Proofpoint, Inc.

Proofpoint Protection Server® v5.0.4

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.8

Prepared for:

Proofpoint, Inc.
892 Ross Drive
Sunnyvale, CA 94089
Phone: (408) 517-4710
Fax: (408) 517-4711

http://www.proofpoint.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2008-01-16	Amy Nicewick	Initial draft.
0.2	2008-01-29	Amy Nicewick	Updated cover page, SFR names.
0.3	2008-05-01	Amy Nicewick	Addressed PETR 1.0.
0.4	2008-07-30	Amy Nicewick	Addressed verdicts.
0.5	2008-08-05	Amy Nicewick	Addressed verdicts.
0.6	2008-08-26	Amy Nicewick	Addressed verdict.
0.7	2008-09-08	Amy Nicewick	Changed version of Mozilla Firefox.
0.8	2008-10-08	Amy Nicewick	Added registered trademark to TOE name.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the Proofpoint, Inc. Proofpoint Protection Server v5.0.4, and will hereafter be referred to as the TOE throughout this document. The TOE is the Proofpoint Protection Server v5.0.4 (PPS), an enterprise messaging security solution that defends against inbound and outbound messaging threats.

1.1 Purpose

- This ST provides mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats in the following sections:
- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications that relate to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	Proofpoint, Inc. Proofpoint Protection Server® v5.0.4 Security Target
ST Version	Version 0.8
Author	Corsec Security, Inc. Amy Nicewick
TOE Identification	Proofpoint, Inc. Proofpoint Protection Server® v5.0.4 build 176
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (aligned with ISO[1]/IEC[2] 15408:2005); CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted Common Evaluation Methodology (CEM) as of 2008/01/28 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level (EAL)	EAL2+ (Augmented with ALC_FLR.1)
Keywords	Proofpoint, PPS, anti-spam, anti-virus, zero hour, email, firewall

1.3 Conventions and Terminology

1.3.1 Conventions

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

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements of the text of the SFRs are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement. Refinements of the name of the SFRs are identified using *italicized text in the SFR title* (e.g., Security alarms *for Spam Detection*).
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

[1] ISO – International Organization for Standardization
[2] IEC – International Electrotechnical Commission

1.3.2 Terminology

Regulatory Compliance – Compliance with United States federal regulations regarding non-public information, such as protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA), and personal financial information as defined by the Gramm-Leach-Bliley Act (GLBA).

Digital Assets – Confidential corporate documents, such as internal memos, specifications, press releases, price lists, and organizational charts.

2 TOE Description

The TOE Description provides an overview of the TOE. This section describes the general capabilities and security functionality of the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type, describing the product, and defining the specific evaluated configuration.

2.1 Product Type

Proofpoint Protection Server® (PPS) is a perimeter email gateway software that integrates virus protection, spam detection, regulatory compliance, and digital asset protection into a comprehensive message management solution.

2.2 Product Description

PPS is designed to defend an Information Technology (IT) environment from internal and external email-based threats by scanning all inbound and outbound emails for spam, viruses, connection-level attacks, prohibited text, and other user-definable data. Customers who deploy PPS are typically concerned with one or more of the following:

- Preventing the receipt of spam
- Preventing the sending or receipt of offensive emails
- Ensuring email compliance with various regulations, such as HIPAA
- Protecting the privacy and security of customer, company, and employee data, such as Social Security Numbers
- Preventing the loss of intellectual property and trade secrets

PPS is available for purchase in three forms:

- PPS software only (to be installed on customer-provided hardware)
- As a VMWare Virtual Appliance (to be run on customer-provided hardware via VMWare Player, Workstation, Server, or ESX Server)
- As a stand-alone appliance (called the Proofpoint Messaging Security Gateway)

The TOE is defined as a software-only TOE that is installed on an appliance (Proofpoint Messaging Security Gateway) provided by Proofpoint. The appliance hardware and proprietary Linux Operating System (PLINX) are defined in Section 2.3 as part of the IT environment outside the TOE boundary. The PPS supported digest email clients, which are excluded from the evaluation, include:

Microsoft Outlook
Microsoft Outlook Express
Microsoft Outlook Web Access 5.5, 2000, and 2003
Mozilla Thunderbird 2
Netscape 7.1 Email
Webmail – Lotus iNotes, Lotus Notes, Messenger Express, and Microsoft Outlook Web Access
Lotus R5 version 5.0.12 or later, Lotus R6.5 email clients

Figure 1 below shows the details of a typical deployment configuration of the TOE:

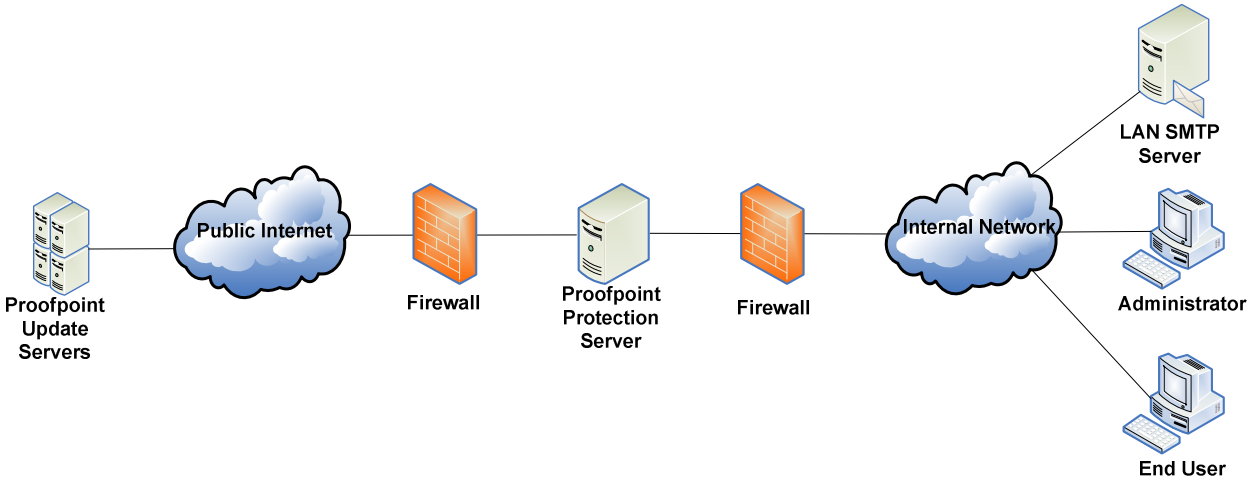

Figure 1 – Typical Deployment Configuration of the TOE[3]

2.2.1 Brief Description of the Various Components of the TOE

The functionality, databases, files, external interfaces, and other components that compose the PPS software include the following:

- Filtering Agent
- Reinject Queue
- Quarantine Consolidation functionality
- Log Consolidation and Summary functionality
- Update Utilities
- Web Servers (e.g., End-user Web Server, Admin Web Server, and API Service Web Server)
- Log Files
- MySQL databases (e.g., Message Queue Database, Quarantine Database, Log Database, User Database, etc.)

PPS offers a web-based management interface for reporting, configuration, and management tasks. Administrators can access the management functionality remotely over HTTPS. End users can manage their own email message digests remotely over Secure Hypertext Transfer Protocol (HTTPS). In addition, PPS can automatically retrieve signature and software updates from Proofpoint-administered servers over HTTPS. The Dynamic Update Service distributes and manages the latest module updates, software patch updates, or system upgrades from the Proofpoint-hosted update servers. PPS can also integrate with enterprise identity management systems such as Active Directory, Domino Directory, and other LDAP-based sources using LDAPS, as well as a Domain Name Service (DNS) server.

The majority of PPS's main functionality is performed by the Filtering Agent. This component includes the following functionality:

- Spam detection: checks for matches with known Spam signatures
- Regulatory compliance: provides policy-based filtering for violations of privacy-based or financial transaction regulations

[3] LAN – Local Area Network; SMTP – Simple Mail Transfer Protocol

- Digital asset protection: protects confidential information from accidental or deliberate disclosure via email
- Email firewall: provides policy-based allow/deny functionality for email traffic
- Virus Protection: interacts with third-party Anti-Virus engines to scan emails for viruses
- Zero hour attack prevention: periodically checks with Commtouch (a Proofpoint partner) for signatures of botnet attacks and other emerging attacks

Sendmail[4] receives all incoming emails and passes the SMTP commands and data to the Filtering Agent for processing. Depending on the licensing and configuration of the system, the messages are processed in a given order by the activated modules of the Filtering Agent (listed above). Those messages that the Filtering Agent matches to signatures are either placed into a quarantine database, modified, discarded, or rejected. All modification commands are passed back to Sendmail prior to delivery of the email to an external SMTP server. Administrators and End Users may view the emails in the quarantine database and release them if they choose.

All receipt and processing of emails is logged in the Log Files. There are log files for the following types of information:

- activity generated by the filtering agents
- activity generated by End User Digests
- messages passed from Sendmail to the Proofpoint Protection Server for filtering (this applies only on versions of PPS deployed on a Proofpoint appliance)
- activity generated by administration server login

The log files are periodically consolidated and deleted by the Log Consolidation component, which reformats and combines the data from these ASCII log files and inserts them into the Log Database. The Log Summary component periodically scans the Log Database and generates summary reports that are also entered into the Log Database for later viewing by Administrators.

There are three separate instances of Apache Web Server running in the PPS: the End User Web Server, the Admin Web Server, and the Application Programming Interface (API) Service Web Server. The End User Web Server provides a web-based interface for end users to log in and manage their personal email quarantines. Once end users are authenticated against credentials stored in the User Database, they are able to manage the emails in their quarantines. The Admin Web Server provides a more feature-rich version of the End User Web Server for use by PPS administrators. Successfully authenticated administrators may manage not only all emails in the quarantine database, but also the logs in the Log Database, the user credentials in the User Database, and the configuration of the entire product. (PPS does provide a Command Line Interface (CLI), but it is excluded from this evaluation.)

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the TOE are included in evaluation.

2.3.1 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 perimeter email gateway software which runs on a proprietary Linux Operating System (PLINX), and hardware compliant to the minimum software and hardware requirements as listed in Section 2.3.1.1. The TOE is installed on hardware installed in a network environment. The evaluated configuration of the TOE is a single-appliance deployment. The physical TOE boundary and a typical TOE deployment are depicted in Figure 2 below.

[4] Sendmail is part of the TOE environment.

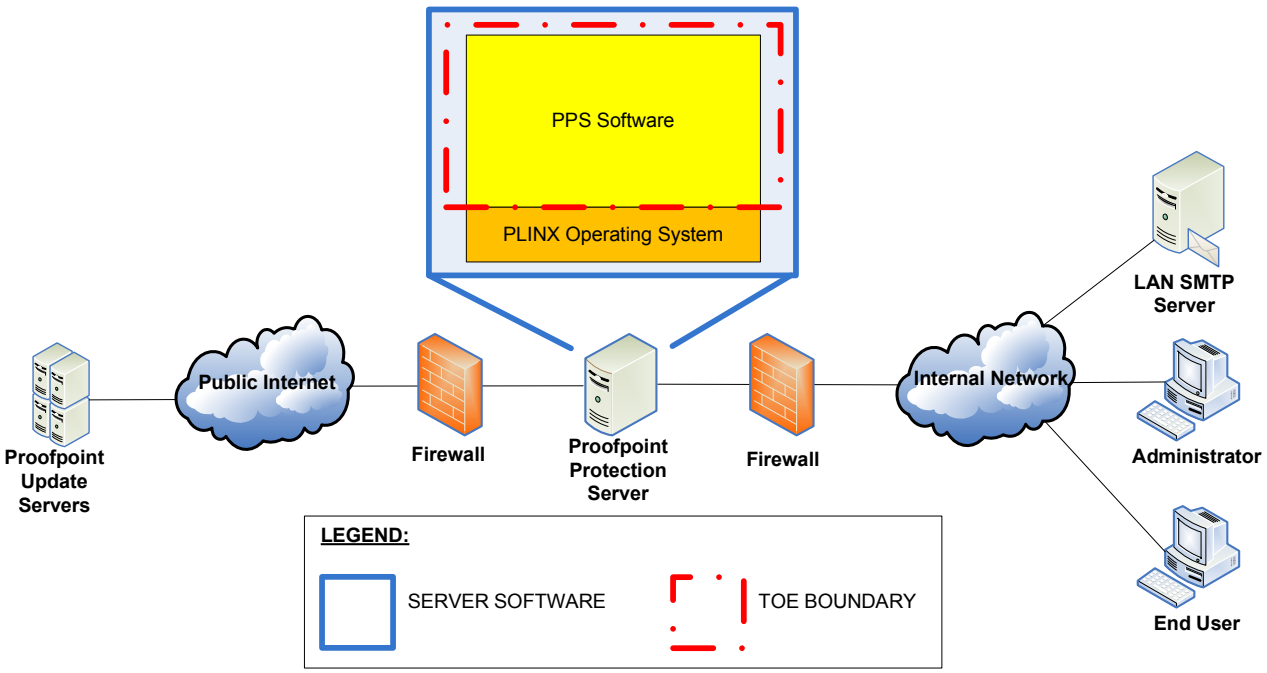

Figure 2 - Physical TOE Boundary

2.3.1.1 TOE Supporting Software and Hardware

The following list specifies the minimum system requirements for the proper operation of the TOE:

- PLINX Operating System v5.0.4.176 (proprietary Proofpoint OS)
- Minimum memory size: 2 Gigabytes (GB)
- Minimum available disk space: 80 GB
- X86 processor (Pentium 4, Xeon, Core, Core 2, Athlon, or Opteron)
- Sendmail v8.13.16

For purposes of the CC evaluation, the TOE was tested on the Proofpoint Messaging Security Gateway appliance, model number 840.

PPS supported browsers include:

Microsoft® Internet Explorer 6.0 or higher
Mozilla Firefox 2.0 or higher

2.3.2 Logical Boundary

The security functional requirements implemented by the TOE are usefully grouped under the following Security Functional Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)

2.3.2.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit data. Administrators can configure log retention periods and the level of information collected. Administrators can also view log entries through the management interface or through system log files.

Violation analysis is performed by comparing customer-defined policies against incoming and outgoing emails to determine if they contain spam, viruses, or other content violations. Analysis on the system functions is also performed. Security alarms are then issued by the TOE for spam detection, content match, mail policy violations, and system events.

2.3.2.2 User Data Protection

The TOE allows authorized administrators to enforce a rigid policy for users and administrators accessing the TOE. Super-user administrators can create Super-user accounts and Limited Administrator accounts for other administrators with pre-defined privilege levels. For new Limited Administrator accounts, the Super-user can set which modules the Limited Administrator may manage.

There is no way for a Limited Administrator to change his own role, or grant himself additional privileges. Privilege levels are pre-defined and only a Super-user administrator can change them. Super-user administrators cannot change their own permission level.

Authorized administrators can also create groups and End User accounts with pre-defined permissions.

Using the Administrative Interface, administrators with appropriate permissions can craft policies to manage the email traffic.

End Users may also be configured to allow the users to manage their emails through a web browser. End Users may use browser links to process End User Digest actions such as releasing messages and requesting a safelist.

2.3.2.3 Identification and Authentication

Administrators and end users must be authenticated before they can perform any management tasks on the TOE or TOE data. Administrators authenticate with a userid and password through a web browser, and, once authenticated, can perform the management tasks for which they have been given access. End users may authenticate with a userid and password through a web browser, and, once authenticated, can perform management tasks on their end user digests and anti-spam policies.

2.3.2.4 Security Management

The TOE supports two administrative roles: Super-users (user id “admin”) and Limited Administrators. Super-users have full privileges to add, change, and delete other administrators from the system, as well as to configure and access all components of the TOE. Limited Administrators have limited access to specific components on the TOE, as configured by the Super-user. Super-users configure access by End Users to End User Digests as appropriate.

2.3.2.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features. These features include identification and authentication.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

All features and functionality of the TOE discussed in this document are included in the evaluated configuration, with the following exceptions:

- CLI (except for initial configuration)
- Simple Network Management Protocol (SNMP) v1 and v2
- Network Content Sentry (NCS)
- Secure Messaging
- POP3 retrieval of end user digest
- Use of LDAP by filtering modules for recipient verification
- SSH for remote administration
- SMTP Turbocharge

3 Security Environment

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:

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

3.1 Assumptions

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

Table 2 - Assumptions

Name	Description
A.DB_INTEGRITY	The integrity of data maintained by the MySQL database is always ensured.
A.DNS	DNS information received by the TOE is reliable.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.NO_EVIL	Authorized administrators are non-hostile and are appropriately trained to use, configure and maintain the TOE.
A.PHYS_SEC	The TOE resides in a physically controlled access facility that prevents unauthorized physical access.

3.2 Threats to Security

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

Attackers who are not TOE administrators: 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/parameters and no physical access to the TOE.

TOE administrators: 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/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 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.

The following threats are applicable:

Table 3 - Threats

Name	Description
T.RESOURCE_CONSUME	Threat agents may flood the TOE with spam, consuming resources such as memory, bandwidth, processor time, and data storage, and thus limit the TOE's ability to execute its security functions efficiently.
T.EMAIL_FIREWALL	A threat agent may try to violate the mail dissemination policy of the TOE by sending information that is identified as inappropriate because of its origin, destination, or subject content.
T.VIRUS	A threat agent may try to violate the mail dissemination policies of the TOE by sending information containing a virus or an emerging virus.
T.REG_COMP	A threat agent may circulate non-public information through the TOE in violation of its mail policy.
T.DIGITAL_ASSETS	A threat agent may circulate confidential information through the TOE in violation of its mail policy.
T.SYS_FAILURE	A threat agent may take advantage of unexpected termination of one or more of the TOE's Security Functions (SF) and send inappropriate information through the TOE in violation of its policies.

Name	Description
T.NO_AUDIT	A threat agent may perform security-relevant operations on the TOE without being held accountable for it.
T.NEW_EXPLOITS	A threat agent may modify the message content suitably or use variants in the send or recipient information in order to defeat the protection services offered by the TOE.
T.BYPASS	A threat agent may bypass one or more of the TOE's security functions and send malicious data through the TOE to the End Users.
T.BRUTE_FORCE	A threat agent may repeatedly try to guess authentication data in order to gain unauthorized access to the TOE.
T.IA	A threat agent may attempt to compromise the TOE by attempting actions that it is not authorized to perform on the TOE.
TE.AUTH_CAPTURE	A threat agent may execute a process on the TOE that captures the authentication data of a valid user of the TOE in order to gain unauthorized access to the TOE.
TE.INFO_CAPTURE	An external attacker or malicious insider may sniff the communication channel between the TOE and an external IT entity in order to capture or modify messages, authentication data, or other information sent between the two.
TE.MASQUERADE	A threat agent masquerading as the TOE may capture valid identification and authentication data for a legitimate user of the TOE in order to gain unauthorized access to the TOE.

3.3 Organizational Security Policies

There are no Organizational Security Policies defined for this TOE.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment to meet the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

Table 4 - Security Objectives for the TOE

Name	Description
O.SPAM	The TOE shall be able to define characteristics for spam and take configured action when such characteristics are recognized.
O.EMAIL_FIREWALL	The TOE shall be able to prevent specific types of information being sent to or from specific entities, and shall take specified actions on incoming messages based on their sender address, recipient address, or message or attachment content.
O.VIRUS	The TOE shall take specified actions on incoming messages identified as containing a virus or an emerging virus.
O.REG_COMP	The TOE shall take specified actions on outgoing messages identified as containing non-public information.
O.DIGITAL_ASSETS	The TOE shall take specified actions on outgoing messages identified as containing confidential information.
O.NOTIFICATION	The TOE shall generate and deliver alerts upon detecting failure of any of its functional components.
O.LOG	The TOE shall generate logs of all the security-relevant operations performed on the TOE.

Name	Description
O.CONFIG	The TOE shall provide administrative tools to enable authorized administrators to effectively configure and maintain the TOE.
O.REF_MED	All inbound or outbound mail into or out of the TOE, unless explicitly allowed by the TOE administrator, shall be examined by each of the TOE's configured filters before being forwarded to its destination.
O.BOUNDED_AUTH	The TOE shall bound the number of failed authentication attempts to some configurable value in order to prevent brute force attacks against the TOE.
O.AUTHENTICATION	The TOE shall require that users of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.
O.SEC_ACCESS	The TOE shall ensure that only those authorized users are granted access to the security functions, configurations, and associated data.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

Table 5 - IT Security Objectives

Name	Description
OE.DOMAIN_SEP	The IT Environment shall ensure that the execution of code within the TOE cannot be interfered with or tampered with by any untrusted subject.
OE.TIMESTAMP	The IT Environment must provide reliable timestamps to the TOE.

Name	Description
OE.TRUSTED_INFO	Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.

4.2.2 Non-IT Security Objectives

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

Table 6 - Non-IT Security Objectives

Name	Description
NOE.TRUSTED_ENV	The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 7 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 7 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_ARP.1(a)	Security alarms for Spam Detection		✓	✓	✓
FAU_ARP.1(b)	Security alarms for Email Firewall policy violation		✓	✓	✓
FAU_ARP.1(c)	Security alarms for Virus Detection		✓	✓	✓
FAU_ARP.1(d)	Security alarms for Regulatory Compliance policy violation		✓	✓	✓
FAU_ARP.1(e)	Security alarms for Digital Assets policy violation		✓	✓	✓
FAU_ARP.1(f)	Security alarms for System Alert Notification		✓	✓	✓
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAA.1(a)	Potential violation analysis for Spam Detection		✓		✓
FAU_SAA.1(b)	Potential violation analysis for Email Firewall policy		✓		✓
FAU_SAA.1(c)	Potential violation analysis for Virus Detection		✓		✓
FAU_SAA.1(d)	Potential violation analysis for Regulatory Compliance policy		✓		✓
FAU_SAA.1(e)	Potential violation analysis for Digital Assets policy		✓		✓

Name	Description	S	A	R	I
FAU_SAA.1(f)	Potential violation analysis for System Alert Notification		✓		✓
FAU_SAR.1	Audit review		✓		
FAU_SEL.1	Selective audit	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data		✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP				

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

Section 5.1 contains the security functional requirement components from the Common Criteria (CC) Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

FAU_ARP.1(a) Security alarms *for Spam Detection*

Hierarchical to: No other components.

FAU_ARP.1.1(a)

The TSF shall take [*one or more of the following actions*] upon ~~detection of a potential security violation~~. **detection of spam in the email message:**

a) Continue filtering the message through all filtering modules
b) Reject the message with an SMTP return code and text
c) Retry – temporarily reject the message due to resource constraints with an SMTP return code and text
d) Discard – accept the message but discard it without providing any information to the sender
e) Re-route the message to another SMTP server
f) If the Quarantine option is selected, the TOE will send a copy of the message to the quarantine database
g) If the Audit Folder option is selected, the TOE will send a copy of the message to the quarantine audit folder
h) If the Change Subject option is selected, the TOE will replace the text in the subject line of the original message
i) If the Change Message Headers option is selected, the TOE will add, delete, or modify the selected email headers
j) If the Annotate Message option is selected, the TOE will annotate the message as configured
k) If the Add Recipients option is selected, the TOE will send the message to additional configured email addresses
l) If the Delete Attachments option is selected, the TOE will remove any attachments from the original message
m) If the Redirect Message option is selected, the TOE will send the original message to a configured email address other than the original recipient's, or place it in the configure folder
n) If the Reply to Sender option is selected, the TOE will send a new email message to the original sender
o) If the Send Message option is selected, the TOE will send a new email message to the original recipient
p) If the Stop Other Rules option is selected, the TOE will stop processing a message once a condition is met of the same SMTP callback that triggers a rule in a given filtering agent module

Dependencies: FAU_SAA.1(a) Potential violation analysis *for Spam Detection*

FAU_ARP.1(b) Security alarms *for Email Firewall policy violation*

Hierarchical to: No other components.

FAU_ARP.1.1(b)

The TSF shall take [*one or more of the following actions*] upon ~~detection of a potential security violation~~. **detection of specific Internet Protocol (IP) address or message content violations in email messages or their attachments:**

a) Deliver the message to the email infrastructure without further processing by the TOE
b) Continue filtering the message through all filtering modules
c) Reject the message with an SMTP return code and text
d) Retry – temporarily reject the message due to resource constraints with an SMTP return code and text

e) Discard – accepts the message but discards it without providing any information to the sender
f) Re-route the message to another SMTP server
g) If the Quarantine option is selected, the TOE will send a copy of the message to the quarantine database
h) If the Audit Folder option is selected, the TOE will send a copy of the message to the quarantine audit folder
i) If the Change Subject option is selected, the TOE will replace the text in the subject line of the original message
j) If the Change Message Headers option is selected, the TOE will add, delete, or modify the selected email headers
k) If the Annotate Message option is selected, the TOE will annotate the message as configured
l) If the Add Recipients option is selected, the TOE will send the message to additional configured email addresses
m) If the Delete Attachments option is selected, the TOE will remove any attachments from the original message
n) If the Redirect Message option is selected, the TOE will send the original message to a configured email address other than the original recipient's, or place it in the configure folder
o) If the Reply to Sender option is selected, the TOE will send a new email message to the original sender
p) If the Send Message option is selected, the TOE will send a new email message to the original recipient
q) If the Stop Other Rules option is selected, the TOE will stop processing a message once a condition is met of the same SMTP callback that triggers a rule in a given filtering agent module
r) If the Sender Policy Framework protocol is enabled, and the Influence Spam MLX Score option is selected, the TOE will change the spam score for the message or classify the message as spam or not spam, according to configured policy

Dependencies: FAU_SAA.1(b) Potential violation analysis *for Email Firewall Violation*

FAU_ARP.1(c) Security alarms *for Virus Detection*

Hierarchical to: No other components.

FAU_ARP.1.1(c)

The TSF shall take [*one or more of the following actions*] upon detection of ~~a potential security violation~~ **a virus in the email by the Virus Detection Filter or Zero-Hour Anti-Virus Filter:**

a) Continue filtering the message through all filtering modules
b) Reject the message with an SMTP return code and text
c) Retry – temporarily reject the message due to resource constraints with an SMTP return code and text
d) Discard – accepts the message but discards it without providing any information to the sender
e) Re-route the message to another SMTP server
f) If the Quarantine option is selected, the TOE will send a copy of the message to the quarantine database
g) If the Audit Folder option is selected, the TOE will send a copy of the message to the quarantine audit folder
h) If the Change Subject option is selected, the TOE will replace the text in the subject line of the original message
i) If the Change Message Headers option is selected, the TOE will add, delete, or modify the selected email headers
j) If the Annotate Message option is selected, the TOE will annotate the message as configured
k) If the Add Recipients option is selected, the TOE will send the message to additional configured email addresses
l) If the Delete Attachments option is selected, the TOE will remove any attachments from the original message

m) If the Redirect Message option is selected, the TOE will send the original message to a configured email address other than the original recipient's, or place it in the configure folder
n) If the Reply to Sender option is selected, the TOE will send a new email message to the original sender
o) If the Send Message option is selected, the TOE will send a new email message to the original recipient
p) If the Stop Other Rules option is selected, the TOE will stop processing a message once a condition is met of the same SMTP callback that triggers a rule in a given filtering agent module
q) If the Attempt to Clean Infected Messages parameter is enabled, the TOE will attempt to clean the message according to configured policy

Dependencies: FAU_SAA.1(c) Potential violation analysis *for Virus Detection*

FAU_ARP.1(d) Security alarms *for Regulatory Compliance policy violation*

Hierarchical to: No other components.

FAU_ARP.1.1(d)

The TSF shall take [*one or more of the following actions*] upon detection of a potential security violation **in Regulatory Compliance policy:**

a) Continue filtering the message through all filtering modules
b) Reject the message with an SMTP return code and text
c) Retry – temporarily reject the message due to resource constraints with an SMTP return code and text
d) Discard – accepts the message but discards it without providing any information to the sender
e) Re-route the message to another SMTP server
f) If the Quarantine option is selected, the TOE will send a copy of the message to the quarantine database
g) If the Audit Folder option is selected, the TOE will send a copy of the message to the quarantine audit folder
h) If the Change Subject option is selected, the TOE will replace the text in the subject line of the original message
i) If the Change Message Headers option is selected, the TOE will add, delete, or modify the selected email headers
j) If the Annotate Message option is selected, the TOE will annotate the message as configured
k) If the Add Recipients option is selected, the TOE will send the message to additional configured email addresses
l) If the Delete Attachments option is selected, the TOE will remove any attachments from the original message
m) If the Redirect Message option is selected, the TOE will send the original message to a configured email address other than the original recipient's, or place it in the configure folder
n) If the Reply to Sender option is selected, the TOE will send a new email message to the original sender
o) If the Send Message option is selected, the TOE will send a new email message to the original recipient
p) If the Stop Other Rules option is selected, the TOE will stop processing a message once a condition is met of the same SMTP callback that triggers a rule in a given filtering agent module
r) If the Sender Policy Framework protocol is enabled, and the Influence Spam MLX Score option is selected, the TOE will change the spam score for the message or classify the message as spam or not spam, according to configured policy

Dependencies: FAU_SAA.1(d) Potential violation analysis *for Regulatory Compliance Policy Violation*

FAU_ARP.1(e) Security alarms *for Digital Assets policy violation*

Hierarchical to: No other components.

FAU_ARP.1.1(e)

The TSF shall take [*one or more of the following actions*] upon detection of a potential security violation **in Digital Assets policy:**

a) Continue filtering the message through all filtering modules
b) Reject the message with an SMTP return code and text
c) Retry – temporarily reject the message due to resource constraints with an SMTP return code and text
d) Discard – accepts the message but discards it without providing any information to the sender
e) Re-route the message to another SMTP server
f) If the Quarantine option is selected, the TOE will send a copy of the message to the quarantine database
g) If the Save Document Content by Default parameter is enabled, the TOE will send a copy of the document in the Document Repository
h) If the Audit Folder option is selected, the TOE will send a copy of the message to the quarantine audit folder
i) If the Change Subject option is selected, the TOE will replace the text in the subject line of the original message
j) If the Change Message Headers option is selected, the TOE will add, delete, or modify the selected email headers
k) If the Annotate Message option is selected, the TOE will annotate the message as configured
l) If the Add Recipients option is selected, the TOE will send the message to additional configured email addresses
m) If the Delete Attachments option is selected, the TOE will remove any attachments from the original message
n) If the Redirect Message option is selected, the TOE will send the original message to a configured email address other than the original recipient's, or place it in the configure folder
o) If the Reply to Sender option is selected, the TOE will send a new email message to the original sender
p) If the Send Message option is selected, the TOE will send a new email message to the original recipient
q) If the Stop Other Rules option is selected, the TOE will stop processing a message once a condition is met of the same SMTP callback that triggers a rule in a given filtering agent module
s) If the Sender Policy Framework protocol is enabled, and the Influence Spam MLX Score option is selected, the TOE will change the spam score for the message or classify the message as spam or not spam, according to configured policy

Dependencies: FAU_SAA.1(e) Potential violation analysis *for Digital Assets Policy Violation*

FAU_ARP.1(f) Security alarms *for System Alert Notification*

Hierarchical to: No other components.

FAU_ARP.1.1(f)

The TSF shall take [*one or more of the following actions*] upon detection of a ~~potential security violation~~ **system alert condition:**

a) Generate an email or html message to the configured address

Dependencies: FAU_SAA.1(f) Potential violation analysis *for System Alert Notification*

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

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

c) [*events listed in Table 8*].

Table 8 - Auditable Events

Component	Auditable Event	Additional Audit Record Contents
FAU_ARP.1(a)	Actions taken due to detection of spam	Policy that was matched, message details
FAU_ARP.1(b)	Actions taken due to imminent security violations in firewall policy	Policy that was matched, message details
FAU_ARP.1(c)	Actions taken due to virus detection	Policy that was matched, message details
FAU_ARP.1(d)	Actions taken due to imminent security violations in regulatory compliance policy	Policy that was matched, message details
FAU_ARP.1(e)	Actions taken due to imminent security violations in digital assets policy	Policy that was matched, message details
FAU_ARP.1(f)	Actions taken due to system alert events	Notification event that was generated

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity, 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, [*events listed in Table 8*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAA.1(a) Potential violation analysis *for Spam Detection*

Hierarchical to: No other components.

FAU_SAA.1.1(a)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2(a)

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*following events:*

a. messages identified as spam

b. messages identified as probable spam.

c. messages identified as adult spam]

known to indicate a potential security violation;

b) [*additional rules as follows:*

a. If an Optout policy is enabled, the TOE will continue to filter the message

b. If no Optout policy is enabled, the TOE will assign a disposition to the message based on the assigned spam score.

].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1(b) Potential violation analysis *for Email Firewall Policy*

Hierarchical to: No other components.

FAU_SAA.1.1(b)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2(b)

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*following events:*

a. messages sent by a specific domain

b. messages destined to a specific user, group, or domain.

c. messages or their attachments containing specific text]

known to indicate a potential security violation;

b) [*additional rules as follows:*

a. If the sender of a message is listed on the Trusted Source List, the TOE delivers the message with no further processing.

b. If the sender of a message is listed on the Blocked List, the TOE rejects the message with no further processing.

].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1(c) Potential violation analysis *for Virus Detection*

Hierarchical to: No other components.

FAU_SAA.1.1(c)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2(c)

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*following events:*

a. messages identified as containing a virus or potential zero-hour virus]

known to indicate a potential security violation;

b) [*additional rules as follows:*

a. If the message is corrupt or missing information, the TOE will process the message according to configured policy

b. If the message is password-protected or contains encrypted data, the TOE will discontinue virus detection filtering

c. If the message contains riskware or spyware, the TOE will discard the message, and send a copy of the message to the quarantine with a new subject header.

d. If the Zero-Hour Anti-Virus module classifies the message as "probable" or "suspected", the original message will be discarded, and a copy will be sent to the quarantine database until new virus signature files are downloaded, then resubmitted to the Virus Detection Module

].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1(d) Potential violation analysis *for Regulatory Compliance Policy*

Hierarchical to: No other components.

FAU_SAA.1.1(d)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2(d)

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*following events:*

a. messages or attachments identified as containing non-public information]

known to indicate a potential security violation;

b) [*no additional rules*].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1(e) Potential violation analysis *for Digital Assets policy*

Hierarchical to: No other components.

FAU_SAA.1.1(e)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2(e)

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*following events:*

a. messages or attachments identified as containing confidential information]

known to indicate a potential security violation;

b) [*no additional rules*].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1(f) Potential violation analysis *for System Alert Notification*

Hierarchical to: No other components.

FAU_SAA.1.1(f)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2(f)

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*following events:*

a. *available system disk space falls below configured threshold*

b. *available TOE disk space falls below configured threshold*

c. *number of messages in an SMTP queue goes above configured threshold*

d. *number of messages for a recipient domain goes above configured threshold*

e. *server is unable to connect to the update server after configured number of tries*

f. *number of messages in Quarantine Queue goes above configured threshold*

g. *number of hours elapsed since the spam engine was last updated goes above configured threshold*

h. *number of hours elapsed since the spam definition files were last updated goes above configured threshold*

i. *number of hours elapsed since the virus engine was last updated goes above configured threshold*

j. *number of hours elapsed since the virus definition files were last updated goes above configured threshold*]

known to indicate a potential security violation;

b) [*no additional rules.*

].

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*Super-users*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1

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

a) [*event type*]

b) [*log file level*].

Dependencies: FAU_GEN.1 Audit data generation, FMT_MTD.1 Management of TSF data

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

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

FAU_STG.1.2

The TSF shall be able to [*prevent*] unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*Access control SFP*] on

[

Subjects: identified and authenticated TOE users;

Objects: data stored on the TOE; and

Operations: All interactions between Subjects and Objects

].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *User role,*
2. *User ID,*
3. *User's permissions*

And Object attributes:

1. *Permissions assigned to objects,*
2. *Absence of permissions assigned to objects*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the subject is the TOE Super-user, then access is granted.*
2. *If a subject requests access to an object that has no assigned permissions, then access is granted.*
3. *If a subject who is not a TOE Super-user requests access to an object that has assigned permissions, the permissions of the subject are examined to determine if the subject has permission to access the object. If a match is found, access is granted.*
4. *If none of the about rules apply, access is denied.*

].

FDP_ACF.1.3

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

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

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

5.1.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [*an administrator configurable positive integer within [1 to 99]*] unsuccessful authentication attempts occur related to [*administrative access authentication attempts*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [*lock out the sending IP address for a configurable period of time*].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [

a) *spam detection filter*

b) *email firewall filter*

c) *virus detection filter*

d) *zero-hour virus detection filter*

e) *regulatory compliance filter*

f) *digital assets filter*

] to [*authorised administrators*].

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Access Control SFP*] to restrict the ability to [*change_default, query, modify, delete*] the security attributes [*management of own password, Appliance configurations, End User Digest configurations, Digital Asset configuration, Email Alert configuration, Email Firewall configuration, Groups and Users configuration, Logs and Reports configuration, Password Policy configuration, Quarantine configuration, Regulatory Compliance configuration, Server Management configuration, Spam Detection configuration, System configuration, Virus Protection configuration, management of End User Digest settings, selection of spam policies, enforcement of module rules, uploading of confidential information to the Document Repository, and report false negatives*] to [*Super-users, Limited Administrators, and End Users who have permission to perform the action on that attribute*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*Super-user*] 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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*perform operations as specified in Table 9*] the [*list of TSF data as specified in Table 9*] to [*authorised administrators*].

Table 9 – Management of TSF data

Functional Component	Operation	TOE Data
FAU_ARP.1(a)	Change	Action taken when spam is detected
FAU_ARP.1(b)	Change	Action taken when firewall policy rules are matched
FAU_ARP.1(c)	Change	Action taken when a virus is detected
FAU_ARP.1(d)	Change	Action taken when regulatory compliance policy rules are matched
FAU_ARP.1(e)	Change	Action taken when digital assets policy rules are matched
FAU_ARP.1(f)	Change	Action taken when system alerts are generated
FAU_SAA.1(a)	Add, modify, remove	Spam detection rules
FAU_SAA.1(b)	Add, modify, remove	Email firewall policy rules

Functional Component	Operation	TOE Data
FAU_SAA.1(c)	Add, modify, remove	Virus and zero-hour virus detection rules
FAU_SAA.1(d)	Add, modify, remove	Regulatory compliance policy rules
FAU_SAA.1(e)	Add, modify, remove	Digital assets policy rules
FAU_SAA.1(f)	Modify	System alert notification rules
FAU_SAR.1	Add, modify, remove	Group of users allowed to read audit records
FAU_SEL.1	Add, modify, remove	Rights to view or change auditable events
FIA_AFL.1	Modify	Number of failed authentication attempts before lockout
FIA_UAU.2	Add, modify, remove	Authorised administrative and end-user passwords
FIA_UID.2	Add, modify, remove	Authorised administrative and end-user usernames
FMT_MOF.1	Modify	Roles that can interact with the TSF
FMT_MTD.1	Add, modify, remove	Group of users that can interact with the TSF data
FMT_SMR.1	Add, modify, remove	Group of users that are part of a role

Dependencies: **FMT_SMF.1 Specification of management functions**

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [

a) Add, remove, and modify rules that identify messages as spam

b) Add, remove, and modify rules that identify messages that should be restricted based on sender, recipient, or content

c) Add, remove, and modify rules that identify messages that contain viruses and potential zero-hour viruses

d) Add, remove, and modify rules that identify messages that contain non-public information

e) Add, remove, and modify rules that identify messages that contain confidential information

f) Add, remove, and modify rules that identify HTTP and FTP posts that contain non-public or confidential information

g) Modify rules that map security-relevant events that occur on the TOE to different alert mechanisms

h) Enable and disable the spam detection filter, email firewall filter, virus detection filter, zero-hour virus detection filter, regulatory compliance filter, and digital assets filter

i) Select the action taken when rules for spam detection filtering, email firewall filtering, virus detection filtering, zero-hour virus detection filtering, regulatory compliance filtering, and digital assets filtering are matched and when system alerts are generated

j) Add, remove, and modify the group of users that are part of a role for viewing or modifying audited events and accessing TSF data and functions].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Super-user, Limited Administrator, End User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. The stated Security Functional Requirement on the IT Environment of the TOE presented in this section has been drawn from Part 2 of CC Version 2.3 and hence conformant to CC Version 2.3 Part 2.

Table 10 - SFRs for the IT Environment

Name	*Description*	*S*	*A*	*R*	*I*
FPT_SEP.1	*TSF domain separation*			✓	
FPT_STM.1	*Reliable time stamps*			✓	
FTP_ITC.1	*Inter-TSF trusted channel*	✓	✓	✓	
FTP_TRP.1	*Trusted path*	✓	✓	✓	

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

5.2.1 Class FPT: Protection of the TOE Environment

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The ~~TSF~~ **TOE Environment** shall maintain a security domain for ~~its own~~ **the TSF's** execution that protects ~~it~~ **the TSF** from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The ~~TSF~~ **TOE Environment** shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The ~~TSF~~ **TOE Environment** shall be able to provide reliable time stamps for ~~it's own~~ **the TSF's** use.

Dependencies: No dependencies

5.2.2 Class FTP: Trusted Path/Channels in the Environment

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1

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

FTP_ITC.1.2

The ~~TSF~~ **TOE Environment** shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*accessing the Proofpoint Update Servers via SSL*].

Dependencies: No dependencies

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1

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

FTP_TRP.1.2

The ~~TSF~~ **TOE Environment** shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The ~~TSF~~ **TOE Environment** shall require the use of the trusted path for

[

a) accessing the web interface via HTTPS

b) accessing the end user digest via HTTPS

].

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 11 – Assurance Requirements summarizes the requirements.

Table 11 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC : Life Cycle Support	ALC_FLR.1 Basic Flaw Remediation
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation

Assurance Requirements	
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 TOE Security Functions

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

Table 12 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_ARP.1(a)	Security alarms for Spam Detection
	FAU_ARP.1(b)	Security alarms for Email Firewall policy violation
	FAU_ARP.1(c)	Security alarms for Virus Detection
	FAU_ARP.1(d)	Security alarms for Regulatory Compliance policy violation
	FAU_ARP.1(e)	Security alarms for Digital Assets policy violation
	FAU_ARP.1(f)	Security alarms for System Alert Notification
	FAU_GEN.1	Audit Data Generation
	FAU_SAA.1(a)	Potential violation analysis for Spam Detection

TOE Security Function	SFR ID	Description
	FAU_SAA.1(b)	Potential violation analysis for Email Firewall policy
	FAU_SAA.1(c)	Potential violation analysis for Virus Detection
	FAU_SAA.1(d)	Potential violation analysis for Regulatory Compliance policy
	FAU_SAA.1(e)	Potential violation analysis for Digital Assets policy
	FAU_SAA.1(f)	Potential violation analysis for System Alert Notification
	FAU_SAR.1	Audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_UAU.2	User authentication before any action

TOE Security Function	SFR ID	Description
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TSF	FPT_RVM.1	Non-bypassability of the TSP

6.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit data. Logs are generated for events generated by the filtering engines.

Administrators can configure log retention periods and the level of information collected. Raw log data is collected based on the configured parameters, such as which events to capture, the retention period, and how many rows of data to maintain. The audit logs are protected by the TOE from unauthorized deletion or modification. Periodically, the log files are consolidated, then zipped, compressed, and moved to another database.

Administrators can view log entries through the management interface. They can view the raw data, or combine the data into reports, such as time-series plots or aggregated data plots. Time-series plots are line graphs that display performance or trends over a period of time. Aggregated data plots are bar charts or pie charts that represent an aggregation of data over a period of time.

Violation analysis is performed by comparing customer-defined policies against incoming and outgoing emails to determine if they contain spam, viruses, or other content violations. Analysis on the system functions is also performed. Security alarms are then issued by the TOE for spam detection, virus detection, content match, mail policy violations, regulatory compliance violations, digital assets violations, and system events. The security alarms can be viewed by authorized administrators through the management interface. Security alarms contain information such as date and time, syslog error level, event id, source name, description, and severity.

TOE Security Functional Requirements Satisfied: FAU_ARP.1(a), FAU_ARP.1(b), FAU_ARP.1(c), FAU_ARP.1(d), FAU_ARP.1(e), FAU_ARP.1(f), FAU_GEN.1, FAU_SAA.1(a), FAU_SAA.1(b), FAU_SAA.1(c), FAU_SAA.1(d), FAU_SAA.1(e), FAU_SAA.1(f), FAU_SAR.1, FAU_SEL.1, FAU_STG.1.

6.1.2 User Data Protection

The TOE allows authorized administrators to enforce a rigid policy for users and administrators accessing the TOE through the Access Control SFP. Super-user administrators can create Super-user accounts and Limited Administrative accounts for other administrators with pre-defined privilege levels. During account creation, the Super-user administrator sets the new administrator's default password and administrator ID, and enters the administrator's name, email address, phone number, and a comment about the account. The Super-user administrator can also flag whether or not the new administrators must change their passwords each time they log into the management interface. For new Limited Administrator accounts, the Super-user can set which modules the Limited Administrator may manage. The choices of modules that a Limited Administrator may manage are:

Appliance Management
Digest
Digital Assets
Email Alert
Email Firewall
Groups and Users
Logs and Reports
Password Policy
Quarantine
Regulatory Compliance
Server Management
Spam Detection
System
Virus Protection

There is no way for a Limited Administrator to change his own role, or grant himself additional privileges. Privilege levels are pre-defined and only a Super-user administrator can change them. Super-user administrators cannot change their own permission level.

Authorized administrators can also create groups and End User accounts with pre-defined permissions. Authorized administrators can define permissions at the global, group, or user level. End User permissions override Group permissions, and Group permissions override global permission. Permissions to manage End User Digest settings, select spam policies, enforce module rules, upload confidential information to the Document Repository, change their own passwords, and report false negatives can be set by the authorized administrators at the Global, Group or End User account level. End Users may also be configured to allow the users to manage their emails either through their email clients, or through a web browser.

Using the Administrative Interface, administrators with appropriate permissions can craft policies to manage the email traffic. There are a large number of options available to manage email traffic, which provide enough flexibility to implement a wide variety of email policies. Policy rules can be chained together to enforce more complex rule sets on varying types of traffic. Email policies can also be crafted to discard email from certain sources or email with specified attachment file names and file types.

End Users may use browser links to process End User Digest actions such as the following:

- Add safe and blocked senders to personal lists
- Remove safe and blocked senders from personal lists
- Suggest safe senders for the Global Safe List
- Request a Summary Digest (lists all messages for an end user currently in the Quarantine)
- Release messages from the Quarantine
- Report false negatives and false positives to Proofpoint
- Request empty Digests (through the web browser only)
- Select a spam policy (through the web browser only)
- Change own password
- View own list of aliases.

The TOE will send an email to the end user and all operations permitted to the end user (except viewing and releasing messages) are completed through a web browser. An end user can enter the URL in a web browser and then enter a login id and password upon prompting by the TOE. The browser then displays the digest commands and messages in the Quarantine for that user.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1.

6.1.3 Identification and Authentication

Administrators and end users must be authenticated before they can perform any management tasks on the TOE or TOE data. Administrators authenticate with a userid and password through a web browser, and, once authenticated, can perform the management tasks to which they have been given access. End users authenticate with a userid and password through a web browser, and, once authenticated, can perform management tasks on their end user digests. An LDAPS interface on the End User Web Server is used in instances where the administrator specifically configures the End Users to identify and authenticate with an existing directory server within the trusted network rather than allowing the End User to authenticate against the User/Group Database. This is an optional feature of the TOE that is not activated by default; the administrator must make the appropriate system configuration changes for this external interface to be functional.

There are two levels of administrative access: Super-user and Limited Administrator. Super-users can perform all administrative tasks on the TOE functions and data. Limited Administrators are given access to specific components by the Super-user. There is one level of end user access, which is given access to individual end user digests by the Super-user.

Unsuccessful attempts to login to the management interface are tracked, and the IP address is locked out after a configurable number of failed login attempts.

Configurable password policies are available on the TOE. The default password policy is:

- a minimum length of seven characters
- contains a mixture of letters and numbers and at least one special character.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_UAU.2, FIA_UID.2.

6.1.4 Security Management

The TOE supports two administrative roles: Super-users (user id “admin”) and Limited Administrators. Super-users have full privileges to add, change, and delete other administrators from the system, as well as to configure and access all components of the TOE. Super-users configure access by End Users to End User Digests as appropriate. Super-users perform all configuration tasks on the various filter modules executed by the TOE, such as

the spam detection filter, the email firewall filter, the virus detection filter, the zero-hour virus detection filter, the regulatory compliance filter, and the digital assets filter.

Limited Administrators have limited access to specific components on the TOE, as configured by the Super-user.

End users have access to individual End User Digests, as configured by the Super-user. End User Digests provide the authorized end user with a list of all messages that have been sent to the quarantine because the messages triggered one or more filtering rules that determined the messages unsafe or undesirable for delivery. End Users cannot see quarantined messages unless allowed to by an administrator. End users can take actions on the quarantined messages, depending on the level access given by the administrator. Some possible actions end users can take include:

- Add safe and blocked users to personal lists
- Remove safe and blocked users from personal lists
- Request a summary digest
- Release messages from the quarantine
- Change personal password.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

6.1.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features. These features include identification and authentication.

TOE Security Functional Requirements Satisfied: FPT_RVM.1.

6.2 TOE Security Assurance Measures

EAL2+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 13 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	Proofpoint Proofpoint Protection Server v5.0.4 - Configuration Management: Capabilities
ADO_DEL.1	Proofpoint Proofpoint Protection Server v5.0.4 - Secure Delivery
ADO_IGS.1	Proofpoint Protection Server Installation Guide

Assurance Component	Assurance Measure
ADV_FSP.1	Proofpoint Proofpoint Protection Server v5.0.4 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	Proofpoint Proofpoint Protection Server v5.0.4 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	Proofpoint Proofpoint Protection Server v5.0.4 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	Proofpoint Administration Guide Proofpoint Protection Server Reference Guide Proofpoint Release Notes Proofpoint Proofpoint Protection Server v5.0.4 – Installation and Administrative Guidance Supplement
AGD_USR.1	(see AGD_ADM.1)
ALC_FLR.1	Proofpoint Proofpoint Protection Server v5.0.4 – Life Cycle Support: Flaw Remediation
ATE_COV.1	Proofpoint Proofpoint Protection Server v5.0.4 – Functional Tests and Coverage
ATE_FUN.1	Proofpoint Proofpoint Protection Server v5.0.4 – Functional Tests and Coverage
AVA_SOF.1	Proofpoint Proofpoint Protection Server v5.0.4 - Vulnerability Assessment
AVA_VLA.1	Proofpoint Proofpoint Protection Server v5.0.4 - Vulnerability Assessment
ATE_IND.2	Proofpoint Proofpoint Protection Server v5.0.4 – Independent Testing

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at Proofpoint. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by Proofpoint to protect against TOE modification during product delivery. The Installation Documentation provided by Proofpoint details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users on configuring the TOE and how those TOE configurations affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they should be exercised.

6.2.4 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The Proofpoint design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

6.2.5 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing, ATE_IND.2: Independent Testing - Sample

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested.

Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

Independent testing is undertaken by the evaluator. The objective is to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests.

6.2.6 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 14 and Table 15 demonstrate the mappings between the assumptions and threats to the security objectives are complete. The following discussion provides detailed evidence of coverage for each assumption and threat.

8.1.1 Security Objectives Rationale Relating to Threats

Table 14 - Threats: Objectives Mapping

Threats	Objectives	Rationale
T.RESOURCE_CONSUME Threat agents may flood the TOE with spam, consuming resources such as memory, bandwidth, processor time, and data storage, and thus limit the TOE's ability to execute its security functions efficiently.	O.SPAM The TOE shall be able to define characteristics for spam and take configured action when such characteristics are recognized.	O.SPAM requires that the TOE take specified actions when spam is identified, thereby rejecting the emails when they appear to come from a known spam source. This limits the number of emails that continue to process through the TOE.
	O.NOTIFICATION The TOE shall generate and deliver alerts upon detecting failure of any of its functional components.	O.NOTIFICATION requires that the TOE generate and deliver alerts upon detecting failure of any of its functional components, thereby allowing the TOE to mitigate attacks by threat agents against those components.
T.EMAIL_FIREWALL A threat agent may try to violate the mail dissemination policy of the TOE by sending information that is identified as inappropriate because of its origin, destination, or subject content.	O.EMAIL_FIREWALL The TOE shall be able to prevent specific types of information being sent to or from specific entities, and shall take specified actions on incoming messages based on their sender address, recipient address, or message or attachment content.	O.EMAIL_FIREWALL requires that the TOE be able to prevent information being sent to or from specific entities, and take specified actions on messages based on the origin, destination, or subject content.
T.VIRUS A threat agent may try to violate the mail dissemination policies of the TOE by sending information containing a virus or an emerging virus.	O.VIRUS The TOE shall take specified actions on incoming messages identified as containing a virus or an emerging virus.	O.VIRUS requires that the TOE take specified actions on incoming messages identified as containing a virus or an emerging virus, thereby mitigating the threat.

Threats	Objectives	Rationale
T.REG_COMP A threat agent may circulate non-public information through the TOE in violation of its mail policy.	O.REG_COMP The TOE shall take specified actions on outgoing messages identified as containing non-public information.	O.REG_COMP requires that the TOE prevent non-public information from leaving the internal network.
T.DIGITAL_ASSETS A threat agent may circulate confidential information through the TOE in violation of its mail policy.	O.DIGITAL_ASSETS The TOE shall take specified actions on outgoing messages identified as containing confidential information.	O.DIGITAL_ASSETS requires that the TOE prevent confidential information from leaving the internal network.
T.SYS_FAILURE A threat agent may take advantage of unexpected termination of one or more of the TOE's Security Functions (SF) and send inappropriate information through the TOE in violation of its policies.	O.NOTIFICATION The TOE shall generate and deliver alerts upon detecting failure of any of its functional components.	O.NOTIFICATION requires that the TOE generate and deliver alerts upon detecting failure of any of its functional components, thereby notifying the administrator of the failure. The administrator can then take action to address the failure, thereby reducing the opportunity for the threat agent to send inappropriate information through the TOE.
T.NO_AUDIT A threat agent may perform security-relevant operations on the TOE without being held accountable for it.	O.LOG The TOE shall generate logs of all the security-relevant operations performed on the TOE.	O.LOG requires that the TOE generate logs of all the security-relevant operations performed on the TOE, enabling the administrator to hold the threat agent accountable for all actions taken on the TOE.
	OE.TIMESTAMP The IT Environment must provide reliable timestamps to the TOE.	OE.TIMESTAMP requires that the IT Environment provide reliable timestamps for use in the audit logs, by which the administrator can hold threat agents accountable for their actions.
T.NEW_EXPLOITS A threat agent may modify the message content suitably or use variants in the send or recipient information in order to defeat the protection services offered by the TOE.	O.CONFIG The TOE shall provide administrative tools to enable authorized administrators to effectively configure and maintain the TOE.	O.CONFIG requires that the TOE provide administrative tools to enable authorized administrators to identify messages that have been modified by a threat agent.
T.BYPASS A threat agent may bypass one or more of the TOE's security functions and send malicious data	O.REF_MED All inbound or outbound mail into or out of the TOE, unless explicitly allowed by the TOE administrator,	O.REF_MED requires that inbound mail be examined for malicious data before being allowed to continue to its destination. If malicious data is found, the TOE will prevent the delivery of

Threats	Objectives	Rationale
through the TOE to the End Users.	shall be examined by each of the TOE's configured filters before being forwarded to its destination.	the email, thereby preventing a threat agent from bypassing the TOE security mechanisms, and passing malicious data through the TOE.
T.BRUTE_FORCE A threat agent may repeatedly try to guess authentication data in order to gain unauthorized access to the TOE.	O.BOUNDED_AUTH The TOE shall bound the number of failed authentication attempts to some configurable value in order to prevent brute force attacks against the TOE.	O.BOUNDED_AUTH requires that the number of failed authentication attempts be bound to a configurable value in order to prevent brute force attacks against the TOE.
T.IA A threat agent may attempt to compromise the TOE by attempting actions that it is not authorized to perform on the TOE.	O.AUTHENTICATION The TOE shall require that users of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.	O.AUTHENTICATION requires that users of the TOE be identified and authenticated before any TSF-mediated activity may be performed by them.
	O.SEC_ACCESS The TOE shall ensure that only those authorized users are granted access to the security functions, configurations, and associated data.	O.SEC_ACCESS requires that the TOE grant access to the security functions, configurations, and associated data only to authorized users of the TOE.
TE.AUTH_CAPTURE A threat agent may execute a process on the TOE that captures the authentication data of a valid user of the TOE in order to gain unauthorized access to the TOE.	OE.DOMAIN_SEP The IT Environment shall ensure that the execution of code within the TOE cannot be interfered with or tampered with by any untrusted subject.	OE.DOMAIN_SEP requires that the IT Environment ensure that the execution of code within the TOE cannot be interfered with or tampered with by any untrusted subject, thereby preventing a threat agent from executing a process on the TOE that captures the authentication data of a valid user.
TE.INFO_CAPTURE An external attacker or malicious insider may sniff the communication channel between the TOE and an external IT entity in order to capture or modify messages, authentication data, or other information sent between the two.	OE.TRUSTED_INFO Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.	OE.TRUSTED_INFO requires that the IT Environment prevent the information being sent between the TOE and trusted external entities from being compromised.
TE.MASQUERADE A threat agent masquerading as the TOE may capture valid identification and authentication	OE.TRUSTED_INFO Information within the TOE will be protected from unauthorized disclosure and modification, and will	OE.TRUSTED_INFO requires that the IT Environment protect information within the TOE from unauthorized disclosure and modification, thereby preventing a threat agent from

Threats	Objectives	Rationale
data for a legitimate user of the TOE in order to gain unauthorized access to the TOE.	never be compromised when sent between the TOE and trusted external entities.	obtaining identification and authentication information from the TOE and then accessing the TOE with it.

8.1.2 Security Objectives Rationale Relating to Assumptions

Table 15 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.DB_INTEGRITY The integrity of data maintained by the MySQL database is always ensured.	OE.TRUSTED_INFO Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.	The OE.TRUSTED_INFO objective ensures that the integrity of the information received by the TOE from trusted external systems is never compromised. This ensures that the integrity of the data maintained by the MySQL database within the TOE is always maintained.
A.DNS DNS information received by the TOE is reliable.	OE.TRUSTED_INFO Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.	The OE.TRUSTED_INFO objective ensures that DNS information received by the TOE will never be compromised during transmission.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIMESTAMP The IT Environment must provide reliable timestamps to the TOE.	The OE.TIMESTAMP objective ensures that the IT Environment shall provide reliable timestamps to the TOE.
A.NO_EVIL Authorized administrators are non-hostile and are appropriately trained to use, configure and maintain the TOE.	NOE.TRUSTED_ENV The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.	The OE.TRUSTED_ENV objective ensures that authorized administrators shall not compromise the TOE.
A.PHYS_SEC The TOE resides in a physically controlled access facility that prevents unauthorized physical access.	NOE.TRUSTED_ENV The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.	The OE.TRUSTED_ENV objective ensures that the TOE shall reside in a physically secure location, that prevents unauthorized physical access.

8.2 Security Functional Requirements Rationale

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

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 16 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.SPAM The TOE shall be able to define characteristics for spam and take configured action when such characteristics are recognized.	FAU_ARP.1(a) Security alarms for Spam Detection	The requirement meets the objective by specifying the actions to be taken by the TOE when spam is detected in a message or attachment.
	FAU_SAA.1(a) Potential violation analysis for Spam Detection	The requirement meets the objective by specifying the rules that identify spam in a message or attachment.
O.EMAIL_FIREWALL The TOE shall be able to prevent specific types of information being sent to or from specific entities, and shall take specified actions on incoming messages based on their sender address, recipient address, or message or attachment content.	FAU_ARP.1(b) Security alarms for Email Firewall policy violation	The requirement meets the objective by specifying the actions to be taken by the TOE when a specific IP address or message or attachment content is in violation of the configured policy.
	FAU_SAA.1(b) Potential violation analysis for Email Firewall policy	The requirement meets the objective by specifying the rules that identify when a specific IP address or message or attachment content is in violation of the configured policy.
O.VIRUS The TOE shall take specified actions on incoming messages identified as containing a virus or an emerging virus.	FAU_ARP.1(c) Security alarms for Virus Detection	The requirement meets the objective by specifying the actions to be taken by the TOE when a virus or potential virus is detected in a message or attachment.
	FAU_SAA.1(c) Potential violation analysis for Virus Detection	The requirement meets the objective by specifying the rules that identify a virus or potential virus in a message or attachment.
O.REG_COMP The TOE shall take specified actions on outgoing messages identified as containing non-public	FAU_ARP.1(d) Security alarms for Regulatory Compliance policy violation	The requirement meets the objective by specifying the actions to be taken by the TOE when non-public information is detected in an outgoing email or attachment.

Objective	Requirements Addressing the Objective	Rationale
information.	FAU_SAA.1(d) Potential violation analysis for Regulatory Compliance policy	The requirement meets the objective by specifying the rules that identify non-public information in an outgoing email or attachment.
O.DIGITAL_ASSETS The TOE shall take specified actions on outgoing messages identified as containing confidential information.	FAU_ARP.1(e) Security alarms for Digital Assets policy violation	The requirement meets the objective by specifying the actions to be taken by the TOE when confidential information is detected in an outgoing email or attachment.
	FAU_SAA.1(e) Potential violation analysis for Digital Assets policy	The requirement meets the objective by specifying the rules that identify confidential information in an outgoing email or attachment.
O.NOTIFICATION The TOE shall generate and deliver alerts upon detecting failure of any of its functional components.	FAU_ARP.1(f) Security alarms for System Alert Notification	The requirement meets the objective by specifying the actions to be taken by the TOE when a system failure occurs.
	FAU_SAA.1(f) Potential violation analysis for System Alert Notification	The requirement meets the objective by specifying the rules that identify a system failure.
O.LOG The TOE shall generate logs of all the security-relevant operations performed on the TOE.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs to authorized users.
	FAU_SEL.1 Selective audit	The requirement meets the objective by specifying the criteria by which the TOE will include or exclude events from the audit trail.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized modification or deletion.
O.CONFIG	FMT_MOF.1	The requirement meets the objective by ensuring that the TOE restricts

Objective	Requirements Addressing the Objective	Rationale
The TOE shall provide administrative tools to enable authorized administrators to effectively configure and maintain the TOE.	Management of security functions behaviour	administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.REF_MED All inbound or outbound mail into or out of the TOE, unless explicitly allowed by the TOE administrator, shall be examined by each of the TOE's configured filters before being forwarded to its destination.	FPT_RVM.1 Non-bypassability of the TSP	The requirement meets the objective by ensuring that authentication functions succeed before users are able to access TSF management functions and data.
O.BOUNDED_AUTH The TOE shall bound the number of failed authentication attempts to some configurable value in order to prevent brute force attacks against the TOE.	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that IT devices at a given IP address may only attempt to authenticate a limited number of times before being locked out.
O.AUTHENTICATION The TOE shall require that users of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE administrative functions is allowed.
O.SEC_ACCESS The TOE shall ensure that only those authorized users are granted access to the security	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that only authorized users gain access to TOE functions and data.

Objective	Requirements Addressing the Objective	Rationale
functions, configurations, and associated data.	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by defining the rules by which authorized users gain access to TOE functions and data.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by defining the permissions each role is granted.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by requiring that only restrictive default values are provided to enforce the Access Control SFP.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Table 17 - Objectives:Environment SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
OE.DOMAIN_SEP The IT Environment shall ensure that the execution of code within the TOE cannot be interfered with or tampered with by any untrusted subject.	FPT_SEP.1 TSF domain separation	The requirement meets the environmental objective by ensuring that the TOE Environment supports security domain separation by providing a dedicated environment for the execution of the TOE.
OE.TIMESTAMP The IT Environment must provide reliable timestamps to the TOE.	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that the Operating System (OS) provides timestamps to the TOE.
OE.TRUSTED_INFO Information within the TOE will be protected from unauthorized disclosure and modification, and will never be compromised when sent between the TOE and trusted external entities.	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by ensuring that the TOE Environment provides a protected channel for transmission of data between the TOE and the Proofpoint Update Servers via SSL.
	FTP_TRP.1 Trusted path	The requirement meets the objective by ensuring that the TOE Environment provides a protected path for transmission of data between the TOE and the users accessing the management interfaces via HTTPS.

8.3 Security Assurance Requirements Rationale

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

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.4 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 2.3 have been made to clarify the content of the SFRs, and make them easier to read:

In Section 5.1.1, the words "detection of spam in the email message" have been added to FAU_ARP.1(a) to provide a more accurate description of the security violation.

In Section 5.1.1, the words "detection of specific IP address or message content violations in email messages or their attachments" have been added to FAU_ARP.1(b) to provide a more accurate description of the security violation.

In Section 5.1.1, the words "virus in the email by the Virus Detection Filter or Zero-Hour Anti-Virus Filter" have been added to FAU_ARP.1(c) to provide a more accurate description of the security violation.

In Section 5.1.1, the words "in Regulatory Compliance policy" have been added to FAU_ARP.1(d) to provide a more accurate description of the security violation.

In Section 5.1.1, the words "in Digital Assets policy" have been added to FAU_ARP.1(e) to provide a more accurate description of the security violation.

In Section 5.1.1, the words "system alert condition" have been added to FAU_ARP.1(f) to provide a more accurate description of the security violation.

In Section 5.2.1, the words "TOE Environment", "the TSF's", "the TSF", and "TOE Environment" have been added to FPT_SEP.1 to indicate that the TOE environment provides the security functionality described.

In Section 5.2.1, the words "TOE Environment" and "the TSF's" have been added to FPT_STM.1 to indicate that the IT environment provides the security functionality described.

In Section 5.2.2, the words "TOE Environment" and "the TSF" have been added to FTP_ITC.1 and FTP_TRP.1 to indicate that the TOE environment provides the security functionality described.

8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 18 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.

Table 18 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_ARP.1(a)	FAU_SAA.1(a)	✓	
FAU_ARP.1(b)	FAU_SAA.1(b)	✓	
FAU_ARP.1(c)	FAU_SAA.1(c)	✓	
FAU_ARP.1(d)	FAU_SAA.1(d)	✓	
FAU_ARP.1(e)	FAU_SAA.1(e)	✓	
FAU_ARP.1(f)	FAU_SAA.1(f)	✓	
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAA.1(a)	FAU_GEN.1	✓	
FAU_SAA.1(b)	FAU_GEN.1	✓	
FAU_SAA.1(c)	FAU_GEN.1	✓	
FAU_SAA.1(d)	FAU_GEN.1	✓	
FAU_SAA.1(e)	FAU_GEN.1	✓	
FAU_SAA.1(f)	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SEL.1	FAU_GEN.1	✓	
	FMT_MTD.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	

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

SFR ID	Dependencies	Dependency Met	Rationale
FTP_ITC.1	No dependencies		
FTP_TRP.1	No dependencies		

8.6 TOE Summary Specification Rationale

8.6.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions works to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 19 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to Strength of Function (SOF) Rationale section.

Table 19 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_ARP.1(a)	The security function implements this SFR by taking a specified action upon detection of spam in an email message or attachment.
	FAU_ARP.1(b)	The security function implements this SFR by taking a specified action upon detection of specific IP address or message content violations in email messages or their attachments.
	FAU_ARP.1(c)	The security function implements this SFR by taking a specified action upon detection of a virus or emerging virus in an email message or attachment.
	FAU_ARP.1(d)	The security function implements this SFR by taking a specified action upon

TOE Security Function	SFR	Rationale
		detection of non-public information in an email message or attachment.
	FAU_ARP.1(e)	The security function implements this SFR by taking a specified action upon detection of confidential information in an email message or attachment.
	FAU_ARP.1(f)	The security function implements this SFR by taking a specified action upon detection of a system alert condition in the TOE.
	FAU_GEN.1	The security function implements this SFR by generating audit records for the specified auditable events.
	FAU_SAA.1(a)	The security function implements this SFR by applying a set of rules to identify messages that contain spam.
	FAU_SAA.1(b)	The security function implements this SFR by applying a set of rules to identify messages that are sent by or destined for a specific user, group, or domain, or that contain specified text.
	FAU_SAA.1(c)	The security function implements this SFR by applying a set of rules to identify messages that contain a virus or emerging virus.
	FAU_SAA.1(d)	The security function implements this SFR by applying a set of rules to identify messages that contain non-public information.
	FAU_SAA.1(e)	The security function implements this SFR by applying a set of rules to identify messages that contain confidential information.
	FAU_SAA.1(f)	The security function implements this SFR by applying a set of rules to identify a system alert condition in the TOE.
	FAU_SAR.1	The security function implements this SFR by ensuring that only authorized

TOE Security Function	SFR	Rationale
		users are able to read the audit information.
	FAU_SEL.1	The security function implements this SFR by including or excluding auditable events based on event type and log file level.
	FAU_STG.1	The security function implements this SFR by protecting audit records from unauthorized deletion and modification.
User data protection	FDP_ACC.1	The security function implements this SFR by defining an Access Control Security Functional Policy, by which permissions for access the TSF are granted.
	FDP_ACF.1	The security function implements this SFR by defining the rules by which administrators and users may gain access to TSF data and functions.
Identification and Authentication	FIA_AFL.1	The security function implements this SFR by locking out any IP address that exceeds the maximum number of unsuccessful authentication attempts.
	FIA_UAU.2	The security function implements this SFR by requiring that each user be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
	FIA_UID.2	The security function implements this SFR by requiring that each user be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Security Management	FMT_MOF.1	The security function implements this SFR by defining the security functions that can be managed by authorized administrators.
	FMT_MSA.1	The security function implements this SFR by defining the actions each role is permitted to perform on each

TOE Security Function	SFR	Rationale
		security attribute.
	FMT_MSA.3	The security function implements this SFR by requiring that restrictive default values are defined to enforce the Access Control SFP.
	FMT_MTD.1	The security function implements this SFR by identifying the actions that can be taken by authorized administrators on TOE data.
	FMT_SMF.1	The security function implements this SFR by defining the management functions that can be performed by the TSF.
	FMT_SMR.1	The security function implements this SFR by identifying the roles maintained by the TSF.
Protection of TSF	FPT_RVM.1	The security function implements this SFR by ensuring that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

8.6.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

While the TOE 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. The chosen assurance level was also selected for conformance with the client's needs.

8.6.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and a description of how they are used at the Proofpoint. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

Configuration Items

8.6.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Proofpoint to protect against TOE modification during product delivery. The Installation Documentation provided by Proofpoint details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

Delivery Procedures
Installation, Generation and Start-Up Procedures

8.6.2.3 Development

The Proofpoint design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

Informal Functional Specification
Descriptive High-Level Design
Informal Representation Correspondence

8.6.2.4 Guidance Documentation

The Proofpoint Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. Proofpoint provides single versions of documents which address the administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

Administrator Guidance
User Guidance

8.6.2.5 Tests

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Proofpoint Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

Evidence of Coverage
Functional Testing

8.6.2.6 Vulnerability and TOE Strength of Function Analyses

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

Strength of TOE Security Function analysis
Vulnerability Analysis

8.7 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL2+ assurance requirements, this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and Department of Defense (DoD) low robustness environments processing unclassified information.

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security functions and security functional requirements which have probabilistic or permutational functions are:

Identification and Authentication - FIA_UAU.2: User authentication before any action

FAI_UAU.2 requires that a password be used to authenticate the user to the TOE prior to any action. These SFRs and security function claim a strength of function rating of SOF-basic. This is consistent with the rating of SOF-basic claimed by the TOE.

9 Acronyms

Table 20 – Acronyms

Acronym	Definition
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DNS	Domain Name Service
DoD	Department of Defense
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
GB	Gigabyte
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
I/O	Input/Output
IP	Internet Protocol

ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
OS	Operating System
PLINX	Proofpoint Linux
PPS	Proofpoint Protection Server
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy