Solera Networks Inc.

Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0

Security Target

Evaluation Assurance Level (EAL): EAL3+
Document Version: 1.7

Prepared for:

Solera Networks Inc.
10713 South Jordan Gateway, Suite 100
South Jordan, Utah 84095
United States of America

Phone: +1 (801) 545-4100
Email: info@soleranetworks.com
http://www.soleranetworks.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0, and will hereafter be referred to as the TOE throughout this document. The TOE is deployed across two systems: the first system runs Solera DeepSee Central Manager v6.5.0 and the second system runs only Solera DeepSee Software v6.5.0. The TOE is management software, network forensic applications, and a supporting operating system that captures, archives, filters and regenerates network traffic data at full-line rates, up to 10 Gigabits per second (Gbps).

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 ST and TOE References

ST Title	Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 Security Target
ST Version	Version 1.7
ST Author	Corsec Security, Inc.
ST Publication Date	9/28/2012
TOE Reference	Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 build 24397

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

Solera Networks Solera DeepSee Software performs deep packet capture, recording and archiving 100% of network traffic at speeds up to 10 Gbps. The complete and accurate record of network traffic provides IT[1] managers with full visibility into all network activities to support root cause discovery, reduce network performance issues, and decrease time-to-resolution. Solera DeepSee Software creates a complete record of network traffic (including both packet headers and payloads), facilitating regeneration, filtering, and playback for later analysis.

The major features of Solera DeepSee Software are:

- Improved network security – Network administrators have comprehensive evidence to better protect against intruders, data leakage, and internal misuse.
- Optimized network performance –Solera DeepSee Software provides a complete network record to replay without affecting the production network, allowing detailed network traffic analysis to uncover areas of the network that may require attention.
- Maximized ROI[2] – Appliance scalability and deployment options allow organizations of all sizes to benefit from deep packet capture and analysis to improve network performance and security.
- Increased network tool options –Solera DeepSee Software works with many management, analysis, and forensic tools (commercial, custom, and open source) to monitor, manage, and secure the network.

The TOE can be deployed in a virtual environment as a VMware virtual image or on Solera provided Dell hardware. The software maintains the same functionality whether deployed on the Dell hardware or on an ESX(i) server.

Solera DeepSee Software can be managed locally on a capture appliance or can be managed by Central Manager. Central Manager is an application that runs on the Solera DeepSee Software and allows management of multiple Solera DeepSee Software appliances and aggregation of the DeepSee data from all managed appliances. Central Manager can manage appliances deployed directly on hardware or in a virtual environment. Multiple appliances can be managed from one Central Manager. Appliances managed by a Central Manager are called Appliances Under Management (AUM).

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a software only TOE that consists of two components. The capture component has Solera DeepSee Software v6.5.0. The management component has Solera DeepSee Central Manager v6.5.0, which includes Solera DeepSee Software with the Central Manager application licensed and enabled. There are two evaluated configurations for the TOE: a DS Configuration that includes both components installed on separate Dell servers, and the Virtual Configuration that includes both components installed on one or more ESX(i) servers. Figure 1 shows the details of the deployment configuration of the TOE. The TOE is installed on hardware that is connected passively and sits undetected on the network without affecting the network performance.

[1] IT – Information Technology
[2] ROI – Return On Investment

Operators can interface with the TOE in one of three ways:

1. The DeepSee Browser Interface is a web-based Graphical User Interface (GUI) that allows authenticated operators to initiate and monitor network traffic capture, filter and replay captured data, transfer captured data to various locations, access stored data, view statistics, and perform general administration of an individual AUM.

   This GUI is accessed using a standard web browser. Operator authentication is required before any services are offered by the DeepSee Browser Interface.

   Solera DeepSee Software includes Solera Networks DeepSee suite of network security applications. DeepSee is available as part of the web GUI, but the appliance must be licensed and appropriately configured to use DeepSee. DeepSee provides the capability to locate and reconstruct specific communication flows or network activities from the network traffic captured by the TOE. DeepSee indexes captured packets from network traffic and identifies specific "flows" (a collection of captured packets making up a communication between two specific network entities) that are important to IT and business users. Organizations can then identify and examine network artifacts such as image files, Word documents, emails, video files, and executables.

2. The Web Services APIs[3] provide access to captured data through simple HTTPS[4] requests. Data retrieval requests can be scripted using commonly available tools like *wget* or *curl*. Limited management functions can be performed through these APIs.

3. The DeepSee Central Manager Interface is a web-based GUI similar to the DeepSee Browser Interface. The primary differences between the two interfaces is that the DeepSee Central Manager Interface aggregates the data of all appliances attached to it and allows users to access more than one appliance from one interface.

Management communications with the module occur over TLSv1[5]-protected communications channels. The TLSv1 protocol and the underlying cryptographic algorithms are provided by OpenSSL. The executable images run over Solera DeepSee Software v6.5.0, which is a Linux-based operating system and includes the DeepSee applications. Solera DeepSee Software supports local identification and authentication.

The TOE can provide the following services in addition to the administrative management services:

- Capture and store network traffic: The TOE assists the underlying hardware in performing network traffic capture process listens on pre-configured interfaces and captures data to the Solera Networks high-speed file system at a line rate of 10 Gbps networks, without any packet loss. All available and connected interfaces on the appliance (such as eth2, eth3, etc.) can be configured to start or stop the capture of network traffic, except eth0 and eth1 because they are dedicated for management tasks.

- Replay the captured network traffic: The captured network traffic is available for analysis in the following ways:

  - **PCAP[6] Files:** Any user can create and download a PCAP file by specifying parameters such as begin and end time, source IP[7] address, or destination port.

[3] API – Application Programming Interface
[4] HTTPS – Hypertext Transfer Protocol Secure
[5] TLSv1 – Transport Layer Security
[6] PCAP – Packet Capture
[7] IP – Internet Protocol

- **Regeneration:** The captured network traffic can be forwarded to a physical network interface in near real-time.
- **Playback:** The historical network data flows can be reconstructed and transmitted to a physical network interface.

- Create and apply filters: Filters can be created for capturing traffic or regenerating the captured traffic. Filters limit the data included in, or extracted from, the captured network data. Once created, a filter definition can be saved as a filter file and reused as needed. Saved filters can be applied to PCAP generation, network regeneration, and network playback.

- Generate and display reports: Multiple reports are generated (apart from audit logs) in the form of a chart, text or graph containing statistics related to network traffic. Various available reports (apart from Log Reports) are the Network System Report, the Size on Disk Report, the Storage System Report, the Total Captured Report, and the Total Filtered Report.

- Extract artificial objects with DeepSee: Solera Networks DeepSee is used to locate and reconstruct specific communication flows or network activities from captured network traffic. DeepSee has the ability to index, search, and reconstruct all network traffic into meaningful flows, including network artifacts. DeepSee is available as part of the DeepSee Browser Interface, but the Solera DeepSee Software must be licensed and appropriately configured to use DeepSee.

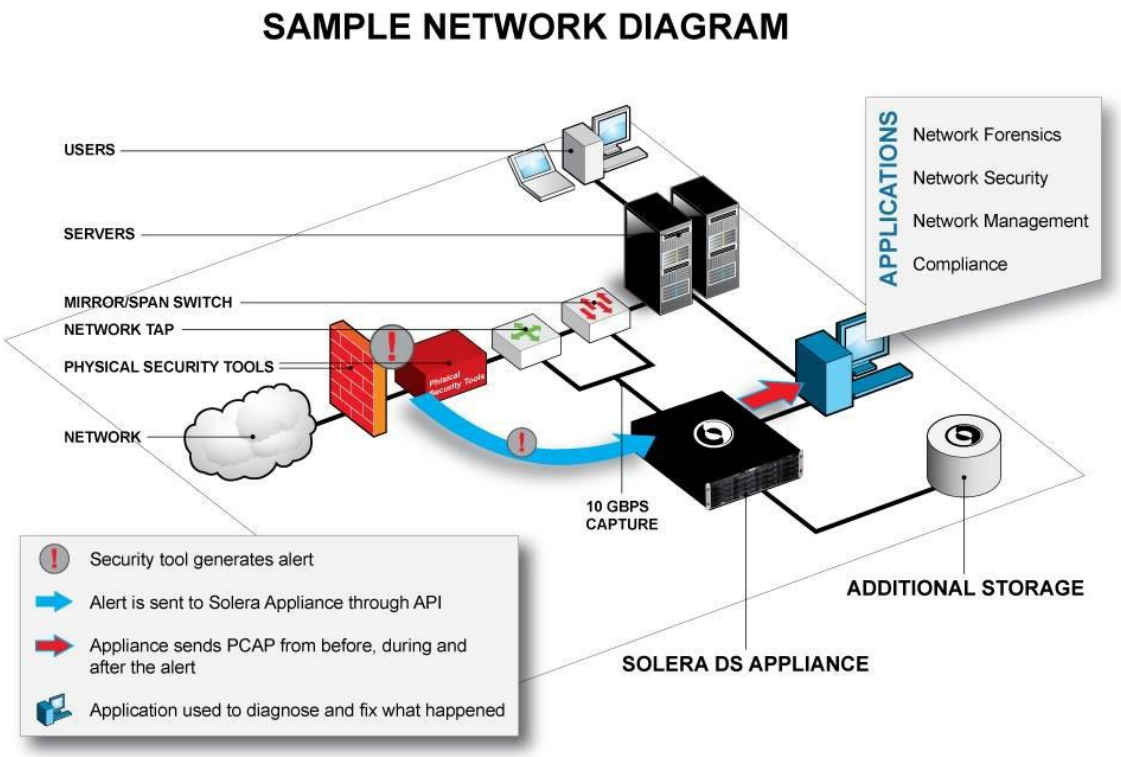

Figure 1 Sample Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The following components are part of the evaluated configuration of the TOE, and work together to provide the TOE functionality. The TOE excludes the physical and logical features and functionality listed in 1.5.3.

1.4.1.1 Solera DeepSee Software

The Solera DeepSee Software v6.5.0 is a Linux-based operating system (OS) that facilitates the DeepSee applications in performing network security applications. The OS provides Identification and Authentication for local users that are created within the OS, but the permissions are enforced by the DeepSee application. It facilitates an administrator in performing operations using basic Linux commands as well as using Linux commands that require root-level permissions. Solera DeepSee Software includes the DeepSee application that performs the network security applications.

1.4.1.2 Central Manager

The Central Manager application is included in Solera DeepSee Central Manager v6.5.0, but must be separately licensed. The Central Manager allows users to manage multiple appliances running Solera DeepSee Software from one central location. When the Central Manager application is licensed and enabled the Solera DeepSee Software on that component will no longer capture network traffic, but will aggregate the traffic data from the attached appliances. The Central Manager communicates with the attached appliances and the management workstation through the management network.

1.4.2 TOE Environment

It is assumed that there will be no untrusted users or software on the TOE. In addition, the TOE is intended to be deployed in a physically secure environment and managed by administrators who are appropriately trained and follow all guidance listed in 1.5.1.2.

The evaluated deployment configuration of the TOE requires the following environmental components:

- Workstation with web browser installed for device management.
- Connection to network traffic via a Switched Port Analyzer (SPAN) port, a network Test Access Point (TAP) or an optical splitter.
- Hardware platform – Table 2 lists the hardware differences for the DS Configuration and Virtual Configuration.

The minimum software and hardware requirements for the TOE environment are listed in Table 2.

Table 2 TOE Environment requirements

Component	Number in DS Configuration	Number in Virtual Configuration	Requirement
Hardware platform to run VMware image	0	2	• 8 GB[8] of RAM[9] • 100 GB of available storage • Dual 2.0 GHz[10] processor speed (or above)
VMware ESX(i) Server	0	2	VMware ESX Server 5.0; or ESXi 5.0
Hardware platform for AUM and Central Manager	2	0	• 1 Dell R720 with Intel Xeon processors for AUM • 1 Dell R720 with Intel Xeon processor for Central Manager Appliance

[8] GB – Gigabyte
[9] RAM – Random Access Memory
[10] GHz – Gigahertz

Component	Number in DS Configuration	Number in Virtual Configuration	Requirement
Management Workstation with web browser	1	1	• Internet Explorer 8, 9 • Firefox 10, 11, 12, 13, 14 • Safari 5 • Chrome 19

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the TOE DS Configuration and ties together all of the components of the TOE and TOE Environment. Figure 3 illustrates the physical scope and the physical boundary of the TOE Virtual Configuration and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a network forensic software solution which runs on Dell hardware appliances or a virtual platform compliant to the minimum software and hardware requirements as listed in Table 3. The TOE is installed as depicted in Figure 2 or Figure 3 below. The essential components for the proper operation of the TOE in the DS configuration are:

- Solera DeepSee Software v6.5.0
- Solera DeepSee Central Manager v6.5.0
- General purpose computer for management workstation
- SPAN or Network TAP

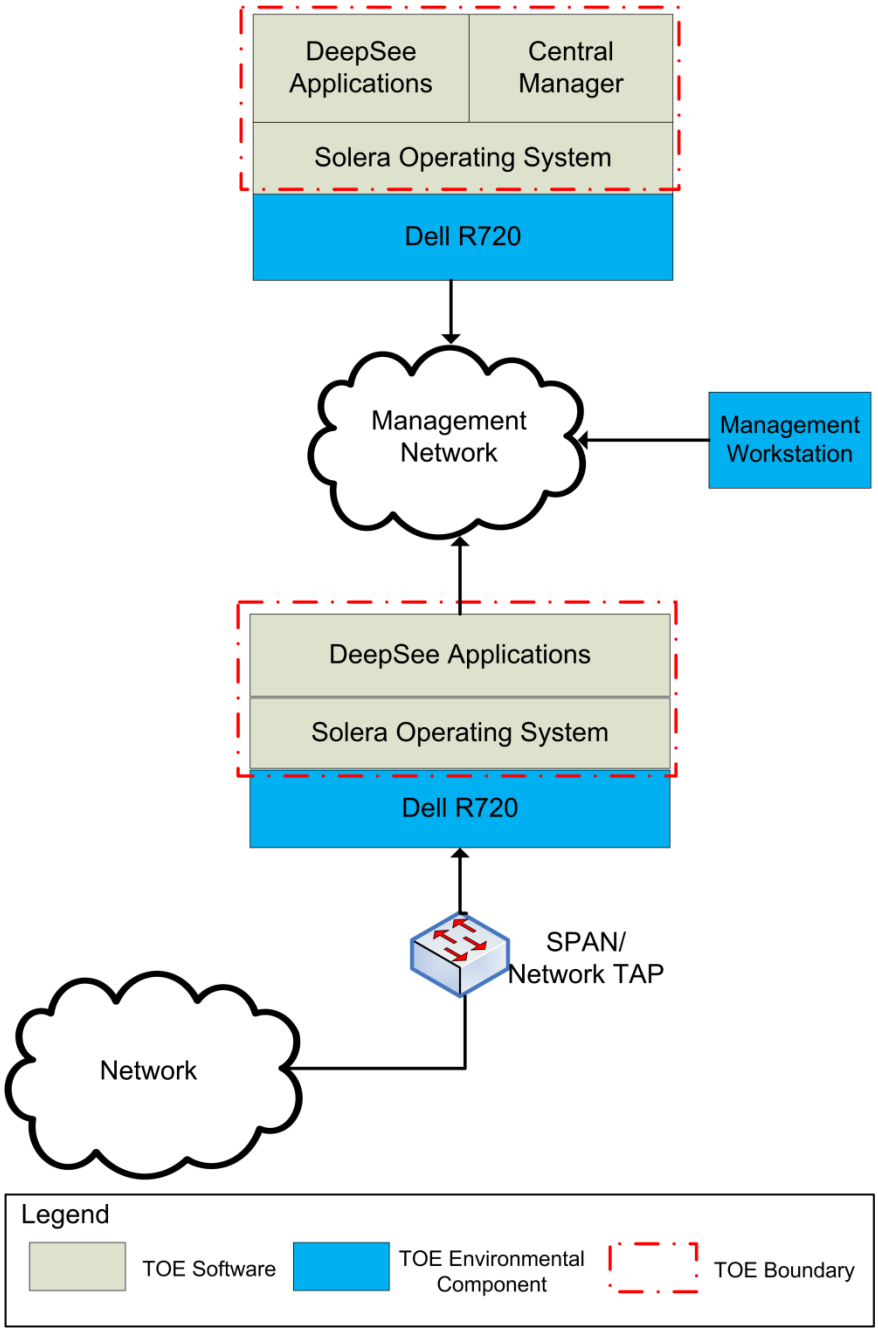

Figure 2 DS Configuration TOE Boundary

The essential components for the proper operation of the TOE in the Solera Virtual Appliance evaluated configuration are:

- Solera DeepSee Software v6.5.0
- Solera DeepSee Central Manager v6.5.0
- General purpose computer for management workstation
- SPAN or Network TAP

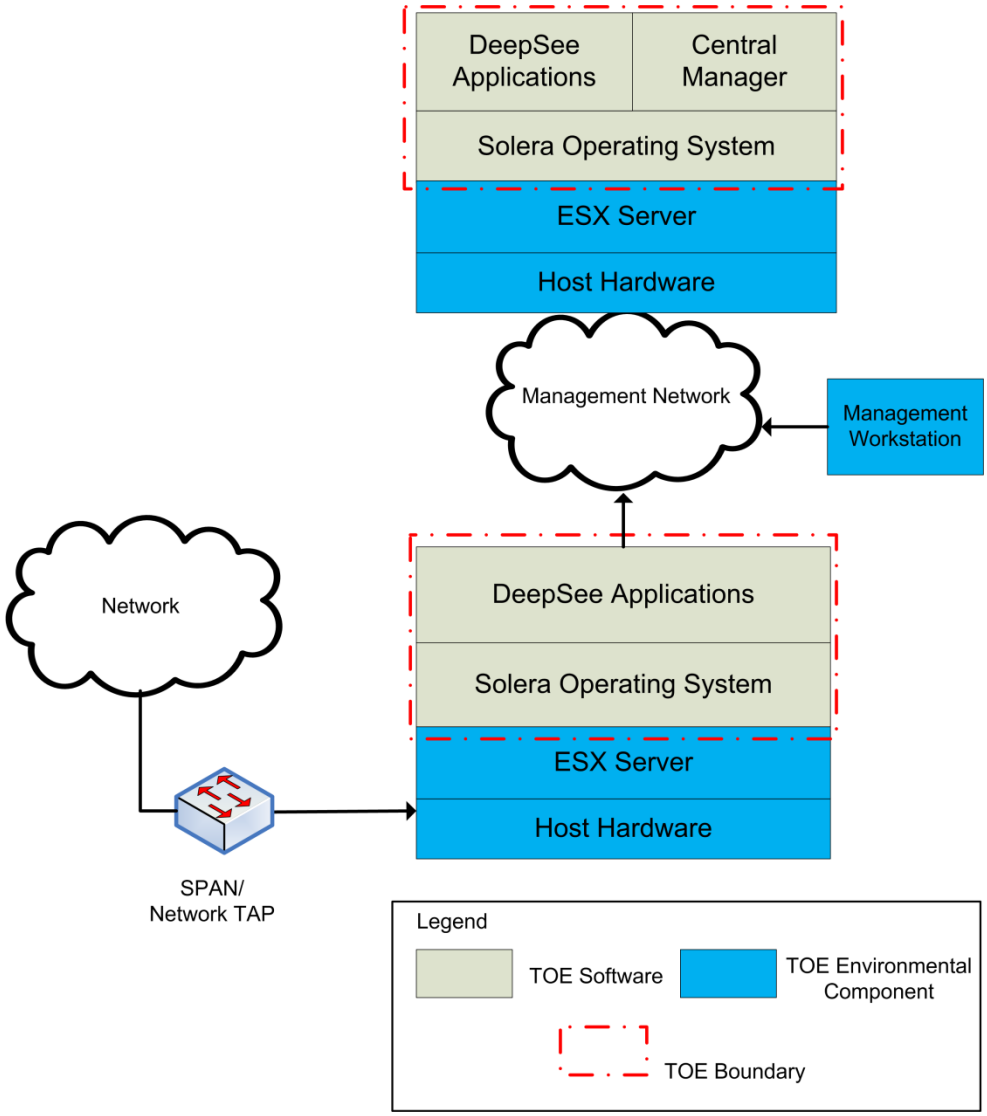

Figure 3 Virtual Configuration TOE Boundary

1.5.1.1 TOE Software

The TOE software is installed on two systems: the management system is installed with Solera DeepSee Central Manager v6.5.0 and licensed for DeepSee applications and Central Manager and the capture system is installed with Solera DeepSee Software and licensed for DeepSee applications only. Table 3 specifies the minimum system requirements for the proper operation of the TOE.

Table 3 TOE Minimum Requirements

Component	Requirement
Central Manager Software	• Solera DeepSee Central Manager v6.5.0
AUM Software	• Solera DeepSee Software v6.5.0

1.5.1.2 Guidance Documentation

The following guides are required reading and are considered to be part of the TOE:

- Solera Networks SoleraSix Administration Guide, March 2012
- Solera Networks SoleraSix Virtual Appliance Installation Guide For VMware ESX Server, April 2012
- Solera Networks SoleraSix Central Manager Guide, March 2012

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trust Path/Channels

1.5.2.1 Security Audit

Solera DeepSee Software generates audit records for the security relevant actions of all authorized users accessing the TOE. It also records all unsuccessful attempts made to access the TOE. The TOE makes sure that only authorized users are allowed to view the Audit and System log records. Audit and System log data can be selected for review and ordered by the Date/Time category.

1.5.2.2 Cryptographic Support

The TOE uses OpenSSL to perform encryption and decryption of management traffic. The TOE implements Cryptographic Algorithm Validation Program (CAVP)-validated cryptographic algorithms to handle all cryptographic functions for the encryption and decryption of data.

Management communications between the TOE and operators occur over TLSv1 protected communications channels. The TLSv1 protocol and the underlying cryptographic algorithms are provided by the OpenSSL cryptographic library.

1.5.2.3 User Data Protection

The TOE enforces the Solera Access Control Policy on users and processes on behalf of users trying to perform operations (such as *Replay traffic*, *Apply or create Filters*, *Generate Reports*, or *Perform DeepSee Analysis*) on the captured network traffic data. Only authorized users or processes are allowed to access and perform operations on the captured data.

1.5.2.4 Identification and Authentication

The TOE requires that all TOE users are authenticated by the TOE. The TOE is responsible for identification of all authenticated users. Users who authenticate to the Central Manager may also be granted permission to access and manage the attached appliance. Users who authenticate to the attached appliance only have access to that appliance.

1.5.2.5 Security Management

The TOE provides administrators with the ability to manage the behavior of security functions and security attributes of an individual appliance through the DeepSee Browser Interface, Web Services API, or through DeepSee Central Manager Interface. The TOE maintains three roles: Administrator, User, and Auditor.

The TOE allows users to be assigned to one of the predefined roles and assume the permissions that are associated with the predefined role. The TOE allows Administrators to manage the attributes associated with the Solera Access Control Policy.

1.5.2.6 Protection of the TSF

The TOE provides reliable time stamps via the OS, which can be changed or set manually by the administrator. The reliable time stamps are used in audit record generation.

The internal communications between the Central Manager and AUM are protected from modification and disclosure by TLSv1, using CAVP-approved algorithms.

1.5.2.7 TOE Access

An administrator can configure the TOE to display a warning banner at the beginning of each login prompt of each session.

1.5.2.8 Trust Path/Channels

The TOE provides a trusted channel between itself and management workstations using TLSv1 and CAVP-validated algorithms. Each user session is a unique HTTPS session that can be initiated by the TOE or the management workstation.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Most features and functionality of Solera DeepSee Software v6.5.0 and Solera DeepSee Central Manager v6.5.0 are part of the evaluated configuration of the TOE. Features/Functionalities that are not part of the evaluated configuration of the TOE are:

- Lightweight Directory Access Protocol authentication
- Hardware platforms
- Command line interface
- Network time protocol
- Simple Network Management Protocol
- Intelligent Platform Management Interface (IPMI)

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2012/05/04 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3+ augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[11] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 5 Threats

Name	Description
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future records from being recorded, thus masking a user's actions.
T.DATA_COMPROMISE	An unauthorized user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or TOE environment.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.PACKET_LOSS	The TOE might not be able to capture all network traffic if it is not deployed and configured appropriately.
T.TAMPERING	A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.

[11] TSF – TOE Security Functionality

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 Assumptions

Name	Description
A.DEPLOY	The TOE is assumed to be deployed in a TOE environment such that the network is configured properly and its size is appropriate for the TOE functionality.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.NOEVIL	TOE users are non-hostile, appropriately trained, and follow all guidance.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 7 Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE will ensure that users gain only authorized access to the TOE, the TOE data and to the resources that TOE controls.
O.AUDIT	The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail.
O.AUDIT_REVIEW	The TOE will provide the capability for only authorized users to view audit information.
O.CRYPTO	The TOE will make cryptographic services available to authorized users and/or user applications that can be both data authentication and data encryption.
O.TIME	The TOE will provide reliable timestamps via the OS.
O.TOE_ADMIN	The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE. The TOE will also provide protections for logged-in administrators.
O.USER_AUTHEN	The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.
O.SECURECOMMS	The TOE requires that information transmitted between the TOE and TOE administrators and between TOE components never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 8 IT Security Objectives

Name	Description
OE.DEPLOY	The TOE must be deployed in the TOE environment such that the network is configured properly and its size is appropriate for the TOE

Name	Description
	functionality.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow and apply all administrator guidance in a trusted manner.

5 Extended Components

There are no TOE Extended Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓	✓	
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

Name	Description	S	A	R	I
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FPT_STM.1	Reliable time stamps				
FTA_TAB.1	Default TOE access banners				
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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) [*Authentication attempts (FIA_UAU.2 & FIA_UID.2), administrative actions (FMT_MSA.1, FMT_MSA.3, FMT_MTD.1), and specifically defined auditable events as listed in* Table 11].

Table 11 Auditable Events

Events	Description
Create or views extraction	User creating or viewing an extraction or extraction artifact
Changes to user accounts	All changes made under **Profile > Account Info**
Regeneration	Starting or deleting regeneration
Playback	Starting or deleting playback
View results	User viewing saved results
Changes to settings	Changes made in the Settings menu to include: • Network • System • Security • Data Retention • Users • Date/Time • License • Web Interface
Password changes	Changes to a user's password
Capture	Start or stop of network capture
PCAP	Creation or deletion of PCAP
Filter	Actions performed under **Capture > Filter**
Login	Login failures
PostgreSQL sessions	Opening or closing a session with PostgreSQL database
Audit log	Viewing or clearing of audit log
System log	Viewing of system log
Reports	User creating or viewing a report
Self-tests	Failure of a power up self-test for the cryptographic functions

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 (if applicable), 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, [*none*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*Administrators, Users, and Auditors*] with the capability to read [*all Audit and System logs*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to apply [*methods of ordering*] of audit data based on [*Date/Time*].

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the 'Cryptographic Operations' column of Table 12*] in accordance with a specified cryptographic algorithm [*listed in the 'Cryptographic Algorithm' column of Table 12*] and cryptographic key sizes [*listed in the 'Key Sizes (bits)' column of Table 12*] that meet the following: [*the list of standards in the 'Standards (Certificate #)' column of Table 12*].

Table 12 Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Encrypt/Decrypt	AES – ECB, CBC	128, 192, 256	NIST FIPS PUB 197 Certificate # 2153
Authentication	HMAC SHA-1	160	NIST FIPS 198 Certificate # 1318
Message Digest	SHA-1	N/A	NIST FIPS 180-3 Certificate # 1873
Key Wrapping	RSA	2048	PKCS#1 v2.1
Sign/Verify	RSA	2048	FIPS 186-2 for Sign/Verify Certificate # 1108

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

Application Note (1): The dependencies listed above have not been met per Canadian Common Criteria Scheme (CCS) Instruction #4.

Application Note (2): The RSA key wrapping is used for key establishment only and is not part of CAVP testing.

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Solera access control SFP*[12]] on [
a) Subjects: Users, Administrators, Auditors and processes on behalf of users;
b) Objects: Captured network traffic data;
c) Operations: Replay Traffic, Apply or Create Filters, Generate Reports, DeepSee Analysis;
].
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Solera access control SFP*] to objects based on the following: [
Subjects: Users, Administrators, Auditors and processes on behalf of users
Subject security attributes: User ID[13]*, password, role, authorized AUM (on Central Manager accounts only).*
Objects: network traffic data
Object security attributes: none].
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
1. *Users who authenticate and are assigned the Auditor role are not permitted to perform any of the operations on the object.*
2. *Users who authenticate and are assigned the User or Administrator roles are permitted to perform all operations on the object.*
3. *Processes may only perform operations for which the user they are acting on behalf of have permission.*
4. *User accounts on Central Manager may only access the TOE through Central Manager.*
5. *User accounts on individual appliance can only access that appliance.*

].
FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

[12] SFP – Security Functional Policy
[13] ID - identifier

6.2.4 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
FIA_UAU.2.1
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Solera access control SFP*] to restrict the ability to [query, modify, [*create*]] the security attributes [*roles, user ID, password, authorized AUM*] to [*Administrators*].

Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Solera access control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Administrators*] to specify alternative initial values to override the default values when ~~an object or information~~ **a user account** is created.

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*the operations listed in column 3 of Table 13*]] the [*TSF Data listed in Column 2 of Table 13*] to [*roles listed in column 1 of Table 13*].

Table 13 Management Functions

Role	TSF Data	Operations
Administrator	*Network settings*	change default, modify, clear, *set*
	Firewall, web interface	*set,* modify, delete, or *clear security configurations*
	Logs	*configure, view, query, clear*
	User accounts	*add,* modify, delete
	Timestamp	modify, *configure*
	AUMs	*view status, add,* delete
	Settings	• *Shutdown system,* • *Generate Customer Service Reports,* • *Enable and disable software licenses,* • *Set data retention and Geolocation settings,* • *Configure connection and disconnection notifications,* • *Add and delete rules and alerts.*
Auditor	*logs*	view, *clear*
User	*password*	modify *their password only*
	logs	view, *clear*

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [
- *Management of Security Attributes;*
- *Management of TSF data*

].
Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*Administrator, User, and Auditor*].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
FPT_ITT.1.1
The TSF shall protect TSF data from [*disclosure and modification*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No dependencies

6.2.7 Class FTA: TOE Access

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Dependencies: No dependencies

6.2.8 Class FTP: Trusted Path/Channel

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communications via the trusted channel for [*management communications between a management workstation and the TOE*].

Dependencies: No dependencies.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3+ augmented with ALC_FLR.2. Table 14 summarizes the requirements.

Table 14 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM[14] coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw Reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class 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
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[14] CM – Configuration Management

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 15 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Cryptographic Support	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TOE Security Functions	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps
TOE Access	FTA_TAB.1	Default TOE access banners
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel

7.1.1 Security Audit

The TOE generates audit records for the security relevant actions of all authorized users accessing the TOE via DeepSee Browser Interface, DeepSee Central Manager Interface, or Web Services API. It also records all unsuccessful attempts made to access the TOE. Audit records are generated for start-up and shutdown of the audit functions as well as for all events listed in Table 11. For all user-related events, the audit records are associated with the identity of the user that caused the event. The TOE ensures that only authorized users are allowed to view the audit records. Audit and System log data can be selected for review and ordered based on the following parameters: Date/Time. Cryptographic self-test error log events are generated, but are not accessible through the Audit or System log. These log messages are only accessible through the OS file system.

The TOE audit records contain the following information:

Table 16 Audit Record Contents

Field	Content
Date/Time	This field contains the date and time for the occurrence of the event.
Priority	This field signifies the priority of the event. Possible values for priority are: Alert, Critical, Debug, Emergency, Error, Informational, Notice, Warning and Unknown.
Category	This field shows the category of the event. Possible values for category are: Capture, DeepSee, Hardware, Misc, Playback, System, User, and Unknown.
Event	This field shows the event that occurred. If the event was unsuccessful it will be listed as failed. If not listed as failed the event was successful.
Additional Details	This field contains additional details regarding the event. This field also indicates the identity of the user responsible for the event, if the event is initiated by a user.

Audit data is stored on the appliance where the event was requested. Authorized users can view audit data of the entire TOE through the DeepSee Central Manager Interface. Authorized users on the DeepSee Browser Interface can only view audit data for that appliance.
TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1 and FAU_SAR.3.

7.1.2 Cryptographic Support

The TOE protects the confidentiality and integrity of all data passed between the management workstation and the TOE and internally between TOE components. The TOE achieves this using OpenSSL to perform encryption and decryption of all management communications. All cryptographic operations performed by the TOE are listed in the 'Cryptographic Operations' column of Table 12.

The TOE implements CAVP-validated cryptographic algorithms to handle all cryptographic functions for the encryption and decryption of data. CAVP certificate numbers for these algorithms are listed in Table 12. Key generation and destruction functions are outside the scope of this certification as specified in CCS Instruction 4.

Management communications between the TOE and operators occur over TLSv1 protected communications channels. The TLSv1 protocol and the underlying cryptographic algorithms are provided by OpenSSL. Users or processes acting on behalf of users access the TOE via the Web Services API over HTTPS secure channel.

Management communications between the Central Manager and the AUM occur over TLSv1 protected communications channels. The TLSv1 protocol and the underlying cryptographic algorithms are provided by OpenSSL. In addition, these communications are routed through a Virtual Private Network (VPN). The VPN cryptography is outside of the scope of the evaluation.
TOE Security Functional Requirements Satisfied: FCS_COP.1.

7.1.3 User Data Protection

The TOE enforces the Solera Access Control Policy on users and processes acting on behalf of users trying to perform operations (such as *Replay Traffic, Apply or Create Filters, Generate Reports,* and *Perform DeepSee Analysis*) on the captured network traffic data. Users or processes are only granted access to operations their role is authorized to perform on the captured data through one of the TOE management interfaces. User accounts that are created on Central Manager can only be accessed through Central Manager; however, they may be assigned access to manage another appliance through the DeepSee Central Manager Interface. User accounts created on an individual appliance can only access and manage that appliance.
TOE Security Functional Requirements Satisfied: FDP_ACC.1 and FDP_ACF.1.

7.1.4 Identification and Authentication

The TOE enforces identification and authentication prior to allowing any access to TOE functionality. The TOE is responsible for identification and authentication of all users accessing the TOE via DeepSee Browser Interface, DeepSee Central Manager Interface or Web Services API. Local identification and authentication is implemented in the underlying Linux-based operating system, with permissions enforced by the application software, not the operating system. Linux's Pluggable Authentication Modules (PAM) infrastructure is used for the implementation and enforcement of authentication.
TOE Security Functional Requirements Satisfied: FIA_UAU.2 and FIA_UID.2.

7.1.5 Security Management

The TOE can be managed through the Central Manager or through the DeepSee Browser Interface on an AUM. Limited management occurs through the Web Services API with no management of users or cryptography allowed. The Web Services API can be used to describe and retrieve previously captured data. Management of the Central Manager appliance can only occur through the DeepSee Central Manager Interface. The TOE provides administrators with the ability to manage security attributes and TSF data through the DeepSee Browser Interface or DeepSee Central Manager Interface. The TOE maintains three roles: Administrator, User, and Auditor. The TOE allows users to be assigned to one of the predefined roles. If the user account exists on the Central Manager, the user may additionally be assigned authorization to access the other appliance from the DeepSee Central Manager Interface. New users are assigned the role of User by default and are only given administrator access when the Administrator box is clicked in the DeepSee Browser Interface or DeepSee Central Manager Interface. The TOE allows Administrators to manage the attributes associated with the Solera Access Control Policy. Only Administrators are allowed to create new user accounts. Each user account has the following attributes: a user ID, password, role, and list of authorized appliances (if on Central Manager). The TOE allows only Administrators to manage the TSF-related data such as configuring or setting the following: Network, Date/Time, Timezone, System, License, Security, Web Interface, Data Retention, Logging, user accounts and DeepSee. Administrators can also manage AUMs, shutdown the system and perform the functions listed in Table 13. The User role cannot perform management except to change their own password once it is created by an Administrator and view the audit logs.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1 and FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE protects management traffic from disclosure and modification as it is sent internally from the Central Manager to the AUM. This communication occurs over HTTPS using TLSv1 and CAVP-validated algorithms.

The TOE provides reliable time stamps via the OS, which, can be changed or set manually by the Administrator. The time stamps are used in audit record generation.
TOE Security Functional Requirements Satisfied: FPT_ITT.1 and FPT_STM.1.

7.1.7 TOE Access

The Administrator can configure the TOE to display an advisory warning message regarding unauthorized use of the TOE at the beginning of each login prompt of each session. This banner can be found on the DeepSee Central Manager Interface and the DeepSee Browser Interface.
TOE Security Functional Requirements Satisfied: FTA_TAB.1.

7.1.8 Trusted Path/Channel

The TOE provides a trusted channel between itself and management workstations using TLSv1 and CAVP-validated algorithms. Each user session is a unique HTTPS session that can be initiated by the TOE or the management workstation. The HTTPS sessions provide assured identification or the workstation and protect TSF data from modification and disclosure. All management traffic into the TOE uses the trusted channel.
TOE Security Functional Requirements Satisfied: FTP_ITC.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target is considered to be Part 2 and Part 3 conformant of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 17 Threats:Objectives Mapping

Threats	Objectives	Rationale
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE. The TOE will also provide protections for logged-in administrators.	O.TOE_ADMIN counters this threat by ensuring that only authorized administrators are able to install and configure the TOE.
	OE.TRUSTED_ADMIN TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN counters this threat by ensuring that the TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow and apply all administrator guidance in a trusted manner
T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future records from being recorded, thus masking a user's actions.	O.ACCESS The TOE will ensure that users gain only authorized access to the TOE, the TOE data and to the resources that TOE controls.	O.ACCESS counters this threat by ensuring that user only gain authorized access to the TOE data, including the audit records.
	O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail.	O.AUDIT counters this threat by ensuring that the TOE is capable of detecting security relevant events and creates records of those events in the audit trail.
	O.AUDIT_REVIEW The TOE will provide the capability for only authorized users to view audit information.	O.AUDIT_REVIEW counters this threat by providing the capability for only authorized users to view audit information.
	O.TIME	O.TIME counters this threat by

Threats	Objectives	Rationale
	The TOE will provide reliable timestamps via the OS.	ensuring that a reliable timestamp is provided for all audit records and that this timestamp cannot be modified by an unauthorized user.
	O.USER_AUTHEN The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.	The objective O.USER_AUTHEN ensures that users are identified and authenticated prior to gaining access to the TOE.
T.DATA_COMPROMISE An unauthorized user may read, modify, delay, or destroy security critical TOE configuration data stored on the TOE or TOE environment.	O.ACCESS The TOE will ensure that users gain only authorized access to the TOE, the TOE data and to the resources that TOE controls.	O.ACCESS counters this threat by ensuring that users gain only authorized access to the TOE and to resources that TOE controls.
	O.CRYPTO The TOE will make cryptographic services available to authorized users and/or user applications that can be both data authentication and data encryption.	O.CRYPTO counters this threat by providing encryption, Authentication, Message Digest and Digital Signature services available to authorized users and/or user applications.
	O.USER_AUTHEN The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.	The objective O.USER_AUTHEN ensures that users are identified and authenticated prior to gaining access to TOE security data.
	O.SECURECOMMS The TOE requires that information transmitted between the TOE and TOE administrators and between TOE components never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.	O.SECURECOMMS counters this threat by ensuring that user communications to the TOE are encrypted. This prevents replay or spoofing of these communications.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.ACCESS The TOE will ensure that users gain only authorized access to the TOE, the TOE data and to the resources that TOE controls.	O.ACCESS counters this threat by ensuring that users gain only authorized access to the TOE, the TOE data and to the resources that TOE controls.
	O.CRYPTO The TOE will make cryptographic services available to authorized users and/or user applications that can be both data authentication and data encryption.	O.CRYPTO counters this threat by ensuring that cryptographic services from the TOE are available to protect communications.
	O.USER_AUTHEN The TOE will uniquely identify and	By ensuring that The TOE is able to identify and authenticate users

Threats	Objectives	Rationale
	authenticate users prior to allowing access to TOE functions and data.	prior to allowing access to TOE administrative functions and data, O.USER_AUTHEN counters this threat.
	O.SECURECOMMS The TOE requires that information transmitted between the TOE and TOE administrators and between TOE components never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.	O.SECURECOMMS counters this threat by ensuring that user communications to the TOE are encrypted. This prevents replay or spoofing of these communications.
T.PACKET_LOSS The TOE might not be able to capture all network traffic if it is not deployed and configured appropriately.	OE.DEPLOY The TOE must be deployed in the TOE environment such that the network is configured properly and its size is appropriate for the TOE functionality.	OE.DEPLOY counters this threat by ensuring that the TOE is deployed in the TOE environment such that the network is configured properly and its size is appropriate for the TOE functionality.
T.TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE. The TOE will also provide protections for logged-in administrators.	O.TOE_ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.DEPLOY The TOE is assumed to be deployed in a TOE environment	OE.DEPLOY The TOE must be deployed in the TOE environment such that the	The TOE will be deployed in the TOE environment such that the network is configured properly

Assumptions	Objectives	Rationale
such that the network is configured properly and its size is appropriate for the TOE functionality.	network is configured properly and its size is appropriate for the TOE functionality.	and its size is appropriate for the TOE functionality. OE.DEPLOY satisfies this assumption.
	OE.TRUSTED_ADMIN TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow and apply all administrator guidance in a trusted manner.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.TRUSTED_ADMIN satisfies this assumption.
A.LOCATE The TOE is located within a controlled access facility.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment protects itself and the TOE from external interference or tampering. OE.PROTECT satisfies this assumption.
	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.TRUSTED_ADMIN TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow and apply all administrator guidance in a trusted manner.	OE.TRUSTED_ADMIN satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	OE.PHYSICAL satisfies the assumption by providing physical security, commensurate with the value of the TOE and the data it contains.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.TRUSTED_ADMIN TOE Administrators are non-hostile, trusted, competent and appropriately trained to follow	OE.TRUSTED_ADMIN satisfies this assumption that users who manage the TOE are trusted, trained, and follow all guidance.

Assumptions	Objectives	Rationale
	and apply all administrator guidance in a trusted manner.	

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no Extended TOE Security Functional Requirements.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended TOE Security Assurance Requirements.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 19 Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE will ensure that users gain only authorized access to the TOE, the TOE data and to the resources that TOE controls.	FDP_ACC.1 Subset access control	The requirement meets the objective by enforcing the Solera Access Control SFP on all subjects and all named objects and all operations among them. The SFP specifies the rules for the operations that can be performed by the subjects on the objects.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by specifying the Solera Access Control SFP rules that will be enforced by the TSF and determines if an operation among subjects and named objects is allowed. Furthermore, it specifies the rules to explicitly authorize or deny access to a named object based upon security attributes.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that all users are authenticated prior to any access to the TOE, or TOE data.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that all users are identified prior to any access to the TOE, or TOE data.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by ensuring that the communications between TOE components are protected from disclosure and modification.
	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that the TOE displays an advisory warning message to all users trying to access the TOE. This banner warns against unauthorized access to the TOE.
O.AUDIT The TOE will provide the capability to detect security relevant events and create records of those events in the audit trail.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
O.AUDIT_REVIEW The TOE will provide the capability for only authorized users to view audit information.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by allowing authorized users to apply methods of ordering (based on Date/Time, Priority, Category, Event and Additional Details) while reviewing the audit trail.
O.CRYPTO The TOE will make cryptographic services available to authorized users and/or user applications that can be both data authentication and data encryption.	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE provides cryptographic services such as confidentiality and integrity for the TOE.
	FTP_ITC.1	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
	Inter-TSF trusted channel	objective by ensuring a trusted channel is created with the cryptographic services of the TOE.
O.TIME The TOE will provide reliable timestamps via the OS.	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized administrators can modify or configure the system time.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that the appliance OS provides reliable timestamp and it can be configured or modified only by authorised administrators.
O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE. The TOE will also provide protections for logged-in administrators.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that every user is authenticated before the TOE performs any TSF-mediated actions on behalf of that user.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that every user is identified before the TOE performs any TSF-mediated actions on behalf of that user.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by entrusting administrators with the ability to manage security attributes for the TOE.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the new users created in the TOE receive restrictive default values for security attributes. The requirement also specifies that only an authorized administrator can change initial values to override the default values when a user is created.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative

Objective	Requirements Addressing the Objective	Rationale
		functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
	FPT_STM.1 Reliable time stamps	The OS provides timestamps to the TOE. The requirement meets the objective by ensuring that only authorised administrators can manually set or changes the system time.
O.USER_AUTHEN The TOE will uniquely identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that every user is authenticated before the TOE performs any TSF-mediated actions on behalf of that user.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that every user is identified before the TOE performs any TSF-mediated actions on behalf of that user.
O.SECURECOMMS The TOE requires that information transmitted between the TOE and TOE administrators and between TOE components never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.	FCS_COP.1 Cryptographic operation	The requirement meets the objective by providing the cryptographic algorithms that are used to secure communications between administrators and TOE and between TOE components.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by requiring that the TSF protect TSF data when transmitted between TOE components.
	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by ensuring that a trusted channel is created to secure communications from the management workstation to the TOE.

8.5.2 Security Assurance Requirements Rationale

EAL3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the

System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

Table 20 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. A rationale is provided for all instances where the dependency has not been met.

Table 20 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FCS_COP.1	FCS_CKM.1	No	FCS_CKM.1 is not included following the guidance of CCS Instruction #4.
	FCS_CKM.4	No	FCS_CKM.4 is not included following the guidance of CCS instruction #4.
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_MSA.1	FMT_SMF.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FPT_ITT.1	No dependencies		
FPT_STM.1	No dependencies		
FTA_TAB.1	No dependencies		
FTP_ITC.1	No dependencies		

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 21 Acronyms

Acronym	Definition
API	Application Programming Interface
AUM	Appliance Under Management
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCS	Canadian Common Criteria Scheme
CM	Configuration Management
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GB	Gigabyte
Gb	Gigabit
Gbps	Gigabits per second
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
NTP	Network Time Protocol
NSS	Network Security Services
OS	Operating System
OSP	Organizational Security Policy
PAM	Pluggable Authentication Modules
PCAP	Packet Capture
PP	Protection Profile
RAM	Random Access Memory
ROI	Return On Investment
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement

Acronym	Definition
SPAN	Switched Port Analyzer
SSH	Secure Shell
ST	Security Target
TAP	Test Access Point
TB	Terabyte
TLSv1	Transport Layer Security version 1
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network

9.2 Terminology

Table 22 Terminology

Term	Definition
Bit	A single binary digit of information (0 or 1).
Byte	A standard unit of measurement of binary information. One Byte consists of eight bits.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com