Deep Discovery Inspector 3.2 Security Target (EAL2+)

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900

Revision History

Rev. #	Description	By	Date of Issue
1.0	Initial release	Roy Luo and Marks Shen	25-August-2012
1.1	Modify for first OR	Roy Luo	22-November-2012
1.3	Modify for OR2	Roy Luo	7-December-2012
1.4	Modification for OR3	Roy Luo	20-December-2012
1.5	Modification based on NIAP recommendation	Roy Luo	24-December-2012
1.6	Modifications for ADV work	Nancy Gow	5-June-2013
1.7	Minor updates		29-July-2013
1.8	New Boundary Diagram (external interfaces only) Reorganized Management Function List to match FSP	Nancy Gow	9-August-2013
1.9	Changes for FAU_STG.2.2 – Prevent modifications rather than detect	Nancy Gow	29-August-2013
2.0	Updated TOE Identification – added final build number	Nancy Gow	18-December-2013
2.1	Clarified CPU identification	Nancy Gow	31-December-2013
2.2	Clarified hardware specifications	Nancy Gow	20-January-2013

Table of Contents

Revision History 2

Table of Contents 3

List of Tables 5

List of Figures 5

Conventions and Terminology 6

Acronyms and Abbreviations 6

Document Organization 7

1 Introduction 8

1.1 ST Reference 8

1.2 TOE Overview 8

1.2.1 Advance Threat Scan Engine 8

1.2.2 Network Virus Scan 9

1.2.3 Network Content Inspection Engine 9

1.2.4 Network Content Correlation Engine 9

1.2.5 Potential Risk File Capture 9

1.2.6 Offline Monitoring 9

1.2.7 Expanded APT detection 9

1.3 Required non-TOE Hardware/Software/Firmware 10

1.3.1 Form Factors 10

1.4 TOE Boundaries 12

1.4.1 Physical Boundary 12

1.4.2 Logical Boundary 15

2 Conformance Claims 17

2.1 CC Conformance Claim 17

2.1.1 CC Version: 3.1.3 17

2.1.2 CC Conformance 17

2.2 Protection Profile (PP) Claim 17

2.3 Conformance Rationale 18

3 Security Problem Definition 19

3.1 Security Threats 19

3.1.1 TOE Threats 19

3.1.2 IT System Threats 19

3.2 Organizational Security Policies 20

3.4 Security Assumptions 21

3.4.1 Intended Usage Assumptions 21

3.4.2 Physical Assumptions 21

3.4.3 Personnel Assumptions 21

4 Security Objectives 22

4.1 IT Security Objectives for the TOE 22

4.2 Security Objectives for the Environment 23
5 Extended Components Definition 24
5.1 Extended Security Functional Components in the PP 24
5.2 Additional Extended Security Functional Components 24
5.2.1 Antivirus Component Requirements (FAV) 25
5.3 Extended Security Requirements Rationale 25
5.3.1 Extended Security Objectives Rationale 25
5.3.2 Extended Security Functional Requirements Rationale 25
5.3.3 Extended Security Functions Rationale 25
6 Security Requirements 26
6.1 Security Functional Requirements 26
6.1.2 Security Audit (FAU) 27
6.1.3 Identification and Authentication (FIA) 28
6.1.4 Security Management (FMT) 29
6.1.5 IDS Component Requirements (IDS) 30
6.1.6 Anti-Virus component requirements (FAV) 31
6.2 Security Assurance Requirements 32
6.2.1 Development 32
6.2.1.1 Security Architecture Description (ADV_ARC.1) 32
6.2.1.2 Security-enforcing Functional Specification (ADV_FSP.2) 33
6.2.1.3 Basic Design (ADV_TDS.1) 33
6.2.2 Guidance Documents 34
6.2.2.1 Operational User Guidance (AGD_OPE.1) 34
6.2.2.2 Preparative Procedures (AGD_PRE.1) 35
6.2.3 Life-cycle Support 35
6.2.3.1 Use of a CM System (ALC_CMC.2) 35
6.2.3.2 Parts of the TOE CM Coverage (ALC_CMS.2) 36
6.2.3.3 Delivery Procedures (ALC_DEL.1) 36
6.2.3.4 Flaw Reporting Procedures (ALC_FLR.2) 36
6.2.4 Tests 37
6.2.4.1 Evidence of Coverage (ATE_COV.1) 37
6.2.4.2 Functional Testing (ATE_FUN.1) 37
6.2.4.3 Independent Testing – Sample (ATE_IND.2) 38
6.2.5 Vulnerability Assessment 38
6.2.5.1 Vulnerability Analysis (AVA_VAN.2) 38
6.3 Security Requirements Rationale 39
6.3.1 Rationale for IT Security Objectives 39
6.3.2 Rationale for Security Objectives in the Environment 46
6.3.3 Security Functional Requirements Rationale 46
6.3.4 Explicitly Stated Requirements Rationale 50
6.3.5 Security Functional Requirements Dependency Rationale 50

6.3.6 TOE IT Security Functions Rationale 51
6.3.7 TOE Security Assurance Measures Rationale 52
7 TOE Summary Specification 54
7.1 Statement of TOE IT Security Functions 54
7.1.1 SF.AUDIT 54
7.1.2 SF.RBAC 54
7.1.3 SF.I&A 55
7.1.4 SF.IDPS 55
7.1.5 SF.AV 55

List of Tables

Table 1-1 Software Appliance System Requirements 11
Table 1-2 Hardware Appliance Specifications 11
Table 1-3 Virtual Appliance System Requirements 12
Table 5-1 TOE Extended Security Functional Requirements 24
Table 5-2 TOE Extended Security Functional Requirements 24
Table 6-1 TOE Security Functional Requirements 26
Table 6-2 Auditable Events 27

List of Figures

Table 1-1 System Requirements 11
Table 1-2 System Requirements 12
Table 5-1 TOE Extended Security Functional Requirements 24
Table 5-2 TOE Extended Security Functional Requirements 24
Table 6-1 TOE Security Functional Requirements 26
Table 6-2 Auditable Events 27

Conventions and Terminology

Throughout this document, operations performed in Common Criteria requirements are highlighted *like this*.

Acronyms and Abbreviations

Acronym	Meaning
APT	Advanced Persistent Threats
CC	Common Criteria for Information Technology Security Evaluation
CCS	Canadian Common Criteria Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CM	Configuration Management
DD	Trend Micro Deep Discovery Inspector
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
SPN	Trend Micro Smart Protection Network
ST	Security Target
TCP/IP	Transmission Control Protocol and Internet Protocol
TMCM	Trend Micro Control Manager
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy

Document Organization

Section 1 Introductory material for the Security Target (ST) and Target of Evaluation (TOE) overview and description

Section 2 Conformance claims for the ST

Section 3 Discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 Security objectives for both the TOE and the TOE environment.

Section 5 Definitions for extended SFRs.

Section 6 Functional and assurance requirements derived from the Common Criteria Parts 2 and 3, respectively, that must be satisfied by the TOE. This section also provides the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

Section 7 Details specific to the TOE implementation of the security measures described in this document

1 Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. An ST describes a set of security requirements and specifications to be used as the basis for evaluation of an identified Information Technology (IT) product.

The subject of this ST document is Deep Discovery Inspector 3.2, developed by Trend Micro, Inc. Throughout this document, this IT product will also be referred to as Deep Discovery Inspector or the Target of Evaluation (TOE).

Deep Discovery Inspector enables its users to create and enforce comprehensive IT security policies that proactively protect sensitive data, applications, hosts or network segments.

1.1 ST Reference

Title:	Trend Micro Deep Discovery Inspector 3.2 Security Target (EAL2+)
ST Version:	2.2
TOE Identification:	Trend Micro Deep Discovery Inspector 3.2, build 1118
PP Identification:	U.S. Government Protection Profile Intrusion Detection System for Basic Robustness, Version 1.7, July 25, 2007
Author:	Trend Micro Deep Discovery Inspector Team
Vetting Status:	Official Release

1.2 TOE Overview

The TOE described in this ST, Trend Micro Deep Discovery Inspector 3.2, is an Intrusion Detection System (IDS) that protects customers' IT networks. This solution is deployed offline in the IT network of customers to monitor network traffic. It can identify both file-based and network-based attacks and malicious behavior. The TOE also takes proactive or preventive measures to ensure the security of the detection, such as:

- Storing detection logs
- Sending alarms to administrators
- Sending cleaning requests to mitigation servers of TrendMicro if they are deployed with the TOE

The TOE is able to protect itself and associated data from unauthorized access or modification and provides an audit trail to ensure accountability for authorized actions.

The TOE includes the following modules and features:

1.2.1 Advance Threat Scan Engine

The Advance Threat Scan Engine is a file-based detection-scanning engine that has true file type, multi-packed files, and IntelliTrap detection. The scan engine performs the actual scanning across the network and uses a virus pattern file to analyze the files passing through the network. The virus pattern file contains binary patterns of known viruses. Trend Micro regularly releases new virus pattern files when new threats are detected.

The virus scan engine uses the following methods of detection:

- True File Type

  Virus writers can quickly rename files to disguise the file's actual type. Deep Discovery Inspector confirms a file's true type by reading the file header and checking the file's internally registered data type. Deep Discovery Inspector only scans file types capable of infection.

  With true file type, Deep Discovery Inspector determines a file's true type and skips inert file types. Inert file types, such as .gif files, make up a large volume of Internet traffic.

- Multi-packed/Multi-layered files

  A multi-packed file is an executable file compressed using more than one packer or compression tool. For example, an executable file double or triple packed with Aspack, UPX, then with Aspack again.

  A multi-layered file is an executable file placed in several containers or layers. A layer consists of a document, an archive, or a combination of both. An example of a multi-layered file is an executable file compressed using Zip compression and placed inside a document.

  These methods hide malicious content by burying them under multiple layers of compression. Traditional antivirus programs cannot detect these threats because traditional antivirus programs do not support layered/compressed/packed file scanning.

- IntelliTrap

  Virus writers often use different file compression schemes to circumvent virus filtering. IntelliTrap helps Deep Discovery Inspector evaluate compressed files that could contain malware.

1.2.2 Network Virus Scan

Deep Discovery Inspector uses a combination of patterns and heuristics to proactively detect network viruses. It monitors network packets and triggers events that can indicate an attack against a network. It can also scan traffic in specific network segments.

1.2.3 Network Content Inspection Engine

Network Content Inspection Engine is a module used by Deep Discovery Inspector to scan the content passing through the network layer.

1.2.4 Network Content Correlation Engine

Network Content Correlation Engine is a module used by Deep Discovery Inspector that implements rules or policies defined by Trend Micro. Trend Micro regularly updates these rules after analyzing the patterns and trends that new and modified viruses exhibit.

1.2.5 Potential Risk File Capture

A potential risk file is a file the Network Content Inspection Engine categorizes as potentially malicious. However, the Virus Scan Engine does not recognize known signature patterns of verified malicious files and does not categorize the file as malicious or as a security risk. Deep Discovery Inspector captures potential risk files, enters a log in the database, and saves a copy of the file. Deep Discovery Inspector captures the file session and threat information as a file header and stores data in the log file.

1.2.6 Offline Monitoring

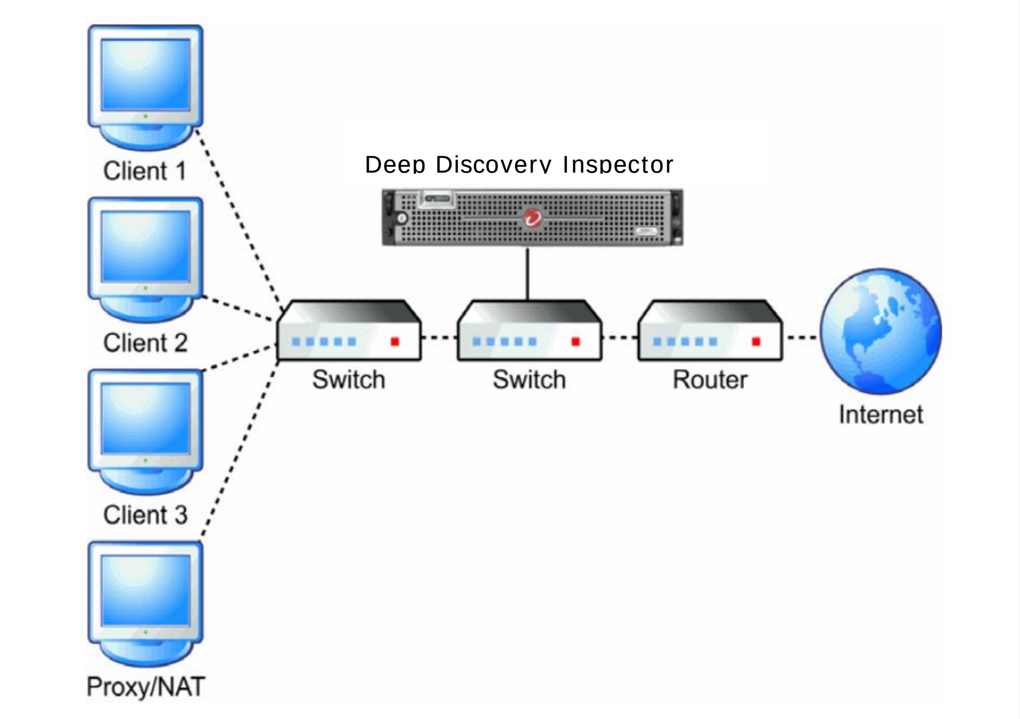
Deep Discovery Inspector deploys in offline mode. It monitors the network traffic by connecting to the mirror port on a switch for minimal or no network interruption.

See Figure 1-1 for the relationship of the TOE to the supporting components required for the operation of Deep Discovery Inspector.

1.2.7 Expanded APT detection

Deep Discover detection engines deliver expanded APT detection capabilities, including a customizable virtual analyzer and updated inspection and correlation rules designed to detect malicious content, communication, and behavior during every stage of an attack sequence.

Figure 1-1 Deep Discovery Inspector Deployment



1.3 Required non-TOE Hardware/Software/Firmware

1.3.1 Form Factors

Deep Discovery Inspector is available in the following form factors:

- As a software appliance that can be installed on a bare-metal server
- As a hardware appliance pre-installed on a server provided by Trend Micro (a bare-metal server pre-installed with the software appliance)
- As a software virtual appliance that can be installed on a bare metal server with VMware™ vSphere™ 4.x & 5.x

Application Note: Full details of the supported system and hardware requirements are available in the Deep Discovery Inspector 3.2 Administrator's Guide.

Software Appliance

The TOE is available as a Software Appliance. It must be installed on a bare-metal server that meets the requirements listed in Table 1-1 System Requirements. The software is packaged as an ISO installation file on the Deep Discovery Inspector installation CD.

Customers who had previously set up a threat discovery appliance can upgrade to the TOE by performing a fresh installation of the software.

Table 1-1 Software Appliance System Requirements

Resources	Requirements
Host Machine	**CPU:** Two Intel™ Quad Core processors (recommended) **RAM:** 8GB minimum **Hard disk space:** 100GB minimum **Network interface card (NIC)**: Two NICs minimum **Note:** For better performance, when installing Deep Discovery Inspector it is recommended to use a plug-in NIC (instead of an onboard NIC) as a data port.

Hardware Appliance

The TOE is also available as a Hardware Appliance, where the software appliance is pre-installed on a performance-tuned bare-metal server. The software is packaged as an ISO installation file on the Deep Discovery Inspector installation CD. It is pre-installed on a purpose-built, hardened, performance-tuned 64-bit Linux operating system. The ISO and checksums are securely transferred to the hardware manufacturer who verifies all required files and produces Hardware Appliance. The following two models of the DDI Hardware Appliance are included in the scope of the evaluation.

Table 1-2 Hardware Appliance Specifications

DDI Model	Specifications
DD 500	**Base Model:** PowerEdge R420 Rack Server **Form Factor:** 1U2S **CPU:** Intel Xenon E5 **RAM:** 8GB **HD:** 500GB x 2, RAID 1 **Network interface card (NIC): 4** (2 on-board, 2 external)
DD 1000	**Base Model:** PowerEdge R420 Rack Server **Form Factor:** 1U2S **CPU:** Intel Xenon E5 x 2 **RAM:** 16GB **HD:** 500GB x 2, RAID 1 **Network interface card (NIC):** 6 (2 on-board, 4 external)

Virtual Appliance

The TOE is also available as a Virtual Appliance, where the software appliance can be installed on a virtual machine. The software is packaged as an ISO installation file on the Deep Discovery Inspector installation CD. Trend Micro recommends enabling virtualization technology in the BIOS when installing VMware ESX/ESXi. Users must verify that the BIOS of the host machine support virtualization technology.

The minimum and recommended virtual machine setting is listed in Table 1-3 System Requirements.

Table 1-3 Virtual Appliance System Requirements

Resources	Requirements
Host Machine	**CPU:** Two Intel™ Quad Core processors (recommended) **RAM:** 8GB minimum **Hard disk space:** 100GB minimum **Network interface card (NIC)**: Two NICs minimum

1.4 TOE Boundaries

1.4.1 Physical Boundary

The physical boundary of the TOE includes the ISO installed file on the Deep Discovery Inspector installation CD for all three versions of the product, and the Hardware Appliance (Models DD 500, DD 1000) supplied by TrendMicro for the Hardware Appliance version.

The Deep Discovery Inspector 3.2 Administrator’s Guide describes the software components contained in the TOE, how to deploy them, and how to configure the TOE and its interfaces after installation.

Figure 1-2 TOE Physical Boundary

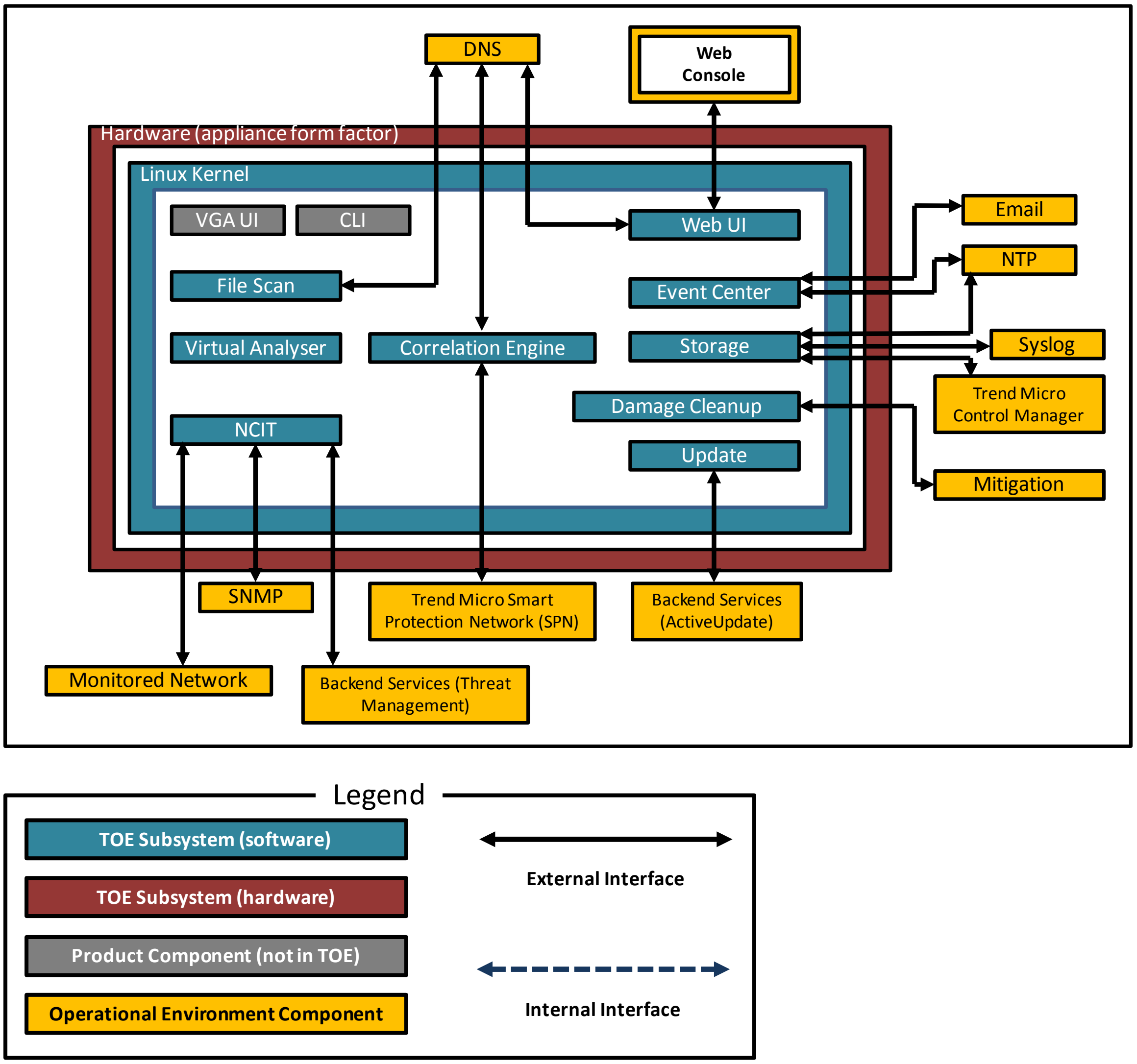


Table 1-3 Evaluated TOE Components

TOE Component	Description
Web UI	This component is an HTTPS web-based console used to configure Deep Discovery Inspector, view system data, and administer the system.
Event Center	This component collects, receives, and distributes module data.
Storage	This component contains a database for storing files, and detection logs and files, along with supplying data to the web-based UI.
Damage Cleanup	This component provides an interface for communicating with the Mitigation module.
File Scan	This component scans suspicious files, based on a signature file pattern.
Update	This component updates the engine used by the TOE function and file pattern from the Trend Micro update server (backend).
Correlation Engine	This component correlates analyzed network traffic with events from other modules.
Virtual Analyzer	This component provides a virtualized environment where untrusted files can be safely inspected.
Linux Kernel	This component optimizes Deep Discovery Inspector performance and security.
Bare-metal Server	This component is the hardware part of Deep Discovery Inspector. (Hardware Appliance only)

Components excluded from the TOE

Table 1-4 Components excluded from the TOE

TOE Component	Description
CLI	This component provides a Command Line Interface (CLI) for debugging the code. This component cannot be activated without a key and is thus excluded from evaluation.
Preconfiguration Console (VGA UI)	The Preconfiguration Console is a terminal communications program that is used for initial configuration of network and system settings and for off-line maintenance and diagnostics. The preferred mode of access to the Preconfiguration Console is through the VGA port of the appliance, therefore this interface is also called the VGA UI. The Preconfiguration Console is not used during the normal run-time operation of the TOE and is therefore excluded from the scope of the evaluation.

Operational Environment

Table 1-5 Operational Environment

TOE Component	Description
Monitored Network	This component provides the network traffic for the TOE to scan.
Mitigation Module	This component performs threat cleanup activities on network endpoints.
Network Time Protocol (NTP)	This component provides accurate timestamps on audit and system data.
Syslog Server	This component collects system and detection log data.
Mail	This component sends email alerts and messages to the Administrator.
Trend Micro Control Manager (TMCM)	This component provides a centralized management function for Deep Discovery Inspector (and other Trend Micro products).
Simple Network Management Protocol (SNMP)	This component provides real-time system status.
Backend services	These include: Active Update server (engine and pattern updates) and Threat Management (customized reporting and analysis).
Trend Micro Smart Protection Network (SPN)	This component provides a URL and file reputation rating service.

Application Note: These components support TOE functions and will be excluded from evaluation.

1.4.2 Logical Boundary

The logical TOE boundary is defined by the security functions performed by the TOE and includes the following:

- SF.AUDIT (Audit)
- SF.RBAC (Role Based Access Control)
- SF.I&A (Identification and Authentication)
- SF.IDPS (Intrusion Detection and Prevention)
- SF.AV (Anti-Virus)

These functions are outlined below, and expanded upon in the Statement of TOE IT Security Functions found in section 7.1 of this document.

SF.AUDIT

Deep Discovery Inspector 3.2 maintains information regarding the administration and management of its security functions as part of the audit records. SF.AUDIT is responsible for the generation, storage, and reviewing of these audit records.

SF.RBAC

Deep Discovery Inspector 3.2 restricts authorized TOE administrators' access to the system using role-based access control. All TOE administrators are assigned roles at creation. Authorized TOE administrators can only access the TOE through the administrative interface. They have full access to the functions permitted by their roles.

SF.I&A

The identification and authentication mechanism used by Deep Discovery Inspector 3.2 is based on user ID and password. For each user being created, the creator is required to assign them with a user ID, an initial password, and a role.

SF.IDPS

The TOE provides intrusion detection and prevention functions. Deep Discovery Inspector detects and identifies evasive threats in real-time, along with providing in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.

SF.AV

The TOE provides anti-virus functions. Data is collected and analyzed for viruses by the TOE. Detection logs and analysis reports are stored in the database. Corresponding actions are taken by the TOE based on the severity of the detected threat.

2 Conformance Claims

2.1 CC Conformance Claim

2.1.1 CC Version: 3.1.3

General Status:	Ready for release
Keywords:	Commercial-off-the-shelf (COTS), intrusion detection, intrusion detection system (IDS), log inspection, integrity monitoring, sensor, scanner, analyzer.

2.1.2 CC Conformance

Trend Micro Deep Discovery Inspector 3.2 is conformant to Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements (version 3.1 revision 3, July 2009) extended.

Trend Micro Deep Discovery Inspector 3.2 is conformant to Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements (version 3.1 revision 3, July 2009).

Deep Discovery Inspector 3.2 is being evaluated to Evaluation Assurance Level 2 augmented with ALC_FLR.2 (EAL2) under the Canadian Common Criteria Scheme (CCS) using the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, version 3.1 revision 3, July 2009.

2.2 Protection Profile (PP) Claim

The ST claims demonstrable conformance to **U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments**, Version 1.7, July 25, 2007.

Demonstrable Compliance in CC v3.1 R3 is defined as follows:

> Demonstrable conformance: the relation between an ST and a PP, where the ST provides a solution which solves the generic security problem in the PP.
>
> The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist, thus allowing the ST author to claim conformance to these PPs simultaneously, thereby saving work. [CC Part 1 p. 15]
>
> Where there is a clear subset-superset type relation between PP and ST in the case of strict conformance, the relation is less clear-cut in the case of demonstrable conformance. STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP. but can do so in any way that is equivalent or more restrictive to that described in the PP. [CC Part1 p. 92]

This ST includes all of the Security Functional Requirements from the PP with the following modifications:

- FAU_STG.2.2 has been modified to state: The TSF shall be able to *prevent* modifications to the audit records.
- FMT_SMF.1 has been added to satisfy the dependencies of FMT_MOF.1 and FMT_MTD.1

  Note: These changes have been approved by the Scheme.
- FPT_STM.1 was deleted since reliable timestamps are provided by the Operational Environment (OE.TIME)

  Note: This Change has been approved by NIAP in PD-0151*: Acceptable Demonstrable Assurance for the IDS System PP v1.7 (BR)* and PD-0152: *Internal Inconsistency within the IDS System PP regarding FPT_STM*
- FAV_ACT.1 and FAV_ALR.1 have been added to reflect the TOE's functionality
- Those SFRs exclusively related to authenticating or communicating TSF data with external IT products, specifically: FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.2, have been replaced by FPT_ITT.1 through the precedence of PD-0097

Application Note: Since the TOE is not a distributed TOE, FPT_ITT.1 does not apply and is not included in this ST.

The security requirements in this ST are equivalent to or more restrictive than the security requirements in the PP. The ST also augments the conformance to the **U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments** with additional SARs in order to increase the level of assurance from EAL2 to EAL2+.

2.3 Conformance Rationale

Deep Discovery Inspector 3.2 is a suitable solution to the generic security problem described in the Intrusion Detection System Protection Profile specified in Section 2.2. The threats, organizational security policies, and assumptions contained in this ST are consistent with those in the PP.

All security functions and assurances in the PP (together with changes resulting from precedent decisions or guidance instructions) are part of this ST and are addressed by Deep Discovery Inspector 3.2.

3 Security Problem Definition

The TOE security environment consists of the threats to security, organizational security policies, and security assumptions as they relate to the TOE. These are described in detail in this section.

3.1 Security Threats

The following identifies threats for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.1.1 TOE Threats

T.COMDIS

An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.COMINT

An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.FACCNT

Unauthorized attempts to access TOE data or security functions may go undetected.

T.INFLUX

An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.IMPCON

An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.LOSSOF

An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT

An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.1.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.FALACT

The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALASC

The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.FALREC

The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.INADVE — Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT — Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

T.MISUSE — Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.SCNCFG — Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC — Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL — Vulnerabilities may exist in the IT System the TOE monitors.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the ST.

P.ANALYZ — Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.ACCACT — Users of the TOE shall be accountable for their actions within the IDS.

P.ACCESS — All data collected and produced by the TOE shall only be used for authorized purposes.

P.DETECT — Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.INTGTY — Data collected and produced by the TOE shall be protected from modification.

P.MANAGE — The TOE shall only be managed by authorized system administrator and administrators.

P.PROTCT — The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.4 Security Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.4.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

3.4.2 Physical Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.4.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the

TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized system administrator and administrators.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs of the TOE.

4.1 IT Security Objectives for the TOE

O.ACCESS	The TOE must allow authorized system administrator and administrators to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.AUDIT_SORT	The TOE will provide the capability to sort the audit information.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The FileScan module must accept data from IDS NCIT module or IDS FileScan module and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.IDSCAN	The Correlation Engine must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The NCIT module must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.VIRUS	The TOE will detect and take action against known viruses introduced to the protected computer via network traffic or removable media.

4.2 Security Objectives for the Environment

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.INTROP The TOE is interoperable with the IT System it monitors.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

5 Extended Components Definition

The extended security functions identified in this section are based on the Antivirus (Extended Requirements) class (FAV) from the **U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments**. Version 1.2, July 25, 2007.

5.1 Extended Security Functional Components in the PP

Table 5-1 TOE Extended Security Functional Requirements

Security Functional Requirement	Name
Extended Security Functional Requirements from the PP	
IDS_SDC.1	System Data Collection (EXT)
IDS_ANL.1	Analyser Analysis (EXT)
IDS_RCT.1	Analyser react (EXT)
IDS_RDR.1	Restricted data review (EXT)
IDS_STG.1	Guarantee of System Data Availability (EXT)
IDS_STG.2	Prevention of System data loss (EXT)

5.2 Additional Extended Security Functional Components

This section identifies extended security functions provided by Deep Discovery Inspector 3.2 that are not part of the IDS System PP. The functions in this extended class detect and act upon discovered viruses.

Table 5-2 TOE Extended Security Functional Requirements

Security Functional Requirement	Name
Extended Security Functional Requirements for the TOE	
FAV_ACT_(EXT).1	Anti-Virus actions
FAV_ALR_(EXT).1	Anti-Virus alerts

FAV_ACT.1 and FAV_ALR.1 are based on the antivirus PP, but their dependency has been changed from FAV_SCN.1, EXP to IDS_SDC.1. The Deep Discovery Inspector scan function is based on network traffic payload. Transferred files are scanned in real-time only; there are no on-demand or scheduled scan functions.

5.2.1 Antivirus Component Requirements (FAV)

Antivirus Actions (FAV_ACT.1, EXT)

FAV_ACT.1.1 (EXT)	Upon detection of a file-based virus, the TSF shall perform the actions specified by the authorized administrator. Actions are administratively configurable on a per-Appliance basis and consist of: Logging the intrusions

Antivirus Alerts (FAV_ALR.1, EXT)

FAV_ALR.1.1 (EXT)	The System shall be able to collect an audit event from a computer indicating detection of a virus. The event shall identify the computer originating the audit event, the virus that was detected and the action taken by the TOE.
FAV_ALR.1.2 (EXT)	The System shall send an alarm to predefined recipients along with logging this event when a virus is detected.

5.3 Extended Security Requirements Rationale

5.3.1 Extended Security Objectives Rationale

The TOE components that address security objectives O.IDSCAN, O.IDSENS, and O.IDANLZ are described in Section 6.3. Similarly, O.VIRUS is included with the security objectives described in Section 6.3.

5.3.2 Extended Security Functional Requirements Rationale

A family of requirements was created to specifically address the data collected and analyzed by the IDS, and is taken from the IDS System PP. This section identifies functionality provided by the TOE to detect, analyse and react to possible intrusions on computers protected by Deep Discovery Inspector 3.2, and address requirements for collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

This extended class of FAV requirements is based on the Anti-Virus PP detailed above, but modified to specifically address the anti-virus functionality provided by the TOE to protect the network environment.

Since the anti-virus functionality is completely integrated with the TOE IDS system for Data Collection and Alerts, there is some overlap of FAV functionality with the IDS_SDC.1 and IDS_RCT.1 described in Section 6. Anti-Virus event data is also protected by the IDS_STG functions described in Section 6. The rationale for the Extended SFRs is described in Section 6.3.3.

5.3.3 Extended Security Functions Rationale

The rationale for the IDS Extended Security Functions SF.IDPS is described in section 6.3.6.

Although the IDS requirements in the PP do contain measures to address the threat of malicious activity in the form of viruses (T.MISACT) entering the System via network traffic, the additional explicitly stated requirements for anti-virus derived from the Anti-Virus PP in order to address the threat of file-based viruses that may enter the system by other means, such as removable media.

The Extended Security Functions Rationale for SF.AV is included in the TOE Security Functions Rationale described in Section 6.3.6.

6 Security Requirements

6.1 Security Functional Requirements

Table 6-1 TOE Security Functional Requirements

Security Requirement	Component	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	FAU_STG.2	Guarantees of audit data availability
	FAU_STG.4	Prevention of audit data loss
Identification and Authentication (FIA)	FIA_UAU.1	Timing of authentication
	FIA_ATD.1	User attribute definition
	FIA_UID.1	Timing of identification
Security Management (FMT)	FMT_MOF.1	Management of security functions behavior
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
IDS Component Requirements (IDS)	IDS_SDC.1	System data collection
	IDS_ANL.1	Analyzer analysis
	IDS_RCT.1	Analyzer react
	IDS_RDR.1	Restricted data review
	IDS_STG.1	Guarantee of system data availability
	IDS_STG.2	Prevention of system data loss
Anti-Virus(FAV)	FAV_ACT_(EXT).1	Anti-virus actions
	FAV_ALR_(EXT).1	Anti-virus alerts

6.1.2 Security Audit (FAU)

Audit Data Generation (FAU_GEN.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 *basic* level of audit

c) *Access to the System and access to the TOE and System data* [FAU_GEN.1.1]

Application Note: The auditable events in b) above are described in Table 6-2 Auditable Events. The System Data in c) above is defined as TSF configuration data.

Table 6-2 Auditable Events

Component	Audited Events	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to system	
FAU_GEN.1	Access to the TOE and system data	Object IDs, requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional information specified in the Details column of Table 6-2 Auditable Events* [FAU_GEN.1.2]

Audit Review (FAU_SAR.1)

The TSF shall provide *authorized System administrators and authorized administrators* with the capability to read *all* *audit information as specified in FAU_GEN.1* from the audit records.[FAU_SAR.1.1]

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

Application Note: Administrators with the default configuration role of “authorized system administrator” and “authorized administrator” are granted access to all TOE audit records.

Restricted Audit Review (FAU_SAR.2)

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

Selectable Audit Review (FAU_SAR.3)

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

Selective Audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type

b) *no other attributes* FAU_SEL.1.1

Guarantees of Audit Data Availability (FAU_STG.2)

The TSF shall protect the stored audit records from unauthorized deletion. FAU_STG.2.1

The TSF shall be able to *prevent* modifications to the audit records. FAU_STG.2.2

The TSF shall ensure that *the latest recorded* audit records will be maintained when the following conditions occur: *audit storage exhaustion .* FAU_STG.2.3

Prevention of Audit Data Loss (FAU_STG.4)

The TSF shall *overwrite the oldest stored audit records* and send an alarm if the audit trail is full. FAU_STG.4.1

6.1.3 Identification and Authentication (FIA)

User Attribute Definition (FIA_ATD.1)

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

a) *User identity*

b) *Authentication data*

c) *Authorizations*

d) *no other attributes* FIA_ATD.1.1

Timing of Authentication (FIA_UAU.1)

The TSF shall allow *no action* on behalf of the user to be performed before the user is authenticated. 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. FIA_UAU.2.2

Timing of Identification (FIA_UID.1)

The TSF shall allow *no action* behalf of the user to be performed before the user is identified. FIA_UID.1.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.1.2

6.1.4 Security Management (FMT)

Management of Security Functions Behavior (FMT_MOF.1)

The TSF shall restrict the ability to *modify the behavior of* the functions *of System data collection, analysis and reaction* to *authorized System administrators and authorized administrators.*FMT_MOF.1.1

Management of TSF Data (FMT_MTD.1)

The TSF shall restrict the ability to query *and add System and audit data, and shall restrict the ability to query and modify all other TOE data* to the *authorized System administrators and authorized administrators*. FMT_MTD.1.1

Application Note: "Audit data" refers to auditable events generated in the FAU_GEN requirement of this ST. "System data" refers to TSF configuration data.

Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1 The TSF shall be capable of performing the following security management functions:

a) View threat data

b) View real time analysis results

c) View system status

d) View top threats detected

e) View DDI detection results

f) Query detection logs

g) Query audit/system logs

h) Configure syslog server

i) Generate reports

j) Configure report notifications

k) Change user passwords

l) Configure alerts

m) Configure logs

n) Configure DDI detections

o) Configure network settings

p) Configure DDI licenses

q) Configure global settings

r) Configure user accounts

Application Note: FMT_SMF.1 is not included in the IDS System PP; however, it needed to be included to satisfy the dependencies of the SFRs FMT_MOF.1 and FMT_MTD.1

Security Roles (FMT_SMR.1)

The TSF shall maintain the roles of *authorized administrator, authorized System administrator.* FMT_SMR.1.1

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

Application Note: The TOE only allows management functions to be performed through Deep Discovery Inspector during its operation, hence the "authorized administrator", "authorized System administrator" roles listed in this SFR are equivalent with regard to the TOE.

6.1.5 IDS Component Requirements (IDS)

System Data Collection (IDS_SDC.1, EXT)

The System shall be able to collect the following information from the targeted IT System resource(s):

a) Start-up and shutdown, network traffic, detected malicious code, detected known vulnerabilities,

b) no other events (EXT) IDS_SDC.1.1

At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event

b) The additional information specified in the *Details* column of Table 6-3 IDS Events (EXT) IDS_SDC.1.2

Table 6-3 IDS Events

Component	Event	Details
IDS_SDC.1	Start-up, shutdown and host system reboot	None
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Start-up and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Application Note: Note that while the IDS_SDC.1 requirement in the PP indicates additional information content, that content is dependent upon the data that is collected. The specific data collected depends on the TOE configuration and the data collection functionality available on specific Operating Systems or platforms.

Analyzer Analysis (IDS_ANL.1, EXT)

The System shall perform the following analysis function(s) on all IDS data received:

a) statistical, signature

b) no other analytical functions (EXT) IDS_ANL.1.1

The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source

b) action taken, data destination (EXT) IDS_ANL.1.2

Analyzer React (IDS_RCT.1, EXT)

The System shall send an alarm to the authorized administrator, the authorized System administrator (if user has enabled this) and record the attempt as a system data record when an intrusion is detected. (EXT) IDS_RCT.1.1

Restricted Data Review (IDS_RDR.1, EXT)

The System shall provide users assigned the authorized administrator roles with the capability to read all data from the System data. (EXT) IDS_RDR.1.1

The System shall provide the System data in a manner suitable for the user to interpret the information. IDS_RDR.1.2 (EXT)

The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXT) IDS_RDR.1.3

Guarantee of System Data Availability (IDS_STG.1, EXT)

The System shall protect the stored System data from unauthorized deletion. (EXT) IDS_STG.1.1

The System shall protect the stored System data from unauthorized modification. (EXT) IDS_STG.1.2

The System shall ensure that *the most recent* System data will be maintained when the following conditions occur:

System data storage exhaustion. (EXT) IDS_STG.1.3

Prevention of System Data Loss (IDS_STG.2, EXT)

The System shall *ignore System data* and send an alarm if the storage capacity has been reached. (EXT) IDS_STG.2.1

6.1.6 Anti-Virus component requirements (FAV)

Application Note: The FAV functionality is available in the Deep Discovery Inspector.

Anti-Virus Actions (FAV_ACT.1, EXT)

Upon detection of a file-based or network-based virus, the TSF shall perform the actions specified by the authorized administrator. Actions consist of:

a) Send the requirement of virus clean or host quarantine to Mitigation Server of TrendMicro

b) Send the file sample to virtual analysis box of TrendMicro

c) *No other actions* FAV_ACT_(EXT).1.1

Anti-Virus Alerts (FAV_ALR.1, EXT)

The System shall be able to collect an audit event after the detection and analysis of a virus. The event shall identify the virus that was detected and the action taken by the TOE. FAV_ALR_(EXT).1.1

The System shall send an alarm to *the authorized system administrator* FAV_ALR_(EXT).1.2

Table 6-4 FAV Events

Component	Event	Details
FAV_ACT_(EXT).1	Action taken in response to detection of a virus	Virus detected, action taken, file or process identifier

6.2 Security Assurance Requirements

This product claims CC Version 3.1.3 Part 3 conformant and claims Evaluation Assurance Level 2 augmented with ALC_FLR.2 (EAL2) including all relevant International Common Criteria interpretations from the Interpreted CEM as of July 2009. The security assurance requirements are listed in Table 6-4 Security Assurance Requirements.

Table 6-4 Security Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.2.1 Development

6.2.1.1 Security Architecture Description (ADV_ARC.1)

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

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

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

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

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

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

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

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

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

6.2.1.2 Security-enforcing Functional Specification (ADV_FSP.2)

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.1D The developer shall provide a functional specification.

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

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

6.2.1.3 Basic Design (ADV_TDS.1)

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.1D The developer shall provide the design of the TOE.

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

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all SFRs.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behavior described in the TOE design is mapped to the TSFIs that invoke it.

6.2.2 Guidance Documents

6.2.2.1 Operational User Guidance (AGD_OPE.1)

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

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

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

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

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

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

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

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

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

6.2.2.2 Preparative Procedures (AGD_PRE.1)

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

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

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

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

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

6.2.3 Life-cycle Support

6.2.3.1 Use of a CM System (ALC_CMC.2)

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

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

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.2.3D The developer shall use a CM system.

6.2.3.2 Parts of the TOE CM Coverage (ALC_CMS.2)

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

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

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

6.2.3.3 Delivery Procedures (ALC_DEL.1)

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

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

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

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

6.2.3.4 Flaw Reporting Procedures (ALC_FLR.2)

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

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

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

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

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

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

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

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

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

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

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

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

6.2.4 Tests

6.2.4.1 Evidence of Coverage (ATE_COV.1)

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

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

6.2.4.2 Functional Testing (ATE_FUN.1)

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

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

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

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

ATE_FUN.1.2D The developer shall provide test documentation.

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

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

6.2.4.3 Independent Testing – Sample (ATE_IND.2)

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

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

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

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

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

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

6.2.5 Vulnerability Assessment

6.2.5.1 Vulnerability Analysis (AVA_VAN.2)

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

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

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing basic attack potential.

6.3 Security Requirements Rationale

This section provides the rationale for the selection of the IT security functions, requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment. This is achieved using a set of cross-referencing tables; each covering two adjacent sets of requirements.

This section also provides the rationale for choosing the IT Assurance Requirements and Measures.

6.3.1 Rationale for IT Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the ST. Table 6-5 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 6-5 Security Environment vs. Objectives

Objectives / Threats and Assumptions		TOE													Environment						
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.VIRUS	O.AUDIT_SORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_PROTECTION
Assumptions	A.ACCESS																		✓		
	A.DYNMIC																	✓	✓		
	A.ASCOPE																		✓		
	A.PROTCT															✓					
	A.LOCATE															✓					
	A.MANAGE																	✓			
	A.NOEVIL														✓	✓	✓				
	A.NOTRUST															✓	✓				
Threats	T.COMINT	✓						✓	✓			✓									
	T.COMDIS	✓						✓	✓												
	T.LOSSOF	✓						✓	✓			✓									
	T.NOHALT		✓	✓	✓			✓	✓												
	T.PRIVIL	✓						✓	✓												
	T.IMPCON						✓	✓	✓						✓						
	T.INFLUX									✓											

Objectives		TOE													Environment						
	T.FACCNT										✓										
	T.SCNCFG		✓																		
	T.SCNMLC		✓										✓								
	T.SCNVUL		✓																		
	T.FALACT					✓															
	T.FALREC				✓																
	T.FALASC				✓																
	T.MISUSE			✓							✓		✓								
	T.INADVE			✓							✓										
	T.MISACT			✓							✓		✓								

Objectives Threats and Assumptions		TOE													Environment						
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.VIRUS	O.AUDIT_SORT	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.AUDIT_PROTECTION
OSPs	P.DETECT		✓	✓							✓		✓							✓	
	P.ANALYZ				✓																
	P.MANAGE	✓					✓	✓	✓						✓		✓	✓			
	P.ACCESS	✓						✓	✓												✓
	P.ACCACT								✓		✓			✓						✓	
	P.INTGTY											✓									
	P.PROTCT									✓						✓					

Table 6-5 Details

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions. The OE.INTROP objective ensures the TOE has the needed access.

Table 6-5 Details

A.DYNMIC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.

A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE

The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators.

The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST

The TOE can only be accessed by authorized system administrator and authorized administrators.

The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access.

The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

T.COMINT

An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access.

The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE data.

The O.INTEGR objective ensures no TOE data will be modified.

The O.PROTCT objective addresses this threat by providing TOE self-protection.

Table 6-5 Details

T.COMDIS

An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access.

The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE data.

The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.LOSSOF

An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access.

The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE data.

The O.INTEGR objective ensures no TOE data will be deleted.

The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT

An unauthorized user may attempt to compromise the continuity of the System’s collection and analysis functions by halting execution of the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE functions.

The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE functions.

The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON

An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE functions.

Table 6-5 Details

T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions. The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of vulnerability. The ST will state whether this threat must be addressed by a Scanner.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources. The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

Table 6-5 Details

T.MISUSE

Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a NCIT module, collect audit and NCIT module data.

T.INADVE

Inadvertent activity and access may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a NCIT module, collect audit and NCIT module data.

T.MISACT

Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE that contains a NCIT module, collect audit and NCIT module data.

P.DETECT

Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

The O.AUDITS, O.IDSENS and O.IDSCAN objectives address this policy by requiring collection of audit, NCIT module, and Correlation Engine data. OE.TIME supports this policy by providing the audit functions with reliable timestamps

P.ANALYZ

Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDANLZ objective requires analytical processes be applied to data collected from NCIT module and Scanners.

P.MANAGE

The TOE shall only be managed by authorized system administrator and administrators.

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use.

The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE functions.

The OE.CREDEN objective requires administrators to protect all authentication data.

The O.PROTCT objective addresses this policy by providing TOE self-protection.

Table 6-5 Details

P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized system administrator and administrators to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection. The OE.AUDIT_PROTECTION objective supports this policy by ensuring that there will be no back door for accessing the audit data using meanings outside the TSC.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. OE.TIME supports this policy by providing the audit functions with reliable timestamps.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of data from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

6.3.2 Rationale for Security Objectives in the Environment

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

6.3.3 Security Functional Requirements Rationale

This section demonstrates that the functional components selected for the ST provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

Table 6-6 Requirements versus Objectives Mapping

Objectives Requirements		TOE													Env	
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.VIRUS	O.AUDIT_SORT	OE.TIME	OE.AUDIT_PROTECTION
TOE	FAU_GEN.1										✓				✓	
	FAU_SAR.1						✓									
	FAU_SAR.2							✓	✓							
	FAU_SAR.3						✓							✓		
	FAU_SEL.1						✓				✓					
	FAU_STG.2	✓						✓	✓	✓		✓				✓
	FAU_STG.4									✓	✓					✓
	FIA_UAU.1							✓	✓							
	FIA_ATD.1								✓							
	FIA_UID.1							✓	✓							
	FMT_MOF.1	✓						✓	✓							
	FMT_MTD.1	✓						✓	✓			✓				
	FMT_SMF.1	✓						✓	✓			✓				
	FMT_SMR.1								✓							
	ADV_ARC.1	✓					✓		✓		✓	✓				
	IDS_SDC.1		✓	✓											✓	

Objectives	TOE													Env	
Requirements	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.VIRUS	O.AUDIT SORT	OE.TIME	OE.AUDIT_PROTECTION
IDS_ANL.1				✓											
IDS_RCT.1					✓										
IDS_RDR.1						✓	✓	✓							
IDS_STG.1	✓						✓	✓	✓		✓				✓
IDS_STG.2									✓						
FAV_ACT.1, EXT												✓			
FAV_ALR.1, EXT												✓			

Table 6-6 Details

O.PROTCT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

The System is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1].

The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized system administrator and authorized administrators of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.IDSCAN

The Correlation Engine must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

A System containing a Correlation Engine is required to collect and store static configuration information of an IT System.

The type of configuration information collected must be defined in the ST [IDS_SDC.1].

Table 6-6 Details

O.IDSENS

The NCIT module must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

A System containing a NCIT module is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1].

O.IDANLZ

The FileScan module must accept data from IDS NCIT module or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

The FileScan module is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.RESPON

The TOE must respond appropriately to analytical conclusions.

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1]

O.EADMIN

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

The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1].

The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

O.IDAUTH

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The System is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2].

The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized system administrator and administrators of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].

Table 6-6 Details

O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2]. The TOE must prevent the loss of audit data in the event that its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of System data in the event that its storage capacity has been reached [IDS_STG.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU_SEL.1]. The TOE must prevent the loss of collected data in the event its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [ADV_ARV.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. The TOE together is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or change audit and System data [FMT_MTD.1, FMT_SMF.1]. The TOE must ensure that all functions to protect the data are not bypassed [ADV_ARC.1]. The TSF must be protected from interference that would prevent it from performing its functions [ADV_ARC.1]**.**
O.VIRUS	The TOE will detect and take action against known viruses introduced to the protected computers. The System takes action to log the intrusions [FAV_ACT.1], and alert the authorised users [FAV_ALR.1].
O.AUDIT_SORT	The System will provide the capability to sort audit information. The System must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3].
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2, IDS_STG.1]. The TOE is informed of data storage exhaustion by the environment and takes appropriate action in protecting the audit data and System data [FAU_STG.2, FAU_STG.4, IDS_STG.2].
OE.TIME	The IT Environment will provide reliable timestamps to the TOE for auditing and detection records. [FAU_GEN.1, IDS_SDC]

6.3.4 Explicitly Stated Requirements Rationale

The claimed Intrusion Defense System PP creates a family of IDS requirements to specifically address the data collected and analyzed by IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

6.3.5 Security Functional Requirements Dependency Rationale

The SFRs in Section 6 do satisfy all the requirement dependencies of the Common Criteria. Table 6-7 Requirement Dependencies Rationale lists each requirement from the ST with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 6-7 Requirement Dependencies Rationale

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	Yes (Reliable time is provided by the IT environment.)
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.2	Yes (FAU_STG.2 is provided in part by the IT environment.)
FIA_UAU.1	FIA_UID.1	Yes
FIA_ATD.1	None	N/A
FIA_UID.1	None	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Yes
IDS_SDC.1, (EXT)	FPT_STM.1	Yes (Reliable time is provided by the IT environment.)
IDS_ANL.1, (EXT)	IDS_SDC.1	Yes
IDS_RCT.1, (EXT)	IDS_SDC.1	Yes
IDS_RDR.1, (EXT)	IDS_SDC.1	Yes
IDS_STG.1, (EXT)	IDS_SDC.1	Yes
IDS_STG.2, (EXT)	IDS_SDC.1	Yes
FAV_ACT.1, (EXT)	IDS_SDC.1	Yes
FAV_ALR.1, (EXT)	IDS_SDC.1	Yes

Application Note: Reliable time is satisfied by the external time server in the Operational Environment (OE.TIME)

6.3.6 TOE IT Security Functions Rationale

This section demonstrates that the security functions selected for the ST provide complete coverage of the defined security functional requirements. The mapping of security functions to SFRs is depicted in the following table, rationales are provided to support the mapping.

Table 6-8 TOE Security Functions Rationale

IT Security Functions	SFRs	Rationale
SF.AUDIT	FAU_GEN.1	SF.AUDIT supports the generation of audit records in accordance with Table 6-2.
	FAU_SAR.1	SF.AUDIT allows only authorized administrators read access to audit information.
	FAU_SAR.2	
	FAU_SAR.3	SF.AUDIT supports the sorting of audit records using records attributes.
	FAU_SEL.1	SF.AUDIT provides the capability of selective auditing.
	FAU_STG.2	SF.AUDIT protects the audit data from deletion as well as guaranteeing the availability of the audit data in the event of storage exhaustion or failure.
	FAU_STG.4	SF.AUDIT prevents auditable events from occurring and records unpreventable events by overwriting the oldest stored audit records when audit trail becomes full.
SF.RBAC	FMT_MOF.1	SF.RBAC allows only administrators with appropriate roles to modify TOE security functions/data.
	FMT_MTD.1	SF.RBAC assigns users with “authorized administrator” role with the right to perform all security functions.
	FMT_SMF.1	SF_RBAC allows the authorized users to perform the management functions that are specified in FMT_SMF.1
	FMT_SMR.1	Authorized administrators are the default roles supported by SF.RBAC.
SF.I&A	FIA_ATD.1	SF.I&A maintains user security attributes.
	FIA_UAU.1	SF.I&A requires users to be positively authenticated, before granting access to the TOE.
	FIA_UID.1	SF.I&A requires users to be positively identified, before granting access to the TOE.
SF.IDPS	IDS_SDC.1	SF.IDPS supports the generation of audit records in accordance with Table 6-3.
	IDS_ANL.1	SF.IDPS performs analysis of network traffic based on statistics, attack signatures or integrity of the network traffic.
	IDS_RCT.1	Upon discovery of attacks, SF.IDPS sends email alarms to the appropriate administrator and prevents the attack.

IT Security Functions	SFRs	Rationale
	IDS_RDR.1	SF.IDPS allows authorized administrators read access to audit information.
	IDS_STG.1	SF.IDPS protects the event logs and overwrites the oldest stored records with newest records upon storage exhaustion.
	IDS_STG.2	
SF.AV	FAV_ACT.1	SF.AV performs an analysis of virus data, and upon discovery of a virus, acts to eliminate the effect of the virus.
	FAV_ALR.1	SF.AV performs an analysis of virus data, and upon discovery of a virus, sends email alarms to the appropriate administrator.

6.3.7 TOE Security Assurance Measures Rationale

This section demonstrates that the Assurance Measures selected for the ST provide complete coverage of the defined security assurance requirements. The mapping of Assurance Measures to SARs is depicted in the following table, descriptions are provided. This list supports the Security Assurance Measures Rationale described in Section 2.3.1.

Table 6-9 TOE Assurance Measures Rationale

Assurance Component	Assurance Measures	Rationale
ADV_ARC.1	Trend Micro Deep Discovery Inspector 3.2 Architectural Design	The Architectural Design provides a description of the security architecture that provides details of the SFR enforcing design. It describes the security domains maintained by the TSF, how the initialisation process is secure, how the TSF protects itself from tampering and prevents bypass of the SFR enforcing functionality.
ADV_FSP.2	Trend Micro Deep Discovery Inspector 3.2 Functional Specification with Complete Summary	The Functional Specification provides a complete summary of the TSF. It includes a description of the security functions provided by the TOE and the external interfaces to the TSF.
ADV_TDS.1	Trend Micro Deep Discovery Inspector 3.2 Modular Design	The Modular Design documentation provides a basic modular design description mapping from the functional specification to the low level in the TOE design. It describes the structure of the TOE in terms of subsystems and modules**.** The design identifies and describes each subsystem of the TSF, the interactions among all subsystems of the TSF, and their mapping to the modules of the TSF. The design describes each SFR-enforcing module and interface in terms of its purpose and relationship with other modules.

Assurance Component	Assurance Measures	Rationale
AGD_OPE.1	Trend Micro Deep Discovery Inspector 3.2 Administrator's Guide	The Deep Discovery Inspector 3.0 Administrator's Guide provides user guidance on how to securely operate the TOE. The Guidance provides descriptions of the security functions provided by the TOE for each user role. Additionally, it provides detailed accurate information for operating the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. It identifies all modes of operation, warnings and error messages, and also describes the security measures for the operation environment that should be followed for secure operation.
AGD_PRE.1	Trend Micro Deep Discovery Inspector 3.2 Administrator's Guide	The Deep Discovery Inspector 3.0 Administrator's Guide provided by Trend Micro details the procedures for secure acceptance, preparation of the operational environment and installation of the TOE, placing the TOE in a secure state.
ALC_CMC.2	Trend Micro – Deep Discovery Inspector 3.2 Configuration	The Life Cycle documentation provides a description of Production support, acceptance procedures and automation at Trend Micro. It describes the system of identification used to uniquely label the TOE, along with the configuration management system and tools used at Trend Micro, and the CM procedures used to control and track TOE changes. The documentation also describes product acceptance and production support procedures used to ensure quality.
ALC_CMS.2	Trend Micro – Deep Discovery Inspector 3.2 Configuration List	The Configuration List uniquely identifies the items that comprise the TOE. This list includes all evaluation evidence, the parts that comprise the TOE, the implementation representation (source code, schematics etc.) and security flaw reports and resolution status.
ALC_DEL.1	Trend Micro – Deep Discovery Inspector 3.2 Delivery Procedures	The Delivery Procedures documentation provides a description of the secure delivery procedures implemented by Trend Micro to protect against TOE modification during product delivery.
ALC_FLR.2	Trend Micro –Deep Discovery Inspector 3.2 Development Life Cycle, Service Engineering	The Service Engineering document outlines the steps taken at Trend Micro to capture, track, and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion. It describes how Trend Micro provides user information on flaws, corrections and guidance on corrective actions.
ATE_COV.1	Trend Micro Deep Discovery Inspector 3.2 Test Coverage Analysis	The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security function interfaces were tested as well as the level of detail to which the TOE was tested.
ATE_FUN.1	Trend Micro Deep Discovery Inspector 3.2 Functional Test Results	Trend Micro Functional Test Results details the overall efforts of the testing and break down the specific steps taken by a tester. It shows that the tests are performed correctly and that the actual results are consistent with those expected.
ATE_IND.2	Trend Micro Deep Discovery Inspector 3.2 TOE	The TOE and equipment necessary to achieve the evaluated configuration
AVA_VAN.2	Trend Micro Deep Discovery Inspector 3.2 Vulnerability Analysis	A focused Vulnerability Assessment is performed by the evaluator to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to potential attacks.

7 TOE Summary Specification

7.1 Statement of TOE IT Security Functions

The TOE provides the following security functions in meeting the SFR's specified in section 6.1:

- SF.AUDIT (Audit)
- SF.RBAC (Role Based Access Control)
- SF.I&A (Identification and Authentication)
- SF.IDPS (Intrusion Detection and Prevention)
- SF.AV (Anti-Virus)

7.1.1 SF.AUDIT

Deep Discovery Inspector 3.2 maintains information regarding the administration and management of its security functions as part of the audit records. This security function addresses the generation; storage and reviewing of these audit records.

Authorized TOE administrators are only allowed to interact with the TOE through a browser-based graphical user interface supported by the Deep Discovery Inspector. All the security relevant actions as specified in Table 6-2 taken by the authorized administrators are recorded as a part of the audit log.

All generated audit records are stored within a database. All audit records include the date and time of the event, type of event, subject identity, the outcome (success or failure) of the event. No TOE administrator has direct access to the database. Reliable time for the audit records is provided by the operational environment.

The audit log review function shall provide the sorting function based on the elements of the audit records.

The TOE records new auditable events (reading of TOE data, user requests failure) by overwriting the oldest auditable events in the database with records of these new events.

Authorized TOE administrators can only read audit records through the TOE's administrative interface; access rights to the audit records are restricted based on their role definition. No administrator is given write access to the audit records; therefore the TSF prevents modifications to the audit records. However, authorized TOE users can delete audit records via the Web Console Log/Report Maintenance menu item. The SF.AUDIT audit logs are all classified as "system events" at the administrative interface.

Authorized TOE administrators are given the capability to read and export the audit logs.

Authorized administrators with appropriate assigned roles have the ability to include or exclude auditable events from the set of audited events based on the audit event type.

Unauthorized users are prevented from any access to the audit records by a combination of the TSF and the Operational Environment:

- The I&A functionality of the TOE prevents access to the TSF and TSF data via the Web Console by unauthorized users.
- The TOE, in all form factors, is hardened with security measures designed and implemented to prevent direct access to the file system, command line console, and root access. The only designed method of interaction with the database is via the Web Console administrative interface that is protected by the identification and authentication functionality of the TOE.
- SSH root access to the device is protected by digital certificate that the TOE stores securely. Even if someone was able to crack the root password there would be no login because the TSF validates the SSH client certificate.
- The PostgreSQL database "write" account is a low privilege account that no one can use to login and change database.

7.1.2 SF.RBAC

Deep Discovery Inspector 3.2 restricts authorized TOE administrators' access to the system using role-based access control.

All TOE administrators are assigned roles at creation.

Authorized TOE administrators can only access the TOE through the administrative interface.

They have full access to the management functions permitted by their roles.

By default, there is only one authorized System administrator.

After Deep Discovery Inspector installation, users can create an authorized administrator role which is allowed access to all TOE and System data via the Web UI administrative interface except the account management function.

7.1.3 SF.I&A

The identification and authentication mechanism used by Deep Discovery Inspector 3.2 is based on user ID and password.

For each user being created, the creator is required to assign them with a user ID, an initial password and a role.

Before users are granted access through the administrative interface, they are required to provide their credentials at the web console and these are verified by the TOE.

Identification is performed by finding the matching administrator based on a case-insensitive match to the user name.

Authentication takes place by matching one-way hashed passwords against values previously stored in the database.

Users are allowed to modify their own passwords; however, they must follow the strong password policy.

7.1.4 SF.IDPS

The TOE provides intrusion detection and prevention functions.

Deep Discovery Inspector detects and identifies evasive threats in real-time, along with providing in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.

All detected intrusions are tagged with a severity by the TOE according to detection rules and patterns. The rules can set to default or customized. Intrusion alarms are sent to the system administrator via email. Mitigation requests are sent to mitigation devices based on the severity of the detected intrusion.

Mitigation devices with network access control functions may prevent the endpoint from accessing the network until the endpoint is free of threats.

Detection records are stored in the Deep Discovery Inspector database for review and report generation. Within each record, the event time, event type, action taken, data source and destination are recorded. Reliable time for the detection records is provided by the operational environment.

Deep Discovery Inspector allows only pre-authorized administrators (with appropriate roles) read access to these event logs.

7.1.5 SF.AV

The TOE provides anti-virus functions. Data is collected, analyzed and stored by Deep Discovery Inspector.

Protection and storage of event data, alerts and email notifications are handled as described for SF.IDPS (above).

The Deep Discovery Inspector is deployed to monitor the traffic of network it protected. The traffic is analysed and scanned by TOE. File based and network based virus shall be detected by scanner of TOE.

When viruses are detected, these records are stored for review and report generation. Within each record, the event time, event type, action taken, and data source are recorded. Authorized system administrator and authorized administrators can use functionalities provided by Deep Discovery Inspector to review the detection results and reports.