Security Target

TRITON APX 8.2

Document Version 1.0

June 23, 2017

Prepared For:

Forcepoint, LLC.

10900 Stonelake Blvd, 3rd Floor,

Austin, TX 78759

www.forcepoint.com

Prepared By:

SafeLogic, Inc

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.safelogic.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the TRITON APX 8.2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the TRITON APX 8.2 developed by Forcepoint, and will hereafter be referred to as the TOE throughout this document. The TOE is a unified solution providing data protection. The TRITON APX provides an email gateway and web scanning services, as well as data loss prevention capabilities.

1.1 ST Reference

ST Title	Security Target: TRITON APX 8.2
ST Revision	1.0
ST Publication Date	June 23, 2017
Author	SafeLogic Inc.

1.2 TOE Reference

TOE Reference	TRITON APX 8.2 with Forcepoint Email Security and Forcepoint Web Security components running on Forcepoint V10000 Appliance.
TOE Type	Web proxy, email gateway and data loss prevention solution

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable.
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE

SECTION	TITLE	DESCRIPTION
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by [*italicized text within brackets*].
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by [<u>underlined text within brackets</u>].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration letter inside parenthesis, for example, FIA_UAU.1.1 (a) and FIA_UAU.1.1 (b) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the terms and acronyms used in this document:

TERM	DEFINITION
ACE	Advanced Classification Engine
CC	Common Criteria
CEM	Common Evaluation Methodology
CentOS	Community Enterprise Operating System
CLI	Command Line Interface
DLP	Data Loss Prevention
DICE	Data Identification and Classification Engine

TERM	DEFINITION
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
URL	Uniform Resource Locator
USB	Universal Serial Bus

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

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

TRITON APX 8.2 provides a data theft prevention solution to secure an organization's data on and off the organization network. The protection provided by TRITON APX solution is delivered by three main components, namely Forcepoint Web Security, Forcepoint DLP and Forcepoint Email Security, and supporting components Forcepoint DLP Endpoint and Network Agent. These components work together to prevent security breaches, productivity loss, and legal issues that might arise due to inappropriate or careless browsing, email messaging and network usage habits. The components are managed using the Forcepoint TRITON Manager.

The TRITON APX solution is highly scalable according to customer strategy to address data theft and data loss. The Forcepoint Web Security, Forcepoint DLP and Forcepoint Email Security can be deployed as individually to address specific customer needs for data theft and loss through specific organization network activities. These solutions can be physical on-premise installations, hybrid deployments or cloud-based deployments. The evaluated deployment of the TRITON APX consists of Forcepoint Web Security and Forcepoint Email Security components installed on a Forcepoint V10000 Web Gateway Appliance with the other TRITON APX components installed on customer-supplied on-premise platforms

Figure 1shows the details of the deployment configuration of the TOE:

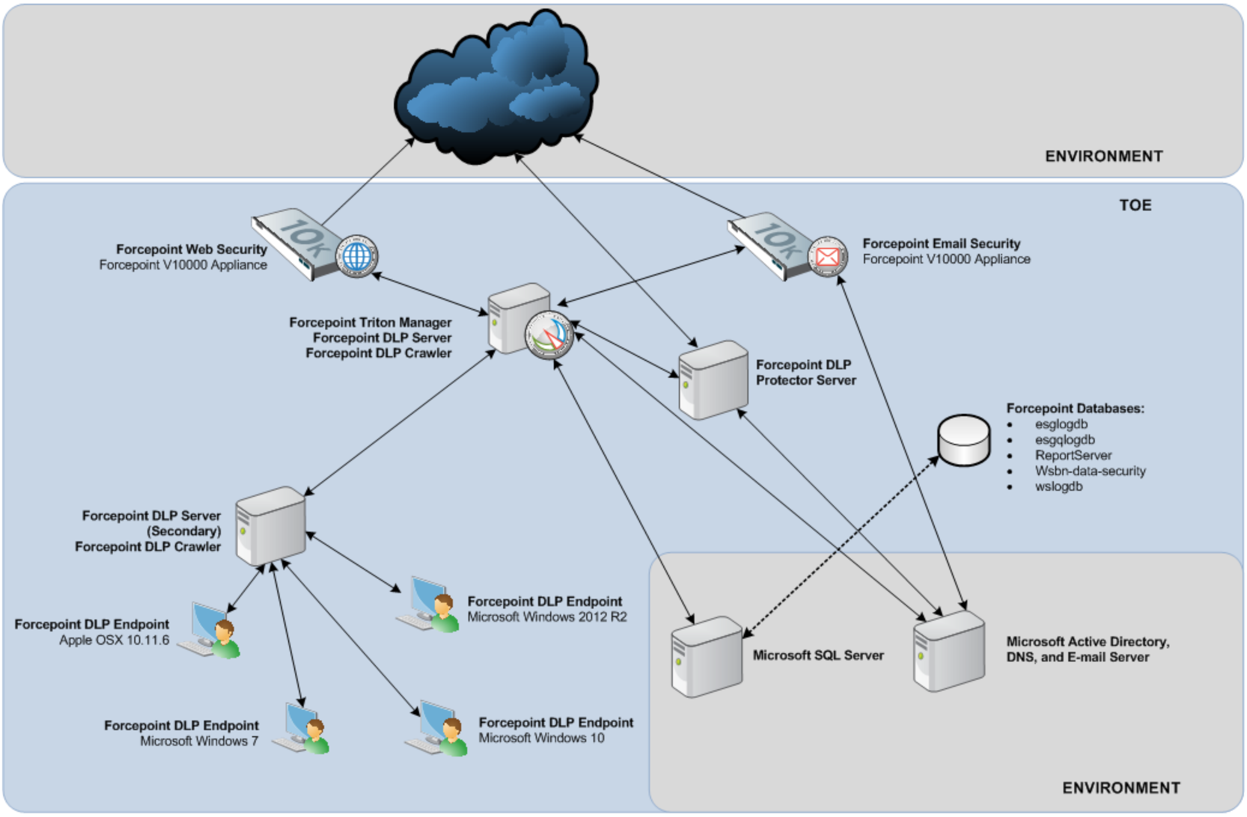

Figure 1 –Deployment of the TOE

1.6.1 Forcepoint Web Security

TRITON Forcepoint Web Security uses predictive analysis provided by the Forcepoint ACE (Advanced Classification Engine). Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executable, offering multiple layers of analysis to help prevent users from accessing unwanted web content. This is achieved through enforcement of filtering policies which specify:

- Category filters, used to apply actions (permit, block) to website categories
- Protocol filters, used to apply actions to Internet applications and non-HTTP protocols

In addition, the Content Gateway performs advanced analysis of web traffic as it flows through the on-premises proxy. Only sites that are not already blocked are further analyzed based on the active policy.

1.6.2 Forcepoint DLP

Data Loss Prevention (DLP) policies enable monitoring and control of the flow of sensitive data throughout an organization. Depending on the Forcepoint DLP configuration, policies can be set up to monitor and control information sent via email and over HTTP and HTTPS channels or emails sent to user’s mobile device and ensure all communications are in line with regulations and compliance laws as required. Also, detecting and remediating potential data theft flows over these channels.

Forcepoint DLP Gateway (appliance for Forcepoint DLP) is a component of Forcepoint DLP that can monitor and report on web traffic in the organization and act as an MTA to monitor, block, quarantine, and encrypt email traffic. The Forcepoint DLP server provides advanced analysis capabilities, while the Forcepoint DLP Gateway intercepts network traffic and either monitors or blocks it, depending on the channel (also referred to as Protector).

To identify data in the network that is to be controlled and protected, Forcepoint DLP Discover policies can be configured and the Crawler component of Forcepoint DLP Discover will perform network discovery tasks to identify and fingerprint the data.

1.6.3 Forcepoint Email Security

Forcepoint Email Security provides comprehensive on-premises email security hosted on a Forcepoint appliance. Each message is processed by a robust set of antivirus and antispam analytics to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

Filters and policies are used to govern analysis of user email messages. The filtering can be configured to provide connection level anti-spam functionality including analysis of IP reputation, RBL, RDNS, SPF, DKIM and DMARC

Three types of policies are available, depending on the direction of the email—inbound, outbound, or internal. Message direction is determined on the basis of an organization’s protected domains:

- Inbound - The sender address is not from a protected domain, and the recipient address is in a protected domain
- Outbound - The sender address is from a protected domain, and the recipient address is not in a protected domain
- Internal - Both the sender and recipient addresses are in a protected domain.

1.6.4 Forcepoint DLP Endpoint

Two Forcepoint endpoint solutions are available to provide both DLP and Web security functionality on the users’ workstations.

The DLP option is provided by the Forcepoint DLP Endpoint Client, which protects an organization from unintended loss of data and also potential data theft. The Forcepoint DLP Endpoint Client is used to extend the Forcepoint DLP functionality to channels that can only be intercepted on the endpoint and to provide coverage for machines when not connected to the domain network. This includes controls such as removable media, application copy-cut-paste, file access, screen capture, LAN, etc. The Forcepoint DLP Endpoint client also provides local Web and Email traffic analysis.

The Forcepoint Web security solution, which is excluded from the scope of the TOE, offers two endpoint Web Security protection options to defend against web threats:

- Forcepoint Web Endpoint
- Forcepoint Remote Filtering Client

1.6.5 Network Agent

The Network Agent is a component of the TRITON Appliance. It provides packet level monitoring of (mainly) non-HTTPS traffic, inspecting the application layer content. The Network Agent filtering is applied by the appliance, irrespective of whether the Forcepoint Email Security or Forcepoint Web Security components are installed on the appliance.

1.6.6 Forcepoint TRITON Manager

The Forcepoint TRITON Manager (also called the TRITON console) is the central configuration interface used to manage TRITON Web, Email, and Data solutions. This manager can be used to customize policies, generate reports, monitor the system, and manage configuration and settings. Administrators authenticate to the Forcepoint TRITON Manager, which provides single sign-on to all TRITON consoles.

1.6.7 TOE Environment

The server components of the TOE are intended to be deployed in a physically-secured cabinet room, room, or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). Access to the physical console or USB ports on the appliance and associated TOE servers should be restricted via a locked data cabinet within the data center. The TOE is intended to be managed by administrators operating under a consistent security policy. In addition, any authentication server used by the TOE (e.g. Active Directory server) should also be hosted within this secured environment. The TOE environment is responsible for providing protection of network communication between the TOE server components[1] and also between the TOE and the administrative user.

The TOE provides a layer of security between an internal and external network (such as between a Local Area Network (LAN) and the Internet). The TOE is meant to control, protect, and monitor the internal network's access to content on the external network. For this behavior to be properly implemented, all controlled protocol traffic must traverse the TOE. The TOE environment is required to provide the necessary configuration to allow this.

[1] Communication between the TOE Secondary AP-DATA Server component and the AP-ENDPOINT DLP client devices is protected by TOE mechanisms.

1.7 TOE Description

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

There are multiple deployments of TRITON APX, which can include various permutations of instances of Forcepoint Email Security, Forcepoint DLP and/or Forcepoint Web Security components using on-premise appliances, cloud services or hybrid deployments. The evaluated deployment supports the TRITON APX components installed on On-Premise equipment, as detailed below.

1.7.1 Physical Boundary

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is the TRITON APX 8.2 solution, including the Forcepoint V10000 G4 appliances on which the Forcepoint Web Security and Forcepoint Email Security components are installed.

The other TRITON APX v8.2 components run on Microsoft Windows Servers and Linux-based soft-appliance as depicted in Figure 2 below. The TRITON V10000 G4 appliance hardware is a standard Dell server running a customized version of the CentOS Linux operating system. The following essential software components in the evaluated configuration are:

- Forcepoint TRITON Manager Unified Installer v8.2.0 (“TRITON820Setup.exe”)
- Forcepoint TRITON Appliance Unified Installer v8.2.0 (“V10000-G4-RecoveryImage-820.iso”)
- Forcepoint DLP Protector software (“DataProtectorMobile82x.iso”)
- Forcepoint DLP Endpoint Package Builder (“AP-EndpointPackage82.zip”)

These comprise the following components:

- Forcepoint TRITON Manager 8.2.0.89
- Forcepoint Web Security 8.2.0.1264
- Forcepoint DLP 8.2.0.92
- Forcepoint Email Security 8.2.0.0101
- Forcepoint DLP Endpoint 8.2.0.2324 (Windows)
- Forcepoint DLP Endpoint 8.2.0.2323 (MacOS).

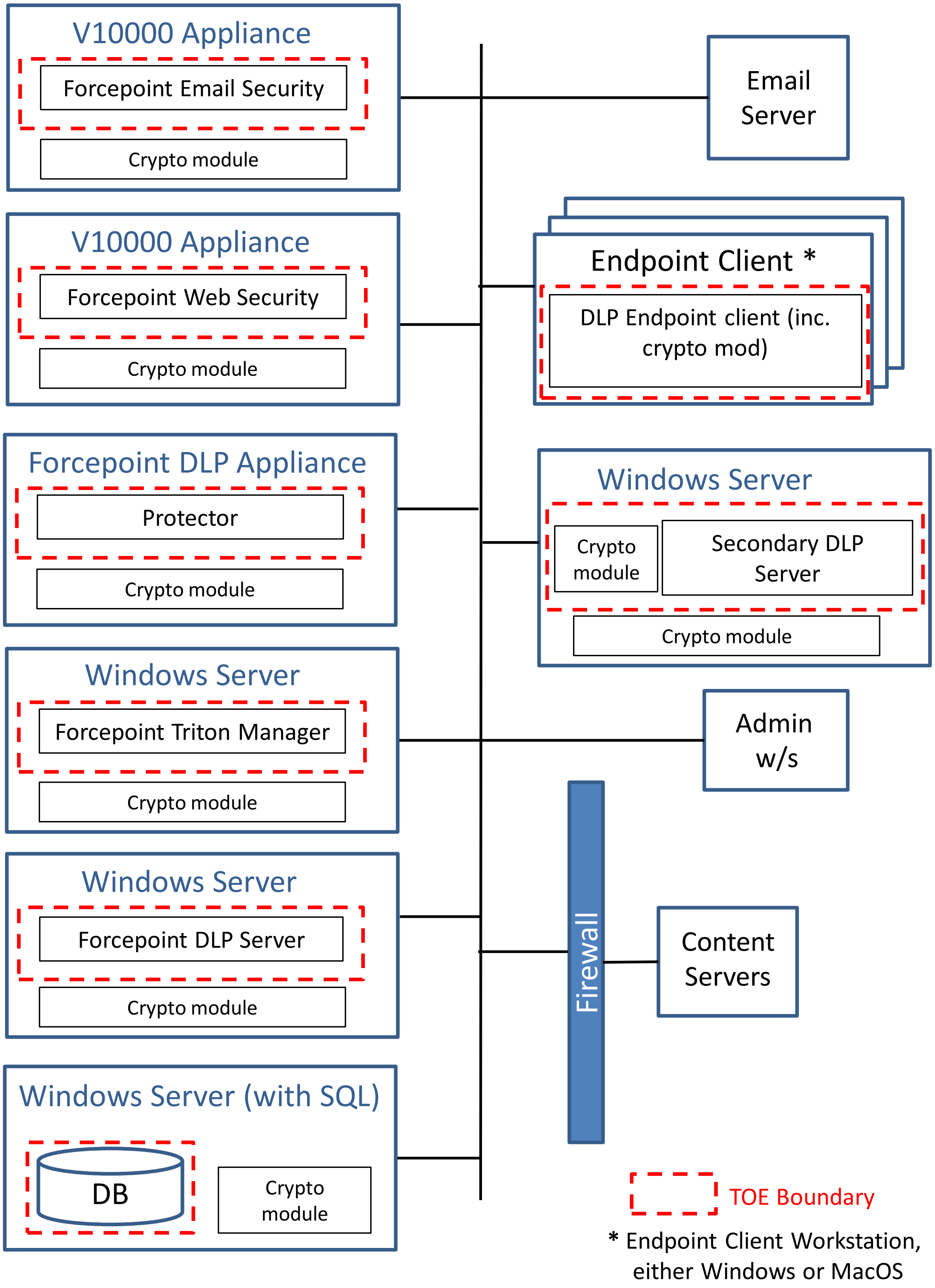

Figure 2 – Physical TOE Boundary

1.7.1.1 TOE Requirements

The TOE is a combination of the Forcepoint V10000 hardware appliance and the TRITON APX v8.2.0 software application suite that provides proxy filtering capabilities.

1.7.1.2 Guidance Documentation

The following guides are required reading and form part of the TOE:

- Installation Guide Forcepoint TRITON APX v8.2.x
- Installation Instructions TRITON AP-Web v8.2.x
- Installation Guide Forcepoint TRITON AP-Data Gateway and Discover v8.2.x
- Installing email protection appliance-based solutions, Email Protection Solutions, Version 8.2.x
- Installation and deployment guide Forcepoint Endpoint Solutions v8.2.x
- TRITON Manager Help Forcepoint TRITON Solutions v8.2.x
- Administrator Help Forcepoint TRITON AP-Web v8.2
- Administrator Help Forcepoint TRITON AP-Data Gateway and Discover v8.2
- Administrator Help Forcepoint TRITON AP-Email v8.2
- V-Series Appliance Manager Help TRITON AP-Web, TRITON AP-Email, Web Filter & Security, Models V10000, V5000. v8.2.x
- Content Gateway Manager Help Forcepoint Content Gateway, v8.2.x
- TRITON AP-Email Personal Email Manager User Help v8.2.x
- Quick Start Guide V10000 G2[2]
- TRITON APX 8.2Common Criteria Guidance Supplement, v1.0

1.7.2 Logical Boundary

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

- Security Audit,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TSF,
- Resource Utilization, and;
- TOE Access

1.7.2.1 Security Audit

The TOE generates audit logs of Forcepoint TRITON Manager activity; recording administrator login attempts, policy changes, and configuration changes in the Audit Logs for each component. Only Super Administrators and System Administrators can review the audit logs.

[2] This is equally applicable to the Forcepoint V10000 G4 appliance

The TOE provides reliable timestamps to accurately record the sequence of events within the audit records.

1.7.2.2 User Data Protection

The TOE enforces web, data and email filters and policies on user traffic (inbound and/or outbound) to prevents internal entities from accessing potentially harmful or inappropriate content on external data, prevent loss of organization data and prevent infected email from entering the network.

1.7.2.3 Identification and Authentication

The TOE enforces identification and authentication for administrators before they can access any management functionality via the CLI.

The TOE also prevents administrators from accessing Forcepoint TRITON Manager content before providing and authenticating a valid identity. The TOE maintains a list of security attributes (such as login credentials) for administrators.

Depending on the web policy applied, unprivileged users are able to browse the internet anonymously.

Email users have to identify and authenticate themselves before the TOE will permit access to their Personal Email Management UI to manage quarantined email messages.

1.7.2.4 Security Management

The TOE provides robust management interfaces that authorized administrators can use to manage the TOE and configure policies to control access to content. By default proxy filtering is enabled, but all traffic is allowed; therefore, the TOE has a permissive default posture.

The TOE defines two categories of administrator — TRITON Administrator and Delegated Administrator.

TRITON Administrator roles manage system-wide operations, such as setting domains, editing user profiles and permissions, and setting up routes and preferences across **all** Web, Email, and Data components. See Table 19 for further details on TRITON Administrator roles.

Delegated Administrators have custom permission sets defined by associating the Delegated Administrator with one or more roles (set of access privileges) across a **single** Email, Web and DLP component. For example, a Delegated Administrator can be granted “Super Administrator” role in the Web component to manage user profiles, permissions, profiles and settings, similar to a TRITON Administrator role, but limited to only the Web component.

There are eight other permission sets that can be applied to Delegated Administrator to manage one or more of the three components within TRITON Manager, as defined in Table 19.

1.7.2.5 Resource Utilization

The TOE enforces maximum limits on usage and availability of controlled traffic.

1.7.2.6 TOE Access

The TOE can assign a limit on the number of concurrent sessions that administrative users are allowed to have with Forcepoint TRITON Manager. If this limit is reached, the TOE prevents any new sessions from being created.

A TRITON console session ends 30 minutes after the last action taken in the user interface (clicking from page to page, entering information, caching changes, or saving changes). A warning message is displayed 5 minutes before session end.

1.7.3 Hardware and Software Supplied by the IT Environment

The TRITON Manager, Web Log Server and Email Log are not hosted on the Forcepoint appliance. These TOE components are installed on Microsoft Windows server (these components are installed on a single server in the evaluated deployment). The TRITON solution also requires a Microsoft SQL Server to host the Log Server Database (the Database and Forcepoint TRITON Manager must be hosted on separate servers).

In the evaluated deployment these components are all installed on Windows Servers, which meet the following requirements:

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR FORCEPOINT TRITON MANAGER
Processor	8 CPU cores (2.5 GHz)
Memory	24 GB RAM
Free Disk Space	550 GB
Operating System	Windows Server 2012 (Standard edition)
Additional Software	Microsoft SQL Server SQL Server 2012 SP2 (installed on a separate platform)

Table 3 - Minimum platform requirements for Forcepoint TRITON Manager (including Forcepoint DLP Forensics repository)

The Forcepoint TRITON Manager is accessed via a web browser on a management workstation using a standard web browser (such as Internet Explorer 11, Firefox 40).

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR MICROSOFT SQL SERVER
Processor	8 CPU cores (2.5 GHz)
Memory	16 GB RAM

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR MICROSOFT SQL SERVER
Free Disk Space	140 GB
Operating System	Windows Server 2012 (Standard edition) with NET Framework Version 3.5
Additional Software	Microsoft SQL Server SQL Server 2012 SP2

Table 4 - Minimum Platform Requirements for Microsoft SQL Server

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR FORCEPOINT DLP (DATA SECURITY) SERVERS (primary and secondary)
Processor	2 Quad-core (2.0 GHz)
Memory	8 GB RAM
Hard Drives	Four 146 GB (RAID 1 + 0)
Free Disk Space	70 GB
Network Interface Cards	2
Operating System	Windows Server 2012 (Standard edition)

Table 5 - Minimum Platform Requirements for Forcepoint DLP Servers

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR FORCEPOINT DLP APPLIANCE (PROTECTOR)
Processor	2 Quad-core (2.0 GHz)
Memory	4 GB RAM
Hard Drives	Four 146 GB (RAID 1 + 0)
Network Interface Cards	2

Table 6 - Minimum Platform Requirements for Forcepoint DLP Appliance

The following minimum platform requirements are necessary for the deployment of the AP-Endpoint component, depending on the type of endpoint device. The platforms may either be physical devices or provided by Citrix XenDesktop v7.6.

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR WINDOWS FORCEPOINT DLP ENDPOINT CLIENT
Processor	1.8 GHz or above
Memory	At least 1GB RAM
Free Disk Space	At least 850 MB free hard disk space (250 MB for installation, 600 MB for operation)
Operating System	Windows 7 Enterprise SP1 x64, Windows 10 Enterprise Anniversary Edition x64, Windows Server 2012 R2 SP2 x64

Table 7 - Minimum Platform Requirements for Microsoft Endpoint

PLATFORM COMPONENT	MINIMUM REQUIREMENTS FOR MACOS FORCEPOINT DLP ENDPOINT CLIENT
Memory	At least 1 GB RAM
Free Disk Space	At least 500 MB free hard disk space (375 MB for installation, 125 MB for operation)
Operating System	Apple MacOS 10.11.6

Table 8 - Minimum Platform Requirements for MAC Endpoint

1.8 TOE Environment

The TOE is intended to be deployed in a physically-secured cabinet room, room, or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). Access to the physical console or USB ports on the appliance should be restricted via a locked data cabinet within the data center. The TOE is intended to be managed by administrators operating under a consistent security policy. All network connections between TOE components are to be routed within the physically secured location, providing protection of the communication between distributed components of the TOE.

The TOE provides a layer of security between an internal and external network (such as between a Local Area Network (LAN) and the Internet). The TOE is meant to control, protect, and monitor the internal network's access to content on the external network. For this behavior to be properly implemented, all controlled protocol traffic must traverse the TOE. The TOE environment is required to provide the necessary configuration to allow this.

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

In addition to Forcepoint V10000 G4 appliance specified in Section 1.7.1 above, there are a number of other TRITON appliances available which have not been tested during the evaluation, including V5000 and earlier versions of the V10000. Also the components hosted on Microsoft platforms are supported on Microsoft Server 2008 (Standard or Enterprise) R2 or R2 SP1, Microsoft Server 2012 (Standard edition) and Microsoft SQL Server 2008 R2, 2012 and 2014.

Features/Functionality/Components that are not part of the evaluated configuration of the TOE are:

- Hybrid Services (Web Hybrid Module and the Email Hybrid Module).
- Optional Web components, including Remote Filtering Server, Sync Service, and transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent).
- Forcepoint DLP Endpoint used in Forcepoint DLP hybrid and cloud deployments.
- Forcepoint DLP Endpoint Web and Remote Filtering clients.

2 Conformance Claims

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

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) Part 2 **extended** and Part 3 **conformant**.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

2.3 Evaluation Assurance Level

The TOE claims conformance to Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

3 Security Problem Definition

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

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

3.1 Threats

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

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

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

THREAT	DESCRIPTION
T.EXTERNAL_CONTENT	A user on the internal network may access or post content to an external network that has been deemed inappropriate or potentially harmful to the internal network.
T.DATA_LOSS	A user may intentionally or inadvertently release sensitive data to unauthorized recipients.
T.MASQUERADE	A user may masquerade as another entity in order to gain unauthorized access to user data or TRITON-APX controlled resources.
T.NACCESS	An unauthorized person or external IT entity may be able to view or modify TRITON-APX configuration and control data by hijacking an unattended administrator session.
T.UNAUTHORIZED_ACCESS	A user may gain access to security data controlled by TRITON-APX that they are not authorized to access.
T.RESOURCE	TRITON-APX users or attackers may cause network connection resources to become overused and therefore unavailable.

Table 9 – Threats Addressed by the TOE

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

3.3 Assumptions

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

ASSUMPTION	DESCRIPTION
A.INSTALL	TRITON-APX has been installed and configured according to the appropriate installation guides.
A.NETWORK	All policy-controlled traffic between the internal and external networks traverses TRITON-APX.
A.LOCATE	It is assumed that the TRITON-APX appliance and associated servers are located within the same controlled-access facility and exclude unauthorized access to the internal physical network.[3]
A.NOEVIL	It is assumed that administrators who manage TRITON-APX are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance. Similarly is it assumed that users of the TRITON-APX endpoint component are not negligent or willfully hostile.
A.MANAGE	There are one or more competent individuals assigned to manage TRITON-APX and the security of the information it contains.

Table 10 – Assumptions

[3] This assumption does not extend to the AP-ENDPOINT DLP clients, which are not within the controlled access facility. Therefore, the TOE provides logical protection of the communication between these clients and appliance/server components of the TOE.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

OBJECTIVE	DESCRIPTION
O.AUTHENTICATE	The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their network request matches a traffic policy rule that requires user authentication. The TOE must require the PEM user to authenticate before gaining access to the user's quarantined email.
O.AUDIT	The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record system configuration and traffic policy updates and allow trained administrators to review security-relevant audit events.
O.MANAGE	The TOE must provide secure management of the system configuration and the traffic policies over one or more concurrent sessions.
O.RESOURCE_CONTROL	The TOE must control access to network resources as defined by the traffic policies.
O.DATA_PROTECT	The TOE will take specified actions against transmission of identified files or data.
O.QUOTA	The TOE must be able to place quotas on network connection resources.
O.TIMESTAMP	The TOE must provide a timestamp for its own use.
O.HARMFUL_CONTENT	The TOE must disallow access to malicious content hidden within legitimate network resource requests.
O.PROTECT	The TOE must have the capability to protect configuration data from unauthorized reading or modification.

Table 11 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives for the Environment

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

OBJECTIVE	DESCRIPTION
OE.NETWORK	All policy-controlled protocol traffic between the internal and external network must traverse the TOE.

OBJECTIVE	DESCRIPTION
OE.PROTECT	The IT environment must protect itself and the TOE from external interference or tampering, and must protect the communication between the TOE server components, between the Forcepoint TRITON Manager and the administrator, and between TOE components and (optional) authentication server.
OE.CLIENT	The endpoint client workstations must be logically protected using best security practices, including the installation of anti-virus and anti-spyware software and configuration of PC firewall.

Table 12 – IT Operational Environment Security Objectives

4.2.2 Non-IT Security Objectives for the Environment

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

OBJECTIVE	DESCRIPTION
NOE.ADMIN	The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.
NOE.USER	The Authorized users are trusted to not actively or negligently compromise the security of the component on which the TOE Endpoint component is installed.
NOE.LOCATE	The physical environment must be suitable for supporting computing devices in a physically secure setting.

Table 13 – Non-IT Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 4.3.1 and 4.3.2 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

OBJECTIVE OPS / THREAT / ASSUMPTION	O.AUTHENTICATE	O.AUDIT	O.MANAGE	O.RESOURCE_CONTROL	O.DATA_PROTECT	O.QUOTA	O.TIMESTAMP	O.HARMFUL_CONTENT	O.PROTECT	OE.NETWORK	OE.PROTECT	OE.CLIENT	NOE.ADMIN	NOE.USER	NOE.LOCATE
T.EXTERNAL_CONTENT				✓				✓							
T.DATA_LOSS					✓										
T.MASQUERADE	✓														
T.NACCESS									✓		✓				

OPS / THREAT / ASSUMPTION \ OBJECTIVE	O.AUTHENTICATE	O.AUDIT	O.MANAGE	O.RESOURCE_CONTROL	O.DATA_PROTECT	O.QUOTA	O.TIMESTAMP	O.HARMFUL_CONTENT	O.PROTECT	OE.NETWORK	OE.PROTECT	OE.CLIENT	NOE.ADMIN	NOE.USER	NOE.LOCATE
T.UNAUTHORIZED_ACCESS	✓	✓	✓				✓		✓		✓	✓			
T.RESOURCE						✓									
A.INSTALL													✓		
A.NETWORK										✓					
A.LOCATE															✓
A.NOEVIL													✓	✓	
A.MANAGE													✓		

Table 14 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS	OBJECTIVES	RATIONALE
T.EXTERNAL_CONTENT A user on the internal network may access or post content to an external network that has been deemed inappropriate or potentially harmful to the internal network.	O.RESOURCE_CONTROL The TOE must control access to network resources as defined by the traffic policies.	O.RESOURCE_CONTROL counters this threat by ensuring that network resources controlled by the policies can be blocked when they contain potentially harmful or inappropriate content.
	O.HARMFUL_CONTENT The TOE must disallow access to malicious content hidden within legitimate network resource requests.	O.HARMFUL_CONTENT counters this threat by ensuring that malicious content is removed from trusted content prior to being delivered to the internal network, thereby minimizing the risk of attack to the internal network.
T.DATA_LOSS A user may intentionally or inadvertently release sensitive data to unauthorized recipients.	O.DATA_PROTECT The TOE will take specified actions against transmission of identified files or data.	O.DATA_PROTECT counters this threat by ensuring all content is inspected before it is transmitted outside the organization taking specified actions to ensure sensitive files and data are not released counter to the configured policy.

THREATS	OBJECTIVES	RATIONALE
T.MASQUERADE A user may masquerade as another entity in order to gain unauthorized access to user data or TRITON-APX controlled resources.	O.AUTHENTICATE The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their network request matches a traffic policy rule that requires user authentication. The TOE must require the PEM user to authenticate before gaining access to the user's quarantined email.	O.AUTHENTICATE counters this threat by ensuring that TOE administrators and users supply login credentials before being granted access to services or information, thereby reducing the risk of access by masquerading.
T.NACCESS An unauthorized person or external IT entity may be able to view or modify TRITON-APX configuration and control data by hijacking an unattended administrator session.	O.PROTECT The TOE must have the capability to protect configuration data from unauthorized reading or modification. OE.PROTECT The IT environment must protect itself and the TOE from external interference or tampering, and must protect the communication between the TOE components, between the Forcepoint TRITON Manager and the administrator, and between TOE components and (optional) authentication server.	O.PROTECT help mitigate this threat by ensuring that unattended management sessions do not permit attackers to access management functionality. OE.PROTECT further mitigates this threat by ensuring the IT environment provides protection of the communication between the TOE components, between the Forcepoint TRITON Manager and the administrator, and between TOE components and (optional) authentication server.
T.UNAUTHORIZED_ACCESS A user may gain access to security data controlled by TRITON-APX that they are not authorized to access.	O.AUTHENTICATE The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their network request matches a traffic policy rule that requires user authentication. The TOE must require the PEM user to authenticate before gaining access to the user's quarantined email.	O.AUTHENTICATE counters this threat by ensuring that users supply login credentials before being granted access to any security-relevant information.

THREATS	OBJECTIVES	RATIONALE
	O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record system configuration and traffic policy updates and allow trained administrators to review security-relevant audit events.	O.AUDIT counters this threat by ensuring that the TOE records potential security breaches and suspicious activity, and allows authorized administrators to review this activity.
	O.MANAGE The TOE must provide secure management of the system configuration and the traffic policies over one or more concurrent sessions.	O.MANAGE counters this threat by providing the capability for an administrator to properly configure the management mechanisms of the TOE designed to mitigate this threat.
	O.TIMESTAMP The TOE must provide a timestamp for its own use.	O.TIMESTAMP counters this threat by ensuring that timestamps used in the audit records created by O.AUDIT are reliable. These audit records are used by administrators to observe any suspicious activity.
	O.PROTECT The TOE must have the capability to protect configuration data from unauthorized reading or modification. OE.PROTECT The IT environment must protect itself and the TOE from external interference or tampering, and must protect the communication between the TOE components, between the Forcepoint TRITON Manager and the administrator, and between TOE components and (optional) authentication server. OE.CLIENT The endpoint client workstations must be logically protected using best practices, including the installation of anti-virus and anti-spyware software and configuration of PC firewall.	O.PROTECT helps to mitigate this threat by ensuring that the TOE is capable of protecting management data and access to management functionality from unauthorized access via an unattended management session. OE.PROTECT also helps to mitigate this threat by ensuring the IT environment provides protection of the communication between the TOE components, between the Forcepoint TRITON Manager and the administrator, and between TOE components and (optional) authentication server. OE.CLIENT further mitigates this threat by ensuring the IT environment provided by the endpoint client workstation is protected by best security practices to protect against logical attack against the TOE endpoint component.

THREATS	OBJECTIVES	RATIONALE
T.RESOURCE TRITON-APX users or attackers may cause network connection resources to become overused and therefore unavailable.	O.QUOTA The TOE must be able to place quotas on network connection resources.	O.QUOTA counters this threat by ensuring that the TOE is capable of placing administrator-defined quotas on the network resources, thereby ensuring that those resources do not become unavailable.

Table 15 – Rationale for Mapping of Threats to Objectives for the TOE

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

4.3.1 Security Objectives Rationale Relating to Policies

There are no Policies defined for this Security Target. Therefore, there are no Security Objectives relating to Policies.

4.3.2 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	RATIONALE
A.INSTALL TRITON-APX has been installed and configured according to the appropriate installation guides.	NOE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	NOE.ADMIN upholds this assumption by ensuring that the administrator responsible for the TRITON-APX installs and configures the TRITON-APX according to the guidance documentation.
A.NETWORK All policy-controlled traffic between the internal and external networks traverses TRITON-APX.	OE.NETWORK All policy-controlled protocol traffic between the internal and external network must traverse the TOE.	OE.NETWORK upholds this assumption by ensuring that the IT environment is configured such that no policy-controlled traffic can travel between the internal and external networks without traversing the TRITON-APX.
A.LOCATE It is assumed that the TRITON-APX appliance and associated servers are located within the same controlled-access facility and exclude unauthorized access to the internal physical network.	NOE.LOCATE The physical environment must be suitable for supporting computing devices in a physically secure setting.	NOE.LOCATE upholds this assumption by ensuring that the IT environment is suitable to ensure the proper, secure functioning of the TRITON-APX components and protects the communication between the TRITON-APX components, between the Forcepoint TRITON Manager and the administrator and between the TRITON-APX components and (optional) authentication server.

Assumptions	Objectives	RATIONALE
A.NOEVIL It is assumed that administrators who manage TRITON-APX are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance.	NOE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance. NOE.USER The Authorized users are trusted to not actively or negligently compromise the security of the component on which the TOE Endpoint component is installed.	NOE.ADMIN helps to uphold this assumption by ensuring that administrators are non-hostile, appropriately trained and follow all administrator guidance. NOE.USER further upholds this assumption by ensuring that users are non-hostile and follow best security practice.
A.MANAGE There are one or more competent individuals assigned to manage TRITON-APX and the security of the information it contains.	NOE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	NOE.ADMIN upholds this assumption by ensuring that those responsible for the TRITON-APX provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.

Table 16 – Rationale for Mapping of Assumptions to Objectives for the Environment

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

5 Extended Components Definition

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

5.1 Extended TOE Security Functional Components

This section specifies the extended SFR for the TOE. The extended SFR is organized by class. Table 17 identifies the extended SFR implemented by the TOE.

NAME	DESCRIPTION
FAU_GEN_EXT.1	Security Audit Generation

Table 17 – Extended TOE Security Functional Requirements

5.1.1 Class FAU: Security Audit

5.1.1.1 Security Audit Generation (FAU_GEN_EXT)

Family behaviour

This family is added to the class FAU. This family defines requirements for recording the occurrence of security relevant events that take place under TSF control, and is based on the FAU_GEN family without the requirement to audit the start-up and shutdown of auditing mechanisms (which is not directly transferable to a TOE with distributed, independent components).

Component Leveling

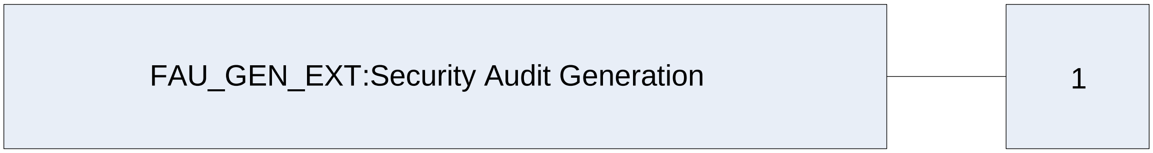

Figure 3 – FAU_GEN_EXT Security Audit Generation family decomposition

FAU_GEN_EXT.1 requires generation of audit records for specified actions and specifies the list of data that shall be recorded in each record.

Management: FAU_GEN_EXT.1

There are no management activities foreseen.

Audit: FAU_GEN_EXT.1

There are no auditable activities foreseen.

FAU_GEN_EXT.1 Security Audit Generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

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

a) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
b) [assignment: other specifically defined auditable events].

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

c) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
d) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

5.3 Rationale for Extended Security Functional Requirements

FAU_GEN_EXT.1.1 is an extended functional requirement that was created to closely match the requirements of FAU_GEN.1, defined in Common Criteria Part 2, but without the requirement for auditing start-up and shutdown events for the TOE, which are not applicable to this TOE with distributed components..

5.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 1.4

6.1 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 18 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Component	DESCRIPTION	S	A	R	I
FAU_GEN_EXT.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FDP_ACC.1(a)	Subset access control		✓		✓
FDP_ACF.1(a)	Security attribute based access control		✓		✓
FDP_ACC.1(b)	Subset access control		✓		✓
FDP_ACF.1(b)	Security attribute based access control		✓		✓
FDP_ACC.1(c)	Subset access control		✓		✓
FDP_ACF.1(c)	Security attribute based access control		✓		✓
FIA_ATD.1	User attribute definition		✓	✓	
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.2	User authentication before any action				
FIA_UID.1	Timing of identification		✓	✓	
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1(a)	Management of security attributes (change)	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes (View)	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(c)	Static attribute initialisation	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SAE.1	Time-limited authorisation		✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security roles		✓	✓	
FPT_STM.1	Reliable time stamps				
FRU_RSA.1(a)	Maximum quotas	✓	✓		✓
FRU_RSA.1(b)	Maximum quotas	✓	✓		✓
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions		✓		
FTA_SSL.3	TSF-initiated termination		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FCS_CKM.1	Cryptographic key generation		✓		
FCS_COP.1	Cryptographic operation		✓		

Table 18 – TOE Functional Components

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

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN_EXT.1 Security Audit Generation (TRITON Audit Log)

Hierarchical to: No other components.

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

a) All auditable events, for the [not specified] level of audit; and

b) [*successful administrator logins, internet usage filter changes, web protection policy changes, email filter changes, email policy changes, data loss prevention policy changes, and appliance configuration changes*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*server affected by the change (IP address) and role affected*].

Dependencies: FPT_STM.1 Reliable time stamps

6.1.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [*Super Administrator, System Administrator*] with the capability to read [*all audit data*] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

6.1.1.3 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

6.1.2 Class FDP: User Data Protection

6.1.2.1 FDP_ACC.1(a) Subset access control (Web)

Hierarchical to: No other components.

FDP_ACC.1.1(a) The TSF shall enforce the [*Internet Access Policy*] on [

1. *Subjects: users*
2. *Objects: external IT entities hosting content*
3. *Operations: retrieving hosted content*].

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.2.2 FDP_ACF.1(a) Security attribute based access control (Web)

Hierarchical to: No other components.

FDP_ACF.1.1(a) The TSF shall enforce the [*Internet Access Policy*] to objects based on the following:

[

Subject attributes:

1. *User name*
2. *User group*
3. *IP address*
4. *Quotas for Access*

Object attributes:

1. *Assigned category*
2. *IP address*
3. *URL*
4. *Protocol*
5. *Keywords*
6. *Web Objects*

].

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If a bandwidth usage quota is defined for the category or protocol, evaluate the current bandwidth:*
    a. *If the bandwidth currently in use is below the defined threshold for the category or protocol, allow access to the content.*
    b. *If the bandwidth currently in use is above or at the defined threshold for the category or protocol, deny access to the content.*
2. *If a "block" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "block page".*
3. *If a "permit" rule is defined for the category or protocol group, allow access*

to the content.

4. *If a "confirm" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "confirmation page" until the user confirms that the access is for business-related purposes.*
5. *If a "quota" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "quota confirmation page". If the user agrees to continue to the content, begin the quota timer for the user.*
6. *If no rule is defined for the content, allow access to the requested content*

].

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*if a "quota" rule is defined and a user has no more browsing quota, the TOE denies access to the user and shows the "block" page*].

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

6.1.2.3 FDP_ACC.1(b) Subset access control (Data)

Hierarchical to: No other components.

FDP_ACC.1.1(b) The TSF shall enforce the [*Data Loss Prevention Policy*] on [

1. *Subjects: users*
2. *Objects: filesystem files, email messages, database entries*
3. *Operations: file access, email transmission, database update*].

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.2.4 FDP_ACF.1(b) Security attribute based access control (Data)

Hierarchical to: No other components.

FDP_ACF.1.1(b) The TSF shall enforce the [*Data Loss Prevention Policy*] to objects based on the following:

[

Subject attributes:

1. *User name*
2. *User group*
3. *Domain*

Object attributes:

1. *Resource type*
2. *Content Classifier*

].

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the accumulated number of matched rules for subject and object attributes is below the threshold (Drip DLP)*
2. *If the number of matched rules for a single transaction matching subject and object attributes is below the threshold*

].

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*if the threshold for matched rules is exceeded or "incident for every matched condition" is configured for a policy*].

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

6.1.2.5 FDP_ACC.1(c) Subset access control (Email)

Hierarchical to: No other components.

FDP_ACC.1.1(c) The TSF shall enforce the [*Email Policy*] on [

1. *Subjects: users*
2. *Objects: email messages*
3. *Operations: receiving email, sending email*].

Dependencies: FDP_ACF.1 Security attribute based access control

6.1.2.6 FDP_ACF.1(c) Security attribute based access control (Email)

Hierarchical to: No other components.

FDP_ACF.1.1(c) The TSF shall enforce the [*Email Policy*] to objects based on the following:

[

Subject attributes:

1. *Email Address*
2. *Group*
3. *IP Address*

Object attributes:

1. *Direction of email message*

].

FDP_ACF.1.2(c) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If message subject and object attributes match a rule with a "Deliver message" action, or*
2. *If message subject and object attributes match a "Resume processing" action as the final filter in the sequence of filters applied to the message*

].

FDP_ACF.1.3(c) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [message *matches Always Permit List*].

FDP_ACF.1.4(c) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*message matches Always Block List, or message matches a rule a "Drop message" action*].

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

6.1.3 Class FIA: Identification and Authentication

6.1.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **administrators**: [*user name, role, password*].

Dependencies: No dependencies

6.1.3.2 FIA_UAU.1 Timing of authentication (administrator)

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [*access to the installation CLI*] on behalf of the ~~user~~ **administrator** to be performed before the ~~user~~ **administrator** is authenticated.

FIA_UAU.1.2 The TSF shall require each ~~user~~ **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

Dependencies: FIA_UID.1 Timing of identification

6.1.3.3 FIA_UAU.2 User authentication before any action (web/email user)

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

6.1.3.4 FIA_UID.1 Timing of identification (administrator)

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [*access to the installation CLI*] on behalf of the ~~user~~ **administrator** to be performed before the ~~user~~ **administrator** is identified.

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

Dependencies: No dependencies

6.1.3.5 FIA_UID.2 User identification before any action (web/email user)

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

6.1.4 Class FMT: Security Management

6.1.4.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [<u>disable, enable, modify the behaviour of</u>] the functions [*Forcepoint Web Security component, Forcepoint Email Security component, Forcepoint DLP component*] to [*Super Administrators, System Administrators and Policy Administrators*].

Dependencies: FMT_SMF.1 Specification of management functions

6.1.4.2 FMT_MSA.1(a) Management of security attributes (change)

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a) The TSF shall enforce the [*Internet Access Policy, Data Loss Policy and Email Policy*] to restrict the ability to [<u>change default, query, modify, delete [*create*]</u>] the security attributes [*internet usage filters, web protection policies, email filters, email policies, data loss prevention policies, and appliance configuration*] to [*Super Administrators, System Administrator and Policy Administrator*].

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

6.1.4.3 FMT_MSA.1(b) Management of security attributes (view)

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b) The TSF shall enforce the [*Internet Access Policy, Data Loss Policy and Email Policy*] to restrict the ability to [query] the security attributes [*internet usage filters, web protection policies, email filters, email policies, data loss prevention policies, and appliance configuration*] to [*Super Administrators, System Administrator Policy Administrator and Auditor*].

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

6.1.4.4 FMT_MSA.3(a) Static attribute initialization (Web)

Hierarchical to: No other components.

FMT_MSA.3.1(a) The TSF shall enforce the [*Internet Access Policy*] to provide [permissive] default values for security attributes that are used to enforce the SFP .

FMT_MSA.3.2(a) The TSF shall allow the [*Super Administrators and Policy Administrators*] to specify alternative initial values to override the default values when an object or information is created.

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

6.1.4.5 FMT_MSA.3(b) Static attribute initialization (Data)

Hierarchical to: No other components.

FMT_MSA.3.1(b) The TSF shall enforce the [*Data Loss Prevention Policy*] to provide [permissive] default values for security attributes that are used to enforce the SFP .

FMT_MSA.3.2(b) The TSF shall allow the [*Super Administrators and Policy Administrators*] to specify alternative initial values to override the default values when an object or information is created.

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

6.1.4.6 FMT_MSA.3(c) Static attribute initialization (Email)

Hierarchical to: No other components.

FMT_MSA.3.1(c) The TSF shall enforce the [*Email Policy*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(c) The TSF shall allow the [*Super Administrators and Policy Administrators*] to specify alternative initial values to override the default values when an object or information is created.

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

6.1.4.7 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [query], [*search, sort, and select*] the [*audit data*] to [*Super Administrators*].

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

6.1.4.8 FMT_SAE.1 Time-limited authorisation

Hierarchical to: No other components.

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [*the administrator management session time*] to [*Super Administrators*].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [*terminate the administrative session*] after the expiration time for the indicated security attribute has passed.

Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

6.1.4.9 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*management of security functions behavior, management of security attributes, and management of TSF data in accordance with Table 19].*

Role	Description	Triton Manager		
Global Security Administrator	Administrators with this permission set have full access across the TRITON Manager; they can add and remove administrators and edit the profiles and permissions of all other administrators.	✓		
Conditional Super Administrator	Administrators with this permission set have access to all general settings within TRITON Manager and can add domains and set up routes and preferences. Permissions are identical to a Global Security Administrator, except they cannot manage other administrators	✓		
Delegated Administrator Role	Description	Email	Web	Data
Super Administrator	Administrators with this role have full access; they can add and remove administrators and edit the profiles and permissions of all other administrators.	✓	✓	✓
Auditor	Administrators with this role can view all configuration settings but not change them.	✓	✓	✓

Delegated Administrator Role	Description	Email	Web	Data
Reporting Administrator	Administrators with this role can edit, run, and schedule reports only.	✓	✓	
System Administrator[4]	Administrators with this role have access to all general settings and can add domains and set up routes and preferences. Permissions are identical to a Super Administrator, except they cannot manage other administrators	✓	✓	✓
Policy Administrator	Administrators with this role can create and manage policies only for the specific users or groups managed by this role. Permissions include reporting and quarantine management for these users and groups	✓	✓	✓
Quarantine Administrator	Administrators with this role can manage specific queues, troubleshoot from logs, and release messages to users from assigned queues.	✓		
Incident Administrator	Administrator with this role can access reports, incident details, and workflow. Manages incident handling.			✓
Group Reporting Administrator	Administrators with this role can edit, run, and schedule reports only for users in specified groups.	✓		
Default	This is the default role for a new administrator. Administrators only assigned to this role can access only reports and the Today page.	✓	✓	✓
Real Time Monitor	Administrators with this role can monitor Internet traffic in real time.		✓	

Table 19 – TRITON Delegated Administrator and TRITON Manager Administrator Roles

Dependencies: No Dependencies

6.1.4.10 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [

TRITON Administrator roles: Global Security Administrator, Conditional Super Administrator;

Delegated Administrator roles: Super Administrator, Auditor, Reporting Administrator, System Administrator, Policy Administrator, Quarantine Administrator, Incident Administrator, Group Reporting Administrator, Default].

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

Dependencies: FIA_UID.1 Timing of identification

[4] This role is labelled “Security Administrator” in the Email delegated roles and “Conditional Super Administrator” in the Web delegated roles.

Application Note: Email and web users who are subject to identification and authentication are not considered to be roles maintained by the TOE as these users are not permitted to access functions of the TOE. The identification and authentication requirements are applied as required by the access control policies.

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Dependencies: No dependencies

6.1.5.2 FRU_RSA.1(a) Maximum quotas

Hierarchical to: No other components.

FRU_RSA.1.1(a) The TSF shall enforce maximum quotas of the following resources: [*access to restricted approved categories*] that [individual user] can use [over a specified period of time].

Dependencies: No dependencies

6.1.5.3 FRU_RSA.1(b) Maximum quotas

Hierarchical to: No other components

FRU_RSA.1.1(b) The TSF shall enforce maximum quotas of the following resources [*bandwidth*] that [defined group of users] can use [simultaneously].

Dependencies: No dependencies

6.1.6 Class FTA: TOE Access

6.1.6.1 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [*if a user exceeds the bandwidth quota for a protocol category defined by policy, any new concurrent sessions within that category will be blocked*].

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [un*limited*] sessions per user.

Dependencies: FIA_UID.1 Timing of identification

6.1.6.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*thirty minutes administrator inactivity*].

Dependencies: No dependencies

6.1.7 Class FPT: Protection of the TSF

6.1.7.1 FPT_ITT.1 *Basic internal TSF data transfer protection*

Hierarchical to: No other components.

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

Dependencies: No dependencies.

Application Note: This requirement relates to the protection of the communication between the Forcepoint DLP server and the Forcepoint DLP Endpoint client device[5].

6.1.8 Class FCS: Cryptography

The requirements in this class relate to the cryptographic functionality provided to support the protection of communication to the client devices which are outside the physically protected environment, namely:

- Secondary Forcepoint DLP server and the Forcepoint DLP Endpoint client device

6.1.8.1 FCS_CKM.1 *Cryptographic key generation (for TLS protocol)*

Hierarchical to: No other components

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*as listed in Table 20*] and specified cryptographic key sizes [*as listed in Table 20*] that meet the following: [*as listed in Table 20*].

Key Generation Algorithm	Key sizes	Standard
HMAC DRBG (AES)	128 bits, 256 bits	None[6]
RSA	2048 bits	X9.31[7]

Table 20 – Key Generation Algorithms

[5] Communication between the TRITON APX server components is protected by the physical environment in accordance with the assumption A.LOCATE.

[6] Based on SP800-90a

[7] RSA key generation is performed in accordance to the X9.31 standard for legacy reasons and backwards compatibility to earlier releases of TRITON APX. The next major release of TRITON will integrate crypto libraries which conform to the FIPS186-4 standard for RSA Key generation.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

6.1.8.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

FCS_COP.1.1 The TSF shall perform [*cryptographic operations as described in Table 21*] in accordance with a specified cryptographic algorithm [*cryptographic algorithms as described in Table 21*] and cryptographic key sizes [*cryptographic key sizes as described in Table 21*] that meet the following: [*cryptographic standards as described in Table 21*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Operation	Cryptographic Algorithm	Key Sizes (bits)	Standard
KeyPair Generation	RSA Key Generation	2048	X9.31
Encryption	AES (operating in CBC mode)	128, 256	AES: ISO 1033-3 CBC mode: ISO 10116
Hashing	SHA-1[8], SHA-256, SHA-384	n/a	ISO 10118-3
Cryptographic signature services	RSA Digital Signature Algorithm (rDSA)	2048	X9.31

Table 21 – Cryptographic operations

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2. The assurance components are summarized in the following table:

CLASS HEADING	ASSURANCE COMPONENT	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification

[8] Not used for signature generation

CLASS HEADING	ASSURANCE COMPONENT	DESCRIPTION
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 22 – Security Assurance Requirements at EAL2 augmented with ALC_FLR.2

6.3 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives

6.3.1 Security Functional Requirements Rationale

6.3.1.1 Rationale for Security Functional Requirements meeting the TOE Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVE	RATIONALE
O.AUTHENTICATE The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their network request matches a traffic policy rule that requires user authentication. The TOE must require the PEM user to authenticate before gaining access to the user's quarantined email.	FIA_ATD.1 User attribute definition	This requirement supports O.AUTHENTICATE by ensuring that the TOE can maintain a list of security attributes used for administrator authentication.
	FIA_UAU.1 Timing of authentication	This requirement supports O.AUTHENTICATE by requiring administrators to authenticate their identities before being allowed access to any TOE management functionality besides the installation CLI.
	FIA_UAU.2 User authentication before any action	This requirement supports O.AUTHENTICATE by requiring users to authenticate their identities before gaining access to network resources.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVE	RATIONALE
	FIA_UID.1 Timing of identification	This requirement supports O.AUTHENTICATE by requiring administrators to identify themselves before being allowed access to any TOE management functionality besides the installation CLI.
	FIA_UID.2 User identification before any action	This requirement supports O.AUTHENTICATE by requiring users to identify themselves before being allowed access to network resources.
O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record system configuration and traffic policy updates and allow trained administrators to review security-relevant audit events.	FAU_GEN_EXT.1 Security Audit Generation	This requirement supports O.AUDIT by ensuring that the TOE generates audit records for events at the "not specified" level of audit.
	FAU_SAR.1 Audit review	This requirement supports O.AUDIT by ensuring that administrators can review the audit records generated by the TOE.
	FAU_SAR.2 Restricted audit review	This requirement supports O.AUDIT by ensuring that only authorized administrators are able to view the audit records generated by the TOE.
	FMT_MTD.1 Management of TSF data	This requirement supports O.AUDIT by ensuring that only authorized administrators are able to manage audit data.
O.MANAGE The TOE must provide secure management of the system configuration and the traffic policies over one or more concurrent sessions.	FMT_MOF.1 Management of security functions behaviour	This requirement supports O.MANAGE by specifying the management activities available for each administrative role to perform.
	FMT_MSA.1(a)(b) Management of security attributes	This requirement supports O.MANAGE by specifying which administrative roles can manage security attributes relating to the network policies.
	FMT_MSA.3(a)(b)(c) Static attribute initialisation	This requirement supports O.MANAGE by defining the default security posture of the network policies, and specifying the administrative roles that can change the policy from the default posture.
	FMT_SMF.1 Specification of Management Functions	This requirement supports O.MANAGE by specifying which management functionality is available for the TOE.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVE	RATIONALE
	FMT_SMR.1 Security roles	This requirement supports O.MANAGE by specifying which roles are available for administrators, and by ensuring that administrators are properly associated with their assigned roles.
	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	This requirement supports O.MANAGE by ensuring that administrators can manage and define the number of concurrent sessions that an end user can run.
O.RESOURCE_CONTROL The TOE must control access to network resources as defined by the traffic policies.	FDP_ACC.1(a) Subset access control	This requirement supports O.RESOURCE_CONTROL by ensuring that the TOE can control access of subjects (users) to objects (external IT entities hosting content).
	FDP_ACF.1(a) Security attribute based access control	This requirement supports O.RESOURCE_CONTROL by ensuring that the TOE can utilize the attributes of the controlled network traffic to enforce the Internet Access Policy.
	FMT_MSA.1(a) Management of security attributes	This requirement supports O.RESOURCE_CONTROL by ensuring that only authorized administrators can modify security attributes associated with the Internet Access Policy.
	FMT_MSA.3(a) Static attribute initialisation	This requirement supports O.RESOURCE_CONTROL by ensuring that the Internet Filtering Policy is permissive by default, and that only authorized administrators can modify this default posture.
O.DATA_PROTECT The TOE will take specified actions against transmission of identified files or data.	FDP_ACC.1(b) Subset access control	This requirement supports O.DATA_PROTECT by ensuring that the TOE can control access of subjects (users) to objects (filesystem files, email messages, database entries).
	FDP_ACF.1(b) Security attribute based access control	This requirement supports O.DATA_PROTECT by ensuring that the TOE can utilize the attributes of the controlled network traffic to enforce the Data Loss Prevention Policy.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVE	RATIONALE
	FMT_MSA.1(b) Management of security attributes	This requirement supports O.RESOURCE_CONTROL by ensuring that only authorized administrators can modify security attributes associated with the Data Loss Prevention Policy.
	FMT_MSA.3(b) Static attribute initialisation	This requirement supports O.RESOURCE_CONTROL by ensuring that the Data Loss Prevention Policy is permissive by default, and that only authorized administrators can modify this default posture.
	FDP_ACC.1(c) Subset access control	This requirement supports O.DATA_PROTECT by ensuring that the TOE can control access of subjects (users) to objects (email messages).
	FDP_ACF.1(c) Security attribute based access control	This requirement supports O.DATA_PROTECT by ensuring that the TOE can utilize the attributes of the controlled email traffic to enforce the Email Policy.
	FMT_MSA.1(c) Management of security attributes	This requirement supports O.RESOURCE_CONTROL by ensuring that only authorized administrators can modify security attributes associated with the Email Policy.
	FMT_MSA.3(c) Static attribute initialisation	This requirement supports O.RESOURCE_CONTROL by ensuring that the Email Policy is permissive by default, and that only authorized administrators can modify this default posture.
O.QUOTA The TOE must be able to place quotas on network connection resources.	FRU_RSA.1(a) Maximum quotas	This requirement supports O.QUOTA by ensuring that the TOE is capable of placing maximum quotas on the number of connections available during a specified time period.
	FRU_RSA.1(b) Maximum quotas	This requirement supports O.QUOTA by ensuring that the TOE places maximum quotas on the bandwidth available for use by different types of traffic.
O.TIMESTAMP The TOE must provide a timestamp for its own use.	FPT_STM.1 Reliable time stamps	This requirement supports O.TIMESTAMP by ensuring that the TOE provides a timestamp for its own use.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVE	RATIONALE
O.HARMFUL_CONTENT The TOE must disallow access to malicious content hidden within legitimate network resource requests.	FDP_ACC.1(a) Subset access control	This requirement supports O.HARMFUL_CONTENT by ensuring that the Internet Filtering Policy can block harmful content that might exist within trusted content.
	FDP_ACF.1(a) Security attribute based access control	This requirement supports O.HARMFUL_CONTENT by ensuring that the TOE can utilize the attributes of the controlled network traffic to enforce the Internet Filter Policy.
	FMT_MSA.1(a) Management of security attributes	This requirement supports O.HARMFUL_CONTENT by ensuring that only authorized administrators can modify security attributes associated with the Proxy Filtering Policy.
	FMT_MSA.3(a) Static attribute initialisation	These requirements support O.HARMFUL_CONTENT by ensuring that the Internet Filtering Policy is permissive by default, but that only authorized administrators can modify this default posture.
O.PROTECT The TOE must have the capability to protect configuration data from unauthorized reading or modification.	FMT_SAE.1 Time-limited authorisation	This requirement supports O.PROTECT by ensuring that authorized administrators can monitor real-time updated data pages without risking an unauthorized individual gaining access to an unattended management session.
	FTA_SSL.3 TSF-initiated termination	This requirement supports O.PROTECT by ensuring that unauthorized individuals do not gain access to the TOE through an unattended management session.
	FPT_ITT.1 FCS_CKM.1 FCS_COP.1	These requirements support O.PROTECT by ensuring the configuration data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client is protected.

Table 23 – Rationale for Mapping of TOE SFRs to Objectives

6.3.1.2 Rationale for Refinements of Security Functional Requirements

The following refinements of SFRs from CC version 3.1 have been made to specify that the SFR applies to administrator identification and authentication instead of user identification and authentication: FIA_ATD.1, FIA_UAU.1, FIA_UID.1.

6.3.1.3 Security Functional Requirements Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 24 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR ID	DEPENDENCY	DEPENDENCY MET	RATIONALE
FAU_GEN_EXT.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	Met by FAU_GEN_EXT.1
FAU_SAR.2	FAU_SAR.1	✓	
FDP_ACC.1(a)	FDP_ACF.1	✓	FDP_ACF.1(a)
FDP_ACF.1(a)	FDP_ACC.1	✓	FDP_ACC.1(a)
	FMT_MSA.3	✓	FMT_MSA.3(a)
FDP_ACC.1(b)	FDP_ACF.1	✓	FDP_ACF.1(b)
FDP_ACF.1(b)	FDP_ACC.1	✓	FDP_ACC.1(b)
	FMT_MSA.3	✓	FMT_MSA.3(b)
FDP_ACC.1(c)	FDP_ACF.1	✓	FDP_ACF.1(c)
FDP_ACF.1(c)	FDP_ACC.1	✓	FDP_ACC.1(c)
	FMT_MSA.3	✓	FMT_MSA.3(c)
FIA_ATD.1	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.2	FIA_UID.1	✓	FIA_UAU.2 applies to user authentication. Although FIA_UID.1 is claimed, it applies to administrator identification. FIA_UID.2 is also claimed, and applies to user identification. Since FIA_UID.2 is hierarchical to FIA_UID.1, this SFR satisfies this requirement.
FIA_UID.1	None	N/A	
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(a)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1	✓	FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACC.1(c)
FMT_MSA.1(b)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1	✓	FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACC.1(c)
FMT_MSA.3(a)	FMT_MSA.1	✓	FMT_MSA.1(a)

SFR ID	DEPENDENCY	DEPENDENCY MET	RATIONALE
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_MSA.1	✓	FMT_MSA.1(a), FMT_MSA.1(b)
	FMT_SMR.1	✓	
FMT_MSA.3(c)	FMT_MSA.1	✓	FMT_MSA.1(a), FMT_MSA.1(b)
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SAE.1	FMT_SMR.1	✓	
	FPT_STM.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_STM.1	None	N/A	
FRU_RSA.1(a)	None	N/A	
FRU_RSA.1(b)	None	N/A	
FTA_MCS.2	FIA_UID.1	✓	
FTA_SSL.3	None	N/A	
FPT_ITT.1	None	N/A	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	N/A	The dependency on FCS_CKM.4 for secure destruction of keys is inapplicable for the implementation of the TOE – see rationale in Section 6.3.1.4.
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	N/A	This dependency is inapplicable for the TOE – see Section 6.3.1.4.

Table 24 – TOE SFR Dependency Rationale

6.3.1.4 FCS_CKM.4 rationale

The dependency on FCS_CKM.4 for secure destruction of keys is not necessary for the implementation of the TOE as the secure sessions are a standard implementation of https. The client only stores a copy of the public key and certificate, which by their very nature are not considered to be sensitive. The symmetric session key generated during the handshake by the client, used to encrypt application data exchanged in the https session, is not persistently stored by either the client or the server. This session key is held in memory and is only valid for that given session. Once the session is terminated the key cannot be used to decrypt subsequent sessions. The attack potential required attempting to extract the key from the client memory following session termination to decrypt traffic captured between the client and server is significantly beyond the attack potential of EAL2. Hence, the satisfaction of the dependency on FCS_CKM.4 is considered to be inapplicable for this TOE.

6.3.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.2. EAL2+ was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. Forcepoint TRITON APX 8.2 is targeted at an environment with good physical security (A.LOCATE) and competent administrators (NOE.ADMIN, A.MANAGE), where EAL 2 should provide adequate assurance. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack. ALC_FLR.2 was chosen to assure that the developer is able to act appropriately upon security flaw reports from TOE users.

This Security Target conforms to Part 2 extended and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

This section identifies the Lifecycle , Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Development and Architecture: TRITON APX 8.2
ADV_FSP.2: Security-Enforcing Functional Specification	Development and Architecture: TRITON APX 8.2
ADV_TDS.1: Basic Design	Development and Architecture: TRITON APX 8.2
AGD_OPE.1: Operational User Guidance	Common Criteria Guidance Supplement: TRITON APX 8.2
AGD_PRE.1: Preparative Procedures	Common Criteria Guidance Supplement: TRITON APX 8.2
ALC_CMC.2: Use of a CM System	Configuration Management Document: TRITON APX 8.2
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Document: TRITON APX 8.2
ALC_DEL.1: Delivery Procedures	Secure Delivery Document: TRITON APX 8.2
ALC_FLR.2: Flaw Reporting	Flaw Remediation Document: TRITON APX 8.2
ATE_COV.1: Evidence of Coverage	Functional Test Plan: TRITON APX 8.2
ATE_FUN.1: Functional Testing	Functional Test Plan: TRITON APX 8.2
ATE_IND.2: Independent Testing – Sample	Functional Test Plan: TRITON APX 8.2
AVA_VAN.2: Vulnerability Analysis	Performed and provided by CCTL

Table 25 – Security Assurance Measures

6.3.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from Part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

7 TOE Summary Specification

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

7.1 TOE Security Functions

7.1.1 Security Audit

The TOE generates audit records for all administrator login and logoff events, policy changes, and configuration changes. The TOE Audit Log records contain the following information:

	Description
Action ID	ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the Find Action ID field and clicking Find.
Date & Time	Date and time the action occurred.
Administrator	Name and user name of the administrator that initiated the action.
Access Role	Role of the administrator.
Topic	You can filter the Audit Log by topic types. • Administration - Displays actions performed by administrators during the designated period, such as adding a new access role or configuring user directories. Also displays actions made on administrators, such as adding a new administrator or changing an administrator's permissions. • Log on/Log out - Displays log on and log out actions so you know which administrators where active during the designated period. • Status - Displays actions performed on status reports and logs, such as deleting an entry or creating an audit record. • Policy management - Displays actions performed on policies, such as updating predefined policies, editing quick policies, or creating a new policy. • Reporting - Displays actions performed on reports during the designated period, such as editing or creating a new report. • Incident management - Displays actions performed on incidents, such as deleting incidents.

	• Archiving - Displays actions performed on incident archives, such as deleting or restoring an archive. • System modules - Displays actions performed on system modules, such as editing a configuration or adding a module.
Action Performed	Description of the action performed by the administrator—for example, "exported DLP incident to PDF file".
Details	Additional information about the action. For example, for an action such as adding a policy, rule, or exception, this shows the policy, rule, or exception name. For actions such as previewing or exporting a report, it includes the report name.
Modified Item	Identifies the object that was changed, added, or deleted. For actions performed on incidents (e.g., viewing incident details), it includes the incident ID. For report generation, it includes a task number. Click the link to view additional details.

Table 26 – Audit Record Content

The TOE provides a set of web interfaces that administrators can use to view the recorded audit logs. The Audit Log can be viewed via TRITON GUI by Super Administrators.

The TOE has an internal hardware clock that provides reliable timestamps for the TOE. These timestamps are used when recording events in the audit log.

TOE Security Functional Requirements Satisfied: FAU_GEN_EXT.1, FAU_SAR.1, FAU_SAR.2, FPT_STM.1.

7.1.2 User Data Protection

7.1.2.1 Internet Access Protection

The TOE enforces an Internet Filtering Policy on controlled traffic. The policy allows administrators to define categories of websites and protocols that internal users should be prevented from accessing. Administrators specify the category and protocol restrictions to implement for each user or group of users. User traffic can be controlled in various ways, including allowing access to content, blocking access to content, or enforcing various quotas and bandwidth restrictions.

Policies are based on categories of web content and non-web protocols. Default content categories include adult material, political, business and economy, and many more. Administrators can define policies with these default categories or create new categories to create more customized policies. Default protocol categories include instant messenger, bit torrent, and many others. Like with content categories, administrators can define custom protocol categories to help enforce more customized policies.

Policies detail which filters are to be applied for web protection. Each filter includes:

- The filter type (category filter, limited access filter, or protocol filter)
- The filter name and description
- The filter contents (categories or protocols with actions applied, or a list of sites permitted)
- The number of policies that enforce the selected filter
- Actions for the filter are specified when the filter is created using the Action Buttons:

Filter Type	Action Buttons
Category filter	Use the **Permit**, **Block**, **Confirm**, or **Quota** button to change the action applied to the selected categories. To change the action applied to a parent category and all of its subcategories, first change the action applied to the parent category, and then click **Apply to Subcategories**. To enable keyword blocking, file type blocking, or blocking based on bandwidth, click **Advanced**.
Limited access filter	Use the **Add Sites** and **Add Expressions** button to add permitted URLs, IP addresses, or regular expressions to the filter. To remove a site from the filter, mark the check box next to the URL, IP address, or expression, and then click **Delete**.
Protocol filter	Use the **Permit** or **Block** button to change the action applied to the selected protocols. To change the action applied to all protocols in a protocol group, change the action applied to any protocol in the group, and then click **Apply to Group**. To log data for the selected protocol, or to enable blocking based on bandwidth, click **Advanced**.

The scanning performed to applied the internet protection policies includes use of the Forcepoint ACE (Advanced Classification Engine) to identify malicious lures, exploit kits, emerging threats, botnet communications and other advanced threat activity. Multiple real-time content engines analyse full web page content, active scripts, web links, contextual profiles, files (including executables).

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACF.1(a)

7.1.2.2 Data Loss Prevention

The TOE enforces a Data Loss Prevention policy to protect an organization from information leaks and data loss both at the perimeter and inside the organization. The Forcepoint DLP component can operate alone in the network, or it can be paired with Forcepoint Web Security or Forcepoint Email Security to provide a well-rounded data loss prevention solution. The Forcepoint Web Security DLP module prevents data loss over Web channels such as HTTP, HTTPS, and FTP. The Email DLP module prevents data loss through email.

The DLP policy engine is responsible for parsing data and using analytics to compare it to the rules in the configured policies. Policies can be used to define:

- Who can move and receive data
- What data can and cannot be moved
- Where the data can be sent
- How the data can be sent
- What action to take in case of a policy breach

There are 5 kinds of DLP policies:

1. Email policy. A single email DLP policy can be defined that contains all attributes to be monitored in inbound and outbound messages. For each attribute (for example, the appearance of a defined key phrase), the policy defines whether to permit or quarantine the message, and whether a notification should be sent.
2. Web policy. A single Web DLP policy can be enabled that contains all attributes to be monitored in HTTP, HTTP, and FTP channels, and also specifies websites to which sensitive data cannot be sent.
3. Mobile policy. A single mobile DLP policy can be enabled that contains all attributes to be monitored in email being sent to users' mobile devices. For each attribute (for example, the appearance of a defined key phrase), the policy defines whether to permit or quarantine the message, and whether a notification should be sent.
4. Predefined policy. TRITON Forcepoint DLP comes with a rich set of predefined policies that cover the data requirements for a wide variety of organizations. They include:
   - Acceptable use policies, such as cyberbullying, obscenities, and indecent images.
   - Content protection policies, such as Password Dissemination, Credit Cards, and Financial Information.
   - Regulations, compliance, and standards policies, such as PCI and federal regulations.
   - Data theft indicator policies, such as Suspected Malicious Dissemination and Disgruntled Employee.
5. Custom policy. This provides the ability for administrators to create custom policies specific to the needs of their organisation.

The severity and action to be taken when policy rules are matched can be managed by the administrator. The administrator can define whether incidents should be triggered every time a rule is matched or for the accumulation of matches for a particular source over time (Drip DLP), and also define how matches are counted, the threshold for triggering the incident, the severity to assign breaches, and the action plan to apply.

The TOE has 2 databases for incident and forensics data:

- The incident database contains information about policy breaches, such as what rule was matched, how many times, what were the violation triggers, what was the date, channel, source, ID, and more.
- The forensics repository contains information about the transaction that resulted in the incident, such as the contents of an email body: From:,To:, Cc: fields; attachments, file name, etc.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(b), FDP_ACF.1(b)

7.1.2.3 Email Protection

The TOE enforces an email policy to provide protection for email systems to prevent malicious threats from entering an organization's network. Each message is processed by a robust set of antivirus and antispam analytics to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

Three types of policies are available, depending on the direction of the email—inbound, outbound, or internal. Message direction is determined on the basisof an organization's protected domains:

- Inbound - The sender address is not from a protected domain, and the recipient address is in a protected domain
- Outbound - The sender address is from a protected domain, and the recipient address is not in a protected domain
- Internal - Both the sender and recipient addresses are in a protected domain.

Policies can also be applied to outbound email communications to protect against the loss of sensitive data. The monitoring of outbound emails includes the following:

- Drip DLP monitoring (see section 7.1.2.2 above) to identify where sensitive data is leaked in small quantities over time.

Email messages can be managed on the basis of:

- **Message properties**: including volume, invalid recipient settings, archive message options, message sender verification, enabling Bounce Address Tag Verification (BATV)
- **Connection options**: using real-time blacklists, reverse DNS verification, reputation service, delaying SMTP greeting, enabling SMPT VRFY command, changing SMTP port)

- **True source IP detection**: using message header information and the number of network hops to an email appliance to determine the IP address of the first sender outside the network perimeter)
- **TLS connections**: forcing connections to or from a specific IP or domain group use mandatory Transport Layer Security (TLS) and determine the security level used by that connection)
- **Directory harvest attacks**: limiting the maximum number of messages and connections coming from an IP address over a given time period
- **Relay control options**: limit the domains and IP address groups for which the server is allowed to relay mail
- **Delivery Routes**: Change the order of a user directory- or domain-based route
- **Rewriting email and domain addresses**: specify recipient address rewrite entries for messages to mask address details and redirect message delivery.
- **URL Sandbox**: real-time analysis of uncategorized URLs that are embedded in inbound email

TOE Security Functional Requirements Satisfied: FDP_ACC.1(c), FDP_ACF.1(c)

7.1.3 Identification and Authentication

7.1.3.1 Administrators

The TOE requires administrators to identify and authenticate themselves with the TOE before gaining access to any of the management functionality available via the web interface or CLI once the TOE is deployed. (The installation CLI is only available when configuring the appliance prior to deployment by directly connecting to the serial port or monitor and keyboard ports on the appliance and does not require administrators to be identified and authenticated when accessing it. This is because it is assumed that an administrator has already been granted physical access to the appliance and identification and authentication is enforced at the CLI once installation has been completed.)

Administrators connect to the TRITON Manager, and are prompted to enter their authentication credentials before access to the Forcepoint TRITON Manager is permitted. Successful authentication to the TRITON Manager provides single sign-on to all TRITON consoles. The TOE maintains a list of administrator usernames, group membership, and passwords for each administrative account, thereby authenticating access to the relevant TRITON console for the administrator.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UID.1.

7.1.3.2 Users

Depending on the web policy applied, unprivileged users are able to browse the internet anonymously. This web traffic is recorded with unknown user identity and the traffic is attributed based on the client IP address. Identification and authentication can be specified in email and web policies, requiring unprivileged users to identify and authenticate themselves before accessing content through the TOE, such as internet browsing or access to email account

Email users have to identify and authenticate themselves to the TOE before they are able to manage their quarantined email messages through the PEM interface provided by Forcepoint Email Security.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2.

7.1.4 Security Management

The TOE provides a web interface that administrators can use to manage all TOE settings, policies, audit logs, administrator accounts, and user accounts. Administrators are able to access management functionality through a series of screens provided by UI framework contain text boxes, radio buttons, dropdown menus, toggle switches, etc, and Adobe Flash elements for the Dashboard. When managing policy rules, administrators can specify alternative values for the default permissive values assigned to the TOE.

Except when in monitoring only mode (in the Forcepoint Web Security module) administrators are logged out of the web interface after a period of thirty minutes of inactivity.

The roles supported by the Forcepoint TRITON Manager infrastructure are:

- Global Security Administrator- this role has permissions to perform all actions in all modules.
- Conditional Super Administrator[9] – this role has the ability to create administrators with the module the role is associated.
- Delegated Administrator – the only Forcepoint TRITON Manager permission this role has is to reset their password. The role has all permissions within the module it is associated.

Delegated administrators are given access to one or more TRITON consoles (Web, Data, Email). They can also be granted access to the one or more Content Gateway Manager instances. The permissions these administrators have in each TRITON Console depend on which Delegated Administrator Role is assigned to the administrators. The TOE maintains nine roles for Delegated Administrators, as detailed in Table 19.

A Global Security Administrator is a user with equivalent Super Administrator access to all TRITON modules (Web Security, Data Security, and Email Security). Only Super Administrators[10] will policy or higher permissions can review the audit data (audit data is distinct from the reports of user incidents that can be reviewed by Reporting Administrators, System Administrators and Group Reporting Administrators, as well as Super Administrators).

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, FMT_SMR.1, FTA_SSL.3.

[9] This role is labelled “Security Administrator” in the Email delegated role.
[10] Including Global Security Administrator and Conditional Super Administrator.

7.1.5 Resource Utilization

The TOE is capable of limiting access of users to a set of content based on a time limit quota. When the user's time quota has been used up, the TOE then blocks all attempts the user makes to access content within those controlled categories. An example of how this might be used is to allow users an hour each day to browse content that is non-conducive to productivity (such as streaming video sites) without completely restricting the content.

The TOE is capable of limiting the allocation of network bandwidth to a list of categories. Administrators define a threshold that the set of categories should not exceed. If the threshold is reached or exceeded for the overall bandwidth usage for a given user for the set of categories, any future attempts by the user to establish a connection via the set of categories are blocked by the TOE until more bandwidth becomes available.

TOE Security Functional Requirements Satisfied: FRU_RSA.1(a), FRU_RSA.1(b).

7.1.6 TOE Access

The TOE is capable of limiting the number of concurrent sessions users can have based on available bandwidth. If a user attempts to establish a new concurrent session while the bandwidth threshold for that type of traffic is met or exceeded, the TOE will block the new session from being established.

The web interface enforces a hard-coded thirty-minute timeout period for administrative sessions. If an administrator is inactive while logged into the web interface for thirty or more minutes, the TOE terminates the session and the administrator must log in again.

TOE Security Functional Requirements Satisfied: FTA_MCS.2, FTA_SSL.3.

7.1.7 Protection of the TSF

Communications to the Forcepoint DLP Endpoint client devices, from the Secondary Forcepoint DLP Server, are transmitted over HTTPS connections. Communications can include Forcepoint DLP policies to be implemented at the client device and actions taken at the client device as a result of policy application. The messages are transferred via HTTPS. The TOE protects these transmissions between the Secondary Forcepoint DLP server component and the Forcepoint DLP Endpoint client device from disclosure and modification by encrypting the transmissions under TLS v1.0, using the ciphersuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (rsa 2048). The cryptographic services specified in Table 20 and Table 21 are provided by the OpenSSL v1.0.1q crypto module to support the protection of the client/server communication. This ciphersuite is applied by default to all communication between the client and server, and in the evaluated configuration the configuration file on the server is updated to ensure this is the only ciphersuite the server will accept. Session keys will be released from memory when the session is terminated.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FCS_CKM.1, FCS_COP.1

7.2 TOE Summary Specification Rationale

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

The following tables provide a mapping between the TOE's Security Functions and the SFRs.

TSF SFR	Security Audit	User Data Protection	Identification & Authentication	Security Management	Protection of TOE Security Functions	Resource Utilization	TOE Access	Protection of TSF
FAU_GEN_EXT.1	✓							
FAU_SAR.1	✓							
FAU_SAR.2	✓							
FDP_ACC.1(a)		✓						
FDP_ACF.1(a)		✓						
FDP_ACC.1(b)		✓						
FDP_ACF.1(b)		✓						
FDP_ACC.1(c)		✓						
FDP_ACF.1(c)		✓						
FIA_ATD.1			✓					
FIA_UAU.1			✓					
FIA_UAU.2			✓					
FIA_UID.1			✓					
FIA_UID.2			✓					
FMT_MOF.1				✓				
FMT_MSA.1(a)				✓				
FMT_MSA.1(b)				✓				
FMT_MSA.3(a)				✓				
FMT_MSA.3(b)				✓				
FMT_MSA.3(c)				✓				
FMT_MTD.1				✓				
FMT_SAE.1				✓				
FMT_SMF.1				✓				
FMT_SMR.1				✓				
FPT_STM.1					✓			
FRU_RSA.1(a)						✓		
FRU_RSA.1(b)						✓		
FTA_MCS.2							✓	
FTA_SSL.3							✓	
FPT_ITT.1								✓

TSF / SFR	Security Audit	User Data Protection	Identification & Authentication	Security Management	Protection of TOE Security Functions	Resource Utilization	TOE Access	Protection of TSF
FCS_CKM.1								✓
FCS_COP.1								✓

Table 27 – SFR to TOE Security Functions Mapping