National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Check Point Software Technologies LTD

for

Check Point Endpoint Security E80.30 (Build 8.1.327)

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2014-01-29

Validation Report Number: CCEVS-VR-VID10343-2014

CCTL: Leidos (formerly SAIC) Common Criteria Testing Laboratory

Assurance Level: EAL2 with ALC_FLR.3

Protection Profile Identifier: None

Original Signed By

Acting Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By

Information Assurance Director
National Security Agency

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Check Point Endpoint Security

E80.30 (build 8.1.327)

Report Number:	**CCEVS-VR-VID10343-2014**
Dated:	**29 January 2014**
Version:	**1.0**

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

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

ACKNOWLEDGEMENTS

Validation Team

Ken Elliott
Kenneth Stutterheim
The Aerospace Corporation
Columbia, Maryland

Daniel P. Faigin
The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Dawn Campbell, Lead Evaluator
Leidos Inc.
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of the Check Point Endpoint Security E80.30 (build 8.1.327) product was performed by Leidos, Inc. a Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in December 2013. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The LEIDOS evaluation team determined that the product is Common Criteria Part 2 Conformant and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC_FLR.3. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the LEIDOS evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The TOE is Check Point Endpoint Security E80.30 (build 8.1.327) with the following software blades: Full Disk Encryption, Media Encryption & Port Protection, Firewall & Application Control, Compliance, and Virtual Private Networking (VPN). Check Point Endpoint Security is a workstation security software product that is installed on user desktop and laptop hosts in an enterprise setting. Supported operating systems include: Windows 7 Enterprise, Professional, Ultimate editions (32-bit and 64-bit).

The product provides pre-boot user authentication, cryptographic protection for data stored on hard disks and removable media, enforces defined security policies on all host I/O interfaces (USB, serial, etc.), and provides information flow control for network traffic entering and departing the host. In addition, the product can be configured to invoke third-party components installed on the host that perform malware scanning and analysis. The product audits the security relevant actions it performs, and makes that audit available to authorized remote administrative users.

Check Point Endpoint Security can be used to enforce corporate security compliance policies. The client analyzes the host's compliance status (e.g. patch levels, anti-virus updates, etc.) and can be configured to prevent a non-compliant workstation from gaining access to network resources.

The Endpoint Connect VPN client capability supports establishment of a secure channel between the Check Point Endpoint Security client and a Check Point Security gateway, using the IKE/IPSec security protocols.

Some of the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. Such cryptography has only been asserted as tested by the vendor. Section 6.2 identifies the cryptographic functions that are provided by FIPS-assessed components, and the cryptographic functions that are only asserted as tested by the vendor.

The TOE, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Check Point Endpoint Security E80.30 Security Target (ST).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Check Point Endpoint Security E80.30 (build 8.1.327)
Protection Profile	None
ST:	Check Point Endpoint Security E80.30 Security Target, Version 1.0, January 22, 2014
Evaluation Technical Report	Evaluation Technical Report for Check Point Endpoint Security E80.30, Part 1 (Non-Proprietary), Version 0.2, 23 January 2014 Evaluation Technical Report for Check Point Endpoint Security E80.30, Part 2 (Proprietary), Version 0.2, 23 January 2014.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009
Conformance Result	CC Part 2 conformant and Part 3 conformant, EAL 2 augmented with ALC_FLR.3
Sponsor	Check Point Software Technologies LTD

Item	Identifier
Developer	Check Point Software Technologies LTD
Common Criteria Testing Lab (CCTL)	Leidos Inc., Columbia, MD
CCEVS Validators	Kenneth Elliott Kenneth B Stutterheim Daniel P. Faigin *The Aerospace Corporation*

3 TOE Overview

The TOE is Check Point Endpoint Security E80.30 (build 8.1.327) with the following software blades: Full Disk Encryption, Media Encryption & Port Protection, Firewall & Application Control, Compliance, and VPN. Check Point Endpoint Security E80.30 (build 8.1.327) is a workstation security software product that is installed on user desktop and laptop hosts in an enterprise setting. Supported operating systems include: Windows 7 Enterprise, Professional, Ultimate editions (32-bit and 64-bit).

The product provides pre-boot user authentication, cryptographic protection for data stored on hard disks and removable media, enforces defined security policies on all host I/O interfaces (USB, serial, etc.), and provides information flow control for network traffic entering and departing the host. In addition, the product can be configured to invoke third-party components installed on the host that perform malware scanning and analysis. The product audits the security relevant actions it performs, and makes that audit available to authorized remote administrative users.

Check Point Endpoint Security E80.30 (build 8.1.327) can be used to enforce corporate security compliance policies. The client analyzes the host's compliance status (e.g. patch levels, anti-virus updates, etc.) and can be configured to prevent a non-compliant workstation from gaining access to network resources.

The included Endpoint Connect VPN client capability supports establishment of a secure channel between the Check Point Endpoint Security E80.30 (build 8.1.327) client and a Check Point Security gateway, using the IKE/IPSec security protocols.

The TOE: Check Point Endpoint Security E80.30 (build 8.1.327) is comprised of the following Check Point software blades[1]:

- Full Disk Encryption Blade
- Media Encryption & Port Protection Blade
- Firewall & Application Control Blades
- Compliance Blade
- VPN Blade

These components are installed on a workstation running one of the following Microsoft Windows operating systems: Windows 7 Enterprise, Professional, Ultimate editions (32-bit and 64-bit). The underlying hardware platform and operating system on which the TOE software is installed are considered to be in the TOE Operating Environment, and thus outside the TOE boundary.

The vendor has tested TOE invocation of the following third party anti-virus software: McAfee VirusScan and Kaspersky Antivirus. Invocation of other anti-virus products were not covered by this evaluation; Check Point's support website provides solution id sk68080 that provides a current list of AntiVirus products the vendor claims this product supports. New releases of those products are supported through the Flaw Remediation process. Due to the dynamic nature of AV products TOE users should contact Check Point Support for integration of new AV versions into

[1] Software Blades are security modules purchased by customers independently or in pre-defined bundles. Note that not all software blades are covered by the evaluation.

the TOE. The anti-virus engines themselves are in the operational environment, and thus outside the TOE boundary.

While some basic management capabilities are provided in the client software, Check Point Endpoint clients are designed to be centrally managed. However, management server products are separate products that are not required to effectively use the client. In the context of this ST, the management server is treated as a 'remote user' that can be authorized to perform identified TOE management operations.

4 Assumptions, Threats, and Organizational Security Policies

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and defines the threats that the product is designed to counter.

The security environment is defined in terms of assumptions made by the TOE and threats to the TOE. There are no defined organizational policies.

4.1 Assumptions

The following are the assumptions identified in the Security Target:

- The workstation hardware and operating system will be installed and maintained in a manner that cooperates with the TOE and does not actively seek to disable or otherwise impair or bypass any of the security functions of the TOE.

  Notes: The TOE depends on the underlying platform to ensure that its security functions are protected from tampering, deactivation, interference and bypass. TOE components hook into published operating system interfaces in order to intercept application requests, and TOE security functions depend on the correctness of implementation of these operating system interfaces.

  While the TOE provides self-protection mechanisms intended to prevent users from tampering with its security functions or with overall system integrity, it is also expected that the operating system shall be installed and maintained such that users receive restricted permissions in support of these security objectives. For example, it is expected that users cannot run kernel-level software that might bypass operating system drivers and interacts directly with hardware devices.

  The TOE also relies on the operating system to provide reliable timestamps in support of audit and information flow control functionality.

  System administrators are expected to follow operating system Common Criteria evaluated configuration guidance for operating system installation.

- Authorized users will keep authentication credentials private.

Notes: Users must keep their passwords and PINs secret, and will not let others use their authentication tokens. When entering offline removable media device passwords into EPM Explorer in order to access encrypted data on the removable media on a host outside of the TOE, the user must ensure that the host environment can be trusted not to compromise the password's secrecy.

- When a one-time Remote Help password is generated, the authorized help desk representative will first authenticate the presumed authorized user by means outside of the TOE, and will communicate the password using secure delivery procedures.
- The owners of the TOE must ensure that the private keys used by management servers or security gateways to communicate with the TOE are maintained in a manner that maintains adequate security. It is advised to follow Common Criteria evaluated configuration guidance for other Check Point product installations that interoperate with the TOE to ensure their secure operation.

4.2 Threats

The following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- An unauthorized user with physical access to the workstation may access information stored on the workstation's disk drive.

  Notes: The unauthorized user might attempt to impersonate an authorized user by entering spoofed authentication credentials, or remove the hard drive from the workstation to attempt to extract information stored on the drive.

- An unauthorized user with physical access to the workstation may subvert the workstation's system software or normal boot process.

  Notes: The unauthorized user might attempt to modify the boot record or boot up the workstation from a different device (e.g. floppy disk) in an attempt to subvert authentication mechanisms, or attempt to install spyware by writing it directly to the drive, in order to compromise workstation system integrity.

- An authorized user may circumvent security policy by installing inappropriate software, connecting unauthorized devices to the workstation, or disabling security mechanisms.

  Notes: The user might attempt to install inappropriate software (e.g. unlicensed software or recreational software), connect unauthorized devices (e.g. unencrypted media devices, modems, wireless LAN adapters), or attempt to disable security mechanisms such as anti-virus software or cancel system security updates, thus modifying the system in an unauthorized manner.

- User and system applications may leak inappropriate information.
- Non-malicious applications and services might utilize network services that are not in-line with security policy, leaking inappropriate information to unauthorized entities. For example, some applications connect to software vendor update servers, providing information on workstation configuration.
- Spyware applications installed on the workstation may leak information to external entities.

Notes: Spyware is software that has a hidden, malicious intent to leak information from the workstation to external entities, usually by connecting over the network to subverted servers. Spyware can infect the workstation via various vectors, e.g. in the guise of “freeware”, or even as part of purchased software packages. Spyware may sometimes remain undetected for long periods of time, because it tends not to have visible impact on system behavior.

- Malicious code may be injected into the workstation via workstation device ports, compromising system integrity.

  Notes: This statement is intended to describe the threat of malicious software that attempts to inject itself into the workstation, modifying system or application files as a means of replicating itself and spreading to other hosts. Viral spread vectors may include removable media devices, removable media, or executable content downloaded over the network. Virii are often distinguished from Trojans which spread with the inadvertent help of the authorized user, and from Worms that spread by exploiting network-exposed vulnerabilities or characteristics.

- Malicious code may run on the workstation, attempting to spread to other hosts over the network.

  Notes: The most common worm spread vector is email, a ubiquitous service that is available on most workstations and is allowed to traverse corporate networks and perimeter security devices, both because of the complexity of the common mail application (complexity breeding vulnerabilities), and because of the naivety of users that often inadvertently aid the worm in spreading to others. The worm typically impacts the system adversely in terms of increased network load and decreased availability.

- An unauthorized entity on a connected network may exploit network-exposed vulnerabilities to subvert the workstation.

  Notes: Applications and services might expose vulnerabilities to the network by connecting to external servers over insecure connections, or by listening to network ports and processing network input in an insecure manner, thus allowing the attacker to exploit these vulnerabilities in order to compromise the integrity of the system.

- An unauthorized entity may intercept or modify information in transit between the workstation and remote IT entity.

  Notes: The attacker gains access to the network path between the workstation and another host, and intercepts the information in transit between the two network peers, gaining unauthorized access to the information or maliciously modifying it.

- A program may write information to a removable media device or removable media, and the media might later fall into the hands of an unauthorized user that gains access to the information.

  Notes: The threat agent here is defined as the program that leaks the information, not the unauthorized user, because the latter does not take an active role in the information leakage

4.3 Organizational Security Policies

None.

5 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 extended in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The third-party anti-virus product bundled with the TOE is considered to be outside the boundaries of the TOE. However, the TOE supports a variety of anti-virus products that may be installed on the workstation by the user, independently of the TOE.

All Check Point Endpoint Security E80.30 (build 8.1.327) product functionality is not included in the Target of Evaluation. The following features have not been evaluated as to their correctness:

- **Advanced Password Functionality.** Specifically, although the product supports password complexity requirements and a password history, these capabilities were not covered by the evaluation.
- **Login banners**.
- **Bundled Third-party Anti-Virus Product**. The third-party anti-virus product bundled with the TOE is considered to be outside the boundaries of the TOE. However, the TOE supports a variety of anti-virus products that may be installed on the workstation by the user, independently of the TOE.
- **Smart Cards.** Although authentication using smartcards was included in the evaluation, the capability of the smartcards and the smartcard readers themselves were not.
- **Underlying Hardware and Software Environment.** The TOE components are installed on a workstation running a Microsoft Windows operating system. The underlying hardware platform and operating system on which the TOE software is installed are considered to be outside the TOE.
- **Audit Log Protection.** The TOE protects audit logs when stored locally. Audit logs are stored on the encrypted part of the disk and thus the TOE requires user authentication prior to granting access to local audit logs. Also, the TOE does not provide interfaces to delete audit data. Since there are no SFRs related to local audit storage, the TOE behavior regarding the storage, integrity and overwriting of local audit storage has not be evaluated.
- **Local Audit Review.** Only the remote transmission audit mechanism has been evaluated, including the remote review of audit. Local review of audit does not satisfy the Common Criteria audit requirements; therefore, the local review of audit data was not evaluated and was not tested.

Some Check Point Endpoint Security functionality is specifically excluded and thus its use is ***NOT*** permitted in an evaluated configuration:

- **Software Blades**. The TOE is comprised of the following Check Point software blades: Full Disk Encryption, Media Encryption & Port Protection, Firewall & Application Control, Compliance, and Virtual Private Networking (VPN). The Check Point Endpoint Security also provides two additional blades: the Check Point WebCheck Blade and the Check Point Anti-malware blades. These blades have not been evaluated. They are not permitted, and must not be installed, in an evaluated configuration.
- **Legacy VPN Clients.** The TOE includes the Endpoint Connect VPN, however, the command line option for endpoint connect is not permitted to be used in the evaluated configuration. Additionally, the use of the Check Point Legacy VPN is not permitted in the evaluated configuration.
- **Virtual Keyboard/Character Map.** The Virtual keyboard and character map function of the TOE are NOT permitted in the evaluated configuration.

Lastly, note that the TOE relies on the hardware and the operating system in the environment for reliable timestamps used in audit and cryptography.

6 Architectural Information

6.1 High-Level Architectural Description

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE, Check Point Endpoint Security E80.30 (build 8.1.327), is a software product that is installed on a single workstation in an enterprise setting. Check Point Endpoint Security E80.30 (build 8.1.327) protects the workstation from unauthorized access by physical, network-based, and external device-based threats. The workstation, its operating system, applications running on the workstation, external devices and media (including authentication tokens if used), and any network-based services (such as a Windows Domain Controller) are all outside of the TOE boundary.

The product is a part of the comprehensive Check Point unified security architecture, and as such is typically centrally-managed using other Check Point security management products. Management servers support remote management, log review, and can serve as a centralized key storage repository for removable media encryption. Local user management and log review interfaces are also available.

The product also interacts with Check Point security gateways for remote access VPN.

In the context of this security target, the TOE includes only the Check Point Endpoint Security E80.30 (build 8.1.327) software installed on the workstation—other Check Point components are evaluated separately.

The TOE, Check Point Endpoint Security E80.30 (build 8.1.327) includes the following components:

Full Disk Encryption	
Full Disk Encryption	Controls access to the workstation though pre-boot authentication and user-transparent full disk encryption. This feature prevents unauthorized users with physical access from gaining access to any data on the disk.

Media Encryption & Port Protection	
Port Protection	Controls access to devices through all workstation ports. This feature prevents users from connecting unauthorized devices to client machine ports, providing On/Off/Read Only access control levels.
Removable Media Manager	Restricts the workstation to using only authorized removable media.
Removable Media Encryption (EPM)	Encrypts and protects information stored on removable media devices such as USB disks and external disk drives, and on CDs, and DVDs. Access to data stored on the media is thus restricted to authorized users. Includes the EPM Explorer utility for offline access to the encrypted media. Note that when use of removable encrypted media is required, audio CDs cannot be read or written.

Firewall & Application Control	
Firewall	Personal Firewall for network traffic flowing in and out of the workstation.
Application Control	Controls network information flow permissions on a per-application basis.

Compliance	
Enforcement Rules	Constrains network communication for workstations that do not comply with defined configuration rules, e.g. correct anti-virus version installed.

VPN	
VPN Client	Provides an encrypted and authenticated trusted channel for remote access users connecting through a VPN gateway to internal resources.

Check Point Endpoint Security is a software product produced by Check Point. The product is installed on a workstation hardware platform that is running a Microsoft Windows operating system (Windows 7 Enterprise, Professional, Ultimate editions (32-bit and 64-bit).

The following diagram is a representation of the physical boundaries of the TOE and its components.

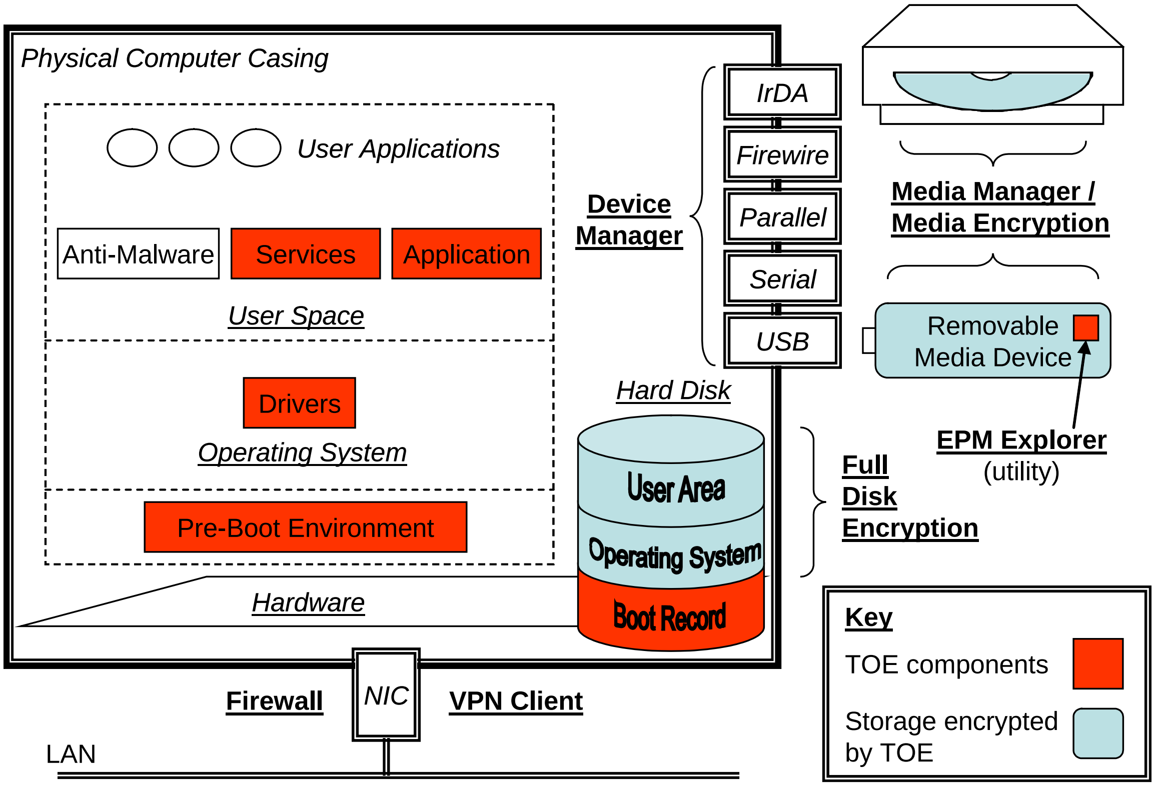

Figure 1. TOE Scope and Physical Boundaries

In addition to kernel-level drivers, the product installs services that are responsible for communication with peer IT entities, management, logging, and compliance testing. A task bar application provides a Graphical User Interface (GUI) that allows the local user to perform security management and log review operations. A Media Import Wizard for encrypting removable optical media is integrated into the operating system's optical media burn interaction, and can also be launched directly from the task bar application.

The different parts of the TOE are depicted in red in Figure 1. The TOE encrypts data stored on the workstation hard disk, and can be configured to encrypt storage on removable media devices and removable media[2] (outside the TOE).

As depicted in Figure 1, the TOE includes an EPM Explorer utility that can be written on encrypted removable media devices. When the encrypted removable media device is inserted into a trusted host outside of the TOE that does not include an installation of Check Point Endpoint Security, the EPM Explorer utility can be used to provide access to the encrypted storage. The security of the data on the removable media device is derived from the fact that it was encrypted by the TOE, using an offline password bound to the TOE's password selection constraints. The TOE assumes that the operational environment is benign with respect to the execution environment of the EPM Explorer utility and to any possible modification of the utility while stored on the device, to prevent compromise of the offline password used to protect the data.

The vendor has tested TOE invocation of the following third party anti-virus software: McAfee VirusScan and Kaspersky Antivirus. Invocation of other anti-virus products were not covered by this evaluation; Check Point's support website provides solution id sk68080 that provides a current list of AntiVirus products the vendor claims this product supports. New releases of those products are supported through the Flaw Remediation process. Due to the dynamic nature of AV products TOE users should contact Check Point Support for integration of new AV versions into the TOE. The anti-virus engines themselves are in the operational environment, and thus outside the TOE boundary.

6.2 Usage of Cryptography

The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. The SFRs in the Cryptographic Support (FCS) class stated in the ST therefore reference external standards that the implementation must meet when providing the required capabilities.

Table 1 summarizes the standards compliance claims made in the ST and states for each the method used to determine compliance (aside from development assurances). The method may be an applicable NIST certificate number or a vendor assertion.

[2] Note that 'removable media device' is a subset of 'removable I/O device', both of which are distinct from 'removable media'. Removable I/O devices are any devices that can be attached and detached, in its entirety, from a host workstation. Removable media devices are those removable I/O devices capable of storing data (e.g., the contents can potentially be written). Removable media includes floppy disks, CDs, and DVDs where the media itself is removable from a device attached to a host workstation.

Table 1. Cryptographic Standards and Method of Determining Compliance

Standard claimed	Cryptographic SFRs	Method of determining compliance
ANSI X9.31-based DRNG	FCS_CKM.1	RNG certs. #90, #222, #250
FIPS 140-2 Level 1	FCS_CKM.1, FCS_CKM.4	Vendor assertion[3]
IKE per RFC 2409	FCS_CKM.2	Vendor assertion
TLS v1.0 per RFC 2246	FCS_CKM.2	Vendor assertion
AES in CBC mode per FIPS PUB 197	FCS_COP.1	AES certs. #257, #430, #466
SHA-1 per NIST PUB FIPS 180-2	FCS_COP.1	SHS certs. #332, #499, #534
MD5 per RFC 1321	FCS_COP.1	Vendor assertion
Triple DES in CBC mode per FIPS PUB 46-3	FCS_COP.1	Triple DES certs. #338, #459
HMAC-SHA-1 and HMAC-SHA-256 per RFC 2104, FIPS PUB 198	FCS_COP.1	HMAC cert. #67, #202
RSA per PKCS#1	FCS_COP.1, FCS_CKM.3	RSA certs. #66, #132, #162
Key wrap per PKCS#5	FCS_CKM.3	Vendor assertion

7 Security Policy

The TOE supports the following security functions:

- Security Audit
- Security Management (Trusted path/channels)
- Blade Security (Cryptographic Support, User Data Protection, Identification and Authentication, Protection of the TSF, Trusted Path/Channels)
    - FDE
    - EPM
    - Device Manager

[3] The Check Point Endpoint Security components identified in the ST each use embedded cryptographic code modules: Full Disk Encryption incorporates the Check Point Crypto Module, FIPS 140-2 certificate #770; Media Encryption & Port Protection incorporates the Reflex Magnetics Cryptographic Library, FIPS 140-2 certificate #784; and VPN is derived from a version of the VPN-1 cryptographic module (FIPS 140-2 certificate #1219). The method of determining compliance is given as ‘vendor assertion’ because the product as a whole has not undergone FIPS 140-2 validation. Also note that while these FIPS 140-2 validations were performed on a subset of the operating systems supported by the TOE, FIPS 140-2 Implementation Guidance G.5 allows vendor porting and re-compilation of a validated software cryptographic module to a compatible operating system that was not included as part of the validation testing, when this does not require source code modifications, as is the case here. The validation status is maintained in this case without re-testing.

- Removable Media Manager
- Firewall
- Application Control
- Program Advisor
- Enforcement Rules (Protection of the TSF)
- VPN Client (Trusted path/channels)

7.1 Security Audit

Security-relevant events from all Check Point Endpoint Security suite components (except for VPN) can be logged in the local audit trail. The audit events are sent to an external central administrative location where they are stored and can be viewed by remote authorized administrators. Although the system permits authorized local users to review the audit trail, the interface provided does not meet the requirements of the Common Criteria, and thus its use was not covered by the evaluation.

7.2 Security Management (Trusted path/channels)

The TOE provides a management application that allows the local user to access and modify product security settings for all Check Point Endpoint Security E80.30 (build 8.1.327) suite components, and to review the audit trail. Remote users are authenticated by their certificates in the context of the establishment of the IKE or TLS secure channel.

In addition, Check Point Endpoint Security provides interfaces for remote users to perform management operations from remote management servers (outside of the TOE) after being identified and authenticated by Check Point Endpoint Security. Audit log records are sent to the remote host, and security policy settings downloaded from the management server update the locally-defined policy.

7.3 Blade Security

7.3.1 Full Disk Encryption (FDE)

Full Disk Encryption (FDE) encrypts the entire hard disk, including all operating system and user areas. Because encryption is performed on a sector by sector basis instead of on the basis of file and directory encryption, all disk contents are protected, including, in addition to normal data files, system files, swap files, temporary files, deleted files, and unused space. This ensures that an unauthorized user that gains physical access to the disk (e.g. in the case of a stolen laptop) cannot access or modify any information.

Users are authenticated by the Pre-Boot Environment, using fixed passwords or smartcards. In addition, a remote help feature allows the user to receive a one-time password that allows the user to login in the case of mislaid authentication credentials, as well as changing a fixed password that has been forgotten. The Pre-Boot Environment maintains an authentication failure counter. When the administrator-configurable threshold is exceeded, the TOE marks the user’s account record as locked, so that further login attempts to this account are denied until the account is unlocked by an authorized administrator or until a preset time interval has passed.

Once authenticated, Check Point Endpoint Security boots up the operating system normally, installing a kernel driver that decrypts disk contents on the fly, transparently to the user, as well as transparently encrypting any updated disk sectors. Encryption is performed using encryption keys that are derived from user credentials. This ensures that Full Disk Encryption is maintained at all times, even when the workstation powers down unexpectedly. It also obviates the need to do a full disk overwrite on discarded disks – the data on the disk is unreadable without the user credentials.

FIPS 140-2 validated cryptography (FIPS 140-2 certificate #770) is used for Full Disk Encryption, using either 256 bit AES or Triple DES as encryption algorithms.

7.3.2 Encryption Policy Manager (EPM)

The Encryption Policy Manager (EPM) provides a configurable Removable Media Encryption capability that extends cryptographic protection to removable media devices. When a removable media device is inserted into a protected workstation, Check Point Endpoint Security can be configured to restrict access only to an encrypted storage area on the device, or conversely to allow only read-only access to prevent information from leaking onto an insecure device.

The Device Encryption Key (DEK) is generated randomly and stored in encrypted form, wrapped by a Key Encryption Key (KEK) that is generated and stored on the management server (outside the TOE), or stored on the media encrypted in a password-based encryption format with a user-entered password, for supporting offline access to the data when the management server is not available. Encryption and decryption are performed transparently when data is written to or read from the removable device. FIPS 140-2 validated 256 bit AES (FIPS 140-2 certificate #784) is used for data encryption.

Check Point Endpoint Security can also be configured to encrypt information written to CD and DVD removable media, when using the operating system’s built-in CD/DVD writing software.

7.3.3 Device Manager

Device Manager controls user access to devices connected to various ports on the workstation, including USB, COM, LPT, PCMCIA, IrDA, Firewire and Bluetooth ports, as well as other devices such as modems, network adaptors, and storage devices.

The administrator can determine for each device whether access is enabled for full access (Read/Write), disabled or set to Read Only, and for removable media and removable media devices, whether the workstation may execute programs from the removable media.

7.3.4 Removable Media Manager

Unauthorized media inserted into a protected workstation may contain malware that might infect the workstation. Check Point Endpoint Security can be configured to reject access to unauthorized removable media devices and floppy disks, or to invoke a content scanner installed in the operational environment of the workstation (e.g. anti-virus software) to authorize the device. Note that the content scanners are not covered by the evaluation.

Check Point Endpoint Security stores a computed permutational hash on the device that represents the data written to the device from authorized Check Point Endpoint Security workstations. When a removable media device or floppy disk is inserted into a protected workstation that does not contain a hash, the Removable Media Manager concludes that this is the first time that the media is imported into Check Point Endpoint Security. When the hash on the device does not match the media contents, it has been modified on an external workstation. In either case, the media requires re-authorization for access to be allowed.

7.3.5 Firewall

Check Point Endpoint Security implements information flow control rules representing a Personal Firewall Policy that mediates all inbound and outbound network traffic from the protected workstation. Traffic can be allowed or blocked based on source and destination addresses, protocols and ports.

7.3.6 Application Control

In addition to the information flow control defined by Firewall Rules, Check Point Endpoint Security implements network access control for programs on the workstation.

Each program can be allowed or blocked from establishing network connections, on the basis of the presumed identity of the peer host (trusted or otherwise), on the basis of whether the program is initiating the connection or listening for one (acting as a server), and the requested protocols and ports. Programs that violate the Application Control rules may also be automatically terminated. Programs are authenticated on execution and when attempting to connect to network resources by calculating a MD5 hash of the program's components and comparing it to the hash stored in the program list.

This feature can provide mitigation for Trojans and spyware that attempt to connect to malicious servers. It can also mitigate viruses that attempt to modify programs on the workstation. Application Control will detect a new or modified program and will prevent it from accessing the network.

The application control blade also provides the capability to invoke third-party anti-virus software. The vendor has tested TOE invocation of the following third party anti-virus software: McAfee VirusScan and Kaspersky Antivirus. Invocation of other anti-virus products were not covered by this evaluation; Check Point's support website provides solution id sk68080 that provides a current list of AntiVirus products the vendor claims this product supports. New releases of those products are supported through the Flaw Remediation process. Due to the dynamic nature of AV products TOE users should contact Check Point Support for integration of new AV versions into the TOE. The anti-virus engines themselves are in the operational environment, and thus outside the TOE boundary.

7.3.7 Program Advisor

Smart Defense Program Advisor is a Check Point service that provides recommendations for Application Control. It can be used to reduce administrative workload by incorporating recommendations from Check Point security professionals about which permissions to assign to common programs.

Customers download Program Advisor recommendations from Check Point into the management server, and may choose to either accept these permission settings or override them with custom settings. This interaction is entirely outside the TOE boundary.

7.3.8 Enforcement Rules (Protection of the TSF)

Check Point Endpoint Security can be configured to monitor the protected workstation for compliance with policy restrictions defined as Enforcement Rules. Enforcement Rules may require a certain anti-virus application to be active, a minimum version of the Check Point Endpoint Security client itself, or the presence or absence of defined registry keys, files, or programs indicating the presence or absence, respectively of a security-relevant component on the workstation.

When an Enforcement Rule is found to be in non-compliance, the user or administrator may receive a notification, or the workstation may be restricted from accessing the network and/or other defined I/O devices, except for a defined “sandbox” area from which the user may download remediation resources.

7.3.9 VPN Client (Trusted path/channels)

Check Point Endpoint Security can be configured to establish VPN trusted channels to Check Point gateway products, using the IKE/IPSec protocols. The gateways’ Encryption Domain (the set of addresses located behind the gateways) is downloaded from the gateway after it is authenticated by its public key certificate. Once the trusted channel is connected, all traffic to and from the gateway’s Encryption Domain is protected from disclosure and modification while traversing the network. The client can also be configured to route all traffic through the VPN tunnel to the gateway (Hub Mode), so that all traffic is filtered by the gateway. The TOE includes the Endpoint Connect VPN; this is the only VPN usable in the evaluated configuration.

8 Documentation

8.1 Product Guidance

The following is list of the guidance documentation, each of which was issued by the developer (and sponsor) and can be obtained on their website and with the product download:

- Endpoint Security CC Evaluated Configuration Administrator Guide Version E80.30, January 2014
- Endpoint Security CC Evaluated Configuration User Guide Version E80.30, September 2013
- Endpoint Security Client E80.30 User Guide, 2 November 2011

Additionally the following *proprietary* evidence was used in the evaluation. It is not generally available to the public.

- Check Point Endpoint Security Life Cycle Version 0.5, November 15, 2013
- Check Point Endpoint Security Test Documentation Version 1.6, November 18, 2013
- Actual Test Results (screenshots)
- Check Point Endpoint Security E80.30 Security Target, Version 1.0, January 22, 2014
- Check Point Endpoint Security Functional Specification Version 0.8, November 19, 2013
- Check Point Endpoint Security TOE Design Specification Version 0.4, November 15, 2013
- Check Point Endpoint Security Architecture Version 0.4, April 14, 2013
- Check Point Endpoint Security Supplementary Evidence:
- Check Point Endpoint Security Ben Gurion Management Client Interface Protocol Specification Version 2.11, not dated

- Check Point Endpoint Security R7x Functional Specification Version 0.22, December 29, 2011
- ZoneLabs Product Architecture Document Zonelabs Protected Document Specification (K2_zpdoc), Version 1.0 September 19, 2013

9 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

Some of the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. Such cryptography has only been asserted as tested by the vendor. Section 6.2 identifies the cryptographic functions that are provided by FIPS-assessed components, and the cryptographic functions that are only asserted as tested by the vendor.

9.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function, more specifically to the security functional requirements tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security Audit, Security Management, Cryptographic Support, User Data Protection, Identification and Authentication, Protection of the TSF, Trusted Path/Channels. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

9.2 Evaluation Team Independent Testing

The evaluation team used a sampling approach versus exercising the entire set of manual tests provided as evidence for the evaluation. The vender test suite is comprised of 66 Test Procedures each containing multiple test cases comprising a total of 190 manual test cases which are directly related and mapped to satisfy the TOE security functions. The vendor's test coverage is quite exhaustive in many cases and provides numerous examples of coverage of the same aspect of a particular security function. Therefore, the test sampling approach was not based on a percentage of test cases as this would not be necessary, nor time and cost efficient.

The tests were run on the on Windows 7 Enterprise SP1 32-bit test configuration described in the developer's test documentation. The documentation describes the configurations that were used in the test configurations.

The evaluation team performed the following sampling approach when determining the sample size:

- Exercise 18 test procedures, which represent a sample size of 27%.
- Test cases include tests from each of the claimed security functions, security audit, cryptographic support, identification and authentication, User data protection, security management, protection of the TSF.
- Test cases included tests covering all TSFI.

The following hardware was used to create the test configurations:

- ESM Machine – Windows 2003 Server
- Domain Controller Machine – Windows 2003 Server
- Internet machine – Windows 2003
- Endpoint PC – Dell E6510 laptop
- Non-Endpoint PC – Lenovo T500 laptop

These machines were configured as follows. All machines were connected to a network switch or hub in accordance with the test setup instructions:

- **ESXi Server Version 5.0** – running the following machine images:
    - **ESM Machine (EMS PC)** – Windows 2003 Server
        - Endpoint Management Server E80.30
        - SmartConsole E80.30 (UEPM Console etc)
        - SmartConsole R75.20
        - Network Share Folder
    - **Domain Controller Machine (EAL.com PC)** – Windows 2003 Server
        - Active Directory
        - DNS Server
    - **Internet Machine (Internet_External PC)** – Windows 2003
        - Web Server
        - FTP server
    - **VPN Management and GW Machine (FW_GW PC)** – Open Server Splat R75.20
    - **FW Host (FW_Host PC) --** Windows XP
        - Web Server
        - FTP server
- **Endpoint PC** – Windows 7 64 bit SP1 installed on Dell E6510 laptop
    - Member of DC Windows domain
    - Endpoint client E80.30
    - USB-connected scanner and printer device (HP OfficeJet 4500)
    - CD-ROM R/W drive
    - Internal Bluetooth Radio Driver (for built-in laptop BT h/w)
    - FileZilla FTP Server v0.9.41
    - Smart Card: Aladdin eToken 32k (eToken #1 and #2)

  - Aladdin PKI RTE V 5.1 SP1 Windows 7 64-bit eToken middleware and smart card driver

- **Endpoint PC2** – Same content as EndpointPC but running Windows 7 32 bit OS on a Lenovo T400 instead
- **Non-Endpoint PC** –Windows 7 installed on a Lenovo T500 laptop
  - SmartConsole E80.30 (UEPM console etc)
  - SmartConsole R75.2

The following additional items were required for testing:

- USB-connected scanner and printer device (HP OfficeJet 4500)
- CD-ROM R/W drive
- Internal Bluetooth Radio Driver (for built-in laptop BT h/w)
- FileZilla FTP Server v0.9.41
- Smart Card: Aladdin eToken 32k (eToken #1 and #2)
- Aladdin PKI RTE V 5.1 SP1 Windows 7 64-bit eToken middleware and smart card driver
- Blank CDs and DVDs –a CD/DVD burn uses up the media, i.e. the media cannot be reused once written.
- CD with executable content.
- USB removable media device – at least three devices are needed for testing:
  - USB#1 – FAT32 formatted
  - USB#2 – FAT32 formatted.
  - USB#3 – encrypted in site “Black”.
  - USB#4- NTFS formatted
  - USB#5- USB 3.0
  - USB#6 – FAT 32 formatted

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

9.3 Vulnerability Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE, identifying a number of vulnerabilities reported against components that are not included in the TOE or otherwise addressed by fixes. Fixes were issued for the two vulnerabilities could potentially apply to the TOE: CVE-2011-4838 and CVE-2012-2753. CVE-2012-2753 was tracked through the bug tracking system to ensure procedures were followed for fixes to the TOE verifying the fix was included in the TOE release. Additionally, the evaluators developed vulnerability tests to address the Protection of the TSF and TOE access security functions.

10 Evaluated Configuration

The TOE is Check Point Endpoint Security E80.30 (build 8.1.327) with the following software blades: Full Disk Encryption, Media Encryption & Port Protection, Firewall & Application

Control, Compliance, and VPN. Check Point Endpoint Security is a workstation security software product that is installed on user desktop and laptop hosts in an enterprise setting. Supported operating systems include: Windows 7 Enterprise, Professional, Ultimate editions (32-bit and 64-bit).

These components are installed on a workstation running a Microsoft Windows operating system. The underlying hardware platform and operating system on which the TOE software is installed are considered to be in the operational environment, and thus outside the TOE.

The vendor has tested TOE invocation of the following third party anti-virus software: McAfee VirusScan and Kaspersky Antivirus. Invocation of other anti-virus products was not covered by this evaluation; Check Point's support website provides solution id sk68080 that provides a current list of AntiVirus products the vendor claims this product supports. New releases of those products are supported through the Flaw Remediation process. Due to the dynamic nature of AV products TOE users should contact Check Point Support for integration of new AV versions into the TOE. The anti-virus engines themselves are in the operational environment, and thus outside the TOE boundary.

While some basic management capabilities are provided in the client software, Check Point Endpoint Security clients are designed to be centrally managed. However, management server products are separate products that are not required to effectively use the client. In the context of this ST, the management server is treated as a 'remote user' that can be authorized to perform identified TOE management operations

All Check Point Endpoint Security E80.30 (build 8.1.327) product functionality is not included in the Target of Evaluation. The following features have not been evaluated as to their correctness:

- **Advanced Password Functionality.** Specifically, although the product supports password complexity requirements and a password history, these capabilities were not covered by the evaluation.
- **Login banners**.
- **Bundled Third-party Anti-Virus Product**. The third-party anti-virus product bundled with the TOE is considered to be outside the boundaries of the TOE. However, the TOE supports a variety of anti-virus products that may be installed on the workstation by the user, independently of the TOE.
- **Smart Cards.** Although authentication using smartcards was included in the evaluation, the capability of the smartcards and the smartcard readers themselves were not.
- **Underlying Hardware and Software Environment.** The TOE components are installed on a workstation running a Microsoft Windows operating system. The underlying hardware platform and operating system on which the TOE software is installed are considered to be outside the TOE.
- **Audit Log Protection.** The TOE protects audit logs when stored locally. Audit logs are stored on the encrypted part of the disk and thus the TOE requires user authentication prior to granting access to local audit logs. Also, the TOE does not provide interfaces to delete audit data. Since there are no SFRs related to local audit storage, the TOE behavior regarding the storage, integrity and overwriting of local audit storage has not be evaluated.
- **Local Audit Review.** Only the remote transmission audit mechanism has been evaluated, including the remote review of audit. Local review of audit does not satisfy the Common

Criteria audit requirements; therefore, the local review of audit data was not evaluated and was not tested.

Some Check Point Endpoint Security functionality is specifically excluded and thus its use is ***NOT*** permitted in an evaluated configuration:

- **Software Blades**. The TOE is comprised of the following Check Point software blades: Full Disk Encryption, Media Encryption & Port Protection, Firewall & Application Control, Compliance, and Virtual Private Networking (VPN). The Check Point Endpoint Security also provides two additional blades: the Check Point WebCheck Blade and the Check Point Anti-malware blades. These blades have not been evaluated. They are not permitted, and must not be installed, in an evaluated configuration.
- **Legacy VPN Clients.** The TOE includes the Endpoint Connect VPN, however, the command line option for endpoint connect is not permitted to be used in the evaluated configuration. Additionally, the use of the Check Point Legacy VPN is not permitted in the evaluated configuration.
- **Virtual Keyboard/Character Map.** The Virtual keyboard and character map function of the TOE are NOT permitted in the evaluated configuration.

11 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. The product was evaluated and tested against the claims presented in the Check Point Endpoint Security E80.30 Security Target, Version 1.0, dated January 23, 2014.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validator therefore concludes that the evaluation team's results are correct and complete. The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.3" certificate rating be issued for Check Point Endpoint Security E80.30 (build 8.1.327).

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the LEIDOS CCTL. The security assurance requirements are listed in the following table.

12 Validator Comments/Recommendations

The following comments highlight specific concerns or recommendations from the Validator that may be of interest to consumers of this product:

1. Some of the cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. Such cryptography has only been asserted as tested by the vendor. Section 6.2 identifies the cryptographic functions that are provided by FIPS-assessed components, and the cryptographic functions that are only asserted as tested by the vendor.
2. The efficacy of the Anti-Virus scanning was not covered by this evaluation. The vendor only tested the invocation of a subset of the supported virus scanners in accordance with policy.
3. The local audit display mechanism does not display the identity of the subject as part of the audit record (although that information is stored in the record). Due to this, the local audit display mechanism *does not* satisfy the Common Criteria audit mechanism and thus was not covered by the evaluation. To review audit in accordance with Common Criteria requirements, the remote audit review interface must be used.
4. Although the product appears to provide many mechanisms that would support NIST 800-53 controls related to authenticator management (IA-5), the only *evaluated* capabilities are those enumerated in the ST. The additional capabilities provided were not covered by the evaluation.
5. The product does not include SFRs related to protecting against audit data loss. It is the administrator's responsibility to ensure that audit is archived to a safe location on a regular basis in order to prevent audit loss.

13 Security Target

The ST for this product's evaluation is Check Point Endpoint Security E80.30 Security Target, Version 1.0, dated January 22, 2014. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.3.

14 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, July 2009.
4. Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 3, July 2009.
5. Check Point Endpoint Security E80.30 Security Target, Version 1.0, dated January 22, 2014.