Third Brigade Deep Security 5.0 Security Target (EAL3+)

Revision 1.4

Issued: 22-May-2007

Third Brigade, Inc.
40 Hines Road
Suite 200
Ottawa, Ontario, Canada
K2K 2M5
+1-866-684-7332

Prepared By: NUVO Network Management Inc.
2650 Queensview Drive
Suite 100
Ottawa, Ontario, Canada
K2B 8H6
+1-613-721-6886

Revision History

Rev. #	Description	By	Date of Issue
0.1	Initial draft	Huan Zhou	26-Sep-2006
0.2	First draft	Huan Zhou	26-Oct-2006
0.3	Second Draft, Updated the EAL claim.	Huan Zhou	04-Dec-2006
1.0	Final draft	Huan Zhou	11-Dec-2006
1.1	Updated in accordance to OR 01	Huan Zhou	13-Dec-2006
1.2	Section 8.7 updated in accordance to the CB's comment	Huan Zhou	20-Mar-2007
1.3	Change of TOE version and minor changes to Chapters 2, 6 and 8.	Huan Zhou	18-Apr-2007
1.4	Updated SFR claim FAU_STG.4 and other relevant information in Chapters 6 and 8	Huan Zhou	22-May-2007

Table of Contents

List of Figures

List of Tables

Conventions and Terminology

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

Acronyms and Abbreviations

Acronym	Meaning
CC	Common Criteria for Information Technology Security Evaluation
CCS	Canadian Common Criteria Scheme
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirements
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TBD	To Be Determined
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy

Document Organization

Section 1 provides the introductory material and identification information for the Security Target

Section 2 provides general purpose and TOE description

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

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria Parts 2 and 3, respectively, that must be satisfied by the TOE.

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

Section 7 contains the claims of Protection Profile conformance for this Security Target.

Section 8 provides the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

1 Introduction

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

The subject of this evaluation described in this ST is the Third Brigade Deep Security 5.0, developed by Third Brigade, Inc. throughout this document; it will also be referred to as Deep Security 5 or the Target of Evaluation (TOE).

Deep Security 5 enables its users to create and enforce comprehensive IT security policies that proactively protect sensitive data, applications, hosts or network segments.

1.1 Identification

Title:	Third Brigade Deep Security 5.0 Security Target (EAL3+)
ST Version:	1.3
TOE Identification:	Third Brigade Deep Security 5.0
PP Identification:	Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006
Author:	Huan Zhou
Vetting Status:	Official Release 1.3
CC Version:	2.3
General Status:	Ready for release
Keywords:	Commercial-off-the-shelf (COTS), intrusion detection, intrusion detection system (IDS), intrusion prevention, intrusion prevention system (IPS), sensor, scanner, analyzer.

.

1.2 CC Conformance Claim

The Third Brigade Deep Security 5.0 is conformant to Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements (Version 2.3, August 2005).

All International Common Criteria Interpretations through October, 2006 have been applied.

The Third Brigade Deep Security 5.0 is conformant to Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements (Version 2.3, August 2005). All International Common Criteria Interpretations through September, 2006 have been applied.

The Deep Security 5 is being evaluated to Evaluation Assurance Level 3 augmented with ALC_FLR.1 (EAL3+) under the Canadian Common Criteria Scheme (CCS) using the Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 2.3, August 2005. All International Common Criteria Interpretations through October, 2006 have been applied.

The ST claims conformance to Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006.

2 TOE Description

2.1 Overview

Deep Security 5 is an advanced, intrusion prevention system (IPS). It provides the best and last line of defence against attacks that exploit vulnerabilities in commercial and custom software, including web applications. It enables its users to create and enforce comprehensive IT security policies that proactively protect sensitive data, applications, hosts or network segments.

2.2 TOE Description

Deep security 5 is comprised of a browser-based management console called the Deep Security Manager and small traffic filtering engines called Deep Security Agents.

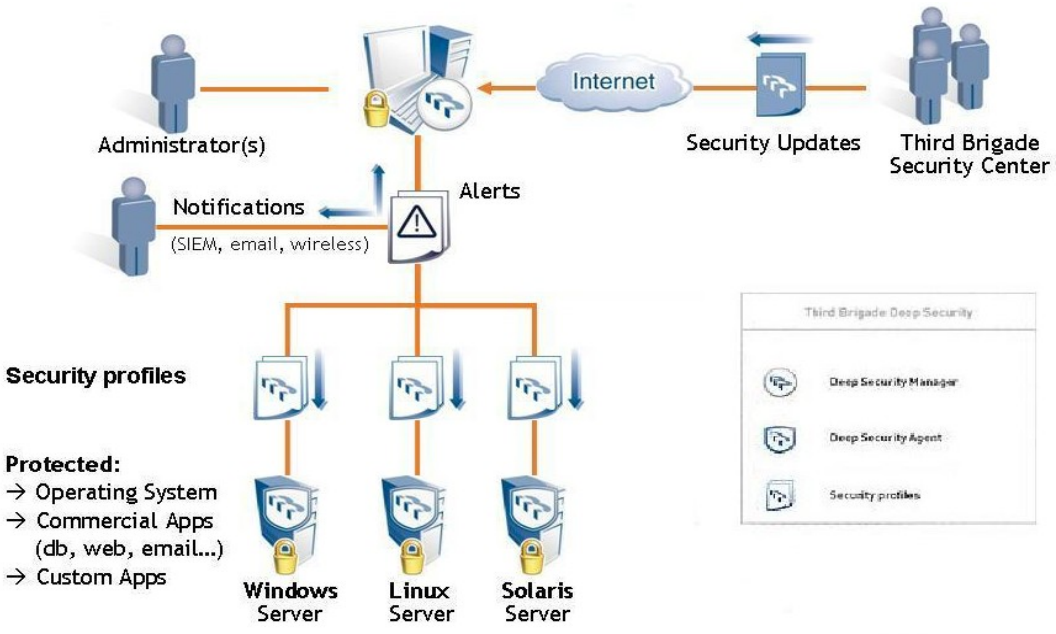
The Agents run on the hosts in your network and implement Security Profiles defined by an Administrator using the Deep Security Manager.

Security Profiles are made up of sets of payload and packet filtering rules selectively applied to network traffic based on a variety of conditions such as application type, interface type, protocol, and direction of traffic flow.

The system can be configured to send alert notifications when particular filters are triggered or when other system events occur.

An administrator uses the Deep Security Manager to define and distribute Security Profiles to the Agents over the network. The Deep Security manager can also be configured to automatically retrieve Security Updates over the internet from Third Brigade Security Center and distribute them to some or all the Agents across your network. For additional security, the administrator can manage the methods and timing of the communications between the Deep Security Manager and individual Agents.

Figure 2-1 Deep security 5 typical deployment



2.2.1 Deep Security Manager

The Deep Security Manager is a powerful, centralized, web-based management system that allows administrators to create and manage comprehensive security policies, and track threats and preventive actions taken in response to them. All of this can be done in real-time, from their desktop.

Security Profiles

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

Dashboard

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

- Extensive system, event and host reporting, with drill-down.
- Graphs of key metrics with trends, with drill-down.
- Detailed event logs, with drill-down, and log forwarding for event correlation with other systems.
- Ability to save multiple personalized dashboard layouts.

Built-in Security

Role-based access allows multiple administrators, each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. Session encryption protects the confidentiality and integrity of information exchanged between components.

2.2.2 Deep Security Agent

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

Firewall Rules

This sophisticated, bi-directional stateful firewall provides complete support for all network protocols, including TCP, UDP and ICMP. Firewall Rules are fully configurable to allow or deny traffic on a per-interface basis, and restrict communication to allowed IP or MAC addresses.

IPS Filters

Software vulnerabilities are shielded from attack through the use of deep packet inspection, which examines application data to and from the host. IPS filters allow, block, log or correct data based on its content. IPS filters protect vulnerabilities from known and unknown attacks by defining expected application data, and blocking malicious data based on its content. IPS filters automatically update to provide the most current, comprehensive protection against known and unknown attacks.

Custom Filters

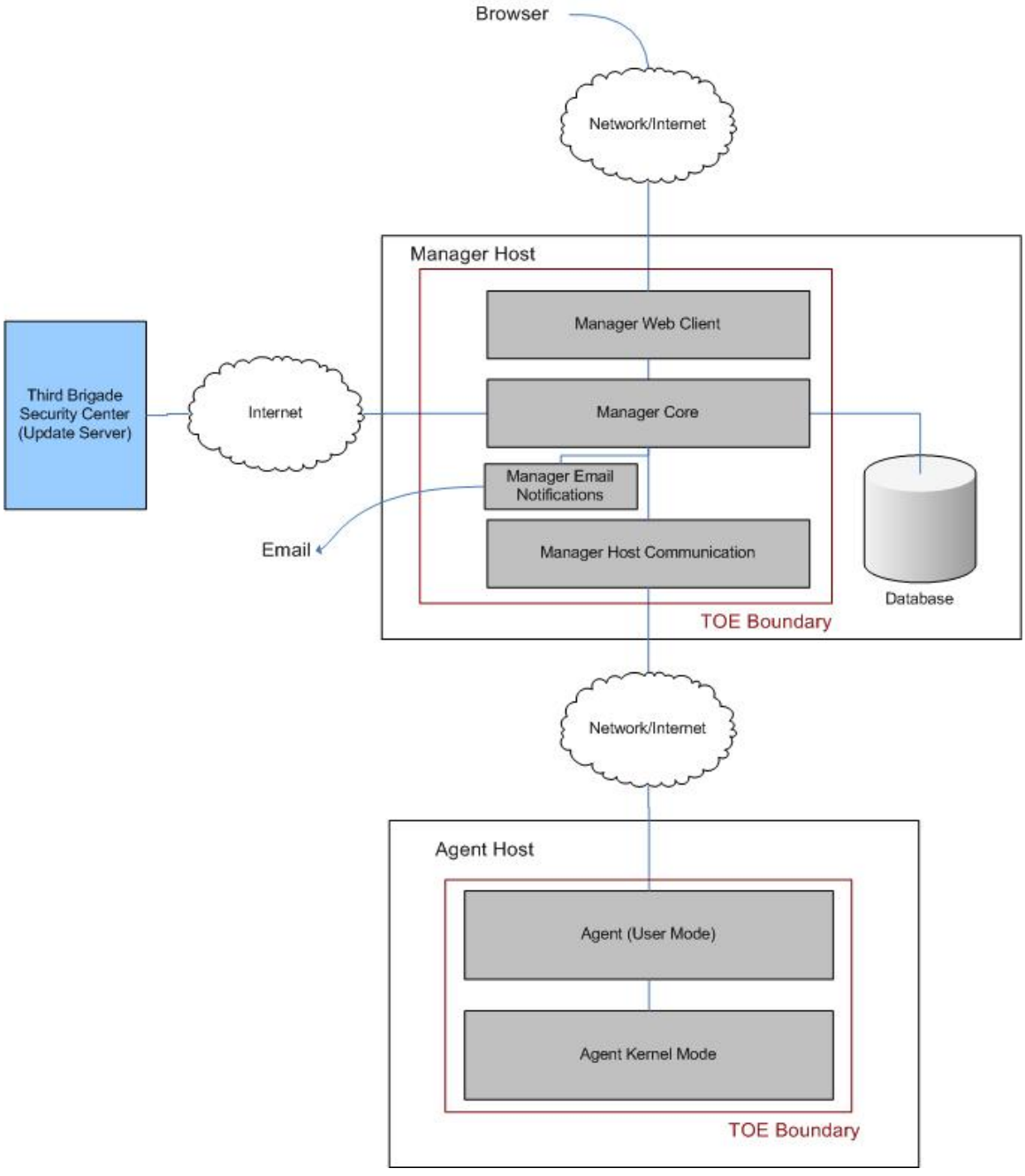
In addition to the filters provided by Third Brigade, clients and integration partners can create filters to support additional protocols or custom applications.

2.3 TOE Boundary and Scope

2.3.1 Physical Boundary

The TOE physical boundary encompasses only the software components of both the deep security manager and the Deep Security Agents.

Figure 2-2 TOE physical boundary



2.3.2 Logical Boundary

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

- SF.AUDIT (Audit)
- SF.RBAC (Role Based Access Control)
- SF.I&A (Identification and Authentication)
- SF.SECCOM (secure intra-TOE communication)
- SF.IDPS (Intrusion detection and prevention)

These descriptions are outlined below and expanded upon in the Statement of TOE IT Security Functions found in section 6.1 of this document.

2.3.2.1 SF.AUDIT

Deep Security 5 maintains information regarding the administration and management of its security functions as part of the audit records. SF.AUDIT is responsible for the generation, storage and reviewing of these audit records.

2.3.2.2 SF.RBAC

Deep Security 5 restricts Authorised TOE administrators' access to the system using role based access control. All TOE administrators are assigned roles at creation. Authorised TOE administrators can only access the TOE through the administrative interface. They have full access to the functions permitted by their roles.

2.3.2.3 SF.I&A

The identification and authentication mechanism used by Deep security 5 is based on user ID and password. For each user being created, the creator is required to assign them with a user id, an initial password and a role.

2.3.2.4 SF.SECCOM

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

2.3.2.5 SF.IDPS

The TOE provides intrusion detection and prevention functions. Data is collected and analyzed by Deep Security Agents and is passed to the Deep Security Manager for review and storage.

2.3.3 Excluded Functionality

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

- Command Line Interface to Deep Security Agent (for installation only)
- Graphical User Interface to the Deep Security Agent (for trouble shooting only)
- Bi-directional stateful firewall capability of the Deep Security Agent
- Application Programming Interface to the Deep Security Manager (disabled by default)

- Command Line Interface to Deep Security Manager (for installation and trouble shooting only)

2.3.4 TOE Environment Configuration

The TOE environment contains the following elements:

Deep Security Manager

- Memory: Minimum RAM 512 MB (1 GB recommended)
- Disk Space: Minimum 100 MB (2 GB recommended)
- Operating System: Windows 2003 Server SP1
- Oracle Database 10g Express Edition
- Tomcat Embedded 5.5.17

Deep Security Agent

- Memory: Minimum RAM 128 MB
- Disk Space: Minimum 5 MB (15 MB recommended, primarily for logging)
- Windows 2003 Server SP1
- Solaris 10
- Linux Red Hat Enterprise Edition 5

3 TOE Security Environment

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

3.1 Security Assumptions

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

3.1.1 Intended Usage Assumptions

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

3.1.2 Physical Assumptions

A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.1.3 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

3.2 Threats to Security

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

3.2.1 TOE Threats

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

3.2.2 IT System Threats

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

T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

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

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P. PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4 Security Objectives

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

4.1 Information Technology (IT) Security Objectives

The following are the TOE security objectives:

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.EXPORT	When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.

4.2 Security Objectives for the Environment

4.2.1 Non-IT Environment Objectives

The TOE's operating environment must satisfy the following objectives.

These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

O.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
O. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
O.INTROP	The TOE is interoperable with the IT System it monitors.

4.2.2 IT Environment Objectives

OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

Table 5-1 TOE Security Functional Requirements

Security Functional Requirement	Name
Security Functional Requirements for the TOE	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.4	Prevention of audit data loss
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
IDS_SDC.1	System Data Collection
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted Data Review
IDS_STG.1	Guarantee of System Data Availability
IDS_STG.2	Prevention of System data loss
Security Functional Requirements for the IT Environment	
FAU_STG.2	Guarantees of audit data availability

Security Functional Requirement	Name
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

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

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

b) All auditable events for the *basic* level of audit; and

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

Table 5-2 Auditable Events

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

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional information specified in the Details column of Table 5-2 Auditable Events.* FAU_GEN.1.2

5.1.1.2 Audit review (FAU_SAR.1)

The TSF shall provide *authorized administrators* with the capability to read *audit information which they has been granted access to* from the audit records.[FAU_SAR.1.1]

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

5.1.1.3 Restricted audit review (FAU_SAR.2)

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

5.1.1.4 Selectable audit review (FAU_SAR.3)

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

5.1.1.5 Selective audit (FAU_SEL.1)

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

a) event type;

b) *no other attributes*.[FAU_SEL.1.1]

5.1.1.6 Prevention of audit data loss (FAU_STG.4)

The TSF shall *prevent auditable events, except those taken by the authorised user with special rights, overwrite the oldest stored audit records* and send an alarm if the audit trail is full.[FAU_STG.4.1]

Application Note: auditable events in general shall be prevented by the TOE upon detection of a full audit trail, for unpreventable events (explained in more detail in Chapter6.1.1), the TOE shall record them by overwriting the oldest stored audit records.

5.1.2 Identification and authentication (FIA)

Application Note: Following NIAP precedent decision 0097, the requirement FIA_AFL.1 has been removed as it was 'incorrectly included [in the PP]'.

5.1.2.1 User attribute definition (FIA_ATD.1)

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

a) *User identity;*

b) *Authentication data;*

c) *Authorisations; and*

d) *no other attributes.*[FIA_ATD.1.1]

5.1.2.2 Timing of authentication (FIA_UAU.1)

The TSF shall allow *no action* on behalf of the user to be performed before the user is authenticated.[FIA_UAU.2.1]

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.[FIA_UAU.2.2]

5.1.2.3 Timing of identification (FIA_UID.1)

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

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

5.1.3 Security management (FMT)

5.1.3.1 Management of security functions behaviour (FMT_MOF.1)

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

5.1.3.2 Management of TSF data (FMT_MTD.1a)

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

5.1.3.3 Management of TSF data (FMT_MTD.1b)

The TSF shall restrict the ability to *query audit data and all other TOE data* to *auditor.* FMT_MTD.1.1

5.1.3.4 Specification of management functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions: *system data management and security function management.*

5.1.3.5 Security roles (FMT_SMR.1)

The TSF shall maintain the roles *authorised administrator, authorised system administrator, Full Access and Auditor roles.* FMT_SMR.1.1

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

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

5.1.4 Protection of the TOE Security Functions (FPT)

Application Note: Following NIAP precedent decision 0097, the requirements FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 have been replaced with FPT_ITT.1 as they were 'incorrectly included [in the PP]'. The author intended these requirements to protect communications between the components in an IDS system.

5.1.4.1 Basic internal TSF data transfer protection (FPT_ITT.1)

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

5.1.5 IDS component requirements (IDS)

5.1.5.1 System Data Collection (IDS_SDC.1, EXP)

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

a) *Start-up and shutdown, network traffic, detected malicious code, detected known vulnerabilities* and
b) *no other specifically defined events.* IDS_SDC.1.1 (EXP)

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

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

b) The additional information specified in the Details column of Table 5-3 IDS Events. IDS_SDC.1.2 (EXP)

Table 5-3 IDS Events

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

Application Note: Note that while the IDS_SDC.1 requirement in the PP indicates additional information content, that content is dependent upon the data that is collected. Since the TOE only claims to collect network traffic related information, the other information is not relevant.

5.1.5.2 Analyser analysis (IDS_ANL.1, EXP)

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

a) *statistical, signature, integrity;* and

b) *no other analytical functions.* IDS_ANL.1.1 (EXP)

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

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

b) *action taken, Data destination.* IDS_ANL.1.2 (EXP)

5.1.5.3 Analyser react (IDS_RCT.1, EXP)

The System shall send an alarm to *the authorized administrator* and *record the attempt as system data record and terminate the attempt* when an intrusion is detected. IDS_RCT.1.1 (EXP)

5.1.5.4 Restricted Data Review (IDS_RDR.1, EXP)

The System shall provide *users assigned the Full Access and auditor roles* with the capability to read *all System data* from the System data. IDS_RDR.1.1 (EXP)

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

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

5.1.5.5 Guarantee of System Data Availability (IDS_STG.1, EXP)

The System shall protect the stored System data from unauthorised deletion. IDS_STG.1.1 (EXP)

The System shall protect the stored System data from modification. [IDS_STG.1.2] (EXP)

The System shall ensure that *the most recent* System data will be maintained when the following conditions occur: *System data storage exhaustion*. [IDS_STG.1.3] (EXP)

5.1.5.6 Prevention of System data loss (IDS_STG.2, EXP)

The System shall *overwrite the oldest stored System data* and send an alarm if the storage capacity has been reached. [IDS_STG.2.1] (EXP)

5.2 TOE Security Assurance Requirements

This product claims CC Version 2.3 Part 3 conformant and claims Evaluation Assurance Level 3 augmented with ALC_FLR.1 (EAL3+) including all relevant International Common Criteria interpretations from the Interpreted CEM as of September, 2006. The security assurance requirements are listed in Table 5-5.

Table 5-4 Security Assurance Requirements

Assurance component ID	Assurance component name
ACM_CAP.3	Authorisation controls
ACM_SCP.1	TOE CM coverage
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ALC_FLR.1	Basic flaw remediation
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.1	Examination of guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.3 Statement of Strength of TOE Security Function

Strength of function, as a CC concept, applies to probabilistic or permutational mechanisms that are non-cryptographic in nature. This ST claims SOF-basic for the user identification and authentication SFRs: FIA_UAU.1 and FIA_UID.1 through the user password entry function and its mechanism.

The Strength of Function (SOF) rating of SOF-basic was claimed for this TOE to meet the EAL3+ assurance requirements. The rationale for the chosen level is based on the low attack potential of the threat agents as identified in this ST. The TOE is intended to operate in commercial and

Government low to medium robustness environments processing unclassified information. This security function is consistent with the security objectives described in section 4.

5.4 IT Environment Security Functional Requirements

5.4.1 Security audit (FAU)

5.4.1.1 Guarantees f audit data availability (FAU_STG.2)

The *IT environment* shall protect the stored audit records from unauthorised deletion.[FAU_STG.2.1]

The *IT environment* shall be able to *detect* modifications to the audit records.[FAU_STG.2.2]

The *IT environment* shall ensure that *the previously recorded* audit records will be maintained when the following conditions occur: *failure and attack.*[FAU_STG.2.3]

5.4.2 Protection of the TOE Security Functions (FPT)

5.4.2.1 Non-bypassability of the TSP (FPT_RVM.1)

The *IT environment* shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.[FPT_RVM.1.1]

5.4.2.2 TSF domain separation (FPT_SEP.1)

The *IT environment* shall maintain a security domain for the *TOE's* execution that protects it from interference and tampering by untrusted subjects.[FPT_SEP.1.1]

The *IT environment* shall enforce separation between the security domains of subjects in the TSC.[FPT_SEP.1.2]

5.4.2.3 Reliable time stamps (FPT_STM.1)

The *IT environment* shall be able to provide reliable time stamps for *the TOE to* use.[FPT_STM.1.1]

6 TOE Summary Specification

6.1 Statement of TOE IT Security Functions

The TOE provides the following security functions in meeting the SFR's specified in section 5.1:

- SF.AUDIT (Audit)
- SF.RBAC (Role Based Access Control)
- SF.I&A (Identification and Authentication)
- SF.SECCOM (secure intra-TOE communication)
- SF.IDPS (Intrusion detection and prevention)

6.1.1 SF.AUDIT

Deep Security 5 maintains information regarding the administration and management of its security functions as part of the audit records. This security function addresses the generation; storage and reviewing of these audit records.

Authorised TOE administrators are only allowed to interact with the TOE through a browser based graphical user interface supported by the Deep Security Manager. All the security relevant actions as specified in table 5-2 taken by the authorized administrators are recorded as a part of the audit log.

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

Application Note: The database in concern here is the oracle 10g express edition, and it is responsible to ensure that stored audit data will not be corrupted during system failure or when data storage exhaustion occurs.

When the capacity of the database has been reached, an emergency email is sent to a pre-selected administrator alerting them of the situation. The TOE will prevent TOE users from starting new user sessions with the TOE. For existing live user sessions, any attempts at modifying the TOE data will be prevented and reading of the TOE data remain granted. The TOE records new auditable events such as reading of TOE data, user requests failure by overwriting the oldest auditable events in the database with records of these new events.

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

In addition, an authorised administrator with appropriate roles assigned has the ability to include or exclude auditable events from the set of audited events based on the audit event type.

6.1.2 SF.RBAC

Deep Security 5 restricts Authorised TOE administrators' access to the system using role based access control. All TOE administrators are assigned roles at creation. Authorised TOE administrators can only access the TOE through the administrative interface. They have full access to the functions permitted by their roles.

By default, two predefined roles are available upon successful installation of Deep Security Manager. And these are "Full Access" and "Auditor". Users assigned the "Full Access" role have access to all the system functions, including the capability of defining new roles and assigning users to these roles; Users of the "Auditor" role are only allowed read access to all data/configuration.

6.1.3 SF.I&A

The identification and authentication mechanism used by Deep security 5 is based on user ID and password. For each user being created, the creator is required to assign them with a user id, an initial password and a role.

Before users are granted access through the administrative interface, they are required to provide their credentials at the browser based interface and these are verified by the TOE. Identification is performed by finding the matching administrator based on a case-insensitive match to the username. Authentication take place by matching one-way hashed passwords against values previously stored in the database.

Users are allowed to modify their own passwords; however, they must follow the password policy as specified in section 6.1.6 below.

6.1.4 SF.SECCOM

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

6.1.5 SF.IDPS

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

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

Deep Security Agent sits directly on a host, and defends it by monitoring incoming and outgoing network traffic for protocol deviations or contents that might signal an attack. Authorized administrative Users of the TOE configure the Agents through functionalities offered by the Deep Security Manager. Rules called Filters are defined for each individual agent or a group of agents as a whole to manage their actions. The Deep Security Manager is populated with commonly used filter definitions, targeted at known vulnerabilities for each type of hosts. These filter configurations can be categorized into Firewall Rules, Stateful Configurations, and IPS Filters. Firewall Rules examine the control information of network packets, determines if a network connection should be allowed. Stateful Configuration filters analyze each network packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state

transitions, manages existing network sessions with great efficiency. IPS Filters examine the actual content of a network packet or a sequence of packets performing deep packet inspection. Based on rules predefined as the IPS Filters, various actions are carried out by the agents on these packets: from replacing specifically defined or suspicious byte sequences, to completely dropping packets and resetting the connection.

Deep Security Agents generate log records in accordance with details as specified in table 5-3, regarding its own startup and shut down, the network traffic and malicious codes or vulnerabilities detected, and pass these records to the Deep Security Manager for review, storage and reports generation. Within each record, event time, event type, action taken, data source and destination are recorded. Authorized administrators can use functionalities provided by the Deep Security Manager to control the behavior of the Deep Security Manager log collection process. This could be configured occur on demand or at regular intervals.

Deep Security Manager groups the information received from Deep Security Agents into System, Firewall and IPS events based on their Event ID (type). Generally speaking, the records of Agents Start up and Shut downs are regarded as System Events; Information collected on network traffic and detected known vulnerabilities are grouped into Firewall or IPS events and log data collected regarding the detection of Malicious codes are placed into the IPS events. Deep Security Manager offers only pre-authorized administrators of appropriate roles with read access to these events logs. When a predefined event has been detected, email alarms are sent to pre-selected administrator.

6.1.6 Security Function SOF Rationale

The Strength of Function (SOF) rating of SOF-basic was claimed for the security function SF.I&A to meet the EAL3+ assurance requirements. The rationale for the chosen level is based on the low attack potential of the threat agents as identified in this ST.

SOF-basic is achieved, as security function SF.I&A supports the enforcement of the following password policies:

- Only 5 incorrect sign in attempts are allowed before account lock out
- 8 characters required as the minimum passwords length
- passwords require both letters and numbers
- passwords require both upper and lower case characters
- passwords require non-Alphanumeric characters

This security function is consistent with the security objectives described in section 4.

6.2 TOE Assurance Measures

This section shows the evidence that will be provided by the developer to meet the assurance requirements identified in section 5. The following table provides a mapping of the assurance evidence documentation that demonstrates the satisfaction of the assurance requirements as stated in CC part 3. All the assurance requirements as stated in CC are satisfied by the evidence documents provided.

Table 6-1 TOE Assurance Measures

Assurance component	Assurance Measures
ACM_CAP.3	Third Brigade Development Environment - Configuration Management

Assurance component	Assurance Measures
ACM_SCP.1	Third Brigade Development Environment - Configuration Management
ADO_DEL.1	Third Brigade Development Environment - Product Delivery Procedures
ADO_IGS.1	Deep Security 5.0 Installation and Getting Started
ADV_FSP.1	Third Brigade Deep Security 5.0 Functional Specification
ADV_HLD.2	Third Brigade Deep Security 5.0 High Level design
ADV_RCR.1	Third Brigade Deep Security 5.0 Security Functionality Correspondence
AGD_ADM.1	Deep Security 5.0 User Manual
AGD_USR.1	Deep Security 5.0 User Manual
ALC_DVS.1	Third Brigade Development Environment – Security
ALC_FLR.1	Third Brigade Deep Security 5.0 Flaw Remediation
ATE_COV.2	Third Brigade Deep Security 5.0 Test Coverage Analysis
ATE_DPT.1	Third Brigade Deep Security 5.0 Test Depth Analysis
ATE_FUN.1	Third Brigade Deep Security 5.0 Functional Test Results
AVA_SOF.1	Third Brigade Deep Security 5.0 Security Strength Analysis
AVA_VLA.1	Third Brigade Deep Security 5.0 Vulnerability Analysis

7 PP Claims

The ST claims conformance to Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006.

8 Rationale

8.1 Introduction

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

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

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the ST. Table 8-1 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 8-1 Objectives vs. Security Environment

Objectives / Threats, Assumptions		TOE												Environment							
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME
Assumptions	A.ACCESS																	✓			
	A.DYNMIC																✓	✓			
	A.ASCOPE																	✓			
	A.PROTCT														✓						
	A.LOCATE														✓						
	A.MANAGE																✓				
	A.NOEVIL													✓	✓	✓					
	A.NOTRUST														✓	✓					

		TOE												Environment							
Threats	T.COMINT	✓						✓	✓			✓								✓	
	T.COMDIS	✓						✓	✓				✓							✓	
	T.LOSSOF	✓						✓	✓			✓									
	T.NOHALT		✓	✓	✓			✓	✓												
	T.PRIVIL	✓						✓	✓												
	T.IMPCON						✓	✓	✓					✓							
	T.INFLUX									✓											
	T.FACCNT										✓										
	T.SCNCFG		✓																		
	T.SCNMLC		✓																		
	T.SCNVUL		✓																		
	T.FALACT					✓															
	T.FALREC				✓																
	T.FALASC				✓																
	T.MISUSE			✓							✓										
	T.INADVE			✓							✓										
	T.MISACT			✓							✓										
OSPs	P.DETECT		✓	✓							✓										✓
	P.ANALYZ				✓																
	P.MANAGE	✓					✓	✓	✓					✓		✓	✓				
	P.ACCESS	✓						✓	✓										✓		
	P.ACCACT								✓		✓										✓
	P.INTGTY											✓									
	P.PROTCT									✓					✓					✓	

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

The O.INTROP objective ensures the TOE has the needed access.

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

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

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

	The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
	The O.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
	The O.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
	The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
	The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The TOE can only be accessed by authorized users.
	The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self protection. The OE.PROTECT objective addresses this threat by ensuring that the environment protects the TOE from tempering and enforces the TSC.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective addresses this threat by ensuring that the environment protects the TOE from tempering and enforces the TSC.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self protection.

T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a Scanner.

T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources. The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data. OE.TIME supports this policy by providing the audit functions with reliable time stamps.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken. The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.MANAGE	The TOE shall only be managed by authorized users. The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self protection.

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

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection. The OE.AUDIT_PROTECTION objective supports this policy by ensuring that there will be no back door for accessing the audit data using meanings outside the TSC.

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

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. OE.TIME supports this policy by providing the audit functions with reliable time stamps.

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

The O.INTEGR objective ensures the protection of data from modification.

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

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports this policy by ensuring that the environment protects the TSC.

8.3 Security Functional Requirements Rationale

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

Table 8-2 Requirements vs. Objectives Mapping

Objectives / Requirements		TOE												Env.		
		O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	OE.AUDIT_PROTECTION	OE.PROTECT	OE.TIME
TOE	FAU_GEN.1										✓					
	FAU_SAR.1						✓									
	FAU_SAR.2							✓	✓							

		TOE												Env.		
	FAU_SAR.3						✓									
	FAU_SEL.1						✓				✓					
	FAU_STG.4									✓	✓					
	FIA_UAU.1							✓	✓							
	FIA_ATD.1								✓							
	FIA_UID.1							✓	✓							
	FMT_MOF.1	✓						✓	✓							
	FMT_MTD.1a	✓						✓	✓			✓				
	FMT_MTD.1b	✓						✓	✓			✓				
	FMT_SMF.1							✓	✓							
	FMT_SMR.1								✓							
	FPT_ITT.1											✓	✓			
	IDS_SDC.1		✓	✓												
	IDS_ANL.1				✓											
	IDS_RCT.1					✓										
	IDS_RDR.1						✓	✓	✓							
	IDS_STG.1	✓						✓	✓	✓		✓				
	IDS_STG.2									✓						
Environment	FAU_STG.2	✓						✓	✓	✓		✓		✓		
	FPT_RVM.1	✓					✓		✓		✓	✓			✓	
	FPT_SEP.1	✓					✓		✓		✓	✓			✓	
	FPT_STM.1										✓					✓

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

The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE with appropriate rights assigned may query and add audit and other TOE data [FMT_MTD.1a and FMT_MTD.1b].The environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2]. The environment must ensure that all TOE functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The environment must protect the TSF from interference that would prevent it from performing its functions [FPT_SEP.1].

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

A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1].

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

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

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

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

O.RESPON The TOE must respond appropriately to analytical conclusions.

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

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

The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The environment must ensure that all TOE functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The environment must protect the TSF from interference that would prevent it from performing its functions [FPT_SEP.1].

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. The TOE is required to provide the ability to managing the behavior of functions of the TOE [FMT_SMF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2].

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

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE is required to provide the ability to managing the behavior of functions of the TOE [FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2]. The environment must ensure that all TOE functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The environment must protect the TSF from interference that would prevent it from performing its functions [FPT_SEP.1].

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

The TOE must prevent the loss of audit data in the event that its audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of audit data in the event that its audit trail is full [IDS_STG.2]. The environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2].

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU_SEL.1]. The TOE must prevent the loss of collected data in the event its audit trail is full [FAU_STG.4]. The environment must ensure that all TOE functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The environment must protect the TSF from interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

O.INTEGR The TOE must ensure the integrity of all audit and System data.

The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or change audit and System data [FMT_MTD.1]. The TOE must protect the system data's confidentiality and ensure its integrity when the data is transmitted to between different parts of the TOE [FPT_ITT.1]. The environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2]. The environment must ensure that all TOE functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The

environment must protect the TSF from interference that would prevent it from performing its functions [FPT_SEP.1].

O.EXPORT When any IDS component makes its data available to another IDS components, the TOE will ensure the confidentiality of the System data.

The TOE must protect the system data's confidentiality and ensure its integrity when the data is transmitted to between different parts of the TOE [FPT_ITT.1].

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

The environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, or failure [FAU_STG.2].

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

The IT environment is required to provide reliable timestamps to parts of the TOE [FPT_STM.1].

OE.PROTECT The IT environment will protect itself and the TOE from external interference or tampering.

The environment must ensure that all TOE functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The environment must protect the TSF from interference that would prevent it from performing its functions [FPT_SEP.1].

8.4 Explicitly Stated Requirements Rationale

This Security Target does not identify any explicitly stated requirements. However the claimed PP does create a family of IDS requirements to specifically address the data collected and analysed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.5 Security Functional Requirements Dependency Rationale

The SFRs in Section 5 do satisfy all the requirement dependencies of the Common Criteria. Table 8-3 Requirement Dependencies lists each requirement from the ST with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 8-3 Requirement Dependencies Rationale

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	Yes, FPT_STM.1 is provided by the IT environment.
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	Yes

SFR ID	Dependencies	Dependency Met
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.2	Yes, FAU_STG.2 is provided by the IT environment.
FIA_UAU.1	FIA_UID.1	Yes
FMT_MOF.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 and FMT_SMR.1	Yes
FMT_SMR.1	FIA_UID.1	Yes

8.6 Assurance Requirements Rationale

EAL3+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment, and reasonable assurance is provided to ensure the secure operation of the system.

8.7 TOE Summary Specification Rationale

8.7.1 TOE IT Security Functions Rationale

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

Table 8-4 TOE Security Functions Rationale

IT Security Functions	SFRs	Rationale
SF.AUDIT	FAU_GEN.1	SF.AUDIT supports the generation of audit records in accordance with table 5-2.
	FAU_SAR.1	SF.AUDIT allows only authorised administrators read access to audit information.
	FAU_SAR.2	
	FAU_SAR.3	SF.AUDIT supports the sorting of audit records using records attributes.
	FAU_SEL.1	SF.AUDIT provides the capability of selective auditing.
	FAU_STG.4	SF.AUDIT prevents auditable events from occurring and records unpreventable events by overwriting the oldest stored audit records when audit trail becomes full.
SF.RBAC	FMT_MOF.1	SF.RBAC allows only administrators with appropriate roles to modify TOE security functions/data.

IT Security Functions	SFRs	Rationale
	FMT_MTD.1a	SF.RBAC assigns users with “Full Access” role with the right to perform all security functions.
	FMT_MTD.1b	SF.RBAC allows Auditor only read access to all information.
	FMT_SMF.1	SF.RBAC gives Administrators with appropriate roles access to functions for managing TOE security functions/data.
	FMT_SMR.1	Full Access and Auditor are the default roles supported by SF.RBAC.
SF.I&A	FIA_ATD.1	SF.I&A maintains user security attributes.
	FIA_UAU.1	SF.I&A requires users to be positively authenticated, before granting access to the TOE.
	FIA_UID.1	SF.I&A requires users to be positively identified, before granting access to the TOE.
SF.SECCOM	FPT_ITT.1	SF.SECCOM secures the internal communication using symmetric encryption.
SF.IDPS	IDS_SDC.1	SF.IDPS supports the generation of audit records in accordance with table 5-3.
	IDS_ANL.1	SF.IDPS performs analysis of network traffic based on statistics, attack signatures or integrity of the network traffic.
	IDS_RCT.1	Upon discovery of attacks, SF.IDPS sends email alarms to the appropriate administrator and prevents the attack.
	IDS_RDR.1	SF.IDPS allows authorised administrators read access to audit information.
	IDS_STG.1	SF.IDPS protects the event log and overwrites the oldest stored records with newest records upon storage exhaustion.
	IDS_STG.2	

8.7.2 TOE Strength of Function Rationale

This section demonstrates that the TOE Strength of Function claim made in the ST is consistent.

SOF-basic was claimed for the user identification and authentication SFRs: FIA_UAU.1 and FIA_UID in section 5.3 of this Security Target. SOF-basic was also claimed for the security function SF.I&A in section 6.1.6 of this Security Target.

Because section 5.3 and section 6.1.6 had both claimed SOF-basic, TOE Strength of Function claims are consistent through out this ST.

8.7.3 TOE Assurance Measures Rationale

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

Table 8-5 TOE Assurance Measures Rationale

Assurance component	Assurance Measures	Rationale
ACM_CAP.3	Third Brigade Development Environment - Configuration Management	The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at Third Brigade. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system describes the 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.
ACM_SCP.1		
ADO_DEL.1	Third Brigade Development Environment - Product Delivery Procedures	The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Third Brigade to protect against TOE modification during product delivery.
ADO_IGS.1	Deep Security 5.0 Installation and Getting Started	The Installation Documentation provided by Third Brigade details the procedures for installing the TOE and placing the TOE in a secure state. The Installation Documentation provides guidance to the administrators of the TOE regarding configuration parameters and how they affect the TSF.
ADV_FSP.1	Third Brigade Deep Security 5.0 Functional Specification	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.
ADV_HLD.2	Third Brigade Deep Security 5.0 High Level design	The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TOE. The high-level design identifies the basic structure of the TOE, the major elements, a listing of all interfaces, and the purpose and method of use for each interface including list of effects, exceptions, and errors message for each interface.
ADV_RCR.1	Third Brigade Deep Security 5.0 Security Functionality Correspondence	The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show that the security functions can be traced from the ST description to the Functional Specification, then to the High-Level Design.
AGD_ADM.1	Deep Security 5.0 User Manual	The Deep Security 5.0 Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information for operating the TOE in a secure manner

Assurance component	Assurance Measures	Rationale
AGD_USR.1		and how to effectively use the TSF privileges and protective functions. Third Brigade provides a single version of the document which addresses the administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.
ALC_DVS.1	Third Brigade Development Environment – Security	The Development Security documentation provides a description of the physical and personnel measures used to provide development security at Third Brigade. It describes the procedures that are used by Third Brigade to protect the confidentiality and integrity of the TOE design and implementation.
ALC_FLR.1	Third Brigade Deep Security 5.0 Flaw Remediation	The Flaw Remediation document outlines the steps taken at Third Brigade to capture, track and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion.
ATE_COV.2	Third Brigade Deep Security 5.0 Test Coverage Analysis	The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested.
ATE_DPT.1	Third Brigade Deep Security 5.0 Test Depth Analysis	The Depth Analysis demonstrates the testing performed against the high level design. Depth Analysis also demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested.
ATE_FUN.1	Third Brigade Deep Security 5.0 Functional Test Results	Third Brigade Functional Test Results details the overall efforts of the testing and break down the specific steps taken by a tester.
AVA_SOF.1	Third Brigade Deep Security 5.0 Security Strength Analysis	The Security Strength 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 as claimed in the ST.
AVA_VLA.1	Third Brigade Deep Security 5.0 Vulnerability 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, the document provides evidence of how the TOE is resistant to obvious attacks.