Allow":***
  - ***The TOE will allow access to the network segments that match the values defined in the Source IP attribute to endpoints with addresses that match the values defined in the Target IP attribute and ports and protocols defined in the Target Service attribute.***
- ***If the Action attribute value has been defined as "Block":***
  - ***The TOE will deny access to the network segments that match the values defined in the Source IP attribute to endpoints with addresses that match the values defined in the Target IP attribute and ports and protocols defined in the Target Service attribute.***

].

FDP_ACF.1-2.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

- ***Threat Protection SFP Manual Ignore state (Allow access) has precedence over:***
  - ***Virtual Firewall SFP Block***
- ***Virtual Firewall SFP Allow has precedence over:***
  - ***Threat Protection SFP Block***

  - ***Virtual Firewall SFP Block***
  - ***NAC SFP Manual Block***
  - ***NAC SFP Block***

]**.**

FDP_ACF.1-2.4 The TSF shall explicitly deny access of subjects to objects based on the following rules:

[

- ***Virtual Firewall SFP Block has precedence over:***
  - ***NAC SFP Authentication Servers Allow***
  - ***NAC SFP Manual Allow***
  - ***NAC SFP Allow***

].

Application Note: Virtual Firewall rules are centrally managed. This means rules cannot be added, edited or removed from individual Consoles but must apply to all Appliances installed in the system.

6.1.2.6 FDP_ACF.1-3 Security attribute based access control (Threat Protection)

Hierarchical to:	No other components
Dependencies:	FMT_MSA.3 Static attribute initialisation FDP_ACC.1 Subset access control

FDP_ACF.1-3.1 The TSF shall enforce the ***[CounterACT Threat Protection SFP]*** to objects based on the following:

[

- ***subjects: endpoints***
- ***subject security attributes: SCAN Parameters, Bite Parameters, E-mail Worm Parameters, Service Attack Parameters, Manually Added Host Parameters as defined in FMT_MSA.1-3.1 (see Section 6.1.4.3 FMT_MSA.1-3 Management of security attributes (Threat Protection))***
- ***objects: network domain***
- ***object security attributes: ActiveResponse Range***

].

FDP_ACF.1-3.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

- ***The Appliance inspects the endpoints requesting access to the protected network for matches with the subject and object attributes defined by an Admin or Console User with 'IPS Policy Permission. (see FMT_MSA.1-3.1 in 6.1.4.3 FMT_MSA.1-3 Management of security attributes (Threat Protection)).***

- ***If a CounterACT Appliance detects signs that an endpoint is performing reconnaissance against the protected network, it will issue virtual resource information (a mark). If an endpoint uses a mark to gain access to the network (a bite event) and meets the defined Bite Parameters, the TOE will take the action(s) defined: Monitor, Port Block or Host Block; Notify.***
- ***If a CounterACT Appliance detects an endpoint issuing e-mail that passes the e-mail anomaly threshold as defined by the E-mail Worm Parameters, the TOE will take the action(s) defined: Monitor, Port Block or Host Block; Notify.***
- ***The CounterACT Appliance detects signs that an endpoint is performing reconnaissance against the protected network; it will check the defined Scan Parameters. If it detects that an endpoint has performed a specific probe a defined number of times within a defined time period (a scan) that matches the defined Scan Parameters, the TOE will take the action(s) defined: Monitor or Host Block; Notify.***
- ***The CounterACT Appliance will identify a service attack if a service is heavily probed by multiple hosts, The TOE determines if the service-probing criteria are met based on the size of the network and the defined Service Attack Parameters. If these parameters match the probes being performed by the hosts, the TOE will take the action(s) defined: Monitor, Port Block or Ignore; Notify, for all hosts at the attacked services only. The actions taken by the TOE when it detects a service attack can be customized to apply only to specific ports or port ranges.***
- ***The TOE will take the defined action(s): Host Block, Monitor or Ignore; Notify, when it detects an attempt to access the protected network from a Manually Added Host. Manually Added Hosts are defined by an Admin or Console User with 'IPS Policy' Permission through the Manually Added Host Parameters. Manually Added Hosts cannot be blocked at ports (Port Block).***
- ***If Enterprise Lockdown alerts have been enabled, then if one Appliance in the enterprise has detected event that meets the parameters defined, a lockdown will be sent to the other Appliances, alerting them of the source that performed the event. If the other Appliances detect that the source is communicating with the network they are protecting, the source will be automatically subject to the actions defined.***

].

FDP_ACF.1-3.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[

- ***Threat Protection SFP Manual Ignore state (Allow access) has precedence over:***
  - ***Threat Protection SFP Block***
  - ***Virtual Firewall SFP Block***
  - ***NAC SFP Manual Block***
  - ***NAC SFP Block***
- ***Virtual Firewall SFP Allow has precedence over:***
  - ***Threat Protection SFP Block***

].

FDP_ACF.1-3.4 The TSF shall explicitly deny access of subjects to objects based on the following rules:

[

- ***Threat Protection SFP Block has precedence over:***
    - ***NAC SFP Authentication Servers Allow***
    - ***NAC SFP Manual Allow***
    - ***NAC SFP Allow***

].

6.1.3 Class FIA: Identification and Authentication

6.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when ***[a maximum number configured by an Admin or Console User with 'User Management' Permission of]*** unsuccessful authentication attempts occur related to ***[user login attempts].***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met],*** the TSF shall ***[disable the user account for a pre-defined time period or until the account is reactivated by an Admin or Console User with 'User Management' Permission].***

6.1.3.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

- ***User Name***
- ***Password***
- ***Authentication Method***
- ***Console User (must be selected to have access to the CounterACT Console GUI)***
- ***Permissions***
- ***Password History***

].

6.1.3.3 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet ***[the password policy parameters set by an Admin or a Console User with 'User Management' Permission (See Table 6-5)].***

Table 6-5: Password Policy Rules

Parameter	Description
Minimum Password Length	Minimum number of characters required in all passwords. (cannot be set to less than 6)
Minimum Upper Case	Minimum number of upper case alphabetic characters required in all passwords.
Minimum Lower Case	Minimum number of lower case alphabetic characters required in all passwords.
Minimum Digits	Minimum number of numeric characters required in all passwords.
Minimum Special	Minimum number of special characters required in all passwords.
Expiration Time	Password expires after entered time
Number of Failures	Account will be locked after specified number of login failures
Lockout Period	Account will be locked for the specified time period after specified number of login failures
Password History Count	The number of previous passwords that are maintained for each user that cannot be reused (range is 0 to 100)

6.1.3.4 FIA_UAU_EXT.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.5 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only

[

- ***Enterprise Manager or CounterACT Appliance IP address or host name.***
- ***display of the typed in account name (username)***
- ***typed in password displayed as dots***

]

to the user while the authentication is in progress.

6.1.3.6 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSFmediated actions on behalf of that user.

6.1.4 Class FMT: Security Management

6.1.4.1 FMT_MSA.1-1 Management of security attributes (NAC)

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1-1.1 The TSF shall enforce the ***[CounterACT NAC SFP]*** to restrict the ability to ***[change_default, modify, delete]*** the security attributes ***[***

- ***Subject Attributes:***
    - ***Policy Name***
    - ***Policy Description***
    - ***Activation (defines when hosts will be inspected)***
    - ***Recheck (the conditions under which to recheck hosts that match the policy)***
    - ***Pause/Run Status (for the policy activation detection mechanism)***
    - ***Group(s) membership***
    - ***Policy Scope (range of IP Addresses or Segments)***
    - ***Conditions (one or more of the following connected by Boolean conditions)***
        - ***Authentication***
            - ***Authentication Login***
            - ***HTTP Confirmation Events***
            - ***Signed in Status***
        - ***Device Information***
            - ***Device Interface***
            - ***Device is NAT***
            - ***Device is DHCP Relay***
            - ***Device is DHCP Server***
            - ***DNS Name***
            - ***Domain User***
            - ***IP Address***
            - ***MAC Address***

  - *Member of Group*
  - *NIC Vendor*
  - *NetBIOS Domain*
  - *NetBIOS Hostname*
  - *Nmap – Network Function*
  - *Nmap – OS Class*
  - *Nmap – OS Fingerprint*
  - *Nmap Service version*
  - *Number of IP Addresses*
  - *Open Ports*
  - *Traffic seen*
- *Events*
  - *ARP Spoofing*
  - *Admission*
  - *Malicious Event*
  - *Sessions as Client/Serve*
- *Guest Properties*
  - *Guest Approved By*
  - *Guest Registration Status*
  - *Guest Registration Information - comment*
  - *Guest Registration Information - company*
  - *Guest Registration Information - name*
  - *Guest Registration Information – location*
  - *Guest Registration Information – title*
  - *Guest Registration Login Name*
- *LDAP Attributes*
- *LinuxOS*
  - *Linux Expected Script Result*
  - *Linux File Exists*
  - *Linux File Size*
  - *Linux File Date*
  - *Linux Hostname*
  - *Linux Logged-in User*
  - *Linux Manageable (SecureConnector)*
  - *Linux Manageable (SSH)*
  - *Linux Process Running*
  - *Linux Operating System*
- *Macintosh OS*
  - *Macintosh Expected Script Result*
  - *Macintosh File Date*
  - *Macintosh File Exists*
  - *Macintosh File Size*
  - *Macintosh Hostname*
  - *Macintosh Logged-in User*
  - *Macintosh Manageable (SecureConnector)*
  - *Macintosh Manageable (SSH)*

    - ***Macintosh Process Running***
    - ***Macintosh Software Updates Missing***
    - ***Macintosh OS Version***
- ***SNMP***
    - ***SNMP MIB-II IF Number***
    - ***SNMP MIB-II Sys Description***
    - ***SNMP MIB-II Sys Location***
    - ***SNMP MIB-II System Name***
    - ***SNMP MIB-II Sys Up Time***
    - ***SNMP OID Value***
- ***Switch***
    - ***Switch IP***
    - ***Switch Location***
    - ***Switch Vendor***
    - ***Switch VoIP Port***
    - ***Switch Port Description***
    - ***Switch Port Hosts (number of Hosts on Port)***
    - ***Switch Port Status***
    - ***Switch Port VLAN***
    - ***Switch Port VLAN Name***
    - ***Switch Port Voice VLAN***
    - ***Switch Port Trunk***
- ***Track Change Events***
- ***Windows Applications***
    - ***Applications Installed***
    - ***Instant Messaging Installed***
    - ***Instant Messaging Running***
    - ***Peer-to-Peer Installed***
    - ***Peer-to-Peer Running***
- ***Windows OS***
    - ***Domain Member***
    - ***Expected Script Result***
    - ***External Device Connected***
    - ***External Device Connected (by class)***
    - ***File Date***
    - ***File Exists***
    - ***File Size***
    - ***File Version***
    - ***Is Logged-in***
    - ***Manageable (SecureConnector)***
    - ***Manageable (Domain)***

- ***Manageable (Local)***
- ***Process Running***
- ***Registry Key Exists***
- ***Registry Key Value***
- ***Service Installed***
- ***Service Running***
- ***Shared Directory***
- ***USB Device Information***
- ***Windows OS Version***

- ***Windows Security***
  - ***AntiSpyware Detected***
  - ***AntiVirus Running***
  - ***AntiVirus Installed***
  - ***AntiVirus Update Date***
  - ***Hotfix Installed***
  - ***Microsoft Vulnerabilities***
  - ***Personal Firewall***

- ***Object Attributes:***
  - ***Scope (policy scope)***
- ***Actions (one or more of the following):***
  - ***Authentication Actions***
    - ***HTTP Login***
  - ***Management Actions***
    - ***Add to Group***
    - ***HTTP Host Local Login***
    - ***SecureConnector Start/Stop***
  - ***Notification Actions***
    - ***HTTP Notification Action***
    - ***HTTP Redirection***
    - ***Send E-mail Action***
    - ***Send E-mail to User***
    - ***Instant Notification***
  - ***Remediation Actions***
    - ***Disable USB Devices***

        - ***Kill Instant Messaging Applications***
        - ***Kill Peer to Peer***
        - ***Kill Process on Windows***
        - ***Kill Process on Linux and Macintosh***
        - ***Start Macintosh Updates***
        - ***Windows Self-Remediation***
        - ***Start Windows Updates***
        - ***Run Script Action on Windows***
        - ***Run Script Action on Macintosh and Linux***
        - ***Set Registry Key Action***
        - ***Start AntiVirus on Windows***
        - ***Update AntiVirus on Windows***
    - ***Restriction Actions***
        - ***Assign to VLAN***
        - ***Switch Block***
        - ***Virtual Firewall Block Action***

]

to ***[Admin, Console User with 'NAC Policy' Permission].***

6.1.4.2 FMT_MSA.1-2 Management of security attributes (Virtual Firewall)

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1-2.1 The TSF shall enforce the ***[CounterACT Virtual Firewall SFP]*** to restrict the ability to ***[change_default, modify, delete]*** the security attributes ***[***

- ***Subject Attributes:***
    - ***Target IP : All, Addresses, or Network Segment***
    - ***Target Service: All (all services), Single (port and protocol), or List***
- ***Object Attributes:***
    - ***Source IP: All, Addresses, or Network Segment***
- ***Actions:***

    - ***Block or Allow***

]

to ***[Admin, Console User with 'Virtual Firewall' Permission].***

6.1.4.3 FMT_MSA.1-3 Management of security attributes (Threat Protection)

Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1-3.1 The TSF shall enforce the ***[CounterACT Threat Protection SFP]*** to restrict the ability to ***[change_default, modify, delete]*** the security attributes ***[***

- ***Subject Attributes:***
    - ***Scan Parameters***
        - ***Scan Type***
        - ***Scan Details***
            - ***Scan Method***
            - ***Probe Count***
            - ***Probe Interval (time span)***
    - ***Bite Parameters***
        - ***Bite Type***
        - ***Bite Type Details***
            - ***Mark Type***
    - ***E-mail Worm Parameters***
        - ***Amount***
        - ***Attachment Format***
        - ***Sender***
        - ***Recipient***
        - ***E-mail Worm Frequency Details***
            - ***Anomaly Type***
            - ***Count***
            - ***Duration***
    - ***Service Attack Parameters***
        - ***Service Attack Type (TCP/UDP)***

        - ***Service Attack Details***
            - ***Number of Hosts***
            - ***Duration***
    - ***Manually Added Host Parameters***
        - ***Host IP address***
        - ***Host's State: Host Blocked, Monitored, or Ignored.***
        - ***Blocked Ports***
        - ***State Duration***

- ***Object Attributes:***
    - ***ActiveResponse Range***
- ***Actions:***
    - ***Ignore, Host Block, Port Block, or Monitor; Notify***

]

to [Admin, Console User with ' IPS Policy' Permission].

Application Note: Enterprise Lockdown is a feature of host/port block, where all CounterACT appliances in a multi-appliance configuration participate in the blocking actions, and is not an operation on its own. It is enabled by default.

6.1.4.4 FMT_MSA.3-1 Static attribute initialization (NAC)

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3-1.1 The TSF shall enforce the ***[CounterACT NAC SFP]*** to provide ***[permissive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3-1.2 The TSF shall allow the ***[Admin, Console User with 'NAC Policy' Permission]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5 FMT_MSA.3-2 Static attribute initialization (Virtual Firewall)

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3-2.1 The TSF shall enforce the ***[CounterACT Virtual Firewall SFP]*** to provide ***[permissive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3-2.2 The TSF shall allow the ***[Admin, Console User with 'Virtual Firewall' Permission]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.6 FMT_MSA.3-3 Static attribute initialization (Threat Protection)

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3-3.1 The TSF shall enforce the ***[CounterACT Threat Protection SFP]*** to provide ***[permissive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3-3.2 The TSF shall allow the ***[Admin, Console User with 'IPS Policy' Permission]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.7 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[operations as specified in Table 6-6*** Table 6-6***]*** the ***[TSF data as specified in Table 6-6*** Table 6-6***]*** to ***[user security role as in Table 6-6*** Table 6-6***].***

Table 6-6: Management of TSF Data

User Security Role/Permission	Operations	TSF Data
Admin	Start, stop SecureConnector	N/A
	Create, modify, delete	Channels
	Create, modify, delete	Console Access List
	Configure	Console Memory
	Modify	E-mail Parameters
	Configure	External User Directory Authentication Parameters
	Create, modify delete	Registered Guests
	Configure	Guest Sign-in Page Guest Registration Page Guest Access Approval Messages
	Configure	Guest Authentication Servers
	Generate	Guest Registration codes
	Create, modify, delete	Host Discovery Rules
	Delete host	Host Management List
	Configure	HTTP Proxy Parameters
	Configure	Internal Network
	Create, modify, delete	IP Segments
	Configure	Kerberos Authentication Parameters
	View, release	Locked-Out Users

User Security Role/Permission	Operations	TSF Data
	Define	Network Viewing Permissions
	View	System Health Information
	Create, modify, delete	Web Access List
	All Operations listed below	All TSF Data Listed Below
All Console Users	View	Host Log
Console User with the Permission listed below:		
Audit Trail	View, create, search	Audit Trail Reports
Backup	Backup	CounterACT System Settings
CounterACT Appliance Configuration	Modify	Appliance Configuration Parameters
CounterACT Appliance Control	Restart, start, stop CounterACT Appliances	N/A
	View, create, modify, delete	Mark Naming Rules
Event Log	View, sort, search	System Event Log
Legitimate Traffic	View, create, modify, delete	Legitimate Network Traffic Rules
License Management	Install, manage	CounterACT Licenses
Malicious Traffic	View	Malicious Traffic
Manual State Override	Modify	Host Threat Protection State
	Modify	Host Threat Protection State Maintenance Time
Multiple CounterACT Appliance Management	Manage multiple network Appliances	N/A
NAC Policy Management	View, create, modify, delete, export, import	NAC Policies
	View, modify	NAC Policy Log
	Add, edit	Network Segments and Groups
NAC Policy Status Control	Start, stop, pause, test	NAC Policies, NAC Policy Actions
	Run ‘clear all’, ‘run now’ and ‘summary’ NAC Policy options.	N/A
Operation Mode	Modify	CounterACT System Operation Mode
Plugin Management	Modify	Plugin Configuration Parameters
Plugin Operational	Start, stop, test Plugins	N/A
Reports	Generate, modify, view	Reports
Scheduled Reports	Generate, modify, view	Scheduled Reports
SNMP Configuration	Modify	SNMP Configuration Parameters
Threat Protection Policy	View, create, modify, delete	Threat Protection Policies
	Start, stop	Threat Protection Policies, Threat Protection Policy Actions
	View	Service Attack History
User Management	View, create, modify, delete	User Accounts
	Modify	Password Policy
Virtual Firewall	View, create, modify, delete	Virtual Firewall Policies
	Start, stop	Virtual Firewall Policies, Virtual Firewall Policy Actions
	View	Blocking Log
Vulnerability Assessment	View, create, modify, delete	Vulnerability Scan Parameters
	View, delete	Vulnerability Scan Results
	Run Vulnerability Scans	N/A

6.1.4.8 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[operations as specified in Table 6-6***Table 6-6***].***

6.1.4.9 FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[***

- ***Admin***
- ***Console User***

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: The product also supports the role: "Asset Portal User", however, the Assets Portal component is not included in the TOE.

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from ***[disclosure, modification]*** when it is transmitted between separate parts of the TOE.

6.1.6 Class SSC: Vulnerability scans management (Explicitly Stated)

6.1.6.1 SSC_ACT_EXT.1 Vulnerability scans remediation actions

Hierarchical to: No other components

Dependencies: SSC_ANL_EXT.1 Vulnerability scans analysis

SSC_ACT_EXT.1.1 The TSF shall take

[

One or more of the following actions as indicated in the CounterACT NAC SFP:

- ***Send E-mail, Instant Notification or HTTP Notification to Network Users indicating that Specific Vulnerabilities were Detected***

- ***Disable USB Devices***
- ***Kill Instant Messaging Applications***
- ***Kill Peer to Peer Applications***
- ***Kill a Process on Windows System***
- ***Kill a Process on Linux and Macintosh System***
- ***Start Macintosh Updates for Vulnerability Remediation***
- ***Start Windows Updates for Vulnerability Remediation***
- ***Run Script Action on Windows***
- ***Run Script Action on Macintosh and Linux***
- ***Set Registry Key Action***
- ***Start AntiVirus on Windows***
- ***Update AntiVirus on Windows***
- ***Assign Vulnerable Device to VLAN***
- ***Block a Switch Port (no traffic is allowed through)***
- ***Virtual Firewall Action (block access to and from detected hosts)***
- ***HTTPS Redirection (network users will see a security alert at their desktop Web browser when they attempt to access the Web)***

]

upon detection of a vulnerability in a network device that has been scanned.

6.1.6.2 SSC_ANL_EXT.1 Vulnerability scans analysis

Hierarchical to: No other components.

Dependencies: SSC_SCN_EXT.1 Vulnerability scanning

SSC_ANL_EXT.1.1 The TSF shall be able to apply a set of rules in analyzing the data collected from the endpoints during vulnerability scanning and based upon these rules indicate a vulnerability in those devices.

SSC_ANL_EXT.1.2 The TSF shall enforce the following rules for ***[data collected by vulnerability scans as listed in SSC_SCN_EXP.1]*** known to indicate a device vulnerability: ***[perform remediation actions as indicated in SSC_ACT_EXT.1]***

6.1.6.3 SSC_SCN_EXT.1 Vulnerability scanning

Hierarchical to: No other components

Dependencies: No dependencies

SSC_SCN_EXT.1.1 The TSF shall be able to perform scans to collect the following information from the endpoints on the protected network

[

In addition to the information collected as indicated by the NAC policy (only applies to endpoints that run Windows or MacOS):

- ***Open Services Detected***
- ***Vulnerability Detected***
    - ***Name***
    - ***Category***
    - ***Description***
    - ***Update Time***
    - ***Severity***
    - ***Patch***
    - ***Related Service***
    - ***Reboot required after patch installation***

]

that may indicate a vulnerability in those devices.

6.2 Security Assurance Requirements for the TOE

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) taken from Part 3 of the Common Criteria augmented with ALC_FLR.2. None of the assurance components are refined. The assurance components are listed in Table 6-7.

Table 6-7: EAL4+ Assurance Components

Assurance Class	**Assurance Components**	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4.	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

6.2.1 Class ADV: Development

6.2.1.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1 4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.2 ADV_FSP.4 Complete functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.4.1C The functional specification shall completely represent the TSF.

ADV_FSP.4.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.4.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.4.4C The functional specification shall describe all actions associated with each TSFI.

ADV_FSP.4.5C The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.

ADV_FSP.4.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.4.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.1.3 ADV_IMP.1 Implementation representation of the TSF

Dependencies: ADV_TDS.3 Basic modular design

ALC_TAT.1 Well-defined development tools

Developer action elements:

ADV_IMP.1.1D The developer shall make available the implementation representation for the entire TSF.

ADV_IMP.1.2D The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.

Content and presentation elements:

ADV_IMP.1.1C The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be in the form used by the development personnel.

ADV_IMP.1.3C The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that, for the selected sample of the implementation representation, the information provided meets all requirements for content and presentation of evidence.

6.2.1.4 ADV_TDS.3 Basic modular design

Dependencies: ADV_FSP.4 Complete functional specification

Developer action elements:

ADV_TDS.3.1D The developer shall provide the design of the TOE.

ADV_TDS.3.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.3.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.3.2C The design shall describe the TSF in terms of modules.

ADV_TDS.3.3C The design shall identify all subsystems of the TSF.

ADV_TDS.3.4C The design shall provide a description of each subsystem of the TSF.

ADV_TDS.3.5C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.3.6C The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

ADV_TDS.3.7C The design shall describe each SFR-enforcing module in terms of its purpose and interaction with other modules.

ADV_TDS.3.8C The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with and called interfaces to other modules.

ADV_TDS.3.9C The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

ADV_TDS.3.10C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

Evaluator action elements:

ADV_TDS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.3.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.2 Class AGD: Guidance documents

6.2.2.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 Class ALC: Life-cycle support

6.2.3.1 ALC_CMC.4 Production support, acceptance procedures and automation

Dependencies: ALC_CMS.1 TOE CM coverage

ALC_DVS.1 Identification of security measures

ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.4.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.4.2D The developer shall provide the CM documentation.

ALC_CMC.4.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C The TOE shall be labeled with its unique reference.

ALC_CMC.4.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.4.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

ALC_CMC.4.5C The CM system shall support the production of the TOE by automated means.

ALC_CMC.4.6C The CM documentation shall include a CM plan.

ALC_CMC.4.7C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.4.8C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.4.9C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.2 ALC_CMS.4 Problem tracking CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.4.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.4.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

ALC_CMS.4.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.4.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies

Developer action elements:

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.4 ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

6.2.3.5 ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

6.2.3.6 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies

Developer action elements:

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users' reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.7 ALC_TAT.1 Well-defined development tools

Dependencies: ADV_IMP.1 Implementation representation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify each development tool being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of each development tool.

Content and presentation elements:

ALC_TAT.1.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

ALC_TAT.1.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4 Class ATE: Tests

6.2.4.1 ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.2 ATE_DPT.1 Testing: basic design

Dependencies: ADV_ARC.1 Security architecture description

ADV_TDS.2 Architectural design

ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.3 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.4 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.5 Class AVA: Vulnerability assessment

6.2.5.1 AVA_VAN.3 Focused vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.3 Basic modular design

ADV_IMP.1 Implementation representation of the TSF

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.3.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.3.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.3.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

AVA_VAN.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential.

6.3 Security Requirements Rationale

6.3.1 Dependencies Satisfied

Table 6-8 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 6-8: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	Operational Environment *	N/A
2	FAU_SAR.1	Audit Review	FAU_GEN.1	1
3	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	2
5	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
6	FDP_ACC.1-1	Subset access control (NAC)	FDP_ACF.1	9
7	FDP_ACC.1-2	Subset access control (Virtual Firewall)	FDP_ACF.1	10
8	FDP_ACC.1-3	Subset access control (Threat Protection)	FDP_ACF.1	11
9	FDP_ACF.1-1	Security attribute based access control (NAC)	FMT_MSA.3	21
			FDP_ACC.1	6
10	FDP_ACF.1-2	Security attribute based access control (Virtual Firewall)	FMT_MSA.3	22
			FDP_ACC.1	7
11	FDP_ACF.1-3	Security attribute based access control (Threat Protection)	FMT_MSA.3	23
			FDP_ACC.1	8
12	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	15 (H)
13	FIA_ATD.1	User attribute definition	None	N/A
14	FIA_SOS.1	Verification of secrets	None	N/A
15	FIA_UAU_EXT.2	User authentication before any action	FIA_UID.1	17 (H)
16	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	15 (H)
17	FIA_UID.2	User identification before any action	None	N/A
18	FMT_MSA.1-1	Management of security attributes (NAC)	FDP_ACC.1 or FDP_IFC.1	6
			FMT_SMR.1	26
			FMT_SMF.1	25
19	FMT_MSA.1-2	Management of security attributes (Virtual Firewall)	FDP_ACC.1 or FDP_IFC.1	7
			FMT_SMR.1	26
			FMT_SMF.1	25
20	FMT_MSA.1-3	Management of security attributes (Threat Protection)	FDP_ACC.1 or FDP_IFC.1	8
			FMT_SMR.1	26
			FMT_SMF.1	25
21	FMT_MSA.3-1	Static attribute initialization (NAC)	FMT_MSA.1	18
			FMT_SMR.1	26
22	FMT_MSA.3-2	Static attribute initialization (Virtual Firewall)	FMT_MSA.1	19
			FMT_SMR.1	26
23	FMT_MSA.3-3	Static attribute initialization (Threat Protection)	FMT_MSA.1	20
			FMT_SMR.1	26
24	FMT_MTD.1	Management of TSF data	FMT_SMR.1	26

Ite m	SFR ID	SFR Title	Dependencies	Item Reference
			FMT_SMF.1	25
25	FMT_SMF.1	Specification of Management Functions	None	N/A
26	FMT_SMR.1	Security roles	FIA_UID.1	17 (H)
27	FPT_ITT.1	Basic internal TSF data transfer protection	None	N/A
29	SSC_ACT_EXT.1	Vulnerability scans remediation actions	SSC_ANL_EXT.1	30
30	SSC_ANL_EXT.1	Vulnerability scans analysis	SSC_SCN_EXT.1	31
31	SSC_SCN_EXT. 1	Vulnerability scanning	None	N/A

* Reliable timestamps for use by the audit functions are provided by an external time server in the Operational Environment (OE.Time).

6.3.2 Functional Requirements

Table 6-9 traces each SFR back to the security objectives for the TOE.

Table 6-9: Requirements vs. Objectives Mapping

	O.Admin	O.Audit	O.IDAuth	O.IDProtect	O.Integrity	O.NetworkAccess	O.Scanning	O.TOEAccess
FAU_GEN.1		X						
FAU_SAR.1	X							
FAU_SAR.2								X
FAU_SAR.3	X							
FAU_STG.1					X			
FDP_ACC.1-1						X		
FDP_ACC.1-2						X		
FDP_ACC.1-3						X		
FDP_ACF.1-1						X		
FDP_ACF.1-2						X		
FDP_ACF.1-3						X		
FIA_AFL.1				X				
FIA_ATD.1			X					
FIA_SOS.1				X				
FIA_UAU_EXT.2			X					X
FIA_UAU.7				X				
FIA_UID.2			X					X
FMT_MSA.1-1	X					X		X
FMT_MSA.1-2	X					X		X
FMT_MSA.1-3	X					X		X
FMT_MSA.3-1	X					X		X
FMT_MSA.3-2	X					X		X
FMT_MSA.3-3	X					X		X
FMT_MTD.1	X							X
FMT_SMF.1	X							
FMT_SMR.1			X					X
FPT_ITT.1					X			
SSC_ACT_EXT.1							X	
SSC_ANL_EXT.1							X	
SSC_SCN_EXT.1							X	

O.Admin: The TOE must include a set of functions that allow effective management of its functions and data.

The TOE is required to provide a set of administrative functions for authorized users [FMT_MTD.1, FMT_SMF.1]. The TOE must provide the ability to review and manage the audit trail of the system [FAU_SAR.1, FAU_SAR.3]. The TOE must also provide authorized users with the capability to set the parameters of the Network Access Control policies [FMT_MSA.1-1, FMT_MSA.1-2, FMT_MSA.1-3, FMT_MSA.3-1, FMT_MSA.3-2, FMT_MSA.3-3].

O.Audit: The TOE must record audit records for data accesses and use of the system functions.

> The TOE is required to generate audit records of security relevant events, including: system generated events, use of the administrative functions, and attempted access of the protected network [FAU_GEN.1].

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

> Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU_EXT.2]. Security attributes of users must be defined to enforce the authentication policy of the TOE [FIA_ATD.1]. The TOE must be able to recognize the different administrative roles that exist for the TOE [FMT_SMR.1].

O.IDProtect: The TOE must provide mechanisms to protect user identification and authentication.

> The TOE is required to enforce a password policy to support strong passwords [FIA_SOS.1], support authentication failure handling on user login [FIA_AFL.1] and mask the user's authentication data on login [FIA_UAU.7]

O.Integrity: The TOE must ensure the integrity of all audit and system data.

> The TOE is required to protect the audit data from modification and unauthorized deletion [FAU_STG.1]. The TOE must also protect data being transferred between TOE components from disclosure and modification [FPT_ITT.1].

O.NetworkAccess: The TOE must control access to the protected network based on security policies and the attributes of the endpoints attempting access to the protected network.

> The TOE is required to control access to the protected network based on Network Access Control policies and the attributes of the endpoints attempting access. The TOE must support the NAC Policy [FDP_ACC.1-1, FDP_ACF.1-1, FMT_MSA.1-1, FMT_MSA.31], the Virtual Firewall Policy [FDP_ACC.1-2, FDP_ACF.1-2, FMT_MSA.1-2, FMT_MSA.32], and the Threat Protection Policy [FDP_ACC.1-3, FDP_ACF.1-3, FMT_MSA.1-3, FMT_MSA.3-3].

O.Scanning: The TOE must support the detection and remediation of potential vulnerabilities on the endpoints attempting access to the protected network by collecting and analyzing configuration data from those devices.

> The TOE is required to conduct vulnerability scans. The TOE must collect configuration data from endpoints attempting network access [SSC_SCN_EXT.1], analyze the collected data [SSC_ANL_EXT.1] and perform administrator configured remediation actions if a potential vulnerability is detected [SSC_ACT_EXT.1].

O.TOEAccess: The TOE must allow authorized users to access only appropriate TOE functions and data.

> The TOE must support access to management functions based on administrative roles. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU_EXT.2]. Once authenticated, the users have access to TOE functions and data based on their assigned administrative role [FMT_SMR.1]. The TOE must allow access to the functions and data provided by the administrative GUI (including creation and modification of the Network Access Control policies) only to users with the proper administrative role and permissions [FMT_SMR.1, FMT_MTD.1, FMT_MSA.1-1, FMT_MSA.1-2, FMT_MSA.1-3, FMT_MSA.3-1, FMT_MSA.3-2, FMT_MSA.3-3]. The TOE is also required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2].

6.3.3 Assurance Rationale

Evaluation Assurance Level 4 (EAL) 4+ was chosen because it provides appropriate assurance measures for the expected application of the product. EAL4+ ensures a product is methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It also requires a moderate to high level of independently assured security. The security assurance requirement AVA_VAN.3 includes an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of Enhanced-Basic.

As appropriate for selection of EAL4+ for the expected uses of the TOE, some confidence in correct operation is required, but the threats to security are not viewed as serious. Independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

7 TOE Summary Specification

7.1 IT Security Functions

Section 7.1 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section **Error! Reference source not found.**: Logical Scope of the TOE.

The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Functions	Sub-Functions	SFRs
Security Audit	AU-1 Audit Generation	FAU_GEN.1
	AU-2 Audit Review	FAU_SAR.1
		FAU_SAR.2
		FAU_SAR.3
	AU-3 Audit Protection	FAU_STG.1
Network Access Control	NAC-1 NAC Policy	FDP_ACC.1-1
		FDP_ACF.1-1
		FMT_MSA.1-1
		FMT_MSA.3-1
	NAC-2 Virtual Firewall Policy	FDP_ACC.1-2
		FDP_ACF.1-2
		FMT_MSA.1-2
		FMT_MSA.3-2
	NAC-3 Threat Protection Policy	FDP_ACC.1-3
		FDP_ACF.1-3
		FMT_MSA.1-3
		FMT_MSA.3-3
User Identification and Authentication	IA-1 User Security Attributes	FIA_ATD.1
	IA-2 User Identification & Authentication	FIA_UAU_EXT.2
		FIA_UID.2
	IA-3 User Login Security	FIA_AFL.1
		FIA_SOS.1
		FIA_UAU.7
Security Management	SM-1 Management Functions	FMT_MTD.1
		FMT_SMF.1
	SM-2 Management Security Roles	FMT_SMR.1
Protection of Security	PT-1 Internal Data Transfer Protection	FPT_ITT.1
Vulnerability Scanning	SC-1 Vulnerability Scanning	SSC_SCN_EXT.1
	SC-2 Scanning Analysis	SSC_ANL_EXT.1
	SC-3 Scanning Actions	SSC_ACT_EXT.1

7.1.1 Security Audit Functions

7.1.1.1 AU-1: Audit Generation

(FAU_GEN.1)

The CounterACT Appliance and Enterprise Manager generate audit records of security significant as specified in Table 6-2: Auditable Events. The fields recorded for each of logs are specified in Table 6-3: Audit Record Information.

The TOE maintains three audit logs to record security significant events:

Host Log

The Host Log is used to investigate the activity of specific hosts, and display information about how CounterACT handled those hosts. The log displays information about hosts as they are detected and is continuously updated.

System Event Log

The System Event Log is records information about system activity, for example: successful and failed administrator authentication attempts.

User Audit Trail

The User Audit Trail records information concerning TOE user activity. These logs list for example, the user name of the administrator that updated a policy, stopped or started CounterACT, or updated user passwords. The logs give additional information about the activity, such as the date of the activity and the IP address from which it was carried out.

7.1.1.2 AU-2: Audit Review

(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The CounterACT Console allows only authenticated users with the necessary permissions to view, sort and search the audit records of the three audit logs: Host Log, System Event Log and User Audit Trail.

7.1.1.3 AU-3: Audit Protection

(FAU_STG.1)

As described in Section 7.1.1.2 AU-2: Audit Review, above, access to the audit records is only available through the management interfaces and is limited to only those authenticated users with the necessary roles and permissions. The management interfaces do not allow the audit records to be modified or deleted. Users may clear events from the Console display; however the Event Viewer and the Audit Trail logs maintain information about the cleared events. The audit records are also protected by the access control mechanisms of the DBMS and the OS of the CounterACT Appliances and the Enterprise Manager,

Since the audit function starts automatically with the TOE, and cannot be disabled, all system and TOE user actions are recorded as specified in FAU_GEN.1.

The TOE maintains an audit record limit that, when reached, records new audit event data over the oldest (FIFO). The audit records are not backed up automatically. It is recommended to export the audit logs to an external system using syslog to avoid losing this data.

7.1.2 Network Access Control Functions

7.1.2.1 NAC-1: NAC Policy

(FDP_ACC.1-1, FDP_ACF.1-1, FMT_MSA.1-1, FMT_MSA.3-1)

The TSF enforces three types of Network Access Control: NAC Policies, Virtual Firewall Policies and Threat Protection Policies. The following hierarchies, from highest to lowest, are applied when a host is detected as a result of different policies:

- Threat Protection SFP Manual Ignore state (Allow access)
- Virtual Firewall SFP Allow
- Threat Protection SFP Block
- Virtual Firewall SFP Block
- NAC SFP Authentication Servers Allow
- NAC SFP Manual Allow
- NAC SFP Allow
- NAC SFP Manual Block
- NAC SFP Block

This section specifies how the TOE enforces the first of the three, NAC Policies. NAC Policies are multi-purpose and are of the most importance to the CounterACT user.

An authenticated user with the necessary permission can define NAC Policies to initiate host inspection; specify conditions under which CounterACT should respond to hosts, and define actions to take at hosts that match or do not match the policy requirements.

By default, hosts are inspected by NAC policies every two hours and on any admission event (a network event that indicate the admission of an endpoint into the network.)

NAC policies are defined and managed from the NAC Policy Manager dialog box of the Console interface. The following information appears in the NAC Policy Manager for each policy:

- Pause/Run Status - Indicates if the new policy activation detection mechanism is paused or running. When paused, new policy activation events are ignored.
- Name - The name assigned to the policy.
- Description - The policy description.
- Activation - The parameters defining when hosts will be inspected.
- Condition - The properties inspected on hosts, i.e., specific OS systems, Anti-Virus Updates, registry information, etc.
- Scope - The host or group of hosts that will be inspected for this policy.

- Actions - Measures taken at the host if it matches the policy.
- Recheck - The conditions under which to recheck hosts that match the policy.
- Sub Rules - Instructions to CounterACT regarding how the host should be inspected and handled. Sub rules allow automatic follow-up with hosts after initial detection and handling. Creating sub rules combines separate detection and actions into one automated sequence. These rules are carried in order until a match is found. Once a match is found, the corresponding action is applied to the host and further inspection is stopped. If the host does not match the requirements of the inspection, it is moved to the next inspection rule.

After creating and editing policies, they must be applied from the NAC Policy Manager. This activates all policies.

NAC Policy Templates

CounterACT is delivered with ready-to-use NAC policy templates can that be used to quickly create common NAC policies. Templates are structured as follows:

- A predefined policy name and description
- A policy scope (the hosts that are inspected)
- Conditions - Instructions to CounterACT regarding what host properties to look for
- Actions - Instructions regarding measures to take at endpoints, if those properties are found or not found

The following NAC Policy Templates are included with the product:

Table 7-2: Included NAC Policy Templates

Template Category	Policy Template	Description
Classification	Asset Classification Template (e.g. Windows, Linux , Printers, VoIP)	Creates policies that detect network devices according to these classifications. Discovered hosts are placed in CounterACT groups that are displayed in the Console, Filters section.
	External Device Classification Template (e.g. mass storage devices, disk drives, modems)	
	Virtual Machine Template (e.g. VMware)	
Corporate/Guest Control	Corporate/Guest Control Template	Creates a policy that detects and classifies the network into the following CounterACT groups: • Corporate hosts • Signed in guests • Unauthorized hosts The policy can be defined so that unauthorized hosts are prompted to sign in with valid credentials or register to the network as guests by providing identity information. Options are also available to allow unauthorized hosts to skip the registration process and enter the network with limited access.

Template Category	Policy Template	Description
Compliance	Individual Compliance Templates: • Antivirus • Peer to Peer • Personal Firewall • Instant Messaging	Generate compliance policies, understand the compliance level at the network, guide users to compliance, remediate endpoints
	Macintosh Update Compliance Template	
	Overall Endpoint Compliance Template	
Threats	Malicious Host Template	Detect and remediate threats to the network by enforcing policies against a range of widely used techniques.
	ARP Spoofing Template	
	Impersonation Template	
	Dual Homed Template	
Track Changes	Track Changes Templates: • Application • Host Name • Hardware • Operating System • Shared Folder • Switch • User • Windows Service • New TCP/IP Port	Track changes within the network in order to identify unauthorized changes and remediate possible threats

NAC Custom Policies

Custom policy tools are provided to create NAC policies not covered by NAC templates. Policies are composed of the following elements which are defined by the administrator:

- A unique policy name.
- A policy scope – the range of IP addresses or segments to be inspected for this policy.
- A policy main rule - Hosts that match the main rule are included in the policy inspection. Hosts that don't match this rule are not inspected for this policy.
- Policy sub rule(s) - Sub rules are carried in order until a match is found. Once a match is found, the corresponding action is applied to the host. If the host does not match the requirements of the sub rule, it is moved to the next rule.

Main rules and sub rules consists of:

- A condition - One set of properties that is queried when evaluating hosts.
- Actions - CounterACT measures taken at network hosts

Main rules and sub rules may also contain:

- Exceptions - to exclude specific hosts from inspection.
- Recheck instructions - How often hosts are rechecked that match a policy and under what conditions to perform recheck. By default, hosts are rechecked every 30 minutes, and on any admission event.

Conditions

A condition is pre-defined set of host properties and Boolean relations connecting them — for example, hosts running Windows XP with outdated Symantec anti-virus applications. Administrators can specify CounterACT to apply a policy action to hosts that match (or do not match) the defined conditions criteria. Each condition provides an option to specify which criteria must be met in order for the host to match the policy. Because a condition may include several criteria, a match can be defined to occur when:

- all criteria are met
- none of the criteria are met
- any criterion is met
- at least one criterion is not met

A list of conditions that may be used in the NAC Policy is given in Section 6.1.4.1FMT_MSA.1-1 Management of security attributes (NAC) and a more detailed explanation of each condition is given in p162 – 174 of [USER]. Not all conditions apply to all types of endpoints; please see the details in [USER].

Actions

Actions are measures taken at network endpoints ranging from notices, warnings and alerts to remediation processes, access restrictions and complete blocking. Actions can be incorporated into NAC policies or applied manually on selected network endpoints. Action schedules can be assigned to each NAC Policy action. The Host Details dialog box on the Console interface provides specific information about NAC actions carried out on detected hosts. This information can be viewed from the Control Center once the host has been detected via the NAC Policy. A list of actions that can be assigned when conditions are met is given in Section 6.1.4.1FMT_MSA.1-1 Management of security attributes (NAC). A more detailed explanation of each action is given in p174 – 213 of [USER]. Not all actions apply to all types of endpoints; please see the details in [USER].

Action Thresholds

An action threshold is the maximum percentage of hosts that can be controlled by a specific action type defined at a single Appliance. Action thresholds are designed to automatically implement safeguards when rolling out blocking and restrictive action across your network. For example, if multiple policies that use a blocking action, e.g. Virtual Firewall or Switch block action, have been defined then if an extensive number of hosts matches these policies, more network hosts may be blocked than anticipated.

Threshold policy exceptions can also be created, i.e., policies that are excluded from action threshold calculations. For example, all thresholds when working with policies that handle outside contractors can be excluded.

7.1.2.2 NAC-2: Virtual Firewall Policy

(FDP_ACC.1-2, FDP_ACF.1-2, FMT_MSA.1-2, FMT_MSA.3-2)

The second of the three types of Network Access Control policies enforced by the TSF is the CounterACT Virtual Firewall Policy. An authenticated user with the necessary permission can define a Virtual Firewall Policy to:

- Create network zones or segments that will be closed off entirely as a result of new threats or newly detected vulnerabilities.

- Create network zones or segments that that will be closed off to specific sources.
- Prevent unwanted protocols from being transmitted within the network or between specific network segments.
- Designate business critical services that should always remain open.

Virtual Firewall Policies can be created, deleted and modified by an authenticated user with the necessary permission via the CounterACT Console. A Virtual Firewall Policy consists of rules which specify whether to block or allow access to specified network addresses and can apply to all types of network endpoints.

Virtual Firewall rules are centrally managed. This means rules cannot be added, edited or removed from individual Consoles but must apply to all Appliances installed in the system.

Two types of rules can be defined using the Firewall Policy Pane:

> **Block Rules** - which prevent outbound traffic at source IPs from reaching target IPs. A list of sources and hosts that have been blocked as the result of a Block Rule can be viewed from the Block Events dialog box of the Console.
>
> **Allow Rules** – which allow unconditional access at selected services in the protected and source network. This means access is permitted to and from the host even when it would be prevented by other defined policies. However, Allow Rules are not applied to hosts that are blocked by external systems, i.e. switches, router, VPNs or firewalls.

When defining Block Rules and Allow Rules both source IPs and Target IPs can be defined as *all* (all network addresses), *addresses* (for a single address or a group of addresses) or *network segment* (range of addresses). The administrator can also define the services to block: *all* (all services at the previously defined target IP ranges), *single* (defined by one selected port and protocol) or *list* (for a list of services).

7.1.2.3 NAC-3: Threat Protection Policy

(FDP_ACC.1-3, FDP_ACF.1-3, FMT_MSA.1-3, FMT_MSA.3-3)

The third of the three types of Network Access Control policies enforced by the TSF is the CounterACT Threat Protection Policy. Administrators can define a Threat Protection Policy to define how CounterACT should handle hosts that attempt to infect the network.

The TOE prevents infection attempts by identifying and suppressing malware code before it propagates within the network. The TOE monitors traffic directed toward the network for signs of reconnaissance, and then identifies the techniques used to launch the probing, for example port scans or NetBIOS probes. In response to this activity, the TOE generates virtual resource information sought by malware programs and forwards the information back to them. This information is referred to as a mark. The CounterACT marks were designed to have the same fingerprint as legitimate network responses. In addition, there are controls to further tune the marks to comply with local network naming policies (of host-names and user-names). For example, if the TOE identifies a request for a service at the network, it responds by creating and returning a mark in the form of the service requested. Malware programs should not be able to distinguish between the mark and legitimate network response. When an attempt is made to access the network using the mark, the TOE recognizes it and either continues to monitor the traffic, or prevents it from establishing communication with the network and external domains, or with the service at which the infection attempt took place. When a host uses a mark, it is referred to as a bite event.

The TOE also automatically detects heavily scanned services, and responds by either monitoring or blocking these services. When a service is monitored, CounterACT records all traffic going to the service. When a service is blocked, no communication with that service is permitted. CounterACT also responds to e-mail worms.

A machine from which an IPS event was detected, i.e. a worm infection or malware propagation attempt is referred to as a malicious host.

Threat Protection Policies can be created, deleted and modified by an authenticated user with necessary permission via the CounterACT Console. The Basic Policy and the Threat Protection Policy can be configured as follows:

Basic Policy Settings

The following settings can be configured using the basic policy settings tab:

- **Network Worm Policy**
    - **Action on detection**
        - **Port Block –** the host is prevented from establishing communication at the service it attempted to infect for a specified time period. The Port Block policy can be escalated to the Host Block policy.
        - **Host Block –** the host is prevented from establishing communication with the network for a specified time period.
    - **Notify** - E-mail notification can be sent regarding detections.
    - **NAC Policy –** detection can be part of a NAC policy that can invoke further actions.
- **E-mail Worm Policy**
    - **Action on detection** – can be set to block or monitor the e-mail flow when an e-mail infection is detected.
    - **Notify** - send e-mail notification regarding the e-mail infection detection.
    - **NAC Policy –** detection can be part of a NAC policy that can invoke further actions.

Advanced Policy Tools

The advanced policy tools allow authenticated users with necessary permissions to customize how CounterACT identifies and handles scan and detection events, e-mail worms and make further refinements to the Threat Protection Policy. The advanced policy tools can be used to perform the following:

- Customize Parameters for Each Scan Type
- Customize Scan Recognition Criterion
- Customize Detection Settings
- Customize Detection Type Values
- Customize E-mail Worm Settings
- Customize E-mail Anomaly Recognition Values

- Configure the Block Method
- Configure Service Attack Settings
- Define Manually Added Hosts
- Configure the Range Protected from Malicious Attacks
- Manage Enterprise Lockdown Alerts
- Define Legitimate Activity of Sources
- Define Legitimate E-mail Traffic

7.1.3 User Identification and Authentication Functions

7.1.3.1 IA-1: User Security Attributes

(FIA_ATD.1)

The TSF maintains the following security attributes for each individual TOE user:

- **User Name** (account name, login name)
- **Password** (authentication data)
- **Authentication Method** (”Internal”, “LDAP”, or “Kerberos”)
- **Console User** (must be selected for the user to be able to log in to the CounterACT Console GUI)
- **Permissions** (one or more permissions may be selected for each user)
- **Password History** (list of previous passwords for each user that cannot be reused; the number of passwords stored is set by the Password History Count in the Password Policy)

7.1.3.2 IA-2: User Identification & Authentication

(FIA_UAU_EXT.2, FIA_UID.2)

No actions are allowed, other than entry of identification and authentication data, until successful identification and authentication.

Each individual must be successfully identified and authenticated with a username and password by the TSF or by an authentication service in the Operational Environment that has been invoked by the TSF before access is allowed to the TOE.

TOE user identification and authentication decision (successful/failed) and enforcement are performed by the TSF if the Authentication Method attribute of the user account is set to “Internal”. The TSF uses the security attributes of the user account described in Section 7.1.3.1 above for internal authentication.

Alternately, the TOE can be configured to query an external authentication service for TOE user identification and authentication decision. This authentication method applies to only to user accounts whose Authentication Method attribute is set to “LDAP”, or “Kerberos”.

Supported User Directory types used for external authentication are:

- Microsoft Active Directory
- Sun Java System Directory Server
- Novell eDirectory
- IBM Lotus Notes
- RADIUS
- TACACS

Note: The external authentication server is not included in the TOE.

7.1.3.3 IA-3: User Login Security

(FIA_AFL.1, FIA_SOS.1, FIA_UAU.7)

CounterACT uses multiple means to ensure login security:

Authentication Failure Handling:

An authenticated user with the necessary permissions can manage the settings for password strength parameters, and login failure lockouts through the console.

If a user attempting to gain access makes the maximum number of unsuccessful login attempts that is specified in the password policy, that user account is locked.

The locked out user cannot authenticate to the TOE until the account is manually unlocked by an authenticated user with the necessary permissions or until the lockout period defined in the Password Policy has passed.

Verification of Secrets:

The TOE controls the strength of authentication passwords and authentication failure handling through the parameters in the password policy specified in Table 6-5: Password Policy Rules.

Protected Authentication Feedback:

A user’s authentication data is also protected by the TOE by being masked upon input. The login screen will display in clear text only the username as input and the IP address or host name of the Enterprise Manager or CounterACT Appliance for which the user is requesting access.

7.1.4 Security Management Functions

7.1.4.1 SM-1: Management Functions

(FMT_MTD.1, FMT_SMF.1)

The TOE is capable of performing the security management functions as defined in Table 6-6: Management of TSF Data (See Section 6.1.4.7 FMT_MTD.1 Management of TSF data).

All management functions are limited to the administrative roles: Admin and Console User. The Admin role may perform all operationsTable 6-6: Management of TSF Data while a Console User's functional capabilities are determined by the permission(s) assigned to the account.

A Management Console connected to a standalone CounterACT appliance presents the same set of management functions through its Console GUI as one connected to an Enterprise Manager.

The Console GUI for a CounterACT appliance which is managed by an Enterprise Manager has viewing permissions and update permissions for settings which affect only that specific appliance.

7.1.4.2 SM-2: Management Security Roles

(FMT_SMR.1)

The TOE has two defined roles: Admin and Console User.

CounterACT is installed with an "Admin" user (password is created by the installer) who has access to all Console tools and features. This means that other users do not need to be created in order to operate the system. If required, however, new users can be added. These users are given the "Console User" role and are assigned user permissions which allow, limit or prevent user access to specific Console tools (access to the management functions available through the Console). More than one user permission may be assigned to a Console User. Console Users can be created, deleted or modified by an Admin or a Console User with the necessary permission. The user permissions for the Admin user cannot be modified, however the Admin password may be changed if necessary.

Note: The ForeScout CounterACT product also maintains the role: Asset Portal User. However, the Asset Portal functionality is not in the scope of the evaluation and so this role is not used in the TOE.

7.1.5 Protection of Security Functions

7.1.5.1 PT-1: Internal Data Transfer Protection

(FPT_ITT.1)

The TSF ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured through encryption during both setup and the transition of data.

The types of encrypted communications that can occur between TOE components are:

- For systems with only one Appliance
  - Between the Console and the Appliance
  - Between a SecureConnector and the Appliance
- For systems with more than one CounterACT Appliance
  - Between the Console and the Enterprise Manager
  - Between the Enterprise Manager and an Appliance
  - Between a SecureConnector and an Appliance

SSL is included in the product and installed on each appliance. The following summarizes where it is used:

- Console to/from Appliances and Enterprise Manager
- Enterprise Manager to/from Appliances
- SecureConnector to/from Appliances

Note: the cryptographic functionality of the SSL is not claimed by the vendor and is considered outside the TOE

Note: At installation, the administrator can choose to enable FIPS mode which configures CounterACT to meet updated FIPS 140-2 (Federal Information Processing Standard) requirements.

7.1.6 Vulnerability Scanning Functions

7.1.6.1 SC-1: Vulnerability Scanning

(SSC_SCN_EXT.1)

CounterACT collects vulnerability information from the endpoints on the protected network in addition to information collected as a result of NAC policies (See Section 6.1.4.1 FMT_MSA.1-1 Management of security attributes (NAC)).

There are two methods of performing vulnerability scanning: Automated Protection and Notification, which incorporates vulnerability scanning through a NAC Policy (see Section 7.1.2.1 NAC-1: NAC Policy), and the Vulnerability Scanning Wizard.

Vulnerability Scanning Wizard

The Vulnerability Scanning Wizard only applies to network hosts that run a Windows OS. The Vulnerability Scanning Wizard is run from the CounterACT Console and lets an authenticated user with the necessary permissions to choose:

- Microsoft vulnerabilities to search for in the scan
- Open services to search for in the scan - protocol (e.g., ICMP, …) and port number
- IP ranges of the network to scan (the scan will ignore inactive hosts)

The Vulnerability Scanning Wizard can be used to:

- Plan scheduled scanning
- Carry out immediate scanning
- Generate a report of scan results
- Compare scan results in a PDF format.
- Review scan histories

- Export scan results

Nmap scanning is invoked when Vulnerability Scanning is configured to detect Open Services within the target network range(s).

Scan results appear in the Control Center of the Console and provide information about vulnerable hosts and open services detected. For example the vulnerability that was detected, the host IP, DNS and NetBIOS user name, and the MAC address of the host.

Windows Vulnerability Scanning

Vulnerability Scanning of hosts running Windows is based on ForeScout's remote inspection technology, which handles Microsoft related vulnerabilities.

The Host Property Scanner (HPS) enables the use of the vulnerability scanning tools. In order to reach the full range of deep inspection, administrators need to configure and test the HPS. In addition to scanning for vulnerabilities, the HPS provides generic information of end-points, such as registry key entries, file properties, services, processes and the like. These are used to create custom policies to match specific requirements.

Macintosh/Linux Vulnerability Scanning

The Macintosh/Linux Inspection functionality communicates with endpoints running Macintosh or Linux using SSH remote access and public/private key authentication. This method of inspection avoids using usernames and passwords to access the hosts.

7.1.6.2 SC-2: Scanning Analysis

(SSC_ANL_EXT.1)

When vulnerability scanning is incorporated into a NAC Policy (see Section 7.1.2.1 NAC-1: NAC Policy), the TSF will automatically analyze the data collected by the scan (see 7.1.6.1 SC-1: Vulnerability Scanning) and based on the rules set in the NAC Policy perform the actions indicated in that policy (see 7.1.6.3 SC-3: Scanning Actions).

NAC Policy templates are included with the CounterACT product to look for both Windows vulnerabilities (The Windows Compliance Policy Template) and Macintosh vulnerabilities (Macintosh Vulnerability Updates Templates) See Section 7.1.6.1 SC-1 Vulnerability Scanning.

NAC policies can be created to search for and analyze Microsoft vulnerabilities. This resulting analysis would indicate the existence of Microsoft published vulnerabilities detected on the host. The HPS can detect new vulnerabilities as the information becomes available via an update to the HPS-Vulnerability DB.

7.1.6.3 SC-3: Scanning Actions

(SSC_ACT_EXT.1)

When vulnerability scanning is integrated into a NAC Policy the TSF will take the actions that have been configured for the policy when a vulnerability is detected. These actions can be one or more of the following:

- Send E-mail, Instant Notification ,or HTTP Notification to Network Users indicating that Specific Vulnerabilities were Detected
- Disconnect USB Devices
- Kill Instant Messaging Applications
- Kill Peer to Peer Applications
- Kill a Process on Windows System
- Kill a Process on Linux and Macintosh System
- Start Macintosh Updates for Vulnerability Remediation
- Start Windows Updates for Vulnerability Remediation
- Run Script Action on Windows
- Run Script Action on Macintosh and Linux
- Set Registry Key Action
- Start AntiVirus on Windows
- Update AntiVirus on Windows
- Assign Vulnerable Device to VLAN
- Block a Switch Port (no traffic is allowed through)
- Virtual Firewall Action (block access to and from detected hosts)
- HTTPS Redirection (network users will see a security alert at their desktop Web browser when they attempt to access the Web)

When vulnerability scanning is done through the Vulnerability Wizard (see Section 7.1.6.1 SC-1: Vulnerability Scanning) results appear in the Control Center of the Console. Authenticated users with necessary permissions can manage the vulnerable hosts through the Console Center by:

- Blocking access to or from the vulnerable host.
- Sending E-mail, instant notification, or HTTP notification to the user at vulnerable hosts.
- Running related actions, for example quarantining the vulnerable host to an isolated VLAN, or opening a trouble ticket.

However, these actions are not performed automatically by the TSF and are covered under the TOE's management functionality (see Section 7.1.4.1 SM-1: Management Functions).

7.2 TOE Protection against Interference and Logical Tampering

The TOE consists of both hardware (the CounterACT and Enterprise Manager appliances) and software (the CounterACT and 3rd party applications running on the appliances and the CounterACT Console and SecureConnector components).

The TOE offers only well defined services at its network interfaces that are specifically designed to provide only the services that are necessary to enforce the TSP and not to offer additional services that might be used to interfere with the operation of the TOE.

The TOE protects the security functions it provides through a variety of mechanisms. One of the primary protections is that TOE users must authenticate before any administrative operations can be performed on the system, including creating new policies or viewing the results of the application of those policies. In addition, the TSF data is protected doubly as the system is configured to not accept any management requests or input from the monitored network. All communication between TOE components including the management interface is via a protected network separate from the monitored network that is being protected by the TOE. All data transmitted between TOE components is protected from disclosure and modification by the encryption mechanisms included in the TOE.

Access to the TOE is also protected by the access control functions of the database and operating system -of the CounterACT Appliances and Enterprise Manager. TSF data stored in the database is protected by the security mechanisms of the DBMS of the CounterACT Appliances and Enterprise Manager. Data files and configuration files are protected by the security mechanisms of the operating systems of the CounterACT Appliances and Enterprise Manager.

7.3 TOE Protection against Bypass of Security Functions

The TSF requires that all users successfully authenticate before any TSF functions (other than entering identification and authentication data) can be performed. Once a user is identified and authenticated, access to management functions and TSF data is controlled by a TOE user's assigned security attributes (role and permissions). Operations on TSF data are checked for conformance to the granted level of access, and rejected if not conformant based on the TOE user's security attributes. Authorized TOE users can only view TSF data through the administrative interface. The TSS does not offer general programming capabilities that might offer the opportunity to attempt to bypass the TSP.

All TOE user operations are conducted in the context of an associated TOE user session. This session is allocated only after successful identification and authentication by the TSF or the TSF and Operational Environment working together. The TOE enforces a password policy if native password authentication is being used. The TOE can optionally invoke an external mechanism for user authentication (e.g. LDAP).The TOE also supports authentication failure handling. The TOE user session is destroyed when the corresponding TOE user logs out of that session.

Additionally, the TSF does not accept any commands from or offer any functions to the network that is monitored by the TOE. This ensures that network entities cannot cause the TOE not to apply its TSPs to applicable network traffic.