Triumfant, Inc.
Resolution Manager 4.2

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.2

Prepared for:

Triumfant, Inc.
Three Irvington Center
800 King Farm Boulevard
Suite 220
Rockville, MD 20850
Phone: (301) 917-6280

http://www.triumfant.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	2007-03-20	Amy Nicewick	Initial draft.
0.2	2007-07-31	Amy Nicewick	Addressed verdicts of OR-01 and other Corsec-identified changes.
0.3	2007-09-14	Amy Nicewick	Addressed OR-03 and follow-up verdicts for OR-01.
0.4	2007-09-18	Amy Nicewick	Addressed OR-04.
0.5	2008-02-13	Amy Nicewick	Updated to v4.2.
0.6	2008-02-28	Amy Nicewick	Addressed OR-5 and CB-ASE-OR-1.
0.7	2008-05-22	Greg Milliken	Added Altiris Agent to the list of exluded functionality. Changes added to address OR-07.
0.8	2008-06-30	Greg Milliken	More changes for OR-07.
0.9	2008-08-12	Greg Milliken	Addressed unresolved issues.
1.0	2008-10-16	Amy Nicewick	Removed Altiris from diagram, and changed version number to 4.2.
1.1	2008-12-02	Greg Milliken	Added a clarification to A.REMEDY, NOE.REMEDY, and section 2.2.1. Removed references to Configuration Service.
1.2	2008-12-22	Greg Milliken	Removed configuration service from FRU_FLT.1. Added version info to section 2.2

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 Triumfant Resolution Manager 4.2. The Resolution Manager 4.2 is a software-only incident and problem management system.

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.
- Product Overview (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	Triumfant, Inc. Resolution Manager 4.2 Security Target
ST Version	Version 1.2
Author	Corsec Security, Inc. Amy Nicewick and Matt Keller
TOE Identification	Triumfant Resolution Manager 4.2
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, [August 2005] (aligned with ISO/IEC 15408:2005); CC Part 2 extended; CC Part 3 extended; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted Common Methodology for Information Technology Security Evaluation (CEM) as of 2007/04/25 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level (EAL)	EAL2+ (EAL 2 augmented with ALC_FLR.1 and ADV_SPM.1)
Keywords	Problem Management, Incident Management

1.3 Conventions, Acronyms, 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 presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis 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.

1.3.2 Acronyms

The acronyms used within this ST are described in Section 9 – "Acronyms."

1.3.3 Terminology

The term "operator" is defined in this document to include only those individuals who manage the TOE and manage the TOE Security Function (TSF) data.

The terms "user" and "end-user" are defined in this document as any individual who accesses the targeted system upon which the TOE is installed.

The term "targeted system data" refers to data collected from targeted machines and the analysis results for those targeted machines. For the purposes of CC, this is also the definition of "user data".

2 Product Overview

This section provides an overview of the Resolution Manager 4.2 product. This section describes the general capabilities and security functionality of the product. The product overview 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

Resolution Manager 4.2 is a software-only incident and problem detection and resolution management system. Agents are installed onto workstations, laptops, and servers to gather detailed state and status information. Resolution Manager 4.2 extracts statistically significant relationships from this information and generates an adaptive reference model. This model defines what is normal for that particular managed population at that particular moment in time, and is updated (i.e., adapted) regularly to reflect changes in the managed population. There is an operator-defined set of recognition filters that checks managed machines against the model for invalid settings and undesirable applications. There is also an operator-defined set of policy templates that can be applied to the model to force settings or applications to be accepted as part of the model. These capabilities enable Resolution Manager 4.2 to analyze the state of each machine on a routine basis to discover anomalies, or deviations from normal for a specific customer environment. Anomalies are then correlated and interpreted by recognition filters to produce an actionable result. If this result is a trouble or warning condition, then Resolution Manager 4.2 can be configured to trigger a variety of automated responses to notify administrators or automatically and optionally remediate the condition by precision removal or replacement of the files and registry settings that uniquely identify the condition.

Figure 1 below shows the details of the deployment configuration of the Resolution Manager 4.2:

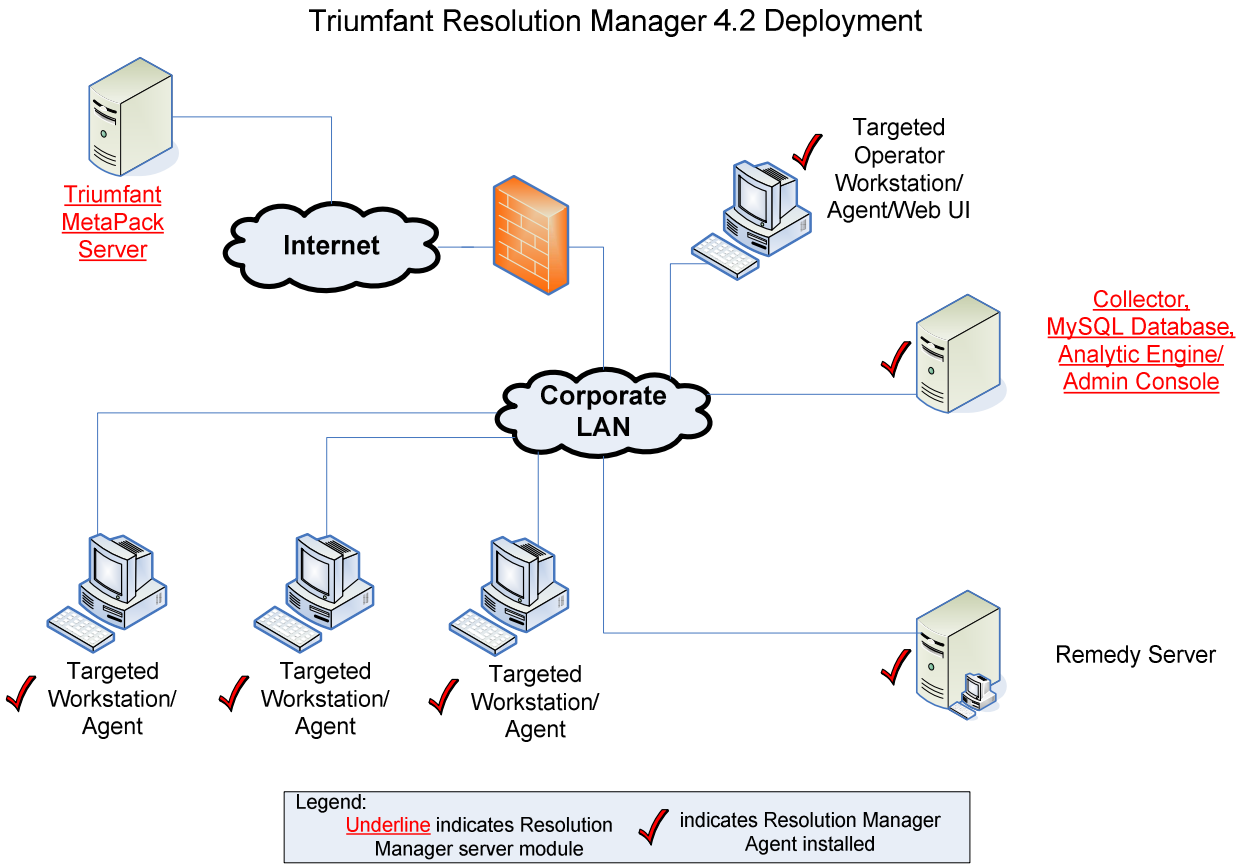

Figure 1 - Deployment Configuration of the Resolution Manager 4.2

2.2 Product Description

Resolution Manager 4.2 is composed of four main components:

- Agent
- Collector
- MySQL Database
- Analytic Engine/Admin Console

For all components except the WebUI, the version for the TOE is 4.2.67. The WebUI version is 4.2.25

Each component can be installed on its own machine, or all components can be loaded on a single machine, if desired. Agents are deployed on all managed machines in a customer environment. For this CC evaluation, the Collector, MySQL Database, and Analytic Engine/Admin Console components will reside on a single customer server. The Resolution Manager 4.2 customer server "calls home" to the Triumfant Metapack Server when it is ready to receive updated recognition filter, policy template, and report information. All server-to-Agent and server-to-Metapack Server transmissions are via HTTPS. The Triumfant Metapack Server provides updated recognition filters, policy templates, and reports to multiple customer implementations of Resolution Manager 4.2.

2.2.1 Brief Description of the Components of the Product

Agent:

The Resolution Manager 4.2 Agent is installed on each targeted machine. Its primary functions are to routinely and systematically gather data and perform remediations as needed. At scheduled intervals (typically once per day) the Agent sends a detailed scan of the state and status of the machine upon which it is installed. This scan includes an examination of the registry, system files, processes, services, ports, application files, performance metrics, and hardware configurations. The results of the scan are compressed and transmitted to the Collector component in the form of a snapshot.

Agent software may be installed on Microsoft Windows XP SP2 operating systems.

Collector:

The Resolution Manager 4.2 Collector resides on a centrally-located server, is comprised of services that manage the actions of the Agents, and collect and process snapshots from the Agents. The Collector also stores and retrieves data from the MySQL database. In addition, the Collector provides WebUI functionality to an operator workstation. The WebUI is a web-based user interface that allows service desk personnel, or operators, to view analysis results produced by Resolution Manager 4.2 and to activate responses. WebUI transmissions between the Collector and the operator workstation are passed via Hypertext Transmission Protocol over SSL (HTTPS).

The Collector optionally provides bi-directional links to a helpdesk application (Remedy) concerning the status of each managed machine. Helpdesk operators use this information to provide aid to end-users and to resolve issues on end-users' workstations.

The Collector communicates with the targeted workstations and with the Remedy application via Internet Information Services (IIS), a web server for use with Microsoft Windows operating systems. These transmissions are recommended to be passed via HTTPS. Collector software may be installed on Microsoft Windows Server 2003 operating systems.

MySQL Database:

The MySQL v5.0 database is bundled with the Resolution Manager 4.2. The database provides non-volatile storage for all non-configuration server data, including recognition filters, policy templates, adaptive reference models, operator authentication data, and diagnostic check results. It also stores all snapshots collected from Agents on the targeted workstations. Snapshots are kept in the database for seven days. MySQL was chosen for its speed. Resolution Manager needs this speed to efficiently and unobtrusively perform its data collection and analysis

functions. The Collectors and the Analytic Engine access and update the MySQL database using Open Database Connectivity (ODBC) Application Programming Interface (API).

The database may be installed on Microsoft Windows Server 2003 operating systems.

Analytic Engine/Admin Console:

The Analytic Engine performs data analysis and provides an administrative console for the Console Operator to perform management functions on the system.

The Analytic Engine generates adaptive reference models, executes scheduled diagnostic checks, and filters diagnostic results. Adaptive reference models reflect the "normal" state of the Agents at a given point in time. These models are then used for comparison with "snapshots" of the Agents to determine whether there are any anomalies present on the managed machines where the Agents are active. There are three types of anomalies that the Analytic Engine could identify.

- Unexpectedly Present – the associated attribute was found in a context where it was not expected. An example of this would be an attribute or application that is unique across the entire managed population.
- Unexpectedly Absent – the associated attribute is considered missing. An example would be the absence of a file that had been determined to be a required component of a "normal" machine.
- Unknown Value – the value associated with the attribute is not normal and the new value violates a consistent, frequently occurring pattern. An example would be a corrupt file whose hash value will be different from that of all the other instances of that file in the managed population.

Email notifications to Resolution Manager 4.2 operators and to Triumfant customer support are transmitted via SMTP from the Analytic Engine. These emails are outgoing only. Resolution Manager 4.2 does not accept incoming emails.

The Admin Console is a thick client user interface that provides the capabilities needed to configure system options, manage analytic tasks, and create recognition filters and policy templates.

Analytic Engine software may be installed on Microsoft Windows Server 2003 operating systems.

2.2.2 The Automated Resolution Process

The Resolution Manager 4.2 performs the following tasks in the automated resolution process:

- Build a Reference Model – The first step in the process is to create a rule base that defines the machine states that are considered "normal" at a given point in time. This rule base is called an adaptive reference model. The Resolution Manager 4.2 generates the model by comparing the detailed state information of one machine to the detailed state information of all other machines in a specified group. The objective of this comparison is to identify patterns that can be turned into rules. For example, if a specified system file is always found in machines that also have a specific registry value, then a pattern exists. The adaptive reference model would then contain a rule that states: if the specified system file is present, then the specified registry value must also exist. By default, adaptive reference models are built weekly.
- Define Policy Templates – Policy templates are very detailed and well-structured means to capture policies. These policy templates can be defined to eliminate vulnerabilities and to reduce the probability of incidents. For example, a policy template could be used to define a policy that specifies the required versions for a set of critical applications. A default set of policy templates is shipped with the product.
- Apply Policies to Models – Once an adaptive reference model is created, policy templates can be applied to the model to adjust the definition of "normal".
- Check Snapshots Against Model – Snapshots are periodically taken of each machine. Snapshots are collections of attributes and values that represent the state of a computer at a particular point in time. The Resolution Manager 4.2 performs a periodic check of the latest snapshots against the most recent adaptive reference model. The output of this check is a set of anomalies. The recommended (and default) period for these checks is one day.

- Diagnose Conditions – Recognition filters are employed by the Resolution Manager 4.2 to interpret the identified anomalies. The result of applying the set of filters to a snapshot is a set of conditions. Some conditions equate to known errors, while others correspond to unknown errors, or problems. If the result is an unknown error, the Resolution Manager 4.2 applies a set of generic recognition filters that focus on unusual changes. If the result is a known error or problem, a response is available. Recognition filters are collections of attributes and values that, taken together, represent the signature of a condition. The Resolution Manager 4.2 provides a set of problem analysis tools that can automatically characterize a new problem and help determine it root cause.
- Activate Responses – Resolution Manager 4.2 automatically recognizes and can respond to known errors. Examples of automated responses include sending notification emails, installing missing updates, correcting corrupted options settings, and removing malicious software. Responses can be triggered automatically or manually, depending on the system configuration.
- Collect New Snapshots – In order to verify that error conditions have been resolved, the Resolution Manager 4.2 collects new snapshots of an individual machine or all the machines in a given group, and executes a new diagnostic check either periodically or on demand.
- Generate Reports – The Resolution Manager 4.2 provides a report generator that produces and distributes a wide variety of report types in multiple document formats. These reports document the results of the automated resolution management process.
- Optional tasks:
    - Define/Export Filters – The problem analysis tools produce outputs that feed directly into the filter creation environment, enabling unknown errors to be identified and stored as known errors. These recognition filters can be exported and shared.
    - Import Filters – New recognition filters are developed by Triumfant, and can regularly be imported by Resolution Manager 4.2. These new recognition filters identify previously unknown conditions. Filters are contained in Metapacks.

Figure 2 provides an outline of the automated resolution process.

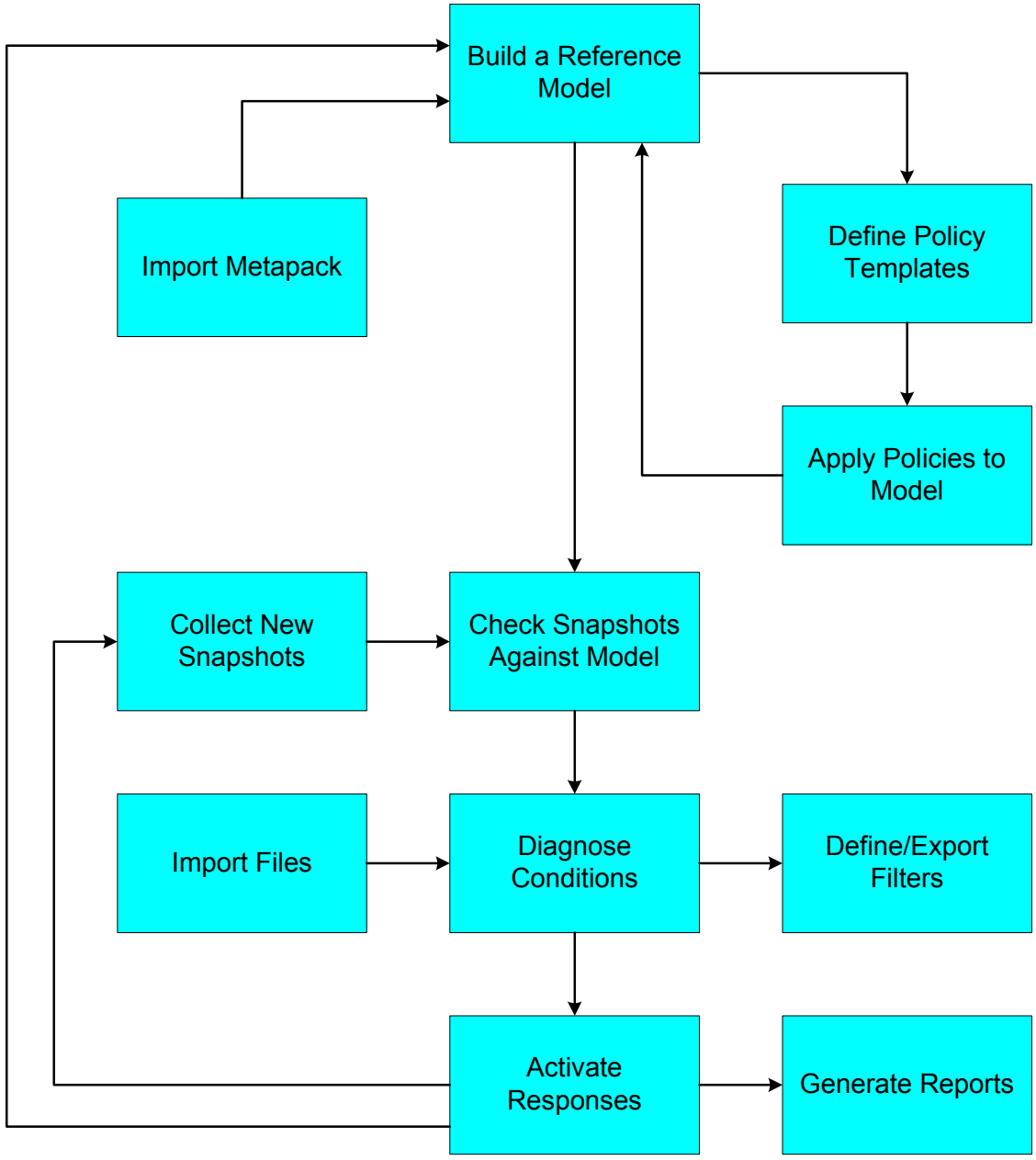

Figure 2 – Resolution Management Process Flow Chart

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the Resolution Manager 4.2 are included in evaluation. These components of the Resolution Manager 4.2 will hereafter be referred to as the TOE throughout this document.

2.3.1 Physical Boundary

Figure 3 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 a software-only incident and problem management system, which runs on Windows platforms compliant to the minimum software and hardware requirements as listed in Table 2 below. The TOE is installed in an Information Technology (IT) environment as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Agent
- Collector
- MySQL Database
- Analytic Engine/Admin Console

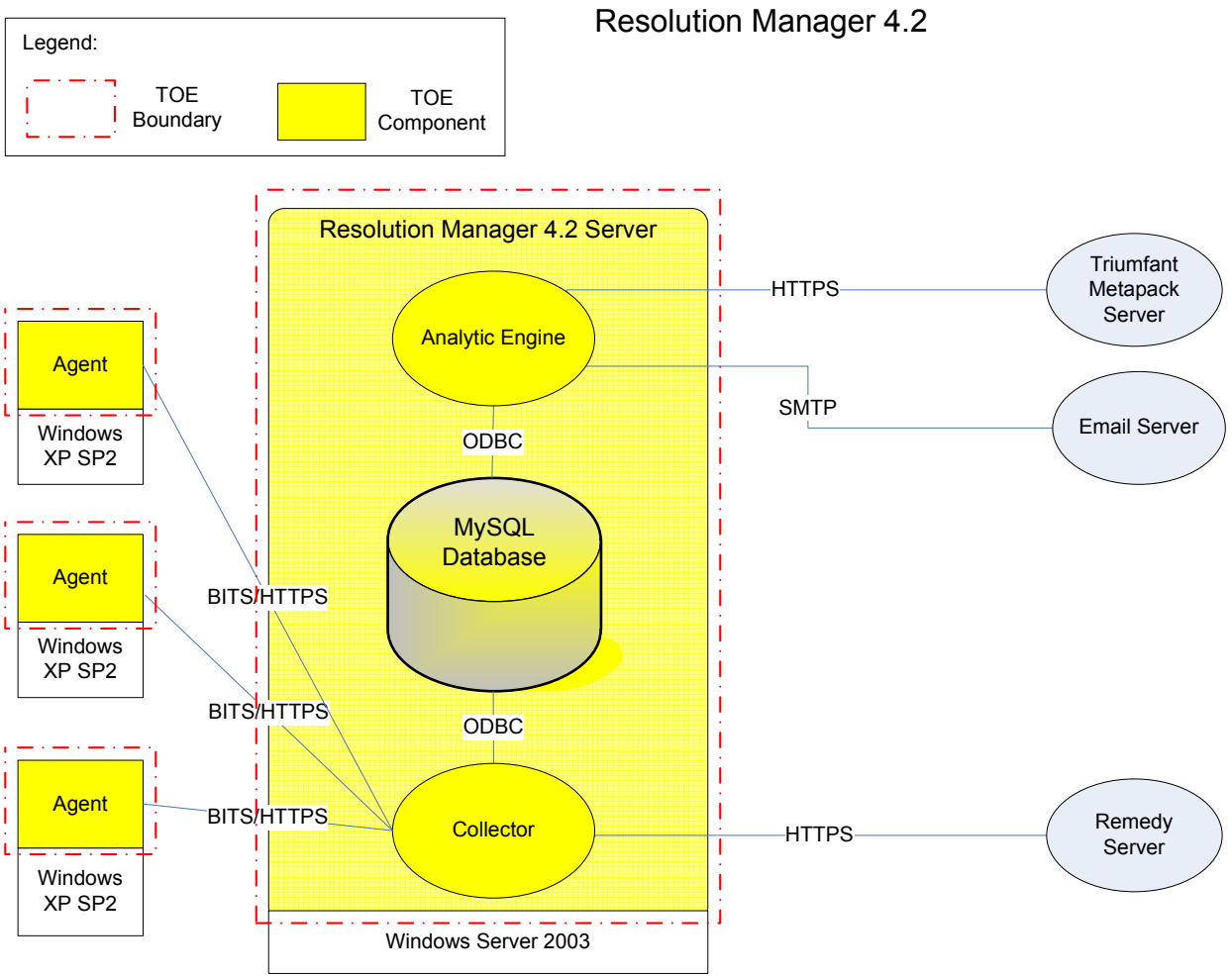

Figure 3 - Physical TOE Boundary

2.3.1.1 TOE Software

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- Agent: The Agent is the data-gathering functionality running on a Windows XP SP2 platform with any number of User Interactive Programs and Third-party Applications installed and running. The hardware, operating system, User Interactive Programs, and Third-party Applications are excluded from the TOE.
- Collector: The Collector is the Agent and WebUI management functionality running on a Windows Server 2003 platform. The hardware and operating system are excluded from the TOE Boundary.

- MySQL Database: The Database is the MySQL database running on a Windows Server 2003 platform. The hardware and operating system are excluded from the TOE Boundary.
- Analytic Engine/Admin Console: The Analytic Engine/Admin Console is the analysis functionality of the system and the thick client user interface utilized by the TOE Console Operator to manage the TSF data. It runs on a Windows Server 2003 platform. The hardware and operating system are excluded from the TOE Boundary.

The Agent may reside on any platform running Microsoft Windows XP SP2 (as shown in Figure 3 above), and on any number of workstations in an enterprise. The Collector, MySQL Database, and Analytic Engine will be housed on a single Windows Server 2003 with the minimum system requirements as specified in Table 2 below:

Table 2 - TOE Minimum Requirements

Category	Requirement
Central Processing Unit (CPU)	One 2+ GigaHertz (GHz) Dual Core Xeon® 5140 or equivalent
Random Access Memory (RAM)	4 GigaBytes (GB)
Network Interface Card (NIC)	1000 Megabits per second (Mbps)
Disk Space	C:\ - 10 GB Other – 100 GB
Software[1]	IIS 6.0 Microsoft .NET Framework 2.0 Background Intelligent Transfer Service (BITS) 1.5

2.3.1.2 TOE Environment

The TOE Environment consists of the Windows operating systems and the hardware platform on which the components are installed. The Triumfant MetaPack Server and the E-mail server are required components of the TOE Environment. The TOE Environment may also contain the Remedy server.

2.3.2 Logical Boundary

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

- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access
- Resolution Manager Functions

2.3.2.1 User Data Protection

The User Data Protection function implements functionality for TOE security functions and TOE security function policies related to protecting the data gathered from the targeted workstations. This functionality is provided by the

[1] The TOE requires this software to run, however, the software listed in Table 2 should be considered part of the TOE environment.

Resolution Manager 4.2 WebUI (on the Collector) and the Admin Console. The TOE controls operator access to data collected from targeted systems, which will be referred to throughout this evaluation as the user data. The paradigm of subjects accessing objects via operations is used to describe the access control rules enforced by the TOE.

2.3.2.2 Identification and Authentication

The Identification and Authentication function provides functionality to establish and verify a claimed operator identity. This ensures that operators are associated with the proper security attributes, such as identity and roles. The TOE supports internally enforced operator username and password based authentication.

2.3.2.3 Security Management

The Security Management function specifies the management of several aspects of the TSF: security attributes, TSF data, and security functions behavior. The definition of the different management roles and their interactions are also part of this security function.

2.3.2.4 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The TOE protects information when specific failures within the TOE occur, such as specific application services. The TOE enforces non-bypassability of the security functions as it is designed in such a way to force access through key security features, such as identification and authentication and role-based access control mediation. The TOE is separated from other processes by the operating system.

2.3.2.5 Resource Utilization

The Resource Utilization function supports the availability of required resources such as storage capacity. Resource Utilization ensures the operation of all other Collector services when a failure occurs in one of the Collector services.

2.3.2.6 TOE Access

The TOE Access function controls the establishment of an operator's session. TOE Access provides TSF-initiated session locking of an interactive session after a configurable period of operator inactivity.

2.3.2.7 Resolution Management Functions

The Resolution Management Functions provide the incident and problem management of the data gathered by the Agents. This data includes file hash values, open network ports, security settings, applications, patches, running processes, services, performance metrics, server logins, disk throughput, and registry keys. The data collected includes date and time of the last snapshot of targeted system data, machine name, machine identifier, and snapshot data collected.

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

The features and functionality that are not part of the evaluated configuration of the TOE are:

- Windows Operating System
- General Purpose Computing Platform (Hardware)
- Other Applications running on the same targeted system as the Resolution Manager Agent
- Remedy Server
- Triumfant Metapack Server
- Altiris Server
- Altiris Agent

- Active Directory authentication

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.

Name	Description
A.NOEVIL	Operators are non-hostile, appropriately trained, and follow all operator guidance.
A.PHYSCAL	The Analytic Engine, the Collector, and the MySQL database components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.CONSOLE	The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data.
A.REMEDY	The TOE Environment will identify and authenticate Remedy helpdesk operators prior to allowing access to TOE administrative functions and data. The TOE and Remedy Server must be placed in a controlled environment

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 operators: 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 operators: 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 operators 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 – Security Objectives.

The following threats are applicable:

Name	Description
T.RES	A user might perform unauthorized actions (e.g., changing of settings or addition, deletion, or modification of software applications) on a targeted IT system which would compromise the security of the targeted IT system or make improper use of system resources.
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.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

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 in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

Name	Description
O.AGENT	The TOE Agent must collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on the Agent machine.
O.COLLECT	The TOE Collector must collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on IT System assets and the Agent machines.
O.ANALYZE	The TOE Analytic Engine must accept data from TOE Agents or TOE Collectors and then apply analytical processes and information to derive conclusions about anomalies.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.IDAUTH	The TOE must be able to identify and authenticate WebUI operators prior to allowing access to TOE administrative functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.INTEGR	The TOE must ensure the integrity of all System data.

O.PROTECT	The TOE must protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows.

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:

Name	Description
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.SEP	The IT Environment will protect the TOE from external interference or tampering.
OE.AUDIT	The IT Environment will gather audit records of start-up, shutdown, and access to the TOE.
OE.SSL	The IT Environment will protect the System data from disclosure during transmission between TOE components.
OE.RVM	The IT Environment will protect TOE data stored temporarily in the environment from external interference or tampering.
OE.CONSOLE	The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data.

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.

Name	Description
NOE.NOEVIL	Operators are non-hostile, appropriately trained, and follow all operator guidance.
NOE.PHYSICAL	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
NOE.REMEDY	The TOE Environment will identify and authenticate Remedy helpdesk operators prior to allowing access to TOE administrative functions and data. The TOE and Remedy Server must be placed in a controlled environment

5 Security Requirements

This section defines the SFRs and 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 3 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 3 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_ROL.1	Basic rollback		✓		
FIA_UAU.2(a)	User authentication before any action			✓	
FIA_UID.2(a)	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_FLS.1	Failure with preservation of secure state		✓		
FPT_RVM.1(a)	Non-bypassability of the TSP				✓
FRU_FLT.1	Degraded fault tolerance		✓		
FTA_SSL.1	TSF-initiated session locking		✓	✓	

RES_SDC.1	System data collection (EXP)				
RES_ANL.1	Analyser analysis (EXP)				
RES_RCT.1	Analyser react (EXP)				
RES_SEL.1	Selective data collection (EXP)				
RES_STG.2	Prevention of System data loss (EXP)				

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

Section 5.1 contains the functional components from the CC Part 2 and five explicitly stated requirements with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 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 [A*ccess Control SFP*] on [*authenticated operators attempting to access targeted system data*].

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 (authenticated operators) attributes:*

1) Role;

OBJECT (targeted system data) attributes:

1) Population Group].

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) a WebUI operator must be authenticated to the TOE; and

2) *the authenticated operator must have the Role of Console Operator, Administrator, SuperUser, ReadOnly, or Helpdesk Operator; and*

3) *the authenticated operator must be authorized to access the Population Group to which the targeted system belongs*].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

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

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

FDP_ROL.1.1

The TSF shall enforce [*Access Control SFP*] to permit the rollback of the [*remediation actions taken by the TOE*] on the [*targeted system*].

FDP_ROL.1.2

The TSF shall permit operations to be rolled back within the [*boundary limit of available disk space on the targeted system to retain the remediated content*].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

5.1.2 Class FIA: Identification and Authentication

FIA_UAU.2(a) User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2(a)User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

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

Dependencies: No dependencies

5.1.3 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 [*perform the actions indicated in Table 4 below*] the functions [*in the Security Function column of Table 4 below*] to [*the roles as specified in Table 4 below*].

Table 4 - Management of Security Functions Behaviour

Roles / Security Function	Console Operator	Administrator	SuperUser	ReadOnly	Helpdesk Operator
Snapshot Collection	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	None	determine the behaviour of, disable, enable, modify the behaviour of
Response Initiation	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	None	determine the behaviour of, disable, enable, modify the behaviour of
Undo Remediation	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	None	determine the behaviour of, disable, enable, modify the behaviour of
Reporting	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of
View Analysis Results	enable	enable	enable	enable	enable

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 [*perform the actions indicated in Table 5 below*] the security attributes [*in the Security Attribute column of Table 5 below*] to [*the roles as specified in Table 5 below*].

Table 5 - Management of Security Attributes

Roles / Security Attribute	Console Operator	Administrator	SuperUser	ReadOnly	Helpdesk Operator
Passwords	None	Create Modify Delete	None	None	None
Usernames	None	Query Create Modify Delete	None	None	None
Roles	None	Change_default Query Modify Delete	None	None	None
Assigned Population Groups	Query Modify Delete	Query Modify Delete	None	None	None

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 [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Console Operator, Administrator*] 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 [*change_default, query, modify, delete*] the [*system options, analytic tasks, recognition filters, policy templates*] to [*Console Operators*].

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: [*security function management, security attribute management, and TSF data management*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Console Operator, Administrator, SuperUser, ReadOnly, and Helpdesk Operator*].

FMT_SMR.1.2

The TSF shall be able to associate ~~users~~ **operators** with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*failure of Data Bridge Service, Agent Management Service, Internal Messaging Service, or Business Object Service*].

Dependencies: ADV_SPM.1 Informal TOE security policy model

FPT_RVM.1(a) 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

5.1.5 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

FRU_FLT.1.1

The TSF shall ensure the operation of [*all other listed services*] when the following failures occur: [*one of the following services is not active: Data Bridge Service, Agent Management Service, Internal Messaging Service, and Business Object Service*].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

5.1.6 Class FTA: TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.

FTA_SSL.1.1

The TSF shall lock an interactive session after [*a default time interval of 60 minutes of WebUI operator inactivity, and when the WebUI operator attempts another action*] by:

a) Clearing or overwriting display devices, making the current contents unreadable;

b) Disabling any activity of the ~~user's~~ **operator's** data access/display devices other than unlocking the session.

FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: [*operator login*].

Dependencies: FIA_UAU.1 Timing of authentication

Application Note: Exceptions to this include reports and analysis results. These do not track operator inactivity.

5.1.7 Class RES: Resolution Manager Functions (RES)

RES_SDC.1 System Data Collection (EXP)

RES_SDC.1.1

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

a) File hash values, open network ports, security settings, applications, patches, running processes, services, performance metrics, server logins, disk throughput, and registry keys; and

b) No other events. (EXP)

RES_SDC.1.2

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

a) Date and time of last snapshot of targeted system data, machine name, machine identifier, snapshot data collected; and

b) No other information. (EXP)

RES_ANL.1 Analyzer analysis (EXP)

RES_ANL.1.1

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

a) Comparison of snapshot of targeted system data to adaptive reference model; and

b) No other events. (EXP)

RES_ANL.1.2

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

a) Date and time of snapshot, type of check task (origin), snapshot identifier, check task identifier, adaptive reference model identifier, adaptive reference model name, customer name, machine name, number of anomalies, severity level, and details of anomalies; and

b) No other events. (EXP)

RES_RCT.1 Analyzer react (EXP)

RES_RCT.1.1

The System may take one or more of the following actions based on operator-defined configurations: Inform (end-user warning), Notify (email to operator), Install software, or Remediate an abnormal condition when an anomaly is detected. (EXP)

RES_STG.2 Prevention of System data loss (EXP)

RES_STG.2.1

The System shall suspend collection of targeted system data and send an alarm if the storage capacity has been reached. (EXP)

RES_SEL.1 Selective data collection (EXP)

RES_SEL.1.1

The TSF shall be able to include or exclude data from the set of collected data based on the following attributes:

a) Rules defined in the recognition filters; and

b) The recognition filters that are configured to be active. (EXP)

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.

Name	Description	S	A	R	I
EXP_FAU_GEN.1	Audit Data Generation				
FPT_ITT.1	Basic internal TSF data transfer protection	✓		✓	
FPT_SEP.1	TSF domain separation			✓	
FPT_STM.1	Reliable time stamps			✓	
FPT_RVM.1(b)	Non-bypassability of the TSP			✓	✓
FIA_UID.2(b)	User identification before any action			✓	
FIA_UAU.2(b)	User authentication before any action			✓	

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

5.2.1 Class FAU: Security Audit in the TOE Environment

EXP_FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

EXP_FAU_GEN.1.1

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

a) Start-up and shutdown of the Resolution Manager functions on the Server;

b) Start-up and shutdown of the Resolution Manager functions on the Agent; and

c) All connections to and disconnections from the WebUI.

EXP_FAU_GEN.1.2

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

a) outcome (start-up or shutdown) of the event; and

b) For WebUI connections, the machine name and port.

Dependencies: No dependencies.

5.2.2 Class FIA: Identification and Authentication

FIA_UAU.2(b) User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The ~~TSF~~ **TOE Environment** shall require each ~~user~~ **Admin Console and Helpdesk operators** to be successfully authenticated before allowing any ~~other~~ TSF-mediated actions on behalf of that ~~user~~ **Admin Console and Helpdesk operators**.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2(b) User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The ~~TSF~~ **TOE Environment** shall require each ~~user~~ **Admin Console and Helpdesk operators** to identify itself before allowing any ~~other~~ TSF-mediated actions on behalf of that ~~user~~ **Admin Console and Helpdesk operators**.

Dependencies: No dependencies

5.2.3 Class FPT: Protection of the TOE Environment

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

The ~~TSF~~ **TOE Environment** shall protect TSF data from [*disclosure*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

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 TOE's** execution that protects it 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 ~~its own~~ **the TOE's** use.

Dependencies: No dependencies

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

Hierarchical to: No other components.

FPT_RVM.1.1

The ~~TSF~~ **TOE Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function ~~within the TSC~~ **accessing TOE data** is allowed to proceed.

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 and ADV_SPM.1. Table 6 – Assurance Requirements summarizes the requirements.

Table 6 – 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
	ADV_SPM.1 Informal security policy model
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
	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 are suitable to satisfy the necessary requirements.

Table 7 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ROL.1	Basic rollback
Identification and Authentication	FIA_UAU.2(a)	User authentication before any action
	FIA_UID.2(a)	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 TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	FPT_RVM.1(a)	Non-bypassability of the TSP
Resource Utilization	FRU_FLT.1	Degraded fault tolerance
TOE Access	FTA_SSL.1	TSF-initiated session locking
Resolution Manager Functions	RES_SDC.1	System data collection (EXP)
	RES_ANL.1	Analyser analysis (EXP)
	RES_RCT.1	Analyser react (EXP)
	RES_SEL.1	Selective data collection (EXP)
	RES_STG.2	Prevention of System data loss (EXP)

6.1.1 User Data Protection

The TOE implements User Data Protection functionality via the Access Control Security Functional Policy (SFP). This functionality is provided by the Resolution Manager 4.2 WebUI and Admin Console. The Collector and the Admin Console do this by controlling access by operators to the data collected for analysis. The subjects that are regulated by this function are authenticated operators. The operation that these subjects perform is access to the collected data. The object accessed is the targeted system data. The Access Control SFP defines how specific subjects can access specific objects and what operations they can perform on those objects. The subject and object attributes are used to determine the access of the subject to the object. The security function allows an authenticated operator to access the targeted system data based on the operator's role and the Population Group to which the targeted system belongs.

The User Data Protection functionality also enforces access control on the rollback of remediations on the targeted systems. Only authenticated operators with permission to access the Population Group to which a targeted system belongs will be permitted to perform remediation rollback on the targeted system.

TOE Security Functional Requirements Satisfied: [FDP_ACC.1, FDP_ACF.1, FDP_ROL.1].

6.1.2 Identification and Authentication

The Identification and Authentication function ensures that the TOE operator that is requesting a service has identified and authenticated prior to requesting a service from the TOE. For each WebUI operator, the TOE stores the following security attributes in the database: username, password, role, and assigned population group. When TOE operators enter their usernames and passwords at the WebUI interface, the information is passed to the Collector, where it is verified against the username and password stored in the TOE. If the provided username and password match, the TOE operator is assigned the roles and given permission to access the assigned Population Groups associated with that username. The first action that operators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the TOE operator is not able to perform any TOE security functionality.

To access the Admin Console, a TOE operator must first identify and authenticate to the TOE environment to attain physical access to the Admin Console before any action can be performed on the TOE (see A.CONSOLE). In other words, in order to gain physical access to the Admin Console, an individual must have the proper credentials to enter the room in which the Admin Console is housed. Authenticated TOE operators with physical access to the Admin Console are considered to hold the role of Console Operator. No further identification (e.g., username) or authentication (e.g., password) is required for access to the TOE

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

6.1.3 Security Management

Operators use the Admin Console interface to perform management of the TSF data and TSF functionality. Operators use the WebUI interface to perform management of the user data and security attributes, and to perform Resolution Manager tasks, such as responses to abnormal conditions and snapshot collection. The Security Management function implements and enforces the different management roles supported by the TOE: Console Operator, Administrator, SuperUser, ReadOnly, and Helpdesk Operator. Each role enforced by this TSF has different privileges to configure the behavior of the TOE. For example, Administrators can collect snapshots and issue responses, and have the right to change security attributes.

The TOE enforces which roles have access to TSF data and security attributes, such as system options and usernames. Console Operators have the ability to access and modify the configuration data, such as system options, analytic tasks, recognition filters, and policy templates. They may also access the assigned population groups

security attribute. Administrators have the ability to access and modify security attributes, as well as activate all WebUI interface functions. SuperUsers and Read-only operators cannot access or modify any configurations or security attributes. SuperUsers may view analysis results, initiate responses, and activate analysis functions. ReadOnly operators may only view analysis results, and create, edit, delete, and run reports on previously collected data. Helpdesk Operators may view the status of the machines to which they are granted access and remediate known errors on those machines.

TOE Security Functional Requirements Satisfied: [FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1].

6.1.4 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF and of the TSF data. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified. The TSF provides for a secure state given failures of specific services, such as the Data Bridge Service, Agent Management Service, General Messaging Service, and Business Object Service. If one of these services fails, all the other services will continue to operate.

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. Each subject's and operator's security privileges are separated. It is not possible to perform any actions on the system without successfully authenticating. Once an operator has been authenticated, they are bound to the appropriate roles and any privileges defined by the TOE access control. For any operator to perform a TOE operation an authenticated and authorized administrative operator must have granted that operator the rights to perform that operation. These privileges are granted on a per operator basis. Since all access control rights are checked by the TOE's mechanisms and the TOE uses unique attributes for each operator, then the TSF maintains separation between different operators. As an example, if an operator without explicit permission tries to edit a filter, the operator will not be able to save the changes.

TOE Security Functional Requirements Satisfied: [FPT_FLS.1, FPT_RVM.1].

6.1.5 Resource Utilization

The Resource Utilization function supports the availability of required resources. Resource Utilization ensures the operation of all other services when a failure occurs in one of the following services: Data Bridge Service, Agent Management Service, General Messaging Service, and Business Object Service.

TOE Security Functional Requirements Satisfied: [FRU_FLT.1].

6.1.6 TOE Access

The TOE Access function controls the establishment of an operator's session. TOE Access provides TSF-initiated session locking of an interactive session after a configurable time interval of WebUI operator inactivity, defaulting to 60 minutes, and when the WebUI operator attempts another action. This is implemented by clearing or overwriting display devices, making the current contents unreadable, and by disabling any activity of the operator's data access and display devices other than unlocking the session. The operator may unlock the session only by re-identifying and re-authenticating to the TOE.

TOE Security Functional Requirements Satisfied: [FTA_SSL.1].

6.1.7 Resolution Manager Functions

The Resolution Manager Functions implement the problem and incident management functionality. The targeted system data is generated by Agents installed on individual targeted machines. Data gathered by the Agents include file hash values, open network ports, security settings, applications, patches, running processes, services, performance metrics, server logins, disk throughput, and registry keys for each targeted system. Data collected include date and time of last snapshot of targeted system data, machine name, machine identifier, and snapshot data collected. The TOE then analyzes this data to identify anomalies. The TOE either automatically remediates the anomalies, or provides the TOE operator with information concerning the anomalies so the operator can take the appropriate action.

When an operator authenticates to the Server, the TOE provides the operator with the capability to select which data will be gathered based on the rules defined in the recognition filters, and to configure which recognition filters are active. The TOE protects this data from loss by stopping collection and generating an alert email to a pre-defined email address when the storage capacity has been reached.

TOE Security Functional Requirements Satisfied: [RES_SDC.1, RES_ANL.1, RES_RCT.1, RES_SEL.1, RES_STG.2].

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.

Note to Evaluator: The final versions of these documents have not yet been produced. The version numbers will be completed when the evaluation is close to completion and the documents have been finalized.

Table 8 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	Triumfant Resolution Manager 4.2 - Configuration Management
ADO_DEL.1	Triumfant Resolution Manager 4.2 - Secure Delivery
ADO_IGS.1	Triumfant Resolution Manager 4.2 Installation Guide Triumfant Resolution Manager 4.2 - Guidance Supplement
ADV_FSP.1	Triumfant Resolution Manager 4.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	Triumfant Resolution Manager 4.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	Triumfant Resolution Manager 4.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_SPM.1	Triumfant Resolution Manager 4.2 - Informal Security Policy Model
AGD_ADM.1	Triumfant Resolution Manager 4.2 - System Administration Guide Triumfant Resolution Manager 4.2 - Guidance Supplement
AGD_USR.1	Triumfant Resolution Manager 4.2 - Web Interface User's Guide
ALC_FLR.1	Triumfant Resolution Manager 4.2 - Flaw Remediation
ATE_COV.1	Triumfant Resolution Manager 4.2 - Functional Tests and Coverage

Assurance Component	Assurance Measure
ATE_FUN.1	Triumfant Resolution Manager 4.2 – Functional Tests and Coverage
AVA_SOF.1	Triumfant Resolution Manager 4.2 - Vulnerability Assessment
AVA_VLA.1	Triumfant Resolution Manager 4.2 - Vulnerability Assessment

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 Triumfant. 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 Triumfant to protect against TOE modification during product delivery. The Installation Documentation provided by Triumfant 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 need to be exercised.

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

The Triumfant 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 ADV_SPM.1: Informal Security Policy Model

The Security Policy Model provides assurance that all of the security functions in the Functional Specification are sufficient to enforce the policies in the TSP. An informal model is provided for a subset of the TSP policies and the correspondence between the Functional Specification, the Security Policy Model, and the subset of policies is established.

6.2.6 ALC_FLR.1: Basic Flaw Remediation

The Flaw Remediation document outlines the steps taken at Triumfant to capture, track and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion.

6.2.7 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing

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.

6.2.8 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 Strength of Function (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. This section 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 and threat.

8.1.1 Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.RES A user might perform unauthorized actions (e.g., changing of settings or addition, deletion, or modification of software applications) on a targeted IT system which would compromise the security of the targeted IT system or make improper use of system resources.	O.AGENT The TOE Agent must collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on the Agent machine.	O.AGENT requires that the TOE Agent collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on the Agent machine.
	O.COLLECT The TOE Collector must collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on IT System assets and the Agent machines.	O.COLLECT requires that the TOE Collector collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on IT System assets and the Agent.
	O.ANALYZE The TOE Analytic Engine must accept data from TOE Agents or TOE Collectors and then apply analytical processes and information to derive conclusions about anomalies.	O.ANALYZE requires that the TOE Analytic Server accept data from TOE Agents or TOE Collectors and then apply analytical processes and information to derive conclusions about anomalies.
	O.RESPON The TOE must respond appropriately to analytical conclusions.	O.RESPON requires that the TOE respond appropriately to analytical conclusions.

	O.PROTECT The TOE must protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.	This threat is primarily diminished by the O.PROTECT objective, which requires that the TOE protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports the other objectives by providing for reliable timestamps to be used by the TOE.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective supports the other objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.RVM The IT Environment will protect TOE data stored temporarily in the environment from external interference or tampering.	The OE.RVM objective counters this threat by requiring external entities to access the TOE security functions before being able to access TOE data stored in the environment.
	OE.CONSOLE The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data.	The OE.CONSOLE objective counters this threat by requiring TOE users to authenticate with the TOE environment before performing any actions on the TOE.
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.	O.ANALYZE The TOE Analytic Engine must accept data from TOE Agents or TOE Collectors and then apply analytical processes and information to derive conclusions about anomalies.	The O.ANALYZE objective requires that the TOE Analytic Server accept data from TOE Agents or TOE Collectors and then apply analytical processes and information to derive conclusions about anomalies.
	O.RESPON The TOE must respond appropriately to analytical conclusions.	The O.RESPON objective requires that the TOE respond appropriately to analytical conclusions.
	O.IDAUTH The TOE must be able to identify and authenticate WebUI operators prior to allowing access to TOE administrative functions and data.	The O.IDAUTH objective requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data.

	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	O.INTEGR The TOE must ensure the integrity of all System data.	This threat is primarily diminished by the O.INTEGR objective, which requires that the TOE ensure the integrity of all System data.
	O.PROTECT The TOE must protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.	The O.PROTECT objective requires that the TOE protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.AUDIT The IT Environment will gather audit records of start-up, shutdown, and access to the TOE.	The OE.AUDIT objective supports the other objectives by requiring the recording of audit records for review by a TOE administrator.
	OE.SSL The IT Environment will protect the System data from disclosure during transmission between TOE components.	The OE.SSL objective supports the other objectives by ensuring the security of the System data as it is transmitted between TOE components.
	OE.RVM The IT Environment will protect TOE data stored temporarily in the environment from external interference or tampering.	The OE.RVM objective counters this threat by requiring external entities to access the TOE security functions before being able to access TOE data stored in the environment.
	OE.CONSOLE The TOE Environment will identify and authenticate console operators prior to	The OE.CONSOLE objective counters this threat by requiring TOE users to authenticate with the TOE environment before performing any

	allowing access to TOE administrative functions and data.	actions on 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.	O.IDAUTH The TOE must be able to identify and authenticate WebUI operators prior to allowing access to TOE administrative functions and data.	This threat is primarily diminished by the O.IDAUTH objective, which requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	O.PROTECT The TOE must protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.	The O.PROTECT objective requires that the TOE protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.AUDIT The IT Environment will gather audit records of start-up, shutdown, and access to the TOE.	The OE.AUDIT objective supports the other objectives by requiring the recording of audit records for review by a TOE administrator.
	OE.CONSOLE The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data.	The OE.CONSOLE objective counters this threat by requiring TOE users to authenticate with the TOE environment before performing any actions on the TOE.
T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE	O.OFLOWS The TOE must appropriately handle potential System data storage overflows.	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

cannot handle.	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.
	OE.SEP The IT Environment will protect the TOE from external interference or tampering.	The OE.SEP objective supports this objective by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
	OE.CONSOLE The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data.	The OE.CONSOLE objective counters this threat by requiring TOE users to authenticate with the TOE environment before performing any actions on the TOE.

8.1.2 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.NOEVIL Operators are non-hostile, appropriately trained, and follow all operator guidance.	NOE.NOEVIL Operators are non-hostile, appropriately trained, and follow all operator guidance.	The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.
A.PHYSCAL The Analytic Engine, the Collector, and the MySQL database components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	NOE.PHYSICAL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	The NOE.PHYSCL objective requires that the Analytic Engine, the Collector, and the MySQL Database components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.REMEDY The TOE Environment will identify and authenticate Remedy helpdesk operators prior to allowing access to TOE administrative functions and data. The TOE and Remedy Server must be placed in a controlled environment	NOE.REMEDY The TOE Environment will identify and authenticate Remedy helpdesk operators prior to allowing access to TOE administrative functions and data. The TOE and Remedy Server must be placed in a controlled environment	The NOE.REMEDY objective requires that the TOE Environment will identify and authenticate Remedy helpdesk operators prior to allowing access to TOE administrative functions and data.

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

Objective	Requirements Addressing the Objective	Rationale
O.AGENT The TOE Agent must collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on the Agent machine.	RES_SDC.1 System data collection (EXP)	A System containing an Agent is required to collect events potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on the Agent machine.
	RES_SEL.1 Selective data collection (EXP)	RES_SEL supports this objective by enabling the system to include or exclude information from the set of collected information based on rules defined in recognition filters that are configured to be active.
O.COLLECT The TOE Collector must collect and store information about all events that are potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on IT System assets and the Agent machines.	RES_SDC.1 System data collection (EXP)	The TOE Collector is required to collect information potentially indicative of inappropriate activity that may have resulted from unauthorized changing of settings, or unauthorized addition, deletion, or modification of software applications on IT System assets and the Agent.
	RES_SEL.1 Selective data collection (EXP)	RES_SEL supports this objective by enabling the system to include or exclude information from the set of collected information based on rules defined in recognition filters that are configured to be active.
O.ANALYZE The TOE Analytic Engine must accept data from TOE Agents or TOE Collectors and then apply analytical processes and information to derive conclusions about anomalies.	RES_ANL.1 Analyser analysis (EXP)	The TOE is required to perform analysis and generate results.
O.RESPON The TOE must respond appropriately to analytical	FDP_ROL.1 Basic rollback	The TOE must permit the rollback of remediation actions on the targeted system.

conclusions.	RES_RCT.1 Analyser react (EXP)	The TOE is required to respond accordingly in the event an anomaly is detected.
O.IDAUTH The TOE must be able to identify and authenticate WebUI operators prior to allowing access to TOE administrative functions and data.	FIA_UAU.2(a) User authentication before any action	The TOE will not give any access to an operator until the TOE has identified and authenticated the operator.
	FIA_UID.2(a) User identification before any action	The TOE will not give any access to an operator until the TOE has identified and authenticated the operator.
	FPT_RVM.1(a) Non-bypassability of the TSP	The TOE must ensure that all functions to protect the data are not bypassed.
	FTA_SSL.1 TSF-initiated session locking	The TOE enforces session locking after a configurable period of inactivity.
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FDP_ACC.1 Subset access control	The TOE allows only authorized operators to access targeted system data.
	FDP_ACF.1 Security attribute based access control	The TOE must ensure that only specified authorized and authenticated roles access the population groups in the targeted system data.
	FIA_UAU.2(a) User authentication before any action	The TOE will not give any access to an operator until the TOE has identified and authenticated the operator.
	FIA_UID.2(a) User identification before any action	The TOE will not give any access to an operator until the TOE has identified and authenticated the operator.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized operators of the TOE.
	FMT_MSA.1 Management of security attributes	The TOE restricts the ability to manage security attributes to authorized operators.

	FMT_MSA.3 Static Attribute Initialisation	The TOE allows only authorized operators to specify alternative initial values to override the default values when an object or information is created.
	FMT_MTD.1 Management of TSF data	Only authorized operators of the System may change the default of, query, modify, or delete System data.
	FMT_SMF.1 Specification of management functions	This objective is supported by FMT_SMF.1, which requires that security function management, security attribute management, and TSF data management is enforced by the TOE.
	FMT_SMR.1 Security roles	The TOE maintains and associates users with roles
	FTA_SSL.1 TSF-initiated session locking	The TOE locks an operator's interactive session after a configurable time interval of operator inactivity.
O.INTEGR The TOE must ensure the integrity of all System data.	FDP_ACC.1 Subset access control	The TOE must ensure that only authenticated operators access the targeted system data.
	FDP_ACF.1 Security attribute based access control	The TOE must ensure that only specified authorized and authenticated roles access the population groups in the targeted system data.
	FDP_ROL.1 Basic rollback	The TOE enforces rollback of remediation actions taken by the TOE on the targeted system.
	FMT_MTD.1 Management of TSF data	Only authorized operators of the System may change the default of, query, modify, or delete System data.
	FPT_FLS.1 Failure with preservation of secure state	The TOE must preserve a secure state when specific failures occur in the TOE.
	FPT_RVM.1(a)	The TOE must ensure that all functions to protect the data are not

	Non-bypassability of the TSP	bypassed.
	FRU_FLT.1 Degraded fault tolerance	The TOE ensures the operation of all other services when one service fails.
	RES_STG.2 Prevention of System data loss (EXP)	The System is required to stop collecting targeted system data if the storage capacity has been reached.
O.PROTECT The TOE must protect itself and the targeted IT system from unauthorized modifications and access to its functions and data.	FDP_ACC.1 Subset access control	The TOE must ensure that only authenticated operators access the targeted system data.
	FDP_ACF.1 Security attribute based access control	The TOE must ensure that only specified authorized and authenticated roles access the population groups in the targeted system data.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized operators of the TOE.
	FMT_MSA.1 Management of security attributes	The TOE restricts the ability to manage security attributes to authorized operators.
	FMT_MSA.3 Static Attribute Initialisation	The TOE allows only authorized operators to specify alternative initial values to override the default values when an object or information is created.
	FMT_MTD.1 Management of TSF data	Only authorized operators of the System may change the default of, query, modify, or delete System data.
	FMT_SMF.1 Specification of management functions	This objective is supported by FMT_SMF.1, which requires that security function management, security attribute management, and TSF data management is enforced by the TOE.
	FMT_SMR.1 Security roles	The TOE maintains and associates users with roles.

	FPT_RVM.1(a) Non-bypassability of the TSP	The TOE must ensure that all functions to protect the data are not bypassed.
	FTA_SSL.1 TSF-initiated session locking	The TOE locks an operator's interactive session after a configurable time interval of operator inactivity.
O.OFLOWS The TOE must appropriately handle potential System data storage overflows.	RES_STG.2 Prevention of System data loss (EXP)	The TOE is required to guarantee the availability of the collected user data in the event of storage exhaustion.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.TIME The IT Environment will provide reliable timestamps to the TOE.	FPT_STM.1 Reliable time stamps	The IT Environment is required to provide reliable timestamps to the TOE.
OE.SEP The IT Environment will protect the TOE from external interference or tampering.	FPT_SEP.1 TSF domain separation	The IT Environment must protect the TOE from interference that would prevent it from performing its functions.
OE.AUDIT The IT Environment will gather audit records of start-up, shutdown, and access to the TOE.	EXP_FAU_GEN.1 Audit Data Generation	The IT Environment must gather audit records of startup, shutdown, and access to the TOE.
OE.SSL The IT Environment will protect the System data from disclosure during transmission between TOE components.	FPT_ITT.1 Basic internal TSF data transfer protection	The IT Environment must protect the System data from disclosure during transmission between TOE components.
OE.RVM The IT Environment will protect TOE data stored temporarily in the environment from external interference or tampering.	FPT_RVM.1(b) Non-bypassability of the TSP	FPT_RVM.1(b) supports this objective by ensuring that TOE security functions cannot be bypassed before allowing access to TOE data.

OE.CONSOLE The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data.	FIA_UID.2(b) User identification before any action	FIA_UID.2(b) supports this objective by requiring the environment to identify Admin Console and Helpdesk operators before granting access the admin console.
	FIA_UAU.2(b) User authentication before any action	FIA_UAU.2(b) supports this objective by requiring the environment to authenticate Admin Console and Helpdesk operators before granting access to the Admin Console.

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.

The augmentation of ADV_SPM.1 was included as a dependency of FPT_FLS.1.

8.4 Rationale for Explicitly-stated Security Functional Requirements

8.4.1 Resolution Manager Functions

A family of Resolution Manager requirements was created to specifically address the data collected and analyzed by the TOE. The IDS Protection Profile (PP) Version 1.6 and FAU_SEL.1 were used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of incident and problem management data (file hash values, open network ports, security settings, applications, patches, running processes, services, performance metrics, server logins, disk throughput, and registry keys), and provide for requirements about collecting, analyzing, and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4.2 Security Audit Function

An explicitly-stated Security Audit requirement was created for the TOE environment to specifically address the audits collected by the operating system and IIS. The Audit Data Generation requirement was used as a model for creating this requirement. The purpose of this requirement is to address the unique nature of the audits collected by the environment. This requirement has no dependencies since the stated requirement embodies all the necessary security functionality. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.5 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:

The title “Class FPT: Protection of the TSF” has been refined to “Class FPT: Protection of the TOE Environment” in Section 5.2.3.

The term “TSF” has been refined to “TOE Environment” in several places in Section 5.2.3.

The term “its own” has been refined to “the TOE’s” in Section 5.2.3.

The term “user” has been refined to “operator” in several SFRs (Sections 5.1.2 and 5.1.3).

FPT_RVM.1(b) has been refined because the function is within the environment and is referring to security provided by the environment, not functionality provided by the TSF.

FIA_UAU.2(b) and FIA_UID.2(b) have been refined because they reside within the environment and are referring to security provided by the environment, not functionality provided by the TSF.

8.6 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 9 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 9 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_ROL.1	FDP_ACC.1	✓	
FIA_UAU.2(a)	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(a)	No dependencies		
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.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_FLS.1	ADV_SPM.1	✓	A Security Policy Model is included in the evaluation.
FPT_RVM.1(a)	No dependencies		
FRU_FLT.1	FPT_FLS.1	✓	
FTA_SSL.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.
RES_SDC.1	No dependencies		
RES_ANL.1	No dependencies		
RES_RCT.1	No dependencies		
RES_SEL.1	No dependencies		
RES_STG.2	No dependencies		
EXP_FAU_GEN.1	No dependencies		

FPT_ITT.1	No dependencies		
FPT_SEP.1	No dependencies		
FPT_STM.1	No dependencies		
FPT_RVM.1(b)	No dependencies		
FIA_UID.2(b)	No dependencies		
FIA_UAU.2(b)	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.

8.7 TOE Summary Specification Rationale

8.7.1 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 work together 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 10 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 SOF Rationale section.

Table 10 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
User Data Protection	FDP_ACC.1	The security function implements this SFR by enforcing the Access Control SFP on authenticated operators attempting to access targeted data. It does this by requiring that operators must be authenticated to the TOE, that the authenticated operator must have the role of Console Operator,

		Administrator, SuperUser, ReadOnly, or Helpdesk Operator, and must be authorized to access the Population Group to which the targeted system belongs.
	FDP_ACF.1	The security function implements this SFR by outlining the rules enforced by the Access Control SFP. The TOE requires that operators must be authenticated to the TOE, that the authenticated operator must have the role of Console Operator, Administrator, SuperUser, ReadOnly, or Helpdesk Operator, and must be authorized to access the Population Group to which the targeted system belongs.
	FDP_ROL.1	The security function implements this SFR by requiring the Access Control SFP to permit rollback of remediation actions taken by the TOE on the targeted system within the boundary limit of available disk space on the targeted system to retain the remediated content.
Identification and Authentication	FIA_UAU.2	The security function implements this SFR by requiring that operators be authenticated before being allowed access to the TSF.
	FIA_UID.2	The security function implements this SFR by requiring that operators identify themselves before being allowed access to the TSF.
Security Management	FMT_MOF.1	The security function implements this SFR by requiring that only authorized operators can modify the behavior of the security functions.
	FMT_MSA.1	The security function implements this SFR by requiring that only authorized operators can manage the security attributes of the TOE, which include passwords, usernames, roles, and assigned population groups.
	FMT_MSA.3	The security function implements this SFR by requiring that only authorized operators may specify alternative initial values to override the default values when an object or information

		is created.
	FMT_MTD.1	The security function implements this SFR by requiring that only authorized operators can modify system options, analytic tasks, recognition filters, and policy templates.
	FMT_SMF.1	The security function implements this SFR by requiring that the following management functions are available: security function management, security attribute management, and TSF data management.
	FMT_SMR.1	The security function implements this SFR by defining the roles used for access control as: Console Operator, Administrator, SuperUser, ReadOnly and Helpdesk Operator.
Protection of TOE Security Functions	FPT_FLS.1	The security function implements this SFR by requiring that the TOE preserve a secure state when a failure of one of the services occurs.
	FPT_RVM.1	The security function implements this SFR by requiring that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Resource Utilization	FRU_FLT.1	The security function implements this SFR by requiring that the operation of all other services continues when one of the following specified services fails: Data Bridge Service, Agent Management Service, Internal Messaging Service, and Business Object Service.
TOE Access	FTA_SSL.1	The security function implements this SFR by requiring that the system lock an interactive session after a configurable period of WebUI operator inactivity, defaulting to 60 minutes, and when the WebUI operator attempts another action. It locks the session by clearing or overwriting display devices and by disabling any activity of the operator's data access/display devices other than unlocking the session.

Resolution Manager Functions	RES_SDC.1	The security function implements this SFR by requiring that the system collect and record the following data from the targeted system resource that can be analyzed to identify anomalies: file hash values, open network ports, security settings, applications, patches, running processes, services, performance metrics, server logins, disk throughput, and registry keys. The system collects and records the following information: data and time of last snapshot of targeted system data, machine name, machined identifier, and snapshot data collected.
	RES_ANL.1	The security function implements this SFR by requiring that comparisons of snapshots of targeted system data to an adaptive reference model are performed in order to identify anomalies. It also records the following information within each analytical result: Date and time of snapshot, type of check task (origin), snapshot identifier, check task identifier, adaptive reference model identifier, adaptive reference model name, customer name, machine name, number of anomalies, severity level, and details of anomalies.
	RES_RCT.1	The security function implements this SFR by requiring that the TOE take one or more of the following specified operator-defined actions when an anomaly is detected: Inform, Notify, Install software, or Remediate an abnormal condition when an anomaly is detected.
	RES_SEL.1	The security function implements this SFR by requiring that the system include or exclude data from the set of collected data based on the rules defined in recognition filters that are configured to be active.
	RES_STG.2	The security function implements this SFR by requiring that the system suspend collection of targeted system data if the storage capacity has been reached until space has been freed by an administrator to allow more

		snapshots to be stored on the server.

8.7.2 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.

8.7.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at Triumfant. 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

8.7.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Triumfant to protect against TOE modification during product delivery. The Installation Documentation provided by Triumfant 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

8.7.2.3 Development

The Triumfant 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.
- The Security Policy Model provides an informal TSP model and it demonstrates correspondence between the functional specification and the TSP model by showing that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. The TSP model describes the rules and characteristics of all policies of the TSP that can be modeled. The model should include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.7.2.4 Guidance Documentation

The Triumfant 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. Triumfant 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

8.7.2.5 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. Triumfant 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

8.7.2.6 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

8.8 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL2+ augmented with ALC_FLR.1 and ADV_SPM.1 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 DOD low robustness environments processing unclassified information.

The relevant security function and security functional requirement which have probabilistic or permutational functions are Identification and Authentication and FIA_UAU.2.

9 Acronyms

Table 11 - Acronyms

Acronym	Definition
API	Application Programming Interface
BITS	Background Intelligent Transfer Service
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
GB	Gigabyte
GHz	Gigahertz
HTTPS	Hypertext Transmission Protocol over SSL
IIS	Internet Information Services
ISO	International Organization for Standardization
IT	Information Technology
Mbps	Megabits per second
NIC	Network Interface Card
ODBC	Open Database Connectivity
RAM	Random Access Memory
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy