BMC Software, PATROL®Perform/Predict, Version 6.5.30

Security Target

Version 1.0

March 15, 2002

Prepared for:

BMC Software, Inc.
2101 City West Boulevard
Houston, TX 77042

Prepared by:

Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

Revisions to Document		
Date	***Version***	***Changes Made***
June 20, 2001	0.1	Original
June 25, 2001	0.2	Changed version of Visualizer per Brian Bourgault
October 19, 2001	0.3	Made corrections per EDR 001
January 9, 2002	0.4	Changed TOE objective, added term, made other relevant changes.
January 15, 2002	0.5	Changed references to Perform user and Perform administrator to Perform user and Perform Administrator. Removed statement about having user set permissions on $BEST1_HOME directory.
January 24, 2002	0.6	Implemented changes per validator comments dated January 22, 2002
March 15, 2002	1.0	Changed version number to 1.0 to reflect final evaluated version.

Table of Contents

List of Tables

List of Figures

1 SECURITY TARGET INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., Target of Evaluation). An ST principally defines:

- A security problem expressed as a set of assumptions about the security aspects of the environment; a list of threats which the product is intended to counter; and any known rules with which the product must comply (in Chapter 3, Security Environment).
- A set of security objectives and a set of security requirements to satisfy the objectives (in Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).
- The IT security functions provided by the Target of Evaluation (TOE) that meet the set of requirements (in Chapter 6, TOE Summary Specification).

2 The structure and contents of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides the information needed to identify and control this ST and its Target of Evaluation (TOE), the BMC Software, PATROL® Perform/Predict, Version 6.5.30 (hereinafter called Perform/Predict). This ST targets an Evaluation Assurance Level (EAL) 2.

ST Title:	BMC Software, PATROL® Perform/Predict, Version 6.5.30, Security Target
ST Version:	Draft Version 0.6
Publication Date:	January 24, 2002
TOE Identification:	BMC Software, PATROL® Perform/Predict, Version 6.5.30
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999
ST Authors:	Computer Sciences Corporation
ST Evaluation:	Computer Sciences Corporation
Key Words:	BMC Software, PATROL® PERFORMANCE, PREDICT, UDR, audit

1.2 References

4 The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, version 2.1, CCIMB-99-031.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

1.3 Conventions, Terminology, and Acronyms

5 This section identifies the formatting conventions used to convey additional information and terminology having specific meaning. It also defines the meanings of acronyms used throughout the remainder of the document.

1.3.1 Conventions

6 This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

1.3.1.1 Operations

7 Paragraph 2.1.4 of Part 2 of the CC defines several operations allowed to be performed on functional requirements; *assignment, refinement*, *selection, and iteration*.

8 The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets, [assignment_value(s)].

9 The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text.**

10 The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized text.*

11 Iterated functional and assurance requirements are given unique identifiers by appending to the CC component name, short name, and functional element name an iteration number inside parenthesis, e.g., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

12 Plain *italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

1.3.1.2 Naming Conventions

13 **Assumptions:** TOE security environment assumptions are given names beginning with "A." and are presented in alphabetical order.

Example:

14 A.ADMIN – Assumption allocated to the TOE as an entity.

15 **Threats:** TOE security threats for the TOE and for the environment are given names beginning with "T." and "TE." respectively, and are presented in alphabetical order.

Examples:

16 T.ATTACK_DATA – Threat to/countered by the TOE as an entity.

17 TE.UNAUTH_USAGE – Threat to/countered by the environment.

18 **Policies:** TOE security environment policies are given names beginning with "P." and are presented in alphabetical order.

Example:

19 P.ACCOUNT – Policy supported by the TOE as an entity.

20 **Objectives:** Security objectives for the TOE and for the environment are given names beginning with "O." and "OE." respectively, and are presented in alphabetical order.

Examples:

21 O.ADMIN – Objective for the TOE as an entity.

22 OE.AUTHORIZATION – Objective for the environment.

1.3.2 Terminology

23 In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the reader of the Security Target.

TERM	DEFINITION
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Human user	Any person who interacts with the TOE.

TERM	DEFINITION
Authorized User	A user that, in accordance with the TOE Security Policy (TSP) may perform an action. (As identified by group membership.)
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.
Authentication data	Information used to verify the claimed identity of a user.
Collection Process	A TOE process that collects pre-defined data for a pre-defined period of time, and results in data that is re-formatted into UDR format for use by the Manager, Predict, Analyze, and Visualizer components of the TOE.

1.3.3 Acronyms

24 The following acronyms are used in this Security Target:

ACRONYM	DEFINITION
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CM	Configuration Management
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
IT	Information Technology
NR	Node Repository
OSP	Organizational Security Policy
PC	Personal Computer
PP	Protection Profile
RDBMS	Relational Database Management System
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UDR	Universal Data Recognition

1.4 Security Target Overview

This ST forms the basis for evaluation of the TOE, known as the BMC Software product PATROL® Perform/Predict, Version 6.5.30.

25 The basic components of Perform/Predict provide a set of tools designed to assist in measuring, evaluating, predicting, and reporting the performance and capacity of distributed systems.

26 The PATROL® for Unix/Windows – Perform and its components are used to monitor, analyze, and generate graphs and reports about system performance.

27 The PATROL® for Unix/Windows – Predict is used to do predictive modeling, response time analysis, and capacity planning for systems.

1.5 Common Criteria Conformance

28 This ST conforms to Part 2 and Part 3 of the CC, Version 2.1 at the EAL 2 level of assurance.

2 TOE DESCRIPTION

29 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

30 Perform/Predict is designed to assist in measuring, evaluating, predicting, and reporting the performance and capacity of distributed systems on a Unix or Windows platform.

2.1.1 Scope and Boundaries of the Evaluated Configuration

31 This section provides a general description of the physical and logical scope and boundaries of the TOE.

2.1.1.1 Physical Scope and Boundary

32 The TOE configuration consists of six major components:

a) Manager
b) Collect
c) UDR Provider
d) Analyze
e) Predict
f) Visualizer

33 The *Manager* component is the management console software that is used for all performance analysis, reporting, prediction and capacity planning tasks.

34 *Collect* collects system and RDBMS performance data on each node it is loaded on. The nodes (to optionally include the PATROL® Performance Manager node) contain the Collect and UDR Provider executables.

35 *UDR Provider* formats the data collected by Collect into UDR format and puts it into a local file (node repository) for later use by Analyze. The method to transfer the local file to the universal repository on the manager console, where Analyze resides, is site-dependent.

36 *Analyze* analyzes the collected data, groups work together into user-defined workloads, builds a model for use by Predict, and creates Visualizer input files for RDBMS metrics and optionally for system metrics.

37 *Predict* evaluates the model created by Analyze to calculate response times, throughput, and other key metrics, and creates Visualizer input files for system metrics.

38 The *Visualizer* executable resides on a Windows-based personal computer (PC). (If the PATROL® Performance Manager node is windows-based, the Visualizer can reside there also.) Visualizer displays graphs illustrating various performance characteristics of the distributed systems, extracted from its performance database. The Visualizer input files can be created in Analyze or Predict or both. The default is to create the Visualizer file in both and then Manager combines the two files to create a single input file for Visualizer. The advantages of the merged file are:

- Some metrics are available only in Analyze
- Response times are only available in Predict
- The automated process of creating the merged files is more efficient and more error free than a manual combination would be.

39 Physically, each TOE platform consists of processor architecture appropriate for the Operating System on which the TOE component runs. The TOE does not include any network components between the PATROL® Performance Manager node, and the Visualizer PC, nor the PATROL® Performance Manager node and the other nodes to be monitored.

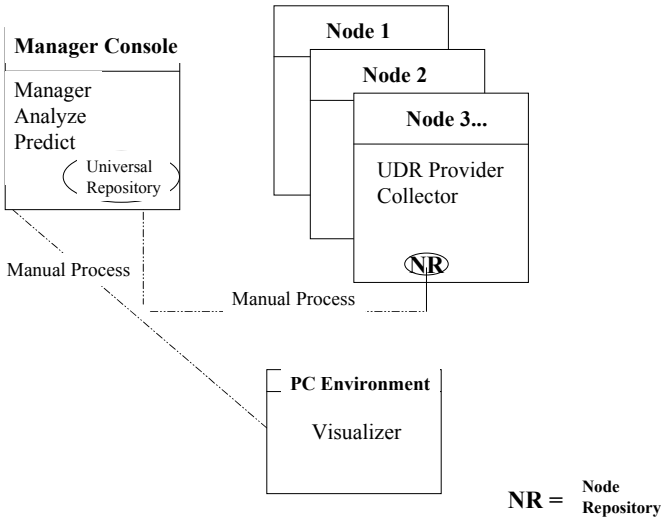
40 The evaluated TOE configuration includes the elements identified in Table 1.

Table 1: Evaluated TOE Configuration Components

Components	Items
Software	BMC Software PATROL® Perform/Predict, version 6.5.30 components: Manager 6.5.30 Collect 6.5.30 UDR Provider 6.5.30 Analyze 6.5.30 Predict 6.5.30 Visualizer 3.5.04 (windows only)

41 Physically, this evaluation focuses on each TOE component composed of the functionally appropriate software on either a Solaris 2.6 or 2.7, a Windows NT 4.0 (SP5), or a Windows 2000 Professional (SP1) computer platform. However, Visualizer is not available in a Unix environment.

42 Figure 2-1 depicts the physical boundary of the TOE.



43

Figure 2-1: Physical TOE Boundary

2.1.1.2 Logical Scope and Boundary

44 The TOE logical boundary consists of the authorization functionality inherent in the UDR Provider component. Figure 2-2 illustrates the logical boundary of the TOE.

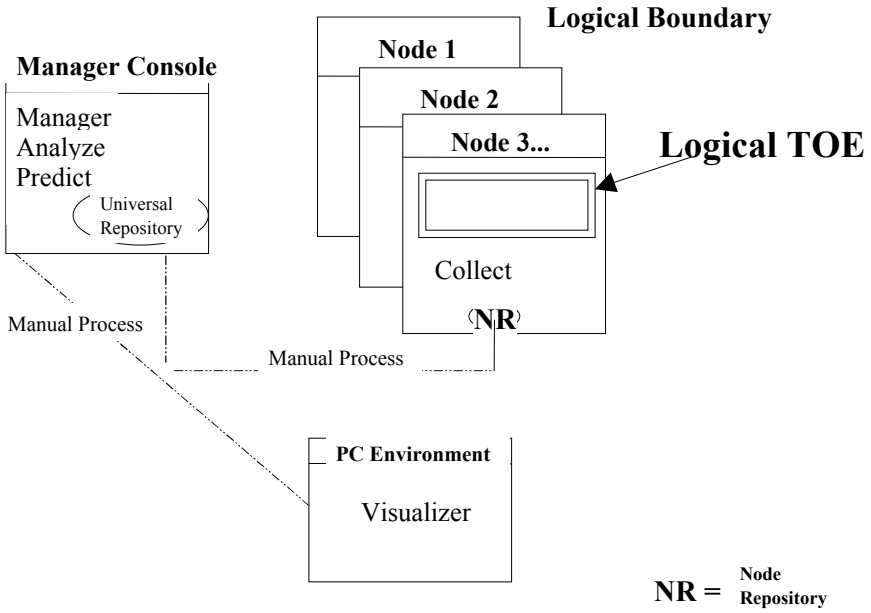


Figure 2-2: TOE Logical Boundary

45 The logical TOE provides the following security feature: user authorization on each node.

46 Although Visualizer in the PC environment and the components on the Manager Console (i.e., Analyze, Manager, and Predict) are part of the physical boundary of the TOE, they are not security-relevant because they provide no security functions. NOTE: The

manager console can also contain the UDR Provider and Collect components to enable the collection of data on that specific workstation.

47 Of these components, only the UDR Provider offers any security functionality. The Manager, Predict, Visualizer and Analyze components only allow for the analysis of collected data. Since these components do not implement any security functions, they are not part of the TOE Security Functions (TSF) and the design of these portions of the TOE does not need to be further described.

48 The authorization.cfg file on each node that UDR Provider and Collect are on is used by UDR Provider to validate a user's authority to start the collection process. The default grants all users full authorization to all information, however, this file can be edited on a per-user basis by assigning any of four permission levels: manage, modify, view, or none. NOTE: In the evaluated configuration, view and none are not applicable because they have no functionality within the secure configuration.

3 TOE SECURITY ENVIRONMENT

49 This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment. NOTE: There are no connectivity aspects because the TOE is not network oriented.

3.1 Assumptions

50 The specific conditions listed in Table 2 are assumed to exist for the secure operation of the TOE.

Table 2: TOE Assumptions

Name	Description
A.ACCESS_CONTROL	The underlying operating systems of Perform/Predict are configured to provide discretionary access control (DAC) to Perform/Predict executables and data files per site policy. *
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. Those assigned to manage the TOE have been appropriately trained.
A.NOEVIL	Administrators are not careless, willfully negligent, nor hostile; and will follow and abide by all administrator guidance; however, they are capable of error.
A.OPERATE_CORRECT	The computer platforms and operating systems software operate correctly.
A.PHYSICAL_PROTECT	The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.

51 *APPLICATION NOTE: The underlying operating system provides discretionary access control to protect the authorization.cfg file from modification by users and prevents unauthorized users from accessing the Perform/Predict installation directory and its contents. These assumptions require that the underlying operating system possess the notion of users and groups along with user and group access permissions. These operating system features are present in the evaluated configuration.

3.2 Threats

52 Threats may be addressed either by the TOE or by its intended environment using personnel, physical, or administrative safeguards.

3.2.1 Threat Addressed by the TOE

Table 3: Threat Addressed by TOE

Name	Description
T.UNAUTH_USAGE	Hostile/unauthorized users with limited attack potential could instantiate a TOE collection process, which could result in the loss of integrity of the collected data.

3.2.2 Threats Addressed by the TOE IT Environment

53 There are no specific threats to the TOE assets against which specific protection within the TOE IT environment is required.

3.3 Organizational Security Policies

54 Table 4 identifies the Organizational Security Policies (OSPs) for the TOE.

Table 4: Organizational Security Policies

Name	Description
P.AUTHORIZATION	The TOE must have the ability to limit the extent of each user's authorization.
P.MANAGE	The TOE must be managed and maintained so that its security function is implemented and preserved throughout its operational lifetime.

4 SECURITY OBJECTIVES

55 The security objectives define the conditions that must be met to counter threats and cover assumptions and organizational security policies. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the TOE IT Environment.

4.1 SECURITY OBJECTIVE FOR THE TOE

56 The security objective that addresses the security concerns of the TOE is identified in Table 5.

Table 5: Security Objective for the TOE

Name	Description
O.START	The TOE must provide functions to ensure that unauthorized users cannot start the collection process.

4.2 SECURITY OBJECTIVES OF THE ENVIRONMENT

57 The security objectives identified for the TOE environment are addressed in Table 6.

Table 6: Security Objectives of the Environment

Name	Description
OE.DISCRETIONARY_ACCESS	The TOE environment must provide discretionary access control (DAC), per site policy, to protect TOE resources and limit TOE application instantiation.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.
OE.PHYSICAL_PROTECTION	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack, which might compromise IT security objectives.
OE.PLATFORM_SUPPORT	The TOE environment must provide reliable platform functions including: correct hardware operation and functionality.

5 IT SECURITY REQUIREMENTS

58 IT security requirements include:

- TOE security requirements, and (optionally)
- TOE IT environment security requirements upon which satisfaction of the TOE's security objectives depend.

59 These requirements are discussed separately below.

5.1 TOE Security Requirements

60 The CC divides security requirements into two categories:

- *Security functional requirements (SFRs)*: requirements for security functions such as information flow control, audit, and identification.
- *Security assurance requirements (SARs)*: provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

61 This section presents the security functional and assurance requirements for the TOE and its supporting IT environment.

5.1.1 TOE Security Functional Requirements

62 Table 7 identifies the Security Functional Requirements (SFRs) for the TOE.

Table 7: TOE Security Functional Requirement

Functional Component ID	Functional Component Name	Dependencies
User Data Protection		
FDP_ACC.1	Subset Access Control	FDP_ACF.1
FDP_ACF.1	Security Attribute-based Access Control	FDP_ACC.1 FMT_MSA.3
Identification and Authentication		
FIA_ATD.1	User Attribute Definition	None
Security Management		
FMT_MSA.3	Static Attribute Initialisation	FMT_MSA.1 FMT_SMR.1

63 Requirements overview: This ST consists of an access control Security Function Policy (SFP) called AUTHORIZE. The subjects under control of this policy are the users defined in the authorization.cfg file of the TOE. The object controlled is the collection process; and the operation the AUTHORIZE SFP controls is the start of the collection process. The SFP states that only authorized node users who are identified in the authorization.cfg file and assigned the manage or modify permission may start the Collect operation of the collection process.

5.1.1.1 Class FDP: User Data Protection

FDP_ACC.1	Access Control Policy
	Hierarchical to: No other components
FDP_ACC.1.1	The TSF shall enforce the [AUTHORIZE SFP] on [users, the collection process, and the START operation].
	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 [AUTHORIZE SFP] to objects based on [modify or manage permission].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [user is named in authorization.cfg with modify or manage permission].
FDP_ACF.1.3	The TSF shall explicitly authorize 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 following additional rules: [None].
	Dependencies: FDP_ACC.1 Subset access control
	FMT_MSA.3 Static attribute initialisation

5.1.1.2 Class FDP: User Data Protection

FIA_ATD.1	User Attribute Definition
	Hierarchical to: No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [modify, or manage].
	Dependencies: No dependencies

5.1.1.3 Class FMT: Security Management

FMT_MSA.3	Static Attribution Initialisation
	Hierarchical to: No other components

FMT_MSA.3.1 The TSF shall enforce the [AUTHORIZE 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 [none] 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

5.1.2 TOE IT Environment Security Functional Requirements

64 Table 8 identifies the Security Functional Requirements (SFRs) for the TOE IT Environment.

Table 8: TOE IT Environment Security Functional Requirements

Functional Component ID	Functional Component Name	Dependencies
Identification and Authentication		
FIA_UAU.2	User Authentication before any action	FIA_UID.1
FIA_UID.2	User Identification before any action	None

5.1.2.1 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

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

Dependencies: No dependencies

FIA_UID.2 User Identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 The **host platform** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.3 SOF Declarations

65 The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

5.1.4 TOE Security Assurance Requirements

66 The Security Assurance Requirements (SARs) for the TOE evaluation are all of the SARs, without refinement, iteration, augmentation, extension, or tailoring, as identified for the EAL 2 level of assurance in CC Part 3, Security Assurance Requirements. These SARs are identified in Table 9.

Table 9: EAL 2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1

6 TOE SUMMARY SPECIFICATION

67 This section presents an overview of the security function implemented by the TOE and the Assurance Measures applied to ensure its correct implementation.

6.1 TOE Security Function

68 This section presents the security function performed by the TOE to satisfy the SFRs identified in Section 5.1.1.

6.1.1 Authorize

69 Perform/Predict provides a methodology for the authorization of users on each node. The default is to grant all authorized users MANAGE (full) authorization to all information.

70 Read/write access to the authorization.cfg file is controlled by the environmental DAC. The owner is set to be the user that installed the product (the Perform administrator), therefore, that user must have at least MODIFY permission on the local node. After successful completion of the installation of Perform/Predict version 6.5.30 (by the authorized BMC engineer), the access permissions on the $BEST1_HOME directory are changed to allow only the Perform user group and (Perform administrator) access. For Unix systems this was done by using the command: chmod 750 $BEST1_HOME. For Windows systems it required changing access to the$BEST1_HOME directory via the folder properties security dialog box. If the authorization file is not on the node, or if the user is not authorized on the local node, UDRProvider will not process a collection request and will exit.

71 Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FIA_ATD.1, and FMT_MSA.3

6.2 Assurance Measures

72 The TOE satisfies the CC EAL 2 assurance requirements presented in Table 9. As evidenced in the following subsections, BMC Software satisfies the stated SARs. This section identifies the Configuration Management, System Delivery Procedures, System Development Procedures, Guidance Documents, Life Cycle Support, Testing, and Vulnerability Analysis assurance measures applied by BMC Software to satisfy the CC EAL 2 assurance requirements.

6.2.1 Configuration Management

73 The Configuration Management (CM) measures applied by BMC Software include providing a reference for the TOE, using a CM system, and providing CM documentation.

74 The CM system uniquely identifies all configuration items (CIs) and provides the measures that are used to maintain and ensure that only authorized changes are made to the configuration items. The CM documentation shows that the CM system, at a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, evidence that demonstrates that the CM system is operating in accordance with the CM plan, and CM documentation. The CM documentation also describes how configuration items are tracked by the CM system.

75 The configuration management measures are documented within the following BMC Software documents:

- BMC Software PATROL®, Configuration Management Plan
- BMC Software PATROL®, Configuration Management: CI List

76 Assurance Requirements Satisfied: ACM_CAP.2

6.2.2 Delivery and Operation

77 The BMC Software PATROL®, Perform/Predict, Version 6.5.30 is delivered to the BMC engineer for installation at the customer's site. Any relevant documentation that describes what components are delivered with PATROL® Perform/Predict version 6.5.30, guidance for initially installing it, and warnings about the importance of properly unpacking, installing, and configuring the TOE are also accessible to the BMC engineer.

78 Assurance Requirements Satisfied: ADO_DEL.1 and ADO_IGS.1

6.2.3 Development

79 The Development documents provided by BMC Software satisfy the CC functional specification and high-level design development requirements, as well as provide a correspondence between that information and this ST. These architecture measures are documented within the following BMC Software documents:

- BMC Software PATROL®, Perform/Predict, Version 6.5.30, Design Document

80 Assurance Requirements Satisfied: ADV_FSP.1, ADV_HLD.1, and ADV_RCR.1.

6.2.4 Guidance

81 The Guidance assurance measures provided by BMC Software include system administrative and user guidance documents and a Technical Bulletin regarding any specifics as to the operation of the evaluated configuration.

82 The system administrative guidance contains the following administrative functions and interfaces:

- Warnings about functions and privileges that should be controlled in a secure processing environment;
- All assumptions regarding user behavior that are relevant to secure operation of the TOE,
- All security parameters under the control of the administrator,
- Indicates secure values as appropriate,
- Descriptions of each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF, which is consistent with all other documentation supplied for evaluation,
- Describes all security requirements for the IT Environment that are relevant to the administrator.

83 The user guidance is consistent with other evaluation documents and contains the following:

- All security requirements for the IT Environment that are relevant to the user functions and interfaces available to the non-administrative user of the TOE,
- The use of user-accessible security functions provided by the TOE,
- Warnings about user-accessible functions and privileges that should be controlled in a secure processing environment,
- All user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found the statement of TOE, security environment;

84 These guidance measures are documented within the following BMC Software documents:

- BMC Software PATROL® for Microsoft Windows 2000 Servers, Release Note, Version 2.1.01, dated February 9, 2001
- BMC Software PATROL® for Unix, Release Note, Version 8.3.04, dated February 9, 2001
- BMC Software PATROL®, Perform/Predict version 6.5.30 Technical Bulletin

85 Assurance Requirements Satisfied: AGD_ADM.1 and AGD_USR.1.

6.2.5 Test

86 The Test assurance provided by BMC Software includes documentation that provides an analysis of the test coverage, an analysis of the depth of testing, and TSF test documentation.

87 The analysis of the test coverage demonstrates correspondence between the tests identified in the test documentation and the TSF as described in the functional specification, and demonstrates that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

88 The analysis of the depth of testing demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and confirms that the information provided meets all requirements for content and presentation of evidence.

89 The TSF test documentation consists of test plans, test procedure descriptions, expected test results and actual test results. The test plans identify the security functions to be tested and describe the goal of the tests to be performed. The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. These scenarios include any ordering dependencies on the results of other tests.

90 The expected test results shall show the anticipated outputs from a successful execution of the test. The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

91 The developer will provide the TOE and an equivalent set of resources equivalent to those that were used in the developer's functional testing of the TSF.

92 These tests measures are documented in the following BMC Software documents:

- BMC Software PATROL®, Perform/Predict Analysis of Coverage
- Secure Perform Agent Product Version 6.5.30 Test Case Inventory, Creation Date: December 5, 2000, Last Update: May 9, 2002

93 Assurance Requirements Satisfied: ATE_COV.1, ATE_FUN.1, and ATE_IND.2.

6.2.6 Vulnerability Assessment

94 The Vulnerability Assessment assurance measures provided by BMC Software include guidance documentation; a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim; and documentation of an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP, and disposition of obvious vulnerabilities.

95 The guidance documents identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation, are complete, clear, consistent and reasonable, list all assumptions about the intended environment, and list all requirements for external security measures (including external procedural, physical and personnel controls).

96 The strength of TOE security function analysis shows, for each mechanism identified in the ST as having a strength of TOE security function claim, that it meets or exceeds the minimum strength level defined in the ST.

97 The vulnerability analysis shows that the developer performed a search analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP and the disposition of obvious vulnerabilities.

98 These measures are documented within the following BMC Software documents:

- BMC Software PATROL® for Unix Performance, Strength of Function Analysis
- BMC Software PATROL® for Unix Performance, Independent Vulnerability Analysis

99 Assurance Requirements Satisfied: AVA_SOF.1, and AVA_VLA.1.

7 PROTECTION PROFILE CLAIMS

100 The BMC Software PATROL® Perform/Predict, Version 6.5.30 Security Target was not written to comply with any Protection Profiles (PPs).

8 RATIONALE

8.1 Security Objectives Rationale

101 This section shows that all TOE threats and organizational security policies are completely covered by security objectives. In addition, Table 10 demonstrates that each objective counters, or addresses, at least one organizational security policy, or TOE threat.

Table 10: TOE Security Objective Rationale Mapping

TOE Security Objective	Threats and Organizational Policies
O.START	T.UNAUTH_USAGE, P.AUTHORIZATION, and P.MANAGE

102 The following objectives are sufficient to address all of the threats and organizational security policies in the ST.

8.1.1 Rationale for TOE Security Objective

103 O.START – This objective is sufficient to counter the TOE threat, T.UNAUTH_USAGE, and to cover the policies, P.AUTHORIZATION and P.MANAGE because it ensures that no unauthorized user can start the collection process on each node.

8.1.2 Rationale for IT Environment Security Objectives

104 This section shows that all threats and assumptions, associated with the IT Environment, are completely covered by security objectives for the IT Environment. In addition, Table 11 demonstrates that each IT Environment security objective counters, or addresses, at least one threat, or assumption. (Note: There are no threats identified for the IT environment.)

Table 11: Security Objectives for the IT Environment Rationale Mapping

IT Environment Security Objectives	Threats and Assumptions
OE.DISCRETIONARY_ACCESS	A.ACCESS_CONTROL
OE.INSTALL	A.MANAGE A.NO_EVIL
OE.PHYSICAL_PROTECTION	A.PHYSICAL_PROTECT
OE.PLATFORM_SUPPORT	A.OPERATE_CORRECT

105 OE.DISCRETIONARY_ACCESS – This objective is sufficient to address the assumption A.ACCESS_CONTROL because it ensures that the host platform discretionary access control (DAC) mechanism (per site policy) will protect TOE data and operation by adhering to site policy.

106 OE.INSTALL – This objective is sufficient to address the assumptions A.MANAGE and A.NO_EVIL because it ensures that the TOE is delivered, installed, managed, and operated in a secure manner by non-hostile individuals.

107 OE.PHYSICAL_PROTECTION – This objective is sufficient to address the assumption A.PHYSICAL_PROTECT because it ensures that the critical parts of the TOE are protected from physical attack.

108 OE.PLATFORM_SUPPORT – This objective is sufficient to address the assumption A.OPERATE_CORRECT because it ensures that the underlying hardware and software operate correctly.

8.2 Security Functional Requirement Rationale

109 The security functional requirement rationale section is provided to demonstrate that the set of security requirements is suitable to meet and traceable to the security objectives.

8.2.1 Traceability and Suitability

110 The following table provides the correspondence mapping between the security objective for the TOE and the requirements to satisfy it:

Table 12: TOE Requirements Mapped to TOE Security Objective

OBJECTIVE SATISFIED	REQUIREMENT
O.START	FDP_ACC.1
O.START	FDP_ACF.1
O.START	FIA_ATD.1
O.START	FMT_MSA.3

111 FDP_ACC.1 requires that each identified SFP be in place for a subset of the possible operations on a subset of the objects in the TOE. The AUTHORIZE SFP requires that only users who are authorized on the node and identified in the authorization.cfg file with modify or manage permission have the ability to start or stop the collection process. Therefore, this requirement satisfies the objective O.START.

112 FDP_ACF.1 allows the TSF to enforce access based upon security attributes and named groups of attributes. The TSF enforces access only to users who are authorized on the node and identified in the authorization.cfg file with modify or manage permission. Because the TSF has a means to ensure that only authorized users can start the collection process, the objective, O.START is satisfied.

113 FIA_ATD.1 allows user security attributes for each user to be maintained individually. The TSF requires that each user who is to be allowed to start the collection process (per site policy) be identified in the authorization.cfg file and be assigned the modify or manage permission. This ensures that the objective O.START is satisfied.

114 FMT_MSA.3 ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. The TSF provides the authorization.cfg file, which is only populated with those users who are permitted to start the collection process.

115 The following table provides the correspondence mapping between security objectives for the TOE IT Environment and the requirements to satisfy them:

Table 13: TOE IT Environment Objectives Mapped to Requirements

OBJECTIVE SATISFIED	REQUIREMENT
OE.DISCRETIONARY_ACCESS	FIA_UAU.2
OE.DISCRETIONARY_ACCESS	FIA_UID.2
OE.INSTALL	NONE
OE.PHYSICAL_PROTECTION	NONE
OE.PLATFORM_SUPPORT	NONE

116 FIA_UAU.2 requires that the TOE IT Environment authenticate all entities prior to TOE interaction with those entities. FIA_UID.2 requires that the TOE IT Environment identify all entities prior to interaction with that entity. Therefore, these SFRs meet the OE.DISCRETIONARY_ACCESS objective because the objective states that, "the TOE environment must provide discretionary access control (DAC) to protect TOE resources and limit TOE application instantiation." These functional requirements ensure that the environment validates the user before the user is authorized access to the TOE. **NOTE:** Those objectives above that are not mapped to SFRs for the IT Environment, are mapped only to assumptions (see Table 11).

8.2.2 Rationale For Assurance Requirements

117 The chosen assurance requirements identified in this ST are drawn from the CC EAL 2 assurance package. This ST has been developed for a generalized environment where there is a low level of risk to the assets. The Security Objectives were reviewed and EAL 2 was found to be sufficient for the developer testing, vulnerability analysis, and the required independent testing.

8.2.3 Requirement Dependency Rationale

118 Table 14 illustrates whether the TOE functional requirement dependencies have been satisfied.

Table 14: Security Functional Requirement Dependency Mapping

Reference Number	SFR Specified in the ST	Dependencies	Is Dependency Satisfied
1	FDP_ACC.1	FDP_ACF.1	2 - Yes
2	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	1 – Yes 4 – No, because it is dependent on site-specific policy.
3	FIA_ATD.1	None	N/A
4	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	No to both, because the TOE does not manage security attributes nor have security roles.

8.2.4 Mutually Supportive

119 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole as evidenced by the following:

120 The choice of security requirements is justified as shown in Sections 8.2.1 and 8.2.2. The choice of SFR and SARs were made based on the assumptions about, the objectives for, and the threats to the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE (Table 10).

121 SFR dependencies have been satisfied as shown in Table 7, Table 8, and Table 14.

122 The SOF claim is valid with the threat environment described in Section 3. The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified in Section 8.3.3 of this Security Target. The SOF claim is commensurate with the EAL 2 level of assurance.

123 The SARs are appropriate for the assurance level of EAL 2 and are satisfied as shown in Section 6.2.

124 The statement of requirements is written using consistent language and do not contain internal contradictions in presenting the security functionality of the TOE.

8.2.5 Rationale for Strength of Function

125 The rationale for the chosen level of SOF-basic is based on the limited attack potential of the threat agents identified in this security target. The CC associates a SOF-basic as being resistant to threats by attackers possessing low attack potential.

8.3 Rationale for TOE Summary Specification

126 This section in conjunction with Section 6 demonstrates that the TOE security function and assurance measures are suitable to meet the TOE security requirements.

8.3.1 TOE Security Functions Satisfy Security Functional Requirements

127 The specified TOE security function works so as to satisfy the TOE security functional requirements. Section 6 includes in the descriptions of the security function a mapping of the security functional requirements to show that each security function is traced to at least one SFR. Table 15 demonstrates that each SFR is covered by at least one TSF. The security function and assurance measures described in the TOE Summary Specification and indicated below are all necessary for the required security functionality claimed for the TOE.

Table 15: SFR to TSF Mapping

TSF	SFR
Authorize	FDP_ACC.1

TSF	SFR
Authorize	FDP_ACF.1
Authorize	FIA_ATD.1
Authorize	FMT_MSA.3

8.3.2 Assurance Measures Comply with Assurance Requirements

128 Section 6.2 of this document identifies the Assurance Measures implemented by BMC Software to satisfy the assurance requirements of EAL 2 as delineated in the table in Annex B of the CC, Part 3. Table 16 maps the Assurance Measures with the Assurance Requirements as stated in Section 5.2.

Table 16: Assurance Compliance Matrix

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ACM_CAP.2	X					
ADO_DEL.1		X				
ADO_IGS.1		X				
ADV_FSP.1			X			
ADV_HLD.1			X			
ADV_RCR.1			X			
AGD_ADM.1				X		
AGD_USR.1				X		
ATE_COV.1					X	
ATE_FUN.1					X	
ATE_IND.2					X	
AVA_SOF.1						X
AVA_VLA.1						X

129 **ACM: Configuration Management**

130 BMC documentation verifies that BMC has implemented a CM Plan that uniquely identifies each version of the TOE. BMC also maintains a configuration list of each TOE version that describes the configuration items that comprise the TOE and the method used to uniquely identify them.

131 **ADO: Delivery and Operation**

132 The BMC Software PATROL® Perform/Predict, Version 6.5.30 is delivered to the BMC engineer for installation at the customer's site. Any relevant documentation that describes what components are delivered with PATROL® Perform/Predict version 6.5.30, guidance for initially installing it, and warnings about the importance of properly unpacking, installing, and configuring the TOE are also accessible to the BMC engineer.

133 **ADV: Development**

134 The Design Document identifies the TSF and its externally visible interfaces, and provides details of the effects, error messages and exceptions of each interface. It describes the TSF in terms of subsystems; the security functionality of each subsystem, and their interfaces.

135 **AGD: Guidance Documents**

136 BMC provides a series of guidance manuals that contain the information needed to satisfy the Guidance Document assurance requirements. These manuals describe the security functions and how to implement them in a secure manner. The operator manuals also provide guidance for the proper secure operation of the TOE.

137 **ATE: Tests**

138 BMC documentation contains satisfactory evidence that the TSF as described was successfully tested. The evaluator will also conduct further testing as well as reproduce the developer's test to ensure that the TSF operates as described.

139 **AVA: Vulnerability Assessment**

140 Section 8.3.3 discusses strength of function of the TOE as SOF-basic because an attacker could not affect the TOE without the proper tools. BMC has developed a Vulnerability Analysis document that addresses obvious weaknesses that could be exploited by an attack.

8.3.3 TOE SOF Claims Rationale

141 The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objective. Section 8.2.1 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because access to the TOE is protected against an attacker of limited ability with no special tools.