Deep Security 20
Security Target v12.0

Revision History

Rev. #	Description	By	Date of Issue
1.0	First version based on DS 11.0 Security Target v50.0	Marion Chase, Marek Buchler	27 Oct 2020
2.0	Updated Figures 1-1 and 1-2 and minor updates to user documentation links and VMWare information	Marion Chase	27 Nov 2020
3.0	Updated in response to OR1	Marion Chase	31 Dec 2020
4.0	Additional updates in response to OR1: Document header formatting update, removed Figure 1-2 to ADV_TDS, clarification of Relay as a component, added DSA/DSVA table of functionality, added mapping table to SF	Marion Chase	18 Jan 2021
5.0	Updated in response to OR4 – added web browser to 1.3 and 1.6.5 Added clarification on API version inclusion/exclusion Updated list of tables	Marion Chase	9 Feb 2021
6.0	Updated software build versions in section 1.1 and platforms in TOE Environment section 1.6.5	Marion Chase	16 March 2021
7.0	Several updates in response to OR8	Marion Chase	4 August 2021
8.0	Additional changes for OR8	Marion Chase	19 August 2021
9.0	Added CAVP certificate references	Marion Chase	21 October 2021
10.0	Updates in response to OR9 and OR 10	Marion Chase	2 December 2021
11.0	Updated to clarify that DSVA version will be automatically updated after deployment	Marion Chase	8 February 2022

Rev. #	Description	By	Date of Issue
12.0	Updated in response to Certifier comments	Marion Chase	30 May 2022

Contents

List of Figures:

List of Tables:

Acronyms and Abbreviations

Acronym	Meaning
Agent	Deep Security Agent
Analyzer	A functional component of the agent that performs an analysis of data provided by Scanners and Sensors to identify potential security issues on a protected computer.
Appliance	Deep Security Virtual Appliance
CC	Common Criteria for Information Technology Security Evaluation
CCS	Canadian Common Criteria Scheme
CEM	Common Methodology for Information Technology Security Evaluation
DSA	Deep Security Agent
DSM	Deep Security Manager
DSR	Deep Security Relay – a Deep Security Agent with Relay functionality enabled

Acronym	Meaning
DSVA	Deep Security Virtual Appliance for VMWare
EAL	Evaluation Assurance Level
GCP	Google Cloud Platform
IT	Information Technology
Manager	Deep Security Manager
PP	Protection Profile
SAR	Security Assurance Requirements
Scanner	A functional component of the agent that collects static configuration information from a protected computer, including detected malicious code and known vulnerabilities, and forwards the collected information to the Analyzer.
Sensor	A functional component of the agent that monitors changes occurring on a protected computer, collects events as they occur, and forwards the collected information to the Analyzer.
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TBD	To Be Determined
TOE	Target of Evaluation
TSC	TSF Scope of Control

Acronym	Meaning
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
VMware ESXi	vSphere ™ ESXi from VMware Inc.

Document Organization

Section 1 provides the introductory material and identification information for the Security Target and a TOE overview and description

Section 2 provides a conformance claims for the ST

Section 3 provides a 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 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains definitions for extended SFRs.

Section 6 contains the 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 describes the details specific to the TOE implementation of the security measures described in this document.

1 Introduction

1.1 ST Reference

Title:	Trend Micro Deep Security 20 Security Target
ST Version:	Deep Security 20 Security Target v10.0
TOE Identification:	Trend Micro **Deep Security 20**
Downloaded Software Packages:	• Deep Security Manager version 20.0.344 • Deep Security Windows Agent version 20.0.0-3288 • Deep Security RHEL Agent version 20.0.0-3288 • Deep Security Virtual Appliance installed software version 20.0.0-877, upgraded to version 20.0.0-3288 Customers can download software packages for these components from the **Software** page of the Trend Micro Deep Security Help Center web site
Author:	Marion Chase
Vetting Status:	Draft

1.2 Deep Security and TOE Overview

The subject of this evaluation described in this ST is Trend Micro Deep Security 20. Throughout this document it will also be referred to as Deep Security 20 or the Target of Evaluation (TOE).

Trend Micro Deep Security is a software intrusion detection and prevention software system that protects customers' IT system servers and applications. This solution can identify suspicious activity and behavior, and take proactive or preventive measures to ensure the security of the machines on which it is deployed. Several protection features are combined in centrally managed software agents, adding a comprehensive suite of protection functionality to the intrusion detection and prevention system.

Deep Security provides the ability to protect itself and associated data from unauthorized access or modification and provides an audit trail to ensure accountability for authorized actions.

Deep Security 20 is comprised of a software management application with a browser-based management console called the Deep Security Manager, and small traffic filtering engines called Deep Security Agents available for various operating systems. In VMware ESXi environments, security protection capabilities can be provided in an agent-less mode with the Deep Security Virtual Appliance. When installing from the Deep Security Agent Software package, administrators can optionally configure additional relay functionality to be enabled. In that case, the installed software then provides both a Deep Security Agent and additional relay functionality. (This additionally enabled functionality is known in the user guidance and in this document as the "Deep Security Relay"). The relay functionality is not available as a stand-alone component and is only available when combined with the Deep Security Agent. The Deep Security Relay facilitates distribution of additional system updates required by the Deep Security system.

Deep Security components inside the TOE Boundary:

- **Deep Security Manager**
- **Deep Security Agent(s) with or without Relay enabled**
- **Deep Security Virtual Appliance**

The **Deep Security Agent** component can be deployed to protect workloads on a hybrid environment of physical, virtual, cloud and containers. The **Deep Security Virtual Appliance** can be deployed on VMware ESXi cloud computing hosts, providing protection services to virtual machines in that environment without requiring the presence of an in-guest Agent. The Appliance protects short lived and reverted virtual machines, as well as virtual machines and other appliances whose operating systems are not directly accessible, even those machines being managed by other administrators. Virtual machines running in this environment can also be protected by the Deep Security Agent in a coordinated approach.

The host platforms on which the above components are running are outside the TOE, as is the database required for the Deep Security Manager.

The system components that are part of the TOE are supported by Trend Micro services common to many Trend Micro products and hosted on web sites outside of the TOE including:

- Smart Protection Network - delivers proactive global threat intelligence against zero-hour threats to ensure that customers' environments are always protected.
- Active Update - provides up-to-date downloads of pattern files, scan engines, programs, and other Trend Micro component files through the Internet.
- Trend Micro Licensing module – maintains and validates the list of issued customer license keys
- Software Download Center – Web site for distribution of Deep Security Software

1.3 TOE Description

Figure 1 - Deep Security 20 Overview

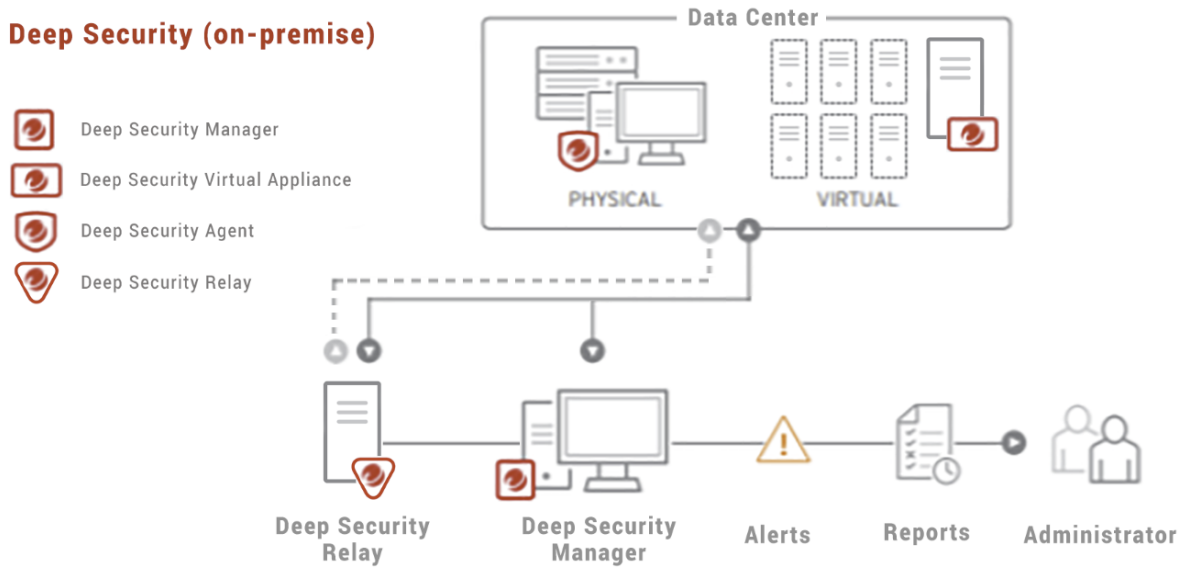

Figure 1 shows a high level view of the Deep Security components in the TOE. The diagram demonstrates the relationship of the components in the TOE to the supporting components required for the operation of Deep Security.

The TOE includes only Deep Security components represented by Trend Micro icons. In Figure 1, these components are: the Deep Security Manager (Manager) installed on a server in the Manager Cluster, the Deep Security Agent (Agent) installed on physical servers or on virtual machines (VMs), and Deep Security Virtual Appliance (Virtual Appliance) installed in a VMware ESXi server environment. Deep Security requires at least one Deep Security Relay. The Deep Security Agent configured as a Deep Security Relay can be installed on physical servers or virtual machines (VMs) and provides a lightweight web server to relay component updates and new software from Trend Micro Smart Protection Network. For ease of deployment the Deep Security Manager installer provides the option to deploy a Deep Security Relay on the same host as the Deep Security Manager host.

Administrators connect to the TOE via a web browser.

The TOE is a system consisting of the following software components:

1.3.1 Deep Security Manager

Deep Security Manager is a powerful, centralized web-based management application that allows Administrators to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. All of this can be done in real-time, from the desktop. Administrators use the Deep Security Manager to control and configure the security protection that is applied to servers protected by Agents and Appliances. The Deep Security Manager is also the centralized application for collection of logs and events relating to the protected servers.

Deployment

The Deep Security Manager requires a running database which is outside the TOE.

The Deep Security Manager is deployed simply by downloading the Deep Security Manager software package from the **Software** page of the Trend Micro Deep Security Help Center web site https://help.deepsecurity.trendmicro.com/software.html and then installing the application on the designated management computer.

Security Policies

Security Policies are templates that specify the security rules to be configured and enforced automatically for one or more Computers. These compact, manageable rule sets make it simple to provide comprehensive security without the need to manage thousands of rules. Default Security Policies provide the necessary rules for a wide range of common Computer configurations, ensuring rapid deployment.

Multi-Level Policy Inheritance

Deep Security supports multiple levels of Security Policy inheritance. A newly created policy can be configured to inherit all or some of its settings from a parent policy. This lets the user create a tree structure of security policies which get progressively more granular and detailed.

Dashboard

The customizable, web-based UI (User Interface) makes it easy to quickly navigate and drill down to specific information. It provides:

- Extensive system, event and Computer reporting, with drill-down capabilities

- Graphs of key metrics with trends, with drill-down
- Detailed event logs, with drill-down
- Ability to save multiple personalized dashboard layouts

Built-in Security

Role-based access allows multiple Users, each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. Digital signatures are used to authenticate system components and verify the integrity of rules. Session encryption protects the confidentiality of information exchanged between components.

1.3.2 Deep Security Agent, Deep Security Virtual Appliance

The Deep Security Agent ("the Agent") is a high performance, small footprint, software component that sits directly on a Computer, and defends it by monitoring incoming and outgoing network traffic for protocol deviations or contents that might signal an attack. When necessary, the Agent intervenes and neutralizes the threat by either blocking or correcting traffic.

The Deep Security Virtual Appliance (DSVA) performs the same functions as the Agent, but is an agent-less implementation specifically designed for VMware NSX-T and NSX-V environments using vSphere ESXi 6.5 and later. The DSVA protects Virtual Machines (VMs) on the same ESXi Server, each with its own individual security policy. The Virtual Appliance uses VMware's APIs and is supported on VMware vSphere 6.5 and later.

Deployment and Policies

Deep Security Agents and Virtual Appliances are deployed by downloading the software packages from the **Software** page of the Trend Micro Deep Security Help Center web site https://help.deepsecurity.trendmicro.com/software.html and importing them to your Deep Security Manager. Imported Agents can then either be installed manually or with a deployment script on the physical or virtual machines to be protected, then using the Manager to activate them. The Virtual Appliance software package must also be downloaded from the **Software** page of the Trend Micro Deep Security Help Center web site and imported to the Deep Security Manager before it can be deployed to the NSX environment. After deploying the downloaded DSVA base version, the DSVA can be automatically upgraded to the same version as an imported Agent.

The deployed Agents/Virtual Appliances implement Security Policies defined by an Administrator using the Deep Security Manager.

Security Policies are made up of sets of rules and configuration settings that can be applied to one or more protected computers. Security Policies can be selectively applied to network traffic based on a variety of conditions such as application type, interface type, protocol, and direction of traffic flow. Security Policies for malware scans configure the scan operation such as real-time or manual, the type and location of files to be scanned and the behavior when malware is detected. Rules other modules

control which URLs, files, keys, attributes, software applications and logs to monitor, and the action to take when a monitored condition occurs.

The system can be configured to send alert notifications when particular rules are triggered or when other system events occur. An administrator uses the Deep Security Manager to define and distribute Security Policies to the Agents/Virtual Appliances over the network.

For additional security, the administrator can manage the methods and timing of the communications between the Deep Security Manager and individual Agents/Virtual Appliances.

Protection Modules

Table 1-1 Protection Module mapping to Security Functions

Table 1-1 below lists the available Trend Micro Deep Security protection modules and their mapping to the Security Functions described in Section 7

Protection Module	Security Function
Anti-Malware	SF.AV
Web Reputation	SF.IDPS
Stateful firewall	SF.IDPS
Intrusion Prevention: • Intrusion detection and prevention (IDS/IPS) • Web application protection	SF.IDPS
File and system Integrity Monitoring	SF.IDPS and SF.AC
Log Inspection	SF.IDPS
Application Control	SF.AC

Table 1-2 Protection Module Summary for DSA and DSVA

Table 1-2 proves a summary of the Protection Modules available by deploying the DSA and DSVA.

For a more detailed list of all supported features on Agents deployed on all operating systems see https://help.deepsecurity.trendmicro.com/20_0/on-premise/supported-features-by-platform.html

Protection Module DSA or DSVA	Anti-Malware	Web Reputation	Firewall	Intrusion Prevention	Integrity Monitoring	Log Inspection	Application Control
DSA on Windows Server 2019	✓	✓	✓	✓	✓	✓	✓
DSA on Red Hat 7	✓	✓	✓	✓	✓	✓	✓

DSVA on NSX	✓ protects Windows VMs	✓	✓	✓	✓ protects Windows VMs	X	X

Anti-Malware

The Deep Security Agent provides standard Anti-Malware capabilities. Deep Security Anti-Malware for Virtual Machines employs agent-less scanning technology for detecting malicious files on Virtual Machines in a VMware ESXi environment. File writes and reads are remotely scanned by the appliance for malware. The Anti-Malware module is available in both the Agent and Appliance for VMware ESXi. The exact functionality available varies by operating system.

Anti-Malware Configurations specify:

- The applicable real-time policies that apply during different periods of the day/week
- The policy for full scheduled or manual scans
- Exclusions of file types and directories
- Real-time behaviour (scanning reads and/or writes) and applicable actions

Web Reputation

Web Reputation allows blocking access to URLs that are known to serve malicious or risky content by consulting Trend's constantly-updated Smart Protection Network (SPN) database. This capability is provided by the Agent and Appliance.

Web Reputation Configurations specify:

- Whether or not web reputation functionality is on or off
- URLs that are always allowed to be accessed
- Additional URLs to block access to

Stateful Firewall

The Deep Security Firewall module is enterprise-grade, bi-directional, and stateful. It is used to limit communication by source and destination port, IP, MAC addresses, and is protocol-aware. By limiting traffic, the attack surface of systems is reduced, and the risk of unauthorized access to the system is also reduced. The stateful firewall is available in both the Agent and Appliance for VMware ESXi.

Some of the primary features and capabilities of the Deep Security Firewall Rules include:

- Virtual machine isolation: Allows VM's to be isolated virtual environments, providing virtual segmentation without the need to modify virtual switch configurations or network architecture
- Fine-grained filtering: Firewall rules filter traffic based on source and destination IP address, port, MAC address, etc. Different rules can be applied to different network interfaces. For end-

user systems, the firewall is location aware, and is able to limit interface use such that only a single interface can be used at one time.
- Reconnaissance detection: Detect reconnaissance activities such as port scans.
- Flexible control: The stateful firewall is flexible, allowing complete bypass of inspection, when appropriate, in a controlled manner.

Intrusion Prevention

The high-performance deep packet inspection engine intelligently examines the content of network traffic entering and leaving hosts. The traffic is inspected for protocol deviations, content that signals an attack, or policy violations.
Intrusion Prevention protects operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injection and cross-site scripting. Detailed events provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit. The Intrusion Prevention module is available in both the Agent and Appliance for VMware ESXi.

Intrusion Detection and Prevention Rules fall into several categories:

- Vulnerability rules shield a known vulnerability – for example, those disclosed on Microsoft Tuesday – from any number of exploits and exploit variants. Trend Micro Deep Security includes protection for over 100 applications and operating systems, including database, web, email, and FTP servers running on Windows or Linux. Rules that shield newly discovered vulnerabilities are automatically delivered, often within hours, and can be pushed-out to thousands of servers and end-user systems within minutes, without the need for disruptive system restarts.
- Smart rules provide broad protection, and low-level insight, for servers and end-user systems. For operating systems and applications, the rules limit variations of elements of traffic, limiting the ability of attackers to investigate possible attack vectors since many attacks are based on exceeding expected characteristics. For servers and end-user systems, smart rules also provide tremendous insight into application activity and unexpected traffic (HTTP on an unexpected port, use of a web browser on a server, etc.).
- Application Control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules are also used to identify malicious software accessing the network.

Integrity Monitoring

Integrity Monitoring is the ability to monitor critical operating system and application elements (files, directories, registry keys and values, etc.) for changes such as content, ownership, permissions and generate alerts to provide visibility into the changes that have occurred. This capability is provided by the Agent and Appliance for VMware ESXi.

Integrity Monitoring includes:

- Extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.). Addition, modification, or deletion of

Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.

- Auditable reporting is generated within Deep Security Manager, along with alert generations, and automated report creation and delivery.
- Security Policies allow Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Windows 2019 servers use the same operating system rules which are configured in a single Security Policy which is used by several servers. However, each server has unique requirements which are addressed at the individual Host configuration level.
- Flexible, practical monitoring optimizes monitoring activities. The intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.

Log Inspection & Collection

Log Inspection & Collection provides the ability to collect and analyze operating system and application logs for important security events. Log Monitoring enables administrators' visibility into suspicious activity occurring in their environment and is a critical component to any forensic or auditing activities. This capability is provided by the Agent.

Log Inspection Rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a security information and event management (SIEM) system, or centralized logging server for correlation, reporting, and archiving. All events are also securely collected centrally at Deep Security Manager.

Log Inspection enables:

- Suspicious behaviour detection.
- Collecting events across heterogeneous environments containing different operating systems and diverse applications
- Insight and knowledge of important events such as error and informational events (disk full, service start/shutdown, etc.), including administrator activity (administrator login/logout, account lockout, policy change, etc.).

Application Control

Application control scans a computer for an inventory of installed software and creates an initial ruleset. After that, the Deep Security Agent continuously monitors the computer for application software changes, and the administrator can create rules to allow or block specific software when it tries to launch. Application control creates an event when unrecognized software tries to execute. This capability is provided by the Agent.

Application Control Rules:

Application Control uses a local or shared ruleset configuration created by an initial inventory scan of a master computer. The Agent monitors computers for changes to software properties: file name, path or location, time stamp, permissions, file contents.

When Application Control finds new software on a computer, it compares the software file's Hash, File size, Path and File name with entries in its allow or block ruleset to decide whether the software is known or unrecognized.

Application Control uses these configured rules to decide whether to Allow or Block execution of known software.

Administrators can also configure how application control will react when it detects attempts to run unrecognized software (changes that are not already specifically allowed in the rules), so depending on your security posture, you can configure whether application control will allow or block execution of unrecognized software.

Our tested TOE Configuration will include Agent based testing of all modules as well as a combined mode testing using the DSVA for Anti-Malware protection only.

1.3.3 Deep Security Relay

The Deep Security Manager requires at least one Deep Security Agent to be deployed with the relay enabled to automatically retrieve Deep Security Rule Updates and Anti-Malware components over the internet from Trend Micro Smart Protection Network, and distribute them to some or all the Agents/Virtual Appliances across the network. The Deep Security Relay also provides Deep Security Agent plugins through a light-weight web server.

Deployment and Policies

Deep Security Relay is deployed in the same way as an Agent. After the software has been deployed, Relay-specific functionality is enabled from the Deep Security Manager.

As the Deep Security Relay is based on the Deep Security Agent foundation, Relay hosts can also be protected by configuration using Policies.

1.4 TOE Boundary

1.4.1 Physical Boundary

The TOE physical boundary encompasses only the software components of the Deep Security Manager, Deep Security Relay and the Deep Security Agents/Virtual Appliances. The Deep Security 20 On-Premise Administration Guide gives details of the software components contained in the TOE and how to deploy them.

A more detailed TOE diagram is shown in **Figure 1** of the Basic Design (ADV_TDS)

1.4.2 User Guidance References

The **Deep Security 20 Common Criteria Configuration Guid**e (also found here https://help.deepsecurity.trendmicro.com/20_0/on-premise/common-criteria.html?Highlight=common%20criteria) provides details of the configuration steps to configure the TOE environment.

The **Deep Security 20 On-premise Administration Guide** (available from https://help.deepsecurity.trendmicro.com/20_0/on-premise/guide-admin.html?Highlight=admin%20guide) gives details of how to configure the Deep Security system and its interfaces after installation e.g. configuration of the protection modules.

Deep Security 20 **Deploy Deep Security Virtual Appliance** section of the **Deep Security 20 On-premise Administration Guide** (as above), contains guidance for deploying in the NSX environment and is also found https://help.deepsecurity.trendmicro.com/20_0/on-premise/appliance-before.html

Deep Security Agent 20 Linux Kernel Support documentation can be downloaded here http://files.trendmicro.com/documentation/guides/deep_security/Kernel%20Support/20.0/Deep_Security_20_0_kernels_EN.html, and lists the supported linux kernels for Agents.

Deep Security 20 Supported features by Platform Guide provides a detailed list of the supported protection modules and features by host platform and can also be found here https://help.deepsecurity.trendmicro.com/20_0/on-premise/supported-features-by-platform.html?Highlight=supported%20features%20by%20platform

1.4.3 Logical Boundary

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

- SF.AUDIT (Audit)
- SF.RBAC (Role Based Access Control)
- SF.I&A (Identification and Authentication)
- SF.SECCOM (secure intra-TOE, database, and administrator communication)
- SF.IDPS (Intrusion detection and prevention)
- SF.AV (Anti-Virus)
- SF AC (Application Control)

These descriptions 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 Security 20 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 Security 20 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 Security 20 is based on:

- User ID, password and an optional multi-factor authentication (MFA) token. For each user being created, the creator is required to assign them with a user id, an initial password and a role, or
- An external trusted SAML Identity Provider that can specify user and role information.

SF.SECCOM

All communications between the Deep Security Agents/Virtual Appliances and the Deep Security Manager are protected from disclosure or modification. This is achieved by deploying symmetric and asymmetric encryption algorithms for protection of the communication channel.

Communications between DSM and the database are protected using TLS.

Communications between a remote administrator and the DSM web interface is protected using TLS.

SF.IDPS

The TOE provides intrusion detection and prevention functions. The intrusion detection and protection functionality includes Firewall and Intrusion Prevention capabilities. The TOE also provides Integrity Monitoring and Log Inspection functionality for detection of changes on the protected computers, and Web Reputation functionality for blocking malicious URLs. System data is collected and analyzed by Deep Security Agents/Virtual Appliances and is passed to the Deep Security Manager for review and forwarding to external DB storage.

SF.AV

The TOE provides anti-virus functions. Data is collected and analyzed by Deep Security Agents/Virtual Appliances and is passed to the Deep Security Manager for review and forwarding to external DB storage.

SF.AC

The TOE provides application control functions that control software execution on computers protected by Agents. System data is collected and analyzed by the Integrity Monitoring functionality of the Deep Security Agents and is passed to the Deep Security Manager for review and forwarding to external DB storage.

1.4.4 Excluded Functionality

The following features of the TOE are excluded in the Common Criteria Evaluated Configuration of the TOE:

- Command Line Interface to Deep Security Agent (for installation and troubleshooting). Administrators can configure Agent self-protection using the Deep Security Manager that prevents unauthorized use of the dsa_control command.
- Legacy SOAP Application Programming Interface to the Deep Security Manager (disabled by default) and Status Monitoring APIs (disabled by default). This interface has been deprecated and no new features will be added to it.
- Command Line Interface to Deep Security Manager (for installation, initial configuration and trouble-shooting). Use of this interface in a Common Criteria environment is described in the Common Criteria Configuration Guide. Users who access this interface are assumed A.NOEVIL (see 3.3.3)
- Console Access to Deep Security Virtual Appliance (for installation and trouble-shooting only)
- Shift-jis encoding is not supported on agent servers.
- MFA and SAML authentication services are provided by the IT environment, their service providers are outside the scope of this evaluation.
- The Multi-Tenancy feature allows the administrator to create independent instances of Deep Security within their enterprise for individual departments or lines of business within their organization. Multi-tenancy is not tested in this Common Criteria evaluation.

1.4.5 TOE Evaluated Configuration

Trend Micro Deep Security supports multiple host platforms and operating systems for Managers, Agents, Relays and Appliances.

The TOE environment for Common Criteria is evaluated using the following system requirements, non-TOE components and Operating Systems:

Deep Security Manager

- Minimum Memory (based on <500 Agents):
  - 16 GB RAM
  - 8 GB JVM
  - 2 CPUs
- Disk Space: Minimum 1.5 GB (200 GB recommended)
- Deep Security Manager running on Windows Server 2019 (64-bit)
- Database: Microsoft SQL Server 2019

Note: DSM relies on Azul Zulu OpenJDK 8 JRE which is provided as part of the DSM installation package.

The DSM requires the use of a web browser for user interface. The DSM works with many web browsers and cookies must be enabled. Trend Micro recommends using the latest version of Firefox, Microsoft Edge, Google Chrome or Apple Safari.

Deep Security Agent/Deep Security Relay

- Agents/Relays running on the following Operating Systems:
  - Windows Server 2019
  - Linux Red Hat Enterprise Edition 7
- Deep Security Agent:
  - Windows:
    - All protection enabled: Minimum 2 GB RAM (4 GB recommended)
    - Minimum Disk Space: 1 GB
  - Linux
    - All protection enabled: 2 GB RAM (5 GB recommended)
    - Minimum Disk Space: 1 GB
- Deep Security Relay only:
  - Relays are only supported on 64-bit operating systems
  - Windows/Linux: 2 GB RAM (4 GB recommended)
  - Minimum Disk Space: 30 GB for software packages

Deep Security Virtual Appliance

(Based on maximum 10 protected VMs)

- Minimum Memory: 4 GB vRAM
- Minimum Disk Space: 20 GB
- DSVA running on the following Operating System:
  - VMware NSX-T Data Center (NSX-T): VMware vCenter 7.0 with ESXi 7.0

Additional VMware Utilities versions:

- VMware Tools 10.0.6 or newer. The VMWare Tools installation should include VMCI and NSX File introspection drivers.

- VMware vShield Endpoint Security (EPSEC) provides the Thin Agent used to interact with the Deep Security Virtual Appliance when providing agent-less anti-malware protection for each virtual machine. This is the thin client VMware uses to “interact” with the security appliances provided by their partners, and contains the driver for virtual machines to offload file events. Minimum supported EPSECLIB Build Number 15817270.

DNS, NTP and SMTP servers are all required as a part of the TOE's IT environment.

1.5 Required Non-TOE hardware/software/firmware

Full details of the supported operating systems and system requirements are available in the Deep Security 20 Administration Guide which can be downloaded.

Deep Security Manager software is available for installation on a computer using multiple Windows or Linux operating systems, for details see https://help.deepsecurity.trendmicro.com/20_0/on-premise/system-requirements.html. However the evaluated OSs are listed in Section 1.4.5 above.

The Deep Security Manager requires the use of a Database for storing configuration and audit data, and works with Oracle, Postgres or Microsoft SQL Server databases. A detailed list of the recommended system requirements and the supported platforms for the Database can be found in the Administration Guide **System Requirements** section and online https://help.deepsecurity.trendmicro.com/20_0/on-premise/system-requirements.html

To install the Deep Security Agent or Relay requires a physical or virtual machine with a Windows or Linux operating system.

Deep Security is supported on a range of Linux kernels, see http://files.trendmicro.com/documentation/guides/deep_security/Kernel%20Support/20.0/Deep_Security_20_0_kernels_EN.html

Section 1.4.5 provides details of the system requirements used for the TOE environment configuration.

The vCenter, NSX-T and NSX Manager components are part of the VMware vSphere line of products and are required if you are deploying protection using Deep Security Virtual Appliances. vCenter is the central management console for vSphere and provides the connection point for Deep Security Manager to discover and manage Virtual Machines, Virtual Appliances and the components installed in the ESXi environment. NSX Manager is a required component if using agent-less Anti-Malware protection of Virtual Machines. Deep Security Manager connects to NSX Manager to initialize Anti-Malware protection. ESXi is the hypervisor component in the vSphere line of products and is used to host Virtual Machines and Virtual Appliances.

The Deep Security Virtual Appliance can only be installed in a VMWare ESXi environment. The requirements are described in the Administration Guide **Deploy Deep Security Virtual Appliance** section or online here https://help.deepsecurity.trendmicro.com/20_0/on-premise/appliance-before.html

See Section 1.4.5 for more details of the system requirements for the VMWare components used in the TOE environment configuration.

The TOE also requires an IT infrastructure that includes:

- Deep Security Manager and Deep Security Agent access to Trend Micro Smart Protection Network via the internet. Trend Micro Smart Protection Network collects intelligence on global threats and provides updates that supply the new pattern files to block threats sooner.
- Deep Security Manager access to Trend Micro Download Center to download latest agent packages and kernel driver updates

- Connection between the Deep Security Manager and Agent/Appliance components via network or internet.

2 Conformance Claims

2.1 CC Conformance Claim

2.1.1 CC Version: 3.1 Revision 5

General Status: Ready for release

2.1.2 CC Conformance

This ST is based on the following, referenced hereafter as CC:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017.

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017.

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, April 2017.

This ST claims the following CC conformance:

- Part 2 extended.
- Part 3 conformant.

No PP conformance is claimed.

Deep Security 20 is being evaluated to Evaluation Assurance Level 2 augmented with ALC_FLR.1 (EAL2+) under the Canadian Common Criteria Scheme.

2.1.3 Assurance Requirements Rationale

EAL2+ was chosen to provide a level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the System will have incurred a search for obvious flaws to support its

introduction into the non-hostile environment, and reasonable assurance is provided to ensure the secure operation of the system.

The SARs are described in Section 6.2.

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. All these are described in detail in this section.

3.1 Threats to Security

The following are threats identified 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.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.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
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
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to 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.FACCNT	An unauthorized user may attempt to access TOE data or security functions which may go undetected.

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.SCNCFG	An IT administrator may configure improper security configuration settings 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 that have not been remediated by the IT administrator.
T.FALACT	The TOE may fail to react to identified or 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.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	A user of the IT System that the TOE monitors may cause inadvertent activity and access to the System
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an 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.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.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.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Security Assumptions

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

3.3.1 Intended Usage Assumptions

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

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

3.3.2 Physical Assumptions

A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. Physical access to the Deep Security Manager component of the TOE is typically restricted on the premises of the company that owns and administers that component. For IT System computers being protected by the TOE, it is assumed that they are physically protected in a manner appropriate to the security risk and defined usage of each computer.

3.3.3 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, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.TRUST	The TOE can only be accessed by authorized users.

Note: Users with Administrator rights on the Computers being protected by the TOE are not considered to be managers of the TOE. However, as authorized administrators of the IT system computers being monitored, they are considered to be covered by the Personnel Assumptions A.NOEVIL and A.TRUST.

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.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner 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 Sensor 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.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.EXPORT	When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.
O.VIRUS	The TOE will detect and take action against known viruses introduced to the protected computer via network traffic or removable media.
O.AUDIT_SORT	The TOE will provide the capability to sort the audit information
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.APP_CONTROL	The TOE will detect and prevent potentially malicious software applications from executing

4.2 Security Objectives for the Environment

OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is appropriate to the security risk and defined usage of each computer.
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.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is appropriate using best practices for credentials security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.TIME	The IT system must be configured to provide a reliable time source.

5 Extended Components Definition

5.1 Extended Security Functional Components for IDS

The functionality in this extended class addresses the requirements provided by the Deep Security system to detect, analyze and react to possible intrusions on computers protected by Deep Security Agents or Deep Security Virtual Appliances.

The Extended SFR claims in this section are based on the Intrusion Detection System (Extended Requirements) class (IDS) from the **U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments**. Version 1.7, July 25, 2007.

Table 5-1 Extended Security Functional Requirements for IDS

Security Functional Requirement	Name
IDS_SDC.1	System Data Collection (EXT)
IDS_ANL.1	Analyzer Analysis (EXT)
IDS_RCT.1	Analyzer 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)

5.1.1 Intrusion Detection System component requirements (IDS)

System Data Collection (IDS_SDC.1, EXT)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) [selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 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; and

b) The additional information specified in the *Details* column of Table 5-2 System Events.

Table 5-2 IDS System Events

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network Traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration	Source address, destination address
IDS_SDC.1	Data introduction	Object IDS, location of object, 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	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account names for cracked passwords, account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Analyzer analysis (IDS_ANL.1, EXT)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:

a) [selection: *statistical, signature, integrity*]; and

b) [assignment: *other analytical functions*].

IDS_ANL.1.2 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; and

b) [assignment: *other security relevant information about the result*].

Analyzer react (IDS_RCT.1, EXT)

IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

Restricted Data Review (IDS_RDR.1, EXT)

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

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

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

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

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

IDS_ STG.1.2 The System shall protect the stored System data from modification.

IDS_ STG.1.3 The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].

Prevention of System data loss (IDS_STG.2, EXT)

IDS_STG.2.1 The System shall [selection: *'ignore System data', 'prevent System data, except those taken by the authorized user with special rights', 'overwrite the oldest stored System data '*] and send an alarm if the storage capacity has been reached.

5.2 Extended Security Functional Components for AV

This section defines extended security functionality for Anti-Virus (anti-malware) provided by Deep Security.

The functionality in this extended class addresses the requirements provided by the Deep Security Agent and Deep Security Virtual Appliance components of the TOE to detect and act upon viruses discovered.

The Extended SFR claims in this section are based on the Anti-Virus (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.

Table 5-3 TOE Extended Security Functional Requirements for AV

Security Functional Requirement	Name
Extended Security Functional Requirements for the TOE	
FAV_ACT.1	Anti-Virus actions (EXT)
FAV_ALR.1	Anti-Virus Alerts (EXT)
FAV_SCN.1	Anti-Virus Scanning (EXT)

5.2.1 Anti-Virus component requirements (FAV)

Anti-Virus Actions (FAV_ACT.1, EXT)

FAV_ACT.1.1 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-Agent/Appliance basis and consist of:

a) Clean the virus from the file,

b) Quarantine the file,

c) Delete the file

d) [selection: [assignment: *list of other actions*], *no other actions*].

Anti-Virus Alerts (FAV_ALR.1, EXT)

FAV_ALR.1.1 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 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when a virus is detected.

Anti-Virus Scanning (FAV_SCN.1, EXT)

FAV_SCN.1.1 The TSF shall perform real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures.

FAV_SCN.1.2 The TSF shall perform scheduled scans at the time and frequency configured by the authorized administrator.

5.3 Extended Security Functional Components for AC

This section defines extended security functionality for Application Control provided by Deep Security.

The functionality in this extended class addresses the requirements provided by the Deep Security Agent component of the TOE to detect software application changes and allow or block execution.

Table 5-4 TOE Extended Security Functional Requirements for AC

Security Functional Requirement	Name
Extended Security Functional Requirements for the TOE	
FAC_ACT.1	Application Control Actions (EXT)
FAC_ALR.1	Application Control Alerts (EXT)
FAC_SCN.1	Application Control Scanning (EXT)

5.3.1 Application Control component requirements (FAC)

Application Control Actions (FAC_ACT.1, EXT)

FAC_ACT.1.1 Upon detection of an attempt to execute a runnable software file, the TSF shall perform the actions specified by the authorized administrator. Actions are administratively configurable on a per-Agent basis and consist of:

a) Allow execution the file,

b) Block execution of the file,

c) [selection: [assignment: *list of other actions*], *no other actions*].

Application Control Alerts (FAC_ALR.1, EXT)

FAC_ALR.1.1 The System shall be able to collect an audit event from a computer detecting a change to runnable software files. The event shall identify the computer originating the audit event and the software change that was detected

FAC_ALR.1.2 The System shall be able to collect an audit event from a computer indicating an attempt to run an unrecognized software file. The event shall identify the computer originating the audit event, and the action taken by the TOE.

FAC_ALR.1.3 The System shall take [assignment: *appropriate actions*] when an unrecognized file execution is attempted.

Application Control Scanning (FAC_SCN.1, EXT)

FAC_SCN.1.1 The TSF shall perform real-time scans for runnable software file changes.

FAC_SCN.1.2 The TSF shall perform real-time scans for attempts to execute runnable software.

5.4 Extended Security Requirements Rationale

5.4.1 Extended Security Functional Requirements Rationale

The family of IDS requirements was created to specifically address the data collected and analyzed by an Intrusion Defense System. It addresses the functionality provided by the Deep Security system to detect, analyse and react to possible intrusions on computers protected by Deep Security Agents or Deep Security Virtual Appliances, 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.

The extended class of FAV requirements was created specifically address Deep Security's anti-virus functionality to detect, analyze and react to possible malware detected on computers protected by the Deep Security Agents or Deep Security Virtual Appliances.

The extended class of FAC requirements was created specifically address Deep Security's application control functionality to detect, analyze and react to unknown and potentially malicious executable files detected on computers protected by the Deep Security Agents.

Since the Anti-Virus functionality and Application Control functionality are completely integrated with the Deep Security IDS system for Data Collection and Alerts, there is some overlap of FAV and FAC functionality with the IDS_SDC.1 and IDS_RCT.1 described in Section 6. Anti-Virus and Application Control 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.

6 Security Requirements

6.1 Conventions

The CC defines four operations on security functional requirements. The following conventions are used in this ST:

- Assignments are indicated by underlined text.
- Selections are indicated by *italic text*.
  - Assignments within a selection are indicated by *italicized and underlined text*.
- Refinement are indicated by **bold text** for additions and ~~**strike-through bold text**~~ for deletions.
- Iterations are indicated with a typical CC requirement naming followed by a lower case letter.

Other sections use bolding to highlight text of special interest.

6.2 Security Functional Requirements

Table 6-1 TOE Security Functional Requirements

Security Functional Requirement	Name
Security Functional Requirements for the TOE	
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
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection

Security Functional Requirement	Name
FCS_COP.1	Cryptographic Operation
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
FAV_ACT.1	Anti-Virus actions
FAV_ALR.1	Anti-Virus Alerts
FAV_SCN.1	Anti-Virus Scanning
FAC_ACT.1	Application Control actions
FAC_ALR.1	Application Control Alerts
FAC_SCN.1	Application Control Scanning
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted Path

6.2.1 Security audit (FAU)

Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) Access to the System and access to the TOE and System data.

Application Note: The auditable events in b) above are described in Table 6-2. The System Data in c) above is defined as TSF configuration data as well as events collected by the IDS system, the Anti-Virus system and the Application Control system.

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	Object IDs, Requested access
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 behaviour 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
FMT_SMF.1	Use of the management functions	Where modified: data storage parameters, user identification and authentication attributes, user role attributes

Application Note 1: The IDS_SDC and IDS_ANL requirements in this ST address the recording of results from IDS scanning, sensing, and analysing tasks (i.e. System data). The FAV_ALR requirement in this ST addresses the recording of results from Anti-Virus scanning and analyzing tasks (i.e. System data), and the FAC_ALR requirement in this ST addresses the recording of results from Application Control scanning and analyzing tasks (i.e. System data).

Application Note 2: For authenticated /api requests the API key name is treated as a User identity in the same way as administrator account names.

FAU_GEN.1.2

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

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

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

Audit review (FAU_SAR.1)

FAU_SAR.1.1

The TSF shall provide authorized administrators with the capability to read audit information which they have been granted access to from the audit records.

FAU_SAR.1.2

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

Application Note: Administrators with the default configuration roles named "Full Access" and "Auditor" are granted access to all TOE audit records.

Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1

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

Selectable audit review (FAU_SAR.3)

FAU_SAR.1.3

The TSF shall provide the ability to perform sorting of audit data based on date and time, type of event, event ID, event name, target system identity and event originator.

Selective audit (FAU_SEL.1)

FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) *event type;*

b) no other attributes.

Guarantees of audit data availability (FAU_STG.2)

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2

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

FAU_STG.2.3

The TSF shall ensure that the previously recorded stored audit records will be maintained when the following conditions occur: *failure and attack*.

Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1

The TSF shall *prevent auditable events from being sent to the database and store auditable events in temporary disk space* and send an alarm if the audit trail is full.

Application Note: When database space is made available, the events can be written to the database.

6.2.2 Identification and authentication (FIA)

User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

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

a) User identity;

b) Authentication data; and,

c) Authorisations.

Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1

The TSF shall allow limited actions (see Table 6-3) on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

Timing of identification (FIA_UID.1)

FIA_UID.1.1

The TSF shall allow limited actions (see Table 6-3) on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

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

Application Note: Authentication services such as SAML and MFA are outside the scope of the evaluation.

Table 6-3 URLs Accessible Without Authentication/Identification

URL	Description
/SignIn.screen	The Authentication Page
/Error.screen	The Error Screen

URL	Description
/index.jsp	The welcome page that redirects to SignIn.screen
*.gif, *.jpg, *.png, *.ico, *.css, *.js, *.xsd, *.html	Non-secure web application resources
*.csa, *.jsa	Compressed/Pre-build non-secure resources
/vib/*	VIB Files
/rest/apiVersion	Legacy REST API version number

6.2.3 Security management (FMT)

Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1

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

Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1

The TSF shall restrict the ability to *query* the audit data and all other TOE data to the Auditor role and Full Access Role, and shall restrict the ability to *modify* the System and audit data and all other TOE data to the Full Access role.

Application Note: "Audit data" refers to auditable events generated in the FAU_GEN requirement of this ST. "System data" refers to TSF configuration data and to events collected by the IDS_SDC, IDS_ANL, FAV_ALR and FAC_ALR requirements

Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: (audit) data storage parameters, user identification and authentication attributes, user role attributes.

Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the roles Full Access and Auditor.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Application Note: The TOE only allows management functions to be performed through Deep Security Manager during its operation, hence the "authorized administrator", "authorized System administrator" roles listed in this SFR are equivalent with regard to the TOE, and in the default configuration this role is named "Full Access" by the TOE.

6.2.4 Protection of the TOE Security Functions (FPT)

Basic internal TSF data transfer protection (FPT_ITT.1)

FMT_ITT.1.1

The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.

6.2.5 Cryptographic support (FCS)

Application Note: FCS_CKM functions are not listed as dependencies, following the guidance of CCS Instruction Number 4, version 2.0.

Cryptographic operation (FCS_COP.1)

FCS_COP.1.1

The TSF shall perform the cryptographic operations listed in the Cryptographic Operations column of Table 6-4 in accordance with a specified cryptographic algorithm the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 6-4 and cryptographic key sizes the cryptographic key sizes listed in the Key Sizes (bits) column of Table 6-4 that meet the following: the list of standards in the Standards column of Table 6-4.

Table 6-4 Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Size (bits)	Modes	Standard
Symmetric encryption and decryption	AES	128, 256	CBC, GCM	FIPS 197 "Advanced Encryption Standard (AES)"
Message digest, cryptographic hashing	SHA	256, 384, 512	SHA-256, SHA-384, SHA-512	FIPS 180-4 "Secure Hash Standard"
Signature verification, signature generation, and key generation	RSA, DSA	1024, 2048, 3072, 4096	RSA	FIPS 186-4 "Digital Signature Standard (DSS)"

Signature generation, key pair generation, signature verification, public key validation	ECDSA, ECDH	P-224, P-256, P-384, P-521	ECDHE, ECDSA	FIPS 186-4 “Digital Signature Standard (DSS)”
Keyed-hash	HMAC	256	HMAC-SHA-256	FIPS 198-1 “The Keyed-Hash Message Authentication Code”

Application Note: The certificates listed in table 6-4 depend on the Administrator enabling Deep Security in "FIPS Mode" as per the instructions given in the user guidance. When FIPS mode is configured, the software implements TLS 1.2 and uses only the underlying cryptographic modules provided by SafeLogic for this functionality. The list of CAVP certificates can be found in table 7-2.

6.2.6 IDS component requirements (IDS)

System Data Collection (IDS_SDC.1, EXT)

IDS_SDC.1.1

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

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

b) no other events.

IDS_SDC.1.2

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; and

b) The additional information specified in the *Details* column of Table 6-5 IDS Events.

Table 6-5 IDS Events

Component	Event	Details
IDS_SDC.1	Start-up, shutdown and host system reboot	None *[See Application Note2 below]*
IDS_SDC.1	Start-up and shutdown of audit functions	None
IDS_SDC.1	Detected malicious code	Location, identification of code

Component	Event	Details
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability
IDS_SDC.1	Detected attempt to run unrecognized software	Location, identification of software

Application Note: Note that while the IDS_SDC.1 requirement 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.

Application Note2: Deep Security has no control when its services are forced to shut down due to an Operating System shutdown, and in that situation the shutdown event may not be recorded. On Operating systems that permit the graceful shutdown of Deep Security services the shutdown events will be recorded by Deep Security.

Application Note3: Note that the DSVA is expected to run all the time. There is no graceful shutdown of the DSVA as such, the administrator should always investigate the cause if DSVA appears to be offline for no apparent reason.

Analyzer analysis (IDS_ANL.1, EXT)

IDS_ANL.1.1a

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

a) signature*;* and

b) no other functions.

IDS_ANL.1.1b

The System shall perform the following analysis function(s) on URLs requested:

a) Monitor requested URLs (web reputation)

IDS_ANL.1.2

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; and

b) action taken, Data destination.

Analyzer react (IDS_RCT.1, EXT)

IDS_RCT.1.1

The System shall send an alarm to the authorized administrator and record the attempt as system data record and (if configured to do so) terminate the attempt when an intrusion is detected.

Restricted Data Review (IDS_RDR.1, EXT)

IDS_RDR.1.1

The System shall provide users assigned the Full Access and auditor roles with the capability to read all data from the System data.

IDS_RDR.1.2

The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3

The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access

Application Note: Users with the default configuration "Full Access" or "Auditor" roles have the capability to read all System Data and Audit Data. The TOE allows other roles to be defined (by authorized administrators with sufficient privileges) that restrict the review to a sub-set of the System data.

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

IDS_STG.1.1

The System shall protect the stored System data from unauthorized deletion

IDS_STG.1.2

The System shall protect the stored System data from modification.

IDS_STG.1.3

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

Prevention of System data loss (IDS_STG.2, EXT)

IDS_STG.2.1

The System shall *prevent System data from being sent to the database* and send an alarm if the storage capacity has been reached.

6.2.7 Anti-Virus component requirements (FAV)

Application Note: The FAV functionality is only available on computers that are protected by the Deep Security Agents or Virtual Appliance (DSVA) components.

Anti-Virus Actions (FAV_ACT.1, EXT)

FAV_ACT.1.1

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-Agent/DSVA basis and consist of:

a) Clean the virus from the file,

b) Quarantine the file,

c) Delete the file

d) *no other actions.*

Anti-Virus Alerts (FAV_ALR.1, EXT)

FAV_ALR.1.1

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

The System shall send an alarm to the authorized administrator and record the attempt as a system data record.

Table 6-6 FAV Events

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

Application Note: The anti-virus event data collection and administrator alarms are handled by the same mechanisms as the IDS system provided by the IDS_SDC, IDS_RCT and IDS_RDR requirements.

Anti-Virus Scanning (FAV_SCN.1, EXT)

FAV_SCN.1.1

The System shall perform real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures.

FAV_SCN.1.2

The System shall perform scheduled scans at the time and frequency configured by the authorized administrator.

6.2.8 Application Control component requirements (FAC)

Application Note: The FAC functionality is available on computers that are protected by the Deep Security Agent component and not on computers only protected by the Deep Security Virtual Appliance.

Application Control Actions (FAC_ACT.1, EXT)

FAV_ACT.1.1

Upon detection of an attempt to execute a runnable software file, the TSF shall perform the actions specified by the authorized administrator. Actions are administratively configurable on a per-Agent basis and consist of:

a) Allow execution the file,

b) Block execution of the file,

c) *no other actions.*

Application Control Alerts (FAC_ALR.1, EXT)

FAC_ALR.1.1

The System shall be able to collect an audit event from a computer detecting a change to runnable software files. The event shall identify the computer originating the audit event and the software change that was detected.

FAC_ALR.1.2

The System shall be able to collect an audit event from a computer indicating an attempt to run an unrecognized software file. The event shall identify the computer originating the audit event, and the action taken by the TOE.

FAC_ALR.1.3

The System shall record the attempt as system data record when an unrecognized file execution is attempted.

Application Control and Integrity Monitoring (FAC_SCN.1, EXT)

FAC_SCN.1.1

The TSF shall perform real-time scans for runnable software file changes.

FAC_SCN.1.2

The TSF shall perform real-time scans for attempts to execute runnable software.

Table 6-7 FAC Events

Component	Event	Details
FAC_ACT.1	Action taken in response to detection of an attempt to execute an unrecognized runnable file	Action taken, file or process identifier

Application Note: The application control event data collection and administrator alarms are handled by the same mechanisms as the IDS system provided by the IDS_SDC, IDS_RCT and IDS_RDR requirements.

6.2.9 Trusted path/channels (FTP)

Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1

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

FTP_ITC.1.2

The TSF shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for communication with the database.

Trusted path (FTP_TRP.1)

FTP_TRP.1.1

The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification and disclosure*.

FTP_TRP.1.2

The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for *remote administration using the web interface*.

6.3 Security Assurance Requirements

This product claims CC Version 3.1.5 Part 3 conformant and claims Evaluation Assurance Level 2 augmented with ALC_FLR.1 (EAL2+). The security assurance requirements are listed in Table 6-8.

Table 6-8 Security Assurance Requirements

Assurance component ID	Assurance component name
ADV_ARC.1	Security Architecture Description
ADV_FSP.2	Security-enforcing Functional Specification
ADV_TDS.1	Basic Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery Procedures
ALC_FLR.1	Basic Flaw Remediation
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.2	Vulnerability analysis

6.4 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.

6.4.1 Rationale for TOE Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the ST. Table 6-9 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 6-9a Security Environment vs. Objectives: TOE

	Objectives	TOE														
Threats, OS		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.VIRUS	O.APP_CONTROL	O.AUDIT_SORT	O.AUDIT_PROTECTION
Threats	T.COMINT	X						X	X			X					
	T.COMDIS	X						X	X				X				
	T.LOSSOF	X						X	X			X					
	T.NOHALT		X	X	X			X	X								
	T.PRIVIL	X						X	X								
	T.IMPCON						X	X	X								
	T.INFLUX									X							
	T.FACCNT										X						
	T.SCNCFG		X														
	T.SCNMLC		X											X	X		
	T.SCNVUL		X														
	T.FALACT					X											
	T.FALREC				X												
	T.FALASC				X												
	T.MISUSE			X							X			X	X		
	T.INADVE			X							X				X		
	T.MISACT			X							X			X	X		
OS	P.DETECT		X	X							X			X	X		

	P.ANALYZ				X											
	P.MANAGE	X					X	X	X							X	
	P.ACCESS	X						X	X								X
	P.ACCACT								X		X					X	
	P.INTGTY											X					
	P.PROTCT									X							

Table 6-9b Security Environment vs. Objectives: Environment

	Objectives	ENVIRONMENT					
Threats, Assumptions		OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME
Assumptions	A.ACCESS					X	
	A.DYNMIC				X	X	
	A.ASCOPE					X	
	A.PROTCT		X				
	A.LOCATE		X				
	A.MANAGE				X		
	A.NOEVIL	X	X	X			
	A.TRUST		X	X			
Threats	T.COMINT						
	T.COMDIS						
	T.LOSSOF						
	T.NOHALT						
	T.PRIVIL						
	T.IMPCON	X					

	T.INFLUX						
	T.FACCNT						
	T.SCNCFG						
	T.SCNMLC						
	T.SCNVUL						
	T.FALACT						
	T.FALREC						
	T.FALASC						
	T.MISUSE						
	T.INADVE						
	T.MISACT						
OSPs	P.DETECT						X
	P.ANALYZ						
	P.MANAGE	X		X	X		
	P.ACCESS						
	P.ACCACT						X
	P.INTGTY						
	P.PROTCT		X				

Table 6-9c Objectives

Assumption / Threat ID	Description and Objectives
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.
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 be 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, wilfully 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.TRUST	The TOE can only be accessed by authorized users. 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 users 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.
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 users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self protection. The O.EXPORT objective ensures that the confidentiality of data will be maintained during communications.
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 users 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.
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 users 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 users 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 users to access TOE functions.
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	An unauthorized user may attempt to access TOE data or security functions which 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	An IT administrator may configure improper security configuration settings 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.

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, O.VIRUS and O.APP_CONTROL objectives counters this threat by requiring a TOE that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors that have not been remediated by the IT administrator. 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 vulnerability.
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.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.AUDITS, O.IDSENS, O.VIRUS and O.APP_CONTROL objectives address this threat by requiring a TOE that contains a Sensor, collect audit and Sensor data.

T.INADVE	A user of the IT System that the TOE monitors may cause inadvertent activity and access to the System The O.AUDITS, O.IDSENS and O.APP_CONTROL objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor 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, O.IDSENS, O.VIRUS and O.APP_CONTROL objectives address this threat by requiring a TOE that contains a Sensor, collect audit and Sensor 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, O.IDSCAN, O.VIRUS and O.APP_CONTROL objectives address this policy by requiring collection of audit, Sensor, and Scanner data. OE.TIME supports this policy by providing the audit functions with reliable time stamps.
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 Sensors and Scanners.

P.MANAGE	The TOE shall only be managed by authorized users. 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 users 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. The O.AUDIT_SORT objective provides the ability for authorized users to sort audit data to improve effective and appropriate management response to different types of system events.
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 users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection. The O.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 time stamps. O.AUDIT_SORT supports this objective by providing the ability to sort audit records by user identification.
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 assists this policy by requiring the TOE handle disruptions of TOE data storage. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

6.4.2 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.

In particular, the environment contains a Database, which should be managed according to best practices for database security in a production environment.

6.4.3 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 6-10 Requirements vs. Objectives Mapping

	Objectives	TOE														
Requirements		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.VIRUS	O.APP_CONTROL	O.AUDIT_SORT	O.AUDIT_PROTECTION
	FAU_GEN.1										X						
	FAU_SAR.1						X										
	FAU_SAR.2							X	X								
	FAU_SAR.3						X									X	
	FAU_SEL.1						X				X						
	FAU_STG.2	X						X	X	X		X					X
	FAU_STG.4									X	X						X
	FIA_UAU.1							X	X								
	FIA_ATD.1								X								
	FIA_UID.1							X	X								
	FMT_MOF.1	X						X	X								
	FMT_MTD.1	X						X	X			X					
	FMT_SMR.1								X								
	FMT_SMF.1						X										
	FPT_ITT.1											X	X				
	FCS_COP.1	X										X	X				
	IDS_SDC.1		X	X													

	IDS_ANL.1				X											
	IDS_RCT.1					X										
	IDS_RDR.1						X	X	X							
	IDS_STG.1	X						X	X	X		X				X
	IDS_STG.2									X						X
	FTP_ITC.1											X	X			
	FTP_TRP.1											X	X			
	FAV_ACT_(EXT).1													X		
	FAV_ALR_(EXT).1													X		
	FAV_SCN_(EXT).1													X		
	FAC_ACT_(EXT).1														X	
	FAC_ALR_(EXT).1														X	
	FAC_SCN_(EXT).1														X	

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. The System is required to protect the System data from any modification and unauthorized deletion [FCS_COP.1], and 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 users 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].

O.IDSCAN	The Scanner 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 Scanner 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].
O.IDSENS	The Sensor 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 Sensor 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 Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). The Analyzer 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]. TOE must also provide management functions to administrative users [FMT_SMF.1].

O.ACCESS	The TOE must allow authorized users to access only appropriate 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 [IDS_STG.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 behaviour of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.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 behaviour of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

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].
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]. The TOE must protect the system data's confidentiality and ensure its integrity when the data is transmitted between different parts of the TOE [FPT_ITT.1, FCS_COP.1]. The TOE must protect the system data's confidentiality and ensure its integrity when the data is transmitted between trusted Inter-TSF channel and trusted paths [FTP_ITC.1, FTP_TRP.1] to external components.

O.EXPORT	When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data. The TOE must protect the system data's confidentiality and ensure its integrity when the data is transmitted between different parts of the TOE [FPT_ITT.1, FCS_COP.1]. The TOE must protect the system data's confidentiality and ensure its integrity when the data is transmitted between trusted Inter-TSF channel and trusted paths [FTP_ITC.1, FTP_TRP.1] to external components.
O.VIRUS	The TOE will detect and take action against known viruses introduced to the protected computer via network traffic or removable media. The anti-virus Scanner and Sensor collect and store information and passes the data to the analyzer which performs an analysis to identify possible viruses [FAV_SCN.1]. The System takes action to quarantine or remove viruses [FAV_ACT.1], and alert the authorised users [FAV_ALR.1].
O.APP_CONTROL	The TOE will detect and take action against known and unknown executable software files introduced to the protected computer. The application control Scanner and Sensor collect and store information and passes the data to the analyzer which performs an analysis to identify possible unwanted applications [FAC_SCN.1]. The System takes action to block or allow software execution [FAC_ACT.1], and alert the authorised users [FAC_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 System audit trail to include sorting the audit data [FAU_SAR.3].
O.AUDIT_PROTECTION	The TOE uses the capabilities of the IT environment 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].

6.4.4 Explicitly Stated Requirements Rationale

The claimed extended Intrusion Defense System functionality creates a family of IDS requirements to specifically address the data collected and analyzed by an 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.

The explicitly stated Extended (FAV) SFRs in Section 5 are additional requirements created to specifically address Anti-Virus protection for viruses that do not enter via network traffic and therefore may not be detectable by the IDS system. However, this family of requirements uses the same IDS functionality to provide the requirements for collecting, reviewing and managing the data.

The explicitly stated Extended (FAC) SFRs in Section 5 are additional requirements created to specifically address Application Control protection for runnable software applications that are located on the target computer and not detectable by the IDS system. However, this family of requirements uses the same IDS functionality to provide the requirements for collecting, reviewing and managing the data.

6.4.5 Security Functional Requirements Dependency Rationale

The SFRs in Section 6 do satisfy all the requirement dependencies of the Common Criteria. Table 6-11 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 6-11 Requirement Dependencies Rationale

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	Yes, satisfied by operational environment (OE.TIME)
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes

SFR ID	Dependencies	Dependency Met
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes, met by FAU_STG.2 as FAU_STG.2 is hierarchical to FAU_STG.1
FIA_UAU.1	FIA_UID.1	Yes
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	Yes
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	Yes
FMT_SMR.1	FIA_UID.1	Yes
FCS_COP.1	FCS_CKM.1 and FCS_CKM.4	N/A, FCS_CKM functions are not included, following the guidance of CCS Instruction #4, version 2.0.
FTP_ITC.1	None	N/A
FTP_TRP.1	None	N/A

6.4.6 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 6-12 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 authorised 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 “Full Access” role the right to perform security functions that add system and audit data. SF.RBAC assigns users with “Full Access” role the right to perform all security functions that modify TOE data. SF.RBAC allows Auditor only read access to all information.
	FMT_SMR.1	Full Access and Auditor are the default roles supported by SF.RBAC.
	FMT_SMF.1	SF.RBAC provides management functions to administrators.

IT Security Functions	SFRs	Rationale
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.SECCOM	FPT_ITT.1	SF.SECCOM secures the internal communication using symmetric encryption.
	FTP_ITC.1	SF.SECCOM secures communication between DSM and the database.
	FTP_TRP.1	SF.SECCOM secures communication between DSM and a remote administrator's web browser.
	FCS_COP.1	CAVP-validated cryptographic algorithms are used.
SF.IDPS	IDS_SDC.1	SF.IDPS supports the generation of audit records in accordance with Table 6-5.
	IDS_ANL.1	SF.IDPS performs analysis of network traffic based on signature of the network traffic.
	IDS_RCT.1	Upon discovery of attacks, SF.IDPS sends email alarms to the appropriate administrator and prevents the attack.
	IDS_RDR.1	SF.IDPS allows authorised 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	

IT Security Functions	SFRs	Rationale
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
	FAV_SCN.1	SF.AV performs real time scans for viruses
SF.AC	FAC_ACT.1	SF.AC performs an analysis of runnable software file changes, and upon attempt to execute unrecognized software, acts to block potential unwanted execution of the file.
	FAC_ALR.1	SF.AV performs an analysis of application control data, and upon blocking an unrecognized executable, sends email alarms to the appropriate administrator
	FAC_SCN.1	SF.AV performs real time scans for changes to runnable software files

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.SECCOM (secure intra-TOE communication)
- SF.IDPS (Intrusion detection and prevention)
- SF.AV (Anti-Virus)
- SF.AC (Application Control)

7.1.1 SF.AUDIT

Deep Security 20 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 Security Manager. 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 audit records generated 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. An authorized TOE administrator with the appropriate roles assigned has the capability of selecting the system events to be recorded based on Event Type.

When the capacity of the database has been reached, an emergency email is sent to a pre-selected administrator alerting them of the situation. The TOE will prevent TOE users from starting new user sessions with the TOE. For existing live user sessions, any attempts at modifying the TOE data will be prevented.

Authorized TOE administrators can only read audit records through the TOE's administrative interface and their access rights to the audit records is restricted based on their role definition. No administrator is given write access to the audit records. The SF.AUDIT audit logs are all classified as "system events" at the administrative interface. The Authorized TOE administrators are given the capability of sorting the system events to be displayed based on Event Date and Time, Event Type, Event ID/Name, Target System, or User ID of who performed the Action.

7.1.2 SF.RBAC

Deep Security 20 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.

By default, two predefined roles are available upon successful installation of Deep Security Manager. And these are "Full Access" and "Auditor". Users assigned the "Full Access" role have access to all the system functions, including the capability of defining new roles that grant the ability to query and modify a sub-set of System data, and assigning users to these roles. *Application Note: authorized administrators with "Full Access" role can add system data by changing the configuration.*

Users of the "Auditor" role are only allowed read access to all data/configuration. Deep Security 20 provides management functions to administrative users.

7.1.3 SF.I&A

The identification and authentication mechanism used by Deep Security 20 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 browser based interface and these are verified by the TOE. Identification is performed by finding the matching administrator based on a case-insensitive match to the username. 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 should follow the best practices for password policy as outlined in the Deep Security 20 Common Criteria Configuration Guide.

7.1.4 SF.SECCOM

All communications between the Deep Security Agents/Virtual Appliances and the Deep Security Manager are protected from disclosure or modification. This is achieved by deploying symmetric encryption algorithms for protection of the communication channel.

As part of TLS 1.2 communication, a symmetric encryption key is exchanged between DSM and DSA via RSA asymmetric encryption. Furthermore SHA is employed for a variety of purposes including integrity checks, and digests.

Communications between the DSM and the database is protected using TLS 1.2.

Communication between a remote administrator's web browser and DSM is protected using TLS 1.2.

The Deep Security Manager CA private key is generated at install time using the java crypto provider. This CA is then used to generate certificates for Deep Security Agents during activation of Agents.

TLS communication is secured by importing the customer certificate and private key into the DSM java key store.

The following table lists the cipher suites in use for TLS 1.2 communications.

Table 7-1 Cryptographic Protocols

Communication direction	Supported TLS 1.2 cipher suites in FIPS mode
Server	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Client	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

The following table lists the CAVP certificates for each Deep Security software component. The certificates listed here depend on the Administrator enabling Deep Security in "FIPS Mode" as per the instructions given in the user guidance. When FIPS mode is configured, the software uses only the underlying cryptographic modules provided by SafeLogic for this functionality: The DSM uses TrendMicro Java Cryptographic Module Engine. The DSA on Windows uses TrendMicro Cryptographic Module Engine. The DSA on RHEL and DSVA use CryptoComply Server Engine.

Please refer to Section 6.2.5, Table 6-4 for listing of the algorithm functionality and key sizes.

Table 7-2 CAVP Certificates

Deep Security Component	Cryptographic Algorithm	Ciphersuites	CAVP #
DSM	AES	AES-CBC	AES A1983
	SHA	SHA2-256, SHA2-384, SHA2-512	SHA A1983
	RSA	RSA KeyGen, RSA SigGen	RSA A1983
DSA (RedHat 7)	AES	AES-CBC AES-GCM	AES 5650
	SHA	SHA2-256, SHA2-384, SHA2-512	SHS 4531
	RSA	RSA SigGen, RSA SigVer	RSA 3040
	ECDSA	ECDSA KeyGen, ECDSA KeyVer, ECDSA SigGen, ECDSA SIgVer	ECDSA 1524
	HMAC	HMAC-SHA2-256	HMAC 3764
DSVA (CentOS 7)	AES	AES-CBC, AES-CGM	AES 4750
	SHA	SHA2-256, SHA2-384, SHA2-512	SHA 3893
	RSA	RSA SigGen, RSA SigVer	RSA 2594
	ECDSA	ECDSA KeyGen, ECDSA KeyVer, ECDSA SigGen, ECDSA SIgVer	ECDSA 1185
	HMAC	HMAC-SHA2-256	HMAC 3164
DSA (Windows)	AES	AES-CBC AES-GCM	AES A1987
	SHA	SHA2-256, SHA2-384, SHA2-512	SHA A1987
	RSA	RSA SigGen, RSA SigVer	RSA A1987
	ECDSA	ECDSA KeyGen, ECDSA KeyVer, ECDSA SigGen, ECDSA SIgVer	ECDSA A1987
	HMAC	HMAC-SHA2-256	HMAC A1987

7.1.5 SF.IDPS

The TOE provides intrusion detection and prevention functions. Data is first collected, analyzed and stored by Deep Security Agents/Virtual Appliances and is then passed to the Deep Security Manager for consolidated review and storage.

If Deep Security Manager reaches its storage capacity, event data will no longer be collected from Deep Security Agents/Virtual Appliances until space is made available at the Deep Security Manager. If Deep Security Agents/Virtual Appliances reach their log storage capacity they will immediately communicate with Deep Security Manager. Deep Security Manager will raise an Alert and send an Email notification regarding the Agent's lack of storage space to the administrators with a valid email address who have elected to receive notifications and have the view rights to the host.

Deep Security Agents sit directly on a host, and defend it by monitoring incoming and outgoing network traffic for protocol deviations or contents that might signal an attack. Authorized administrative Users of the TOE configure the Agents or Virtual Agents (protecting VMs inside the appliance) through

functionalities offered by the Deep Security Manager. All IDS rules are configurable through Policies and deployed to all Agents and DSVA installations used for agentless protection. Rules are defined for each individual Agent/Virtual Agent or a group of Agents/Virtual Agents as a whole to manage their actions. The Deep Security Manager is populated with commonly used rules, targeted at known vulnerabilities for each type of hosts. These rule configurations can be categorized into Anti-Malware Configurations, Web Reputation Configurations, Firewall Rules, Application Control Rules, Intrusion Prevention Rules, Integrity Monitoring Rules and Log Inspection Rules. Anti-malware rules define the policy for anti-malware real-time and scheduled scans. Web Reputation configurations determine if Web Reputation functionality is on or off and allow specification of additional URLs to allow or block. Firewall Rules examine the control information of network packets, and determine if a network connection should be allowed. Application Control rules determines if an application should be blocked or allowed. IDS/IPS Rules examine the actual content of a network packet or a sequence of packets performing deep packet inspection. Based on predefined Intrusion Prevention Rules, various actions are carried out by the Agents/Virtual Appliances on these packets: from replacing specifically defined or suspicious byte sequences, to completely dropping packets and resetting the connection. Integrity Monitoring rules define the content to be hashed and compared with future scans. Log Inspection Rules define the logs, decoding and parsing techniques for analyzing logs.

Deep Security Agents/Virtual Appliances generate log records in accordance with details as specified in Table 6-5, regarding their own startup and shut down, the network traffic and malicious codes or vulnerabilities detected, and pass these records to the Deep Security Manager for review, storage and reports generation. Within each record, event time, event type, action taken, data source and destination are recorded. Authorized administrators can use functionalities provided by the Deep Security Manager to control the behavior of the Deep Security Manager log collection process. This could be configured occur on demand or at regular intervals.

Deep Security Manager groups the information received from Deep Security Agents/Virtual Appliances into System, Anti-Malware, Web Reputation, Firewall, Application Control Intrusion Prevention, Integrity Monitoring and Log Inspection events based on their Event ID (type). Generally speaking, the records of Agents Start up and Shut downs are regarded as System Events; Information collected on detected known vulnerabilities are grouped into Firewall or Intrusion Prevention events and log data collected regarding the detection of Malicious codes are placed into the Intrusion Prevention events. System integrity changes are collected as Integrity events, and events generated by monitoring the Agent logs are collected as Log Inspection events. Anti-Malware detection, cleaning and quarantining events are collected as Anti-Malware events. Web Reputation URL blocking events are collected as Web Reputation Events.

Once collected by the Deep Security Manager, IDS System Data is stored securely in the audit database, which is protected in part by the hosting IT environment. Action in the event of storage exhaustion is the same as for Audit Events in FAU_STG.2 and FAU_STG.4: collection of System Data from the Agents/Virtual Appliances will be paused until database storage capacity is made available.

Before collection by the Deep Security Manager, IDS System Data is stored temporarily on the disk of host computers being protected by Deep Security Agents / Appliances. This data is protected in part by the hosting IT environment, and can only be deleted by an authorised user with administrative privileges on the host computer. If the temporary storage on the host computer becomes exhausted before the System Data can be collected by the Deep Security Manager, then the oldest events in the temporary storage will be overridden by newer events.

Deep Security Manager offers only pre-authorized administrators of appropriate roles with read access to these events logs. When a predefined event has been detected, email alarms are sent to pre-selected administrators.

7.1.6 SF.AV

The TOE provides anti-virus functions. Data is first collected, analyzed and stored by Deep Security Agents/Virtual Appliances and is then passed to the Deep Security Manager for consolidated review and storage.

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

Deep Security Agents sit directly on a computer, and defend it by monitoring files for viruses based on known signatures. Authorized administrative Users of the TOE configure the Appliances through functionalities offered by the Deep Security Manager. The Anti-Malware Policies contain rules for Real time monitoring, exclusions, actions to be taken, retrieving malicious files, etc. and these policies are deployed to all Agents and DSVA installations used for agentless protection.

Deep Security Virtual Appliances sit on an ESXi host and monitor one or more virtual machines for virus activity in the same way as an Agent, with the exception that files to monitor are passed to it by VMWare.

Deep Security Agents/Virtual Appliances generate Anti-Malware event records in accordance with details as specified in Table 6-6, regarding viruses detected, and pass these records to the Deep Security Manager for review, storage and reports generation. Within each record, event time, event type, action taken, and data source are recorded. Authorized administrators can use functionalities provided by the Deep Security Manager to control the behaviour of the Deep Security Manager log collection process. This could be configured occur on demand or at regular intervals.

Deep Security Manager groups the anti-virus information received from Deep Security Agents/Virtual Appliances into AV events based on their Event ID (type). Deep Security Manager offers only pre-authorized administrators of appropriate roles with read access to these events logs. When a predefined event has been detected, email alarms are sent to pre-selected administrator.

7.1.7 SF.AC

The TOE provides application control functions. Data is first collected, analyzed and stored by Deep Security Agents as part of the Integrity Monitoring capability described in SF.IDFS (above), and is then passed to the Deep Security Manager for consolidated review and storage.

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

Deep Security Agents sit directly on a computer, and defend it by scanning in real-time to monitor software files for changes based on the known signatures previously collected from a baseline inventory scan, determining whether the software is known or unrecognized and generating security events and storing the events on the Deep Security Manager.

Authorized administrative Users of the TOE configure the Agents through functionalities offered by the Deep Security Manager to set the allow or block rules and deploy these policies to the Agents.

Deep Security Agents monitor execution events in real time and block execution of unauthorized applications based on the defined rules and generate appropriate security events which are sent to the Deep Security Manager.

Deep Security Manager groups the application control information received from Deep Security Agents into AC events based on their Event ID (type). Deep Security Manager offers only pre-authorized administrators of appropriate roles with read access to these events logs.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.