Document No. 8014721
Revision No. 1.13
April 20, 2006

STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0 Security Target

Prepared By:

Harris Corporation
Government Communications Systems Division
P.O. Box 8300
Palm Bay, Florida 32902

Document No. 8014721
Revision No. 1.13
April 20, 2006

STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0 Security Target

Prepared By:

Darwin Ammala Date
Security Engineer

Julie Hobbs Date
Systems Engineer

Corinne McNeely Date
Software Engineer

Approved By:

Amanda Pulawski Date
Product Manager

Mike Conroy Date
Software Configuration Manager

Chuck McGregor Date
Software Quality Engineer

Document No. 8014721
Revision No. 1.13
April 20, 2006

Foreword

This document is a Security Target as defined within the *Common Criteria for Evaluation of Information Technology Products*. The product described in this document is developed and maintained by Harris Corporation, Government Communications Systems Division, Melbourne FL.

Harris Corporation, as part of its continuing program to certify security solutions for information systems, promulgates the document ***STAT Guardian™ Vulnerability Management Suite Security Target*** as an evaluation component of SOW #6 – EWA–C050401-002F, Common Criteria EAL 2+ Evaluation for Harris STAT Guardian™ .

The reader may direct questions or comments concerning this document to:

ATTN: STAT Operations, Harris Corporation
Government Communications Systems Division
P.O. Box 8300, Mail Stop 2-11B
Palm Bay, Florida 32902

REVISION HISTORY AND RECORD

Revision	Description of Change	Authority	Date
1.0	Initial Release.	C. McNeely	May 26, 2005
1.1	Updated.	C. McNeely	June 15, 2005
1.2	Incorporated feedback from EWA, from CSE certifier.	C. McNeely, D. Ammala	August 3, 2005
1.3	Incorporated feedback from EWA. Systems review.	J. Hobbs, C.McNeely, D.Ammala	Oct 28, 2005
1.4	Revised TOE Summary Specification for Functional Specification.	C. McNeely	Nov 18, 2005
1.5	Incorporated ORs/CRs from EWA.	C. McNeely	Nov 29, 2005
1.6	Incorporated ORs/CRs from EWA.	C. McNeely	Dec 08, 2005
1.7	Incorporated ORs/CRs from EWA.	C. McNeely	Dec 14, 2005
1.8	Incorporated ORs/CRs from EWA.	C. McNeely	Dec 21, 2005
1.9	Incorporate redlines from EWA site visit.	C. McNeely	January 24, 2006
1.10	Incorporated ORs/CRs from EWA.	C. McNeely	February 28, 2006
1.11	Incorporated ORs/CRs from EWA.	C. McNeely	March 13, 2006
1.12	Incorporated ORs/CRs from EWA.	C. McNeely	April 11, 2006
1.13	Incorporated ORs/CRs from EWA	J.Hobbs	April 20, 2006

Table of Contents

List of Tables

List of Figures

1 SECURITY TARGET INTRODUCTION

1.1 GENERAL

This section presents Security Target (ST) identification and structure information in addition to an overview of the product. A brief discussion of the Security Target development methodology is also provided.

A Security Target document provides the basis for the evaluation of an information technology (IT) product or system under the Common Criteria for Information Security Evaluation (CC). Within the ST the product or system being evaluated is referred to as the Target of Evaluation (TOE). A Security Target principally defines:

- A set of assumptions about the security aspects of the environment, a list of threats the product is intended to counter, and any known rules with which the product must comply (see Section 3, Security Environment).
- A set of security objectives and a set of security requirements are presented in sections four and five, Security Objectives and IT Security Requirements, respectively.
- IT security functions provided by the TOE which meet that set of requirements (see Section 6, TOE Summary Specification).

The structure and contents of this Security Target comply with the requirements specified in the Common Criteria, Part 1, Annex C and Part 3, Chapter 10.

1.2 Security Target Identification

Title: STAT Guardian™ Vulnerability Management Suite (VMS): STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0 Security Target

Registration: 383-4-45

Common Criteria Conformance:

STAT Guardian™ Vulnerability Management Suite (STAT® Scanner 6.4.0, STAT® Patch and Remediation 6.4.0, STAT® Report Center 6.4.0, STAT® Command Center 6.4.0) was developed to Common Criteria version 2.2 Part 2 conformant and Part 3 augmented for a claim of EAL 2+.

Evaluation Assurance Level (EAL):

EAL 2+ with the following augmentations:

ACM_CAP.4, ACM_SCP.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, AVA_MSU.1

Protection Profile Conformance:

The TOE does not claim conformance with any Protection Profile (PP).

Common Criteria Identification:

Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 326, December 2004, with all current approved interpretations.

International Standard:

ISO/IEC 15408:1999

1.3 PRODUCT OVERVIEW

STAT Guardian™ Vulnerability Management Suite (VMS) is a suite of network management tools that provides IT professionals with the capability to perform network vulnerability assessments, apply latest vendor patches, and generate enterprise reports from a single user interface. The STAT Guardian VMS consists of the following individually licensed products:

STAT® Scanner

The newly redesigned STAT Scanner provides the foundation of STAT Guardian VMS with its secure, non-intrusive collection of vulnerability data and detailed Crystal Reports reporting. STAT Scanner 6 performs network vulnerability assessments supporting a wide variety of operating systems, enterprise applications, and software and firmware configurations including:

- Remote discovery and OS identification of machines attached to your network: Microsoft® Windows® NT/2000/XP/2003, Linux variants, HP-UX, Apple® Mac OS X®, BSD-Unix variants, network devices and printers.
- Authenticated vulnerability assessment of the following operating systems: Microsoft Windows NT/2000/XP/2003, Sun™ Solaris™, RedHat® Linux®, Fedora™ Linux, Mandriva Linux™, SuSE Linux®, HP-UX, and Apple® Mac OS X®.
- SNMP-authenticated vulnerability assessment of network devices: Cisco IOS™, Cisco CATOS™, Cisco VPN™, Cisco PIX™, Juniper JUNOS™, Foundry® switches and routers and HP® printers.
- Null-credential vulnerability assessment for open ports, services, and banners.
- Assessment of software defects in enterprise software applications: web browsers, email clients, databases, and web servers.
- Vulnerability cross-referencing with advisory lists: US-CERT, CVE, CIAC, SANS Top 20, NIST, and US Department of Defense, US Army, Navy, and Air Force IAVM.

STAT® Patch and Remediation

STAT Patch and Remediation integrates the vulnerability assessment and enterprise reporting capabilities of STAT Scanner with PatchLink Update™ Server to provide powerful agent-based vulnerability scanning and remediation.

STAT® Report Center

STAT Report Center provides customers with the ability to consolidate vulnerability scan and remediation data from multiple STAT Scanner installations. With STAT Report Center, management users can quickly and easily generate custom reports for the whole enterprise.

STAT® Command Center

STAT Command Center combines the enterprise data collection capabilities of STAT Report Center with the ability to configure and schedule distributed vulnerability scanning and remediation.

1.3.1 Security Target Scope

The STAT Guardian VMS Security Target is aimed towards two audiences. Common Criteria evaluators will use the document to evaluate and determine whether the product meets its claimed Common Criteria certification level. The customer or potential customer may use this ST as a benchmark for comparison of STAT Guardian VMS against other network management systems or as a guidance document for configuring the product securely in an enterprise.

STAT Guardian VMS products are designed for experienced IT security professionals trained in use of vulnerability scanners and remediation techniques. It is assumed product users will not have malicious intent and will configure product host platforms in accordance with product documentation.

For these reasons a claim of SOF-basic is made in that STAT Guardian VMS may be used to gather information from systems located within hostile environments; but the product's components are not designed to resist a direct, administrative level attack against its host operating systems or their communications paths.

STAT Guardian VMS employs secure encryption and network transmission protocols to protect vulnerability data communications from unauthorized disclosure. However, this ST is not intended as a medium for discussion or assessment of the strength of selected encryption algorithms and secure protocols.

STAT Patch and Remediation integrates STAT Scanner with PatchLink Corporation's *PatchLink Update*™ technology to provide agent-based vulnerability scanning and remediation. PatchLink Corporation is independently seeking Common Criteria certification for its *PatchLink Update*™ technology. For this reason the PatchLink Update Server will not be included in the scope of the Security Target Target of Evaluation (TOE).

1.4 CONVENTIONS, TERMINOLOGY AND ACRONYMS

This section distinguishes document formatting conventions and provides STAT Guardian VMS product definitions for terminology having specific meaning within this ST. Abbreviations and acronyms used throughout the document are also clarified.

1.4.1 Conventions

Identifiable font and editing conventions are used to illustrate CC operations on security requirements and to also distinguish text with particular meaning or emphasis. The notation, formatting and conventions used in this ST are largely consistent with those used in its source CC documentation.

The CC allows several operations to be performed on functional requirements. These include *assignment*, *iteration*, *refinement*, and *selection* and are fully defined in paragraph 169 of Part 1 of the CC. The following operations formatting standards are used within this ST.

- The *assignment* operation assigns a specific value to an unspecified parameter. Assignments are represented by plain text within square brackets. [assignment: value(s)]
- *Iteration* allows functional components to be used more than once with varying operations. *Iterative* operations are indicated by appending unique numerical identifiers in parentheses to the component name, short name, and functional element name of requirement. Example: FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).
- The *refinement* operation adds detail or further restricts a requirement. Security requirement refinements are shown in **bold text**.
- The *selection* operation selects one or more options provided by the CC when stating a requirement. Selections are shown with italicized text within square brackets. [selection: *value(s)*]
- Non-bracketed *italicized text* found external to security requirements is used for official document titles or when applying special emphasis to a statement or term.

1.4.2 Terms

ST terminology is aligned with definitions provided by the *Common Criteria for Information Technology Security Evaluation* and the *NSA Glossary of Terms Used in Security and Intrusion Detection*[1] distributed by the NSA Information Systems Security Organization.

Terminology exceptions to the above documentation or any terms unique to this ST have been defined by the STAT Guardian VMS ST authors.

Administrator – A trusted member of an organization given the authority to add, modify or replace TOE system components, permissions, or accounts.

Assets - Information or resources to be protected by the countermeasures of a TOE.

Attack - An attempt to bypass security controls on an IT System. The attack may alter, release, or deny use of data. Attack success depends on the vulnerabilities inherent in the IT System and the effectiveness of existing countermeasures.

[1] NSA *Glossary of Terms Used in Security and Intrusion Detection*, Greg Stocksdale, NSA Information Systems Security Organization, April 1998.

Audit - The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.

Audit Trail - In an IT System, this is a chronological record of system resource use. This may include user login, file access, other defined system activities, and actual or attempted security violations.

Authentication data – Information used to verify the claimed identity of a user.

Authorized User – A user who, in accordance with the TSP, may perform an operation.

Compromise – An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.

Component – The term component may be used in two different contexts in this document: as an individually selectable ST requirement (Security Functional Requirement or Assurance Requirement), or as a logically separate unit of either the TOE architecture or IT operating system.

Confidentiality – Applied assurance that information disclosure is kept within its classification boundaries, with access limited to authorized persons.

Evaluation – CC assessment of a Protection Profile, a Security Target or a Target of Evaluation against defined criteria.

External IT entity – Any IT product or system either untrusted or trusted that is outside of the TOE boundary but interacts with the TOE.

Identity – A unique representation (username/password, key, certificate) identifying a user, which can be a user pseudonym.

Information Technology (IT) System – Individual or combined computer systems and their network.

Integrity – Confidence that information will not be accidentally or maliciously altered or destroyed.

Internal communication channel - A communication channel between separated parts of TOE.

Internal TOE transfer - Communicating data between separated parts of the TOE.

Inter-TSF transfers - Communicating data between the TOE and the security functions of other trusted IT products.

IT Product - A package of IT software, firmware and/or hardware providing a needed functionality. The product may be designed for incorporation within a variety of systems or for a single specified architecture.

Network - Two or more information processing systems interconnected for communication transfer, processing or exchange.

Object – An entity within the TOE Security Function (TSF) scope of control such as a database. The object either contains or receives information and is under operational control of subjects.

Owner – An owner is responsible for granting object access to users on a discretionary and role based basis.

Protection Profile (PP) – An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Privilege – A right to access objects and/or perform operations. A privilege can be granted to some users and not to others.

Remediation – The act of correcting a known vulnerability in application software or operating system. May involve applying a vendor patch or modifying a setting.

Restricted User – Any person with policy granted privileges to access or perform operations on a subset of available data and/or functions in accordance with the TSP.

Role – A predefined set of rules establishing the allowed interactions between a user and the TOE.

Role-Based Access Control (RBAC) – The policy of restricting access to certain data and/or functions based on clearly defined user roles.

Security - A condition that results from the establishment and maintenance of protective measures that ensure a state of defense against unauthorized activity.

Security attributes – Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.

Security Function (SF) – A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP) – A security policy enforced by a security function.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects and distributes information.

Security Target (ST) - A set of security requirements and specifications used as the basis for evaluation of an identified TOE.

STAT Guardian ™ Vulnerability Management Suite (STAT Guardian VMS) - A suite of software tools used to collect, analyze, report and remediate software vulnerabilities on targets in networked environments. The STAT Guardian VMS consists of the following individually licensed products: STAT® Scanner 6, STAT® Patch and Remediation, STAT® Report Center, and STAT® Command Center.

STAT Guardian VMS data – Within this security target the term STAT Guardian VMS data refers to all data stored or transmitted within the boundary of the TOE. TOE data incorporates both TSF data (security attributes used in the execution of TOE functions) and User data (vulnerability and remediation data).

Strength of Function (SOF) -- A qualification of a TOE security function that expresses the minimum effort necessary to defeat designed security behavior by directly attacking underlying security mechanisms.

SOF-basic -- A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

Target – A network asset that is configured as an object of STAT Guardian VMS vulnerability data collection. A network target may be a workstation, server, router, printer or other piece of network equipment.

Target of Evaluation (TOE) - An IT product or system and its associated administrative and user guidance documentation configured and aligned under a Security Target. The Target of Evaluation in this case is the STAT Guardian Vulnerability Management Suite (VMS).

Threat – Capabilities, intentions, and attack methods of adversaries used to exploit IT systems, or a circumstance or event with the potential to cause harm to information or an information system.

TOE Component – indicates logically separate units of the STAT Guardian VMS architecture: STAT Guardian VMS graphical user interface (GUI), the Scanner Engine or Report Center Engine, and the STAT Guardian VMS Database.

TOE Security Functions (TSF) - A set consisting of all security policies, configurations, and products designed into the TOE that are relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) – An official rule set that regulates how information and information assets are managed, protected, and distributed within a TOE.

Transfers outside TSF control – Communicating data to entities not under control of the TSF.

TSF data – Data created by and for the TOE that might affect the operation of the TOE. Within the scope of this ST, TSF data includes information on users and assigned user groups as well as security attributes such as user credentials, certificates, and target credentials.

TSF Scope of Control (TSC) - The set of interactions that occur with or within a TOE and are subject to the rules of the TSP.

User - Any subject or object outside the TOE that interacts with data or information contained within the TOE.

User Data- Data created by and for the user that does not affect the operation of the TSF. Within the scope of this ST, user data includes vulnerability and remediation data.

Vulnerability – A hardware, configuration, or software flaw that leaves an IT System open for potential exploitation via an existing threat. Also a weakness in automated system security procedures, administrative controls, physical layout, or internal controls that could be exploited by an existing threat to gain unauthorized access to information or privileges, could disrupt critical processing, or cause a denial of service condition.

1.4.3 Acronyms

Table 1.4.3 List of Acronyms

ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CERT	Computer Emergency Response Team
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer (SSL)
IP	Internet Protocol
IT	Information Technology
MSDE	Microsoft SQL Server 2000 Desktop Engine
ODBC	Open Database Connectivity
OS	Operating System
POSIX	Portable Operating System Interface
RBAC	Role-Based Access Control
SF	Security Function
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOF	Strength of Function
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
STAT	Security Threat Avoidance Technology
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
VMS	Vulnerability Management Suite
WNet	Microsoft Windows Networking

2 TARGET OF EVALUATION DESCRIPTION

A Target of Evaluation (TOE) description clarifies the scope of the TOE's security requirements and provides a context for evaluation. The TOE's physical and logical boundaries are illustrated and described, as are security conditions for the recommended compliant operational environment.

2.1 EVALUATED CONFIGURATION

A key aspect of STAT Guardian VMS architecture is its modular design. Each STAT Guardian VMS licensed product (STAT Scanner, STAT Patch and Remediation, STAT Report Center, and STAT Command Center) is built from the same reusable system components. For the evaluated configuration we have chosen two systems that demonstrate the combined strength of all of the STAT Guardian VMS products: a STAT Patch and Remediation System and a STAT Command Center System. The STAT Patch and Remediation System integrates the vulnerability assessment and enterprise reporting capabilities of STAT Scanner with PatchLink Update™ Server to provide powerful agent-based vulnerability scanning and remediation. The STAT Command Center System combines the enterprise data collection capabilities of STAT Report Center with the ability to configure and schedule distributed vulnerability scanning and remediation. The *STAT Installation and Security Guide* contains instructions for installing these systems in the evaluated configuration.

Although the PatchLink Update™ Server is not the subject of this evaluation, the evaluated configuration requires an installation of this product to fully demonstrate the capabilities of the STAT Patch and Remediation product. In the evaluated configuration, the PatchLink Update™ Server is co-located on the same host as the STAT Patch and Remediation System. PatchLink Update™ Server uses client software or agents installed on network targets to perform vulnerability assessments and apply vendor patches. For information on remote agent installation please consult the *PatchLinkUpdate 6.1 Quick Start Guide*.

All STAT Guardian VMS products install with a default Microsoft SQL Server Desktop Engine (MSDE) instance. Although STAT Guardian VMS supports installations with any edition of Microsoft SQL Server 2000, the evaluated configuration will use the default MSDE database. The evaluated configuration also requires SQL Server 2000 client tools to manage logon event logs. Microsoft SQL Server 2000 client tools are not provided with the default installation of STAT Guardian VMS products and must be obtained separately.

Tables 2.1.1, 2.1.2, and 2.1.3 list the evaluated software as well as associated unevaluated software. Note that “Part of the IT environment” references all software or hardware defined as outside the TOE boundary but is considered part of the operational IT environment.

2.1.1 STAT Patch and Remediation System

(*) indicates third-party software used by the product.

(**) The evaluated configuration uses Microsoft SQL Server 2000 Enterprise Manager to manage logon events. Microsoft SQL Server 2000 client tools are not installed with STAT Guardian VMS and require a separate SQL Server 2000 license.

Table 2.1.1 STAT Patch and Remediation System Configuration

	Description	**Version**
Within the TOE Boundary	STAT Patch and Remediation	6.4.0, Build 350II
	*Sun Java Runtime Environment (JRE)	1.5.0_02
	*Business Objects Crystal Reports 10 ActiveX Designer Runtime DLL (craxdrt.dll)	10
	*PuTTy Command Line SSH Client (plink.exe)	0.58
	*OpenSSL DLLs (libeay32.dll, ssleay32.dll	0.9.7c
	*Microsoft SQL Server Desktop Engine (MSDE) 2000	2000 SP3a
	Microsoft Windows CryptoAPI DLL (crypt32.dll)	Installed w/ Microsoft Windows OS
	Microsoft Windows NT Event Log DLL (advapi32.dll)	Installed w/ Microsoft Windows OS
Part of the IT environment	Microsoft Windows 2003 Server	2003 SP1
	Microsoft Internet Explorer	6.0 SP1
	Microsoft Internet Information Services (IIS)	6.0
	Microsoft Data Access Components (MDAC)	2.8 SP2
	*Microsoft SQL Server Desktop Engine (MSDE) 2000	2000 SP3a
	**Microsoft SQL Server 2000 Enterprise Manager	8.0
	PatchLink Update Server	6.1.0.110

2.1.2 STAT Command Center System

(*) indicates third-party software used by the product.

(**) The evaluated configuration uses Microsoft SQL Server 2000 Enterprise Manager to manage logon events. Microsoft SQL Server 2000 client tools are not installed with STAT Guardian VMS and require a separate SQL Server 2000 license.

Table 2.1.2 STAT Command Center System Configuration

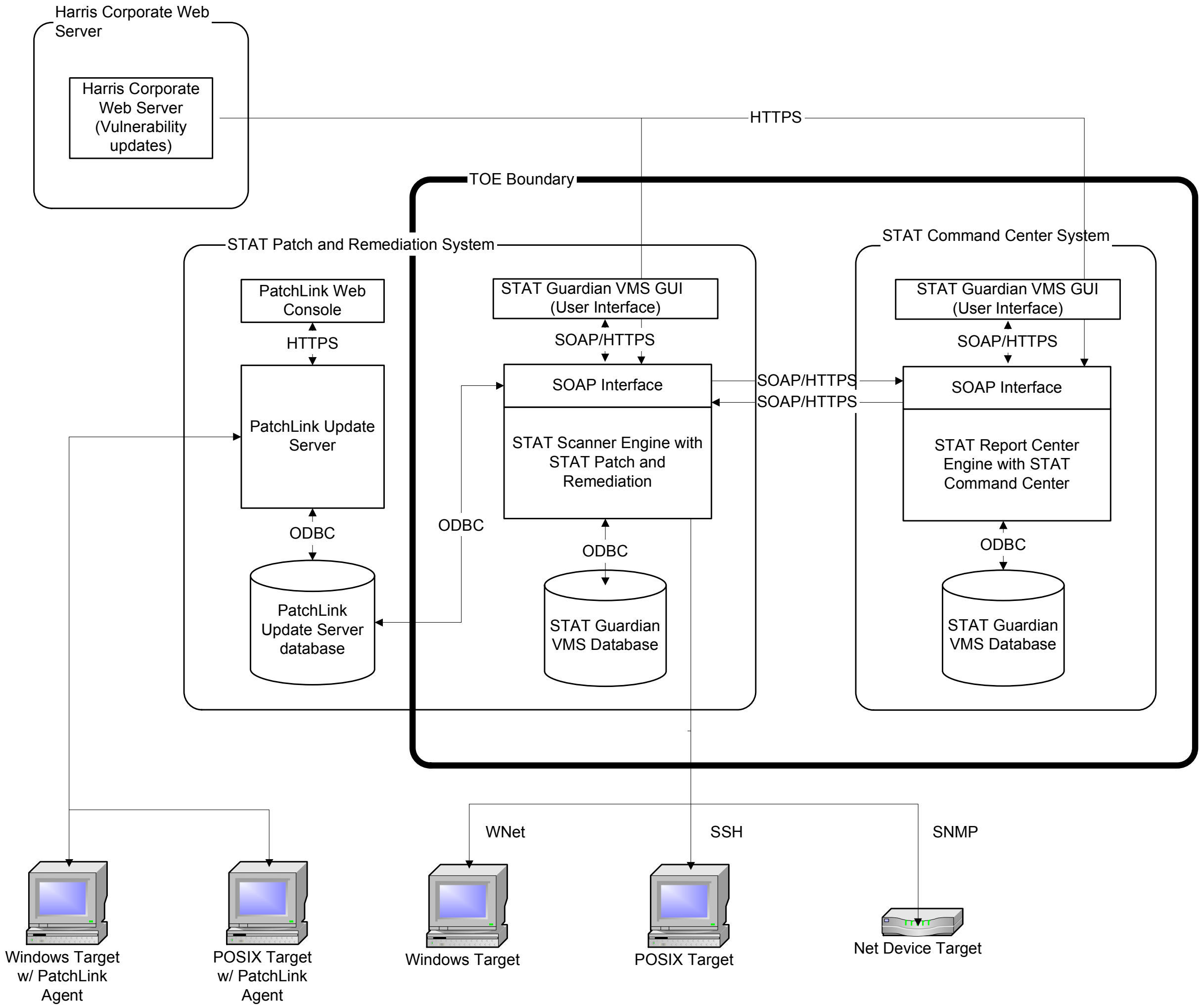
	Description	**Version**
Within the TOE Boundary	STAT Command Center	6.4.0, Build 350II
	*Sun Java Runtime Environment (JRE)	1.5.0_02
	*Business Objects Crystal Reports 10 ActiveX Designer Runtime DLL (craxdrt.dll)	10
	*PuTTy Command Line SSH Client (plink.exe)	0.58
	*OpenSSL DLLs (libeay32.dll, ssleay32.dll	0.9.7c
	*Microsoft SQL Server Desktop Engine (MSDE) 2000	2000 SP3a
	Microsoft Windows CryptoAPI DLL (crypt32.dll)	Installed w/ Microsoft Windows OS
	Microsoft Windows NT Event Log DLL (advapi32.dll)	Installed w/ Microsoft Windows OS
Part of the IT environment	Microsoft Windows 2003 Server	2003 SP1
	Microsoft Internet Explorer	6.0 SP1
	**Microsoft SQL Server 2000 Enterprise Manager	8.0

2.2 TOE BOUNDARY

2.2.1 TOE Physical Boundary

The TOE boundaries and communication paths are shown in Figure 2.1. An explanation of TOE component subsystems and communications follows.

Figure 2.2.1 TOE Physical Scope and Boundary


Harris Corporate Web Server
Harris Corporate Web Server (Vulnerability updates)
HTTPS
TOE Boundary
STAT Patch and Remediation System
PatchLink Web Console
HTTPS
PatchLink Update Server
ODBC
PatchLink Update Server database
STAT Guardian VMS GUI (User Interface)
SOAP/HTTPS
SOAP Interface
STAT Scanner Engine with STAT Patch and Remediation
ODBC
ODBC
STAT Guardian VMS Database
SOAP/HTTPS
SOAP/HTTPS
STAT Command Center System
STAT Guardian VMS GUI (User Interface)
SOAP/HTTPS
SOAP Interface
STAT Report Center Engine with STAT Command Center
ODBC
STAT Guardian VMS Database
WNet
SSH
SNMP
Windows Target w/ PatchLink Agent
POSIX Target w/ PatchLink Agent
Windows Target
POSIX Target
Net Device Target

The STAT Guardian VMS may be decomposed into the following component subsystems:

2.2.1.1 STAT Guardian VMS Graphical User Interface (GUI)

The STAT Guardian VMS Graphical User Interface (GUI) component is the user's access point to product functionality. The user uses the STAT Guardian VMS GUI to connect to either a STAT Scanner or STAT Report Center engine. Based on the type of engine, the GUI will automatically configure itself to present the appropriate interface.

The STAT Guardian VMS GUI is a Java executable and requires a specific Sun Java Runtime Environment (JRE) to operate. If the necessary JRE is not present on the host system at install time, the STAT Guardian VMS Installshield application will install it. For the purposes of this evaluation, the specific JRE installed by the InstallShield will be considered a subcomponent of the STAT Guardian VMS GUI. Any host system pre-existing or later installed JRE versions differing from the version used by STAT Guardian VMS are not touched by the TOE and are not considered a subcomponent of the TOE or GUI. (STAT Guardian VMS 6.4.0)

The GUI communicates with the following internal TOE components:

- Scanner Engine or Report Center Engine – The GUI sends commands and data requests using SOAP calls over HTTPS to a co-located Scanner or Report Center engine service.

2.2.1.2 STAT Scanner Engine

The Scanner Engine runs as a registered Windows service under a local administrator account. The Scanner Engine is a SOAP service that exposes a user interface to discover targets, assess vulnerabilities, and generate custom reports from collected data. The Scanner Engine component uses several third-party licensed executables and libraries in the execution of its functions including but not limited to PuTTy SSH, OpenSSL, Crystal Reports, and several Microsoft libraries including WNet and CryptoAPI. For the purposes of evaluation all of these will be considered subcomponents of the engine.

The Scanner Engine communicates with the following internal TOE components:

- STAT Guardian VMS GUI – The Scanner engine receives commands and data requests from the STAT Guardian VMS GUI over HTTPS.
- STAT Guardian VMS database - The Scanner Engine uses stored procedure calls over ODBC connection to store and retrieve data to the STAT Guardian VMS database.
- STAT Command Center – The Scanner engine may also receive distributed scan and/or remediation requests from remote STAT Command Centers over HTTPS.

The Scanner Engine communicates with the following interfaces external to the TOE:

- Microsoft Windows Registry – The Scanner engine stores and retrieves persistent values in the Windows Registry. Registry keys and key values are protected with Windows ACLs.
- Microsoft Windows Event Log Service – The Scanner Engine generates security event records and logs them to the Windows Event Log Service.
- Harris Corporate Web Server – The Scanner engine automatically retrieves latest vulnerability updates from the STAT Premier Website using dually authenticated HTTPS.

- Remote Windows targets – The Scanner engine supports both authenticated and un-authenticated scanning of remote Windows targets. The Scanner engine uses WNET API to perform authenticated assessment of remote target registry and file systems.
- Remote POSIX targets – The Scanner engine supports both authenticated and un-authenticated scanning of remote POSIX targets. The Scanner engine uses a PuTTy SSH client to assess remote POSIX targets and supports SSH public key authentication.
- Remote Network Devices – The Scanner Engine supports both authenticated and un-authenticated scanning of remote switches, routers, and printers. The Scanner engine uses SNMP to determine firmware versions.

2.2.1.2.1 STAT Patch and Remediation

A STAT Patch and Remediation license key unlocks additional functionality in the Scanner Engine component allowing it to interface with a PatchLink Update Server for agent-based scanning and remediation. For the purposes of this evaluation, this functionality will be considered a subcomponent of the Scanner Engine.

The STAT Patch and Remediation subcomponent allows a Scanner Engine to communicate with the following internal TOE components:

- STAT Guardian VMS GUI – STAT Patch and Remediation provides additional interface functions to the GUI for managing agents, agents groups, and agent vulnerabilities. It also provides functions to perform agent-based vulnerability scanning and remediation.
- STAT Guardian VMS Database – The Scanner Engine uses stored procedure calls over ODBC connection to store and retrieve agent data to the STAT Guardian VMS database.

A STAT Patch and Remediation subcomponent communicates with the following interfaces residing external to the TOE:

- PatchLink Update Server Database - The STAT Patch and Remediation subcomponent retrieves agent data from the PatchLink Update Server via a direct ODBC connection to the PatchLink server’s database. The Scanner engine also uses this connection to schedule agent-based vulnerability scanning and remediation.

2.2.1.3 STAT Report Center Engine

Similar to the STAT Scanner Engine, the STAT Report Center engine runs as a registered Windows service under the local administrative account. However, the STAT Report Center SOAP service exposes a different interface. The Report Center interface allows users to manage, aggregate, and report enterprise vulnerability and remediation data but does not support functions for vulnerability scanning and remediation. The Report Center Engine component utilizes several third-party executables and libraries in the execution of its functions including but not limited to OpenSSL, Crystal Reports, and several Microsoft libraries including CryptoAPI. For the purposes of this evaluation, these libraries and executables will be treated as subcomponents of the Report Center Engine component.

The Report Center Engine communicates with the following internal TOE component:

- STAT Guardian VMS GUI – The Report Center engine receives commands and data requests from the STAT Guardian VMS GUI over HTTPS.

- STAT Guardian VMS database - The Report Center Engine uses stored procedure calls over ODBC connection to store and retrieve consolidated data to the STAT Guardian VMS database.
- Remote Scanner and Report Center Engines – The STAT Report Center aggregates data from multiple STAT Guardian VMS installations. Remote Scanner and Report Center engines transmit scan and remediation data to the Report Center engine over HTTPS.

The Report Center Engine communicates with the following interfaces external to the TOE:

- Microsoft Windows Registry – The Scanner engine stores and retrieves persistent values in the Windows Registry. Registry keys and key values are protected with Windows ACLs.
- Microsoft Windows Event Log Service – The Scanner Engine generates security event records and logs them to the Windows Event Log Service.
- Harris Corporate Web Server – The Scanner engine automatically retrieves latest vulnerability updates from the STAT Premier Website using dually authenticated HTTPS.

2.2.1.3.1 STAT Command Center

A STAT Command Center provides Report Center users with the additional capability to perform distributed scanning and remediation. A STAT Command Center license augments the Report Center interface with functions for configuring and scheduling vulnerability scanning and remediation on multiple remote Scanner systems. For the purposes of this evaluation, this functionality will be considered a subcomponent of the Report Center Engine.

The STAT Command Center subcomponent allows the Report Center Engine to communicate with the following internal TOE components:

- STAT Guardian VMS GUI – The STAT Command Center subcomponent provides additional interface functions to the GUI for configuring and scheduling scan jobs and agent remediation on remote targets.
- Remote Scanner Engines – STAT Command Center performs distributed scanning and remediation by issuing a command directly to the remote Scanner engine's SOAP interface. The outcome of the requested event is reported back to the Report Center's SOAP interface.
- STAT Guardian VMS Database – The Report Center engine uses stored procedure calls over ODBC connection to store and retrieve consolidated data to the STAT Guardian VMS database.

2.2.1.4 STAT Guardian VMS Database

The STAT Guardian VMS Database serves as a repository for both local and remotely collected scan and agent data as well as security attributes. The default installation of the STAT Guardian VMS Database uses Microsoft SQL Server Desktop Engine (MSDE). The MSDE instance shall be considered a subcomponent of the STAT Guardian VMS Database.

The STAT Guardian VMS Database component communicates with the following internal TOE components:

- Scanner Engine or Report Center Engine – Both STAT Scanner and STAT Report Center engines may execute stored procedure calls against the STAT Guardian VMS database.

2.2.2 TOE Logical Boundary

The TOE logical boundary consists of the following security features:

2.2.2.1 Audit Logging

The TOE monitors a comprehensive list of security-related events and records those events to secure logs. Administrators may use these event logs to monitor and control secure usage of the TOE. STAT Guardian VMS uses two separate repositories for security-related events. Successful and unsuccessful logon events are recorded in the SQL Server Logs. Remaining security events are logged to the Windows Event Log. In a properly configured environment, the IT environment is responsible for maintaining the confidentiality and integrity of these event logs.

2.2.2.2 Identification and Authentication

STAT Guardian VMS Security Functional Policies dictate that TOE components are successfully identified and authenticated prior to permitting communication. SFPs also assure that all communications between TOE components and external components in the IT Environment are successfully authenticated. Enforcement of these policies helps prevent man-in-the-middle style attacks in the TOE environment. The following identification and authentication assurances are provided:

- Communications between the GUI and Scanner or Report Center engines requires mutual authentication of both the user and the engine.
- When transmitting data to a remote Report Center for data consolidation, the transmitting Scanner or Report Center engine must successfully authenticate the remote Report Center engine.
- When configuring a remote Scanner for distributed vulnerability scanning or remediation, the Command Center must successfully authenticate both the Scanner user and the remote Scanner engine.
- All stored procedure calls to the STAT Guardian VMS database must be successfully authenticated using either the logged on user’s credentials or the engine service account’s access token.
- When downloading vulnerability updates from the STAT Premier site, STAT Scanner or STAT Report Center engine verifies both the authenticity of the user’s Premier site account as well as the website certificate.
- The STAT Scanner provides multiple authenticated methods of vulnerability assessment of remote network targets including local or domain account authentication to Windows targets, username/password or SSH public key authentication for POSIX targets, and SNMP community string authentication to network devices.
- All transactions between the Scanner engine and PatchLink Update Server are authenticated using the engine service account’s access token.

2.2.2.3 Role-Based Access Control

The sensitive nature of the vulnerability data detected by STAT Guardian VMS products requires the use of a restrictive data management policy. STAT Guardian VMS enforces Role-Based Access Control (RBAC) on TOE functions and data with Guardian user groups. A Guardian user group defines a set of operations or privileges group members may perform with the product. Privileges include the ability to configure and schedule vulnerability scans and remediation, view scan results and agent data, and generate reports. STAT Guardian VMS supports management functions that allow administrators to manage Guardian users and groups. STAT Guardian VMS installs with the following default Guardian user groups defined: Scan User, Advanced Scan User, Remediate User, Advanced Remediate User, Reports User, Manager User and Administrator User.

2.2.2.4 Communications Security

Although the strengths of encryption methods and security protocols are not the subject of this security evaluation, STAT Guardian VMS utilizes these methods to ensure the confidentiality and integrity of its data and communications.

- Transmissions between TOE components are secured via authenticated HTTPS or shared memory.
- Secure network protocols are used in communications between the TOE and external components in the IT environment. STAT Scanner supports SSH public key authentication for POSIX targets for added security.
- Security attributes such as passwords are encrypted with 112 bit 3-DES encryption prior to being stored in either the STAT Guardian VMS database or Windows registry.
- Vulnerability updates are encrypted with 256-bit AES encryption to prevent tampering.

3 TOE SECURITY ENVIRONMENT

3.1 INTRODUCTION

The security environment describes the security aspects of the intended functional and operational TOE environment. Included are assumptions about secure use of the TOE within a standard physical, personnel and connectivity IT environment.

This section catalogs recognized and presumed threats countered by either the TOE or by the TOE's security environment, and defines a baseline of organizational security policy compliance standards. The TOE security environment section also identifies operational assumptions, including physical and procedural security measures applied to the environment in which the STAT Guardian VMS product is installed.

3.2 ASSUMPTIONS

The following section details security assumptions about the TOE and the operating IT environment in which it resides.

A.BACKUP The organization operating the TOE has good backup and recovery procedures allowing the TOE to be recovered to a secure configuration after a hardware failure.

A.NETWORK TOE assets reside in a secure networked environment.

A.NOEVIL TOE users are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by TOE documentation.

A.OSCONFIG The host operating system has been securely installed and configured in accordance with the guidance documentation.

A.PHYSICAL TOE assets, hardware and software, are physically secure and only authorized personnel have physical access to these resources.

A.TOECONFIG The TOE has been securely installed and configured in accordance with guidance documentation.

A.TRAIN Assigned personnel will possess experience and/or appropriate training in supporting and maintaining all aspects of the TOE and the encompassing IT security environment.

3.3 THREATS

Threat agents are either human users or external IT entities not authorized to use the TOE. Additional threat agents may include misconfigured software, operating systems, and/or networks. These threats are reasonably mitigated by the Security Objectives discussed in Section 4 of this ST.

T.DATABASE An unauthorized user may gain access over the STAT Guardian database by bypassing a database security mechanism and use this access to elevate his/her privileges over STAT Guardian VMS functions and/or data.

T.ELEVATE An authorized TOE user may attempt to execute functions and/or view data for which he/she has no authorized privileges.

T.OS An unauthorized user may attempt to gain access over the operating system by bypassing a security mechanism and use this access to elevate his/her privileges over STAT Guardian VMS functions and/or data.

T.SNIFF A networked attacker may attempt to gain unauthorized access to STAT Guardian VMS data by interrupting or monitoring communications between TOE components and between TOE components and networked targets.

T.SPOOF A networked attacker may attempt to view, modify or delete STAT Guardian VMS data by impersonating a TOE component or external IT product.

3.4 ORGANIZATIONAL SECURITY POLICIES

An organizational security policy is a set of rules, practices and procedures imposed by an organization to address its security needs. Organizations attempting to install the STAT Guardian VMS in accordance with this Security Target must enforce the following policies.

P.PASSWORD The TOE Administrator shall enforce all organizational password security policies when assigning user credentials to TOE users.

P.ROLES Organizational role-based access control policies shall determine which individuals are authorized as TOE users and a list of privileges that user shall be permitted.

4 SECURITY OBJECTIVES

4.1 INTRODUCTION

This section identifies the security objectives of the TOE and its supporting IT environment. In the evaluated configuration, we will consider the operating system and its functions part of the IT environment and external to the TOE.

4.2 SECURITY OBJECTIVES FOR THE TOE

The security objectives met by the TOE are discussed in this section.

O.ADMIN The TOE must include a set of administrative functions that allow effective management of its operational and security functions.

O.AUDITS The TOE must record security related events to a secure location.

O.AUTHCOMP The TOE must identify and authenticate TOE components prior to allowing intra-TSF communications.

O.AUTHUSER The TOE must identify and authenticate TOE users prior to allowing users to execute any functions upon the TOE.

O.EXPORT The TOE must ensure confidentiality of User data exported to external IT components.

O.IMPORT The TOE must ensure confidentiality of User data imported from external IT components.

O.ROLES The TOE must enforce Role-Based Access Control for STAT Guardian VMS functions.

4.3 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT

The following section details security objectives maintained by the IT Environment. These objectives do not levy additional requirements for the TOE and are satisfied by procedural or administrative measures.

OE.BACKUP Good backup and recovery procedures exist for the TOE and its data.

OE.DOMAIN The host operating system will provide domain separation and ensure that the TOE cannot be tampered with.

OE.EVTLOG The host operating system on which the TOE is installed must provide a secure repository for security-related events.

OE.GOODUSER Personnel authorized to install, configure, administer, operate and/or maintain the TOE are non-malicious and have been trained in the use of the TOE.

OE.NETWORK The network on which the TOE components reside must be appropriately configured and secured to avoid disclosure of sensitive data.

OE.OSAUTH The user must be successfully authenticated to the host operating system before allowing any access to the TOE.

OE.OSCONFIG The administrative user responsible for installation of the TOE must ensure that hosts on which TOE components will be installed have been properly configured and security hardened. Operating System components used by the TOE (Windows Event Log, System Time, Registry) are secured from unauthorized use and/or modification. Windows user credentials conform to local and domain password restrictions as well as organizational password security policies.

OE.PHYSICAL The physical environment in which the TOE resides must be secured from unauthorized access.

OE.TOECONFIG The administrative user responsible for the TOE must ensure that the TOE is installed and configured in accordance with guidance documentation. TOE user credentials conform to SQL Server database password restrictions as well as organizational password security policies.

5 IT SECURITY REQUIREMENTS

This section defines security requirements met by either the TOE or its IT environment.   Security functional requirements have been selected from Part 2 of the CC. Security Assurance requirements have been selected from Part 3 of the CC for a combines Evaluation Assurance Level (EAL) of 2+.

5.1 TOE SECURITY REQUIREMENTS

The following section lists Security Functional Requirements (SFRs) required meeting TOE security objectives.

Table 5.1 TOE Security Functional Requirements (SFR)

Class	**Component**	**Component Description**
FAU: Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
	FDP_ITT.1	Basic internal transfer protection
FIA: Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
FMT: Security management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_REV.1	Revocation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM.1	Non-bypassability of the TSP

5.1.1 Security Audit (FAU)

Table 5.1.1 details audit requirements for a minimal level of audit fulfilled by the TOE:

Table 5.1.1 TOE Auditable Events

Component	**Event**	**Details**
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.	
FDP_ETC.1	Successful attempts to export information	Vulnerability data and remediation data sent outside the TOE
FDP_IFF.1	Decisions to permit requests for information flow	
FDP_ITC.1	Successful attempts to import user data, including any security attributes	Vulnerability data and remediation data imported into the TOE
FDP_ITT.1	Successful transfers of user data, including the protection method used and any errors that occurred	Internal transfers of vulnerability and remediation data between TOE components
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	Log all unsuccessful attempts to login to STAT Guardian VMS in STAT Guardian VMS database
FIA_UAU.2	Unsuccessful use of the authentication mechanism	Log unsuccessful login attempts to STAT Guardian VMS
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	Audit logs for unsuccessful login includes user identity selection
FMT_MSA.2	All offered and rejected values for a security attribute	Success or failure of security attribute values input into the TOE
FMT_REV.1	Unsuccessful revocation of security attributes	Success or failure of attempts to revoke security attributes
FMT_SMF.1	Use of management functions	Success or failure of attempts to access rule based administrative or management functions
FMT_SMR.1	Modifications to the group of users that are part of a role	Administrative adds or remove a user from a user group. Modification to user group permissions.

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchal to: No other components.

Dependencies: FPT_STM.1 Reliable timestamps

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

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection: minimal] level of audit; and
- [assignment: Use of STAT Guardian VMS component events in addition to the audit capabilities of the underlying operating system]

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

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the ST, [assignment: the additional information specified in the details column of Table 5.1.1 TOE Auditable Events].

5.1.1.2 FAU_GEN.2 User identity association

Hierarchal to: No other components

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset access control

Hierarchal to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce [assignment: GUARDIAN_RBAC_SFP] on [assignment: STAT Guardian VMS functions].

5.1.2.2 FDP_ACC.2 Complete access control

Hierarchal to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP] on [assignment: STAT Guardian VMS functions] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.3 FDP_ACF.1 Security attribute based access control

Hierarchal to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP] to objects based on the [assignment: user identity, user role assigned to that user identity].

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

[assignment: A STAT Guardian VMS user can only perform those functions that a member of the Administrator Users group has specifically assigned to them.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: A member of the Administrator Users group can assign any function to his/herself.]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the

[assignment: A STAT Guardian VMS user will be denied any functions that are not explicitly granted them by a member of the Administrator Users group].

5.1.2.4 FDP_ETC.1 Export of user data without security attributes

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FDP_ETC.1.1 The TSF shall enforce the [assignment: REMEDIATION_DATA_SFP] when exporting user data, controlled under the SFP, outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

5.1.2.5 FDP_IFC.1 Subset information flow control (1)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (1) The TSF shall enforce the [assignment: GUI_SFP] on [assignment: all communications between STAT Guardian VMS GUI and Scanner Engine and/or Report Center Engine.]

5.1.2.6 FDP_IFC.1 Subset information flow control (2)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (2) The TSF shall enforce the [assignment: REPORT_CENTER_SFP] on [assignment: all one-way push of user data from a Scanner Engine and Report Center Engine to a remote Report Center Engine for data aggregation.]

5.1.2.7 FDP_IFC.1 Subset information flow control (3)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (3) The TSF shall enforce the [assignment: COMMAND_CENTER_SFP] on [assignment: all one-way push of job configuration data from a Report Center engine to a remote Scanner Engine for distributed scanning.]

5.1.2.8 FDP_IFC.1 Subset information flow control (4)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (4) The TSF shall enforce the [assignment: VULNERABILITY_DATA_SFP] on [assignment: all transfer of user data between a Scanner Engine or Report Center Engine and the STAT Guardian VMS Database.]

5.1.2.9 FDP_IFC.1 Subset information flow control (5)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (5) The TSF shall enforce the [assignment: VULNERABILITY_UPDATE_SFP] on [assignment: Scanner or Report Center Engines when importing vulnerability updates from the Harris Corporate Web Server.]

5.1.2.10 FDP_IFC.1 Subset information flow control (6)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (6) The TSF shall enforce the [assignment: SCAN_SFP] on [assignment: Scanner Engines when performing authenticated scanning of remote target hosts.]

5.1.2.11 FDP_IFC.1 Subset information flow control (7)

Hierarchal to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 (7) The TSF shall enforce the [assignment: REMEDIATION_DATA_SFP] on [assignment: Scanner Engines when importing and exporting remediation data from PatchLink Server database]

5.1.2.12 FDP_IFF.1 Simple security attributes (1)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (1) TSF shall enforce the [assignment: GUI_SFP] based on the following types of subject and information security attributes: [assignment: (1) identification and authentication of Scanner or Report Center engine (2) identification and authentication of the user credentials].

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the transfer of data between the STAT Guardian VMS GUI and either a Scanner Engine or a Report Center Engine, the following credentials must be provided: (1) The engine must return the SHA-1 of its self-signed certificate to the GUI (1) The GUI must pass the user’s username/password to the Scanner or Report Center Engine].

FDP_IFF.1.3 (1) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (1) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (1) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (1) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.13 FDP_IFF.1 Simple security attributes (2)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (2) The TSF shall enforce the [assignment: REPORT_CENTER_SFP] based on the following types of subject and information security attributes: [assignment: (1) Identification and authentication of the receiving Report Center engine].

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the transfer of user data from a Scanner or Report Center Engine to a remote Report Center Engine the following credentials must be provided: (1) The user must accept the SHA-1 signature of the receiving engines self-signed certificate]

FDP_IFF.1.3 (2) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (2) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (2) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (2) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.14 FDP_IFF.1 Simple security attributes (3)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (3) The TSF shall enforce the [assignment: COMMAND_CENTER_SFP] based on the following types of subject and information security attributes: [assignment: (1) identification and authentication of the receiving Scanner Engine (2) identification and authentication of the Scanner user credentials].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the transfer of data from a Report Center Engine to a remote Scanner Engine the following credentials must be provided: (1) The user must accept the SHA-1 signature of the receiving engines self-signed certificate (2) The transmitting engine must present the receiving engine valid Scanner user credentials]

FDP_IFF.1.3 (3) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (3) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (3) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (3) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.15 FDP_IFF.1 Simple security attributes (4)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (4) The TSF shall enforce the [assignment: VULNERABILITY_DATA_SFP] based on the following types of subject and information security attributes: [assignment: (1) identification and authentication of the user credentials for STAT Guardian VMS Database].

FDP_IFF.1.2 (4) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the transfer of user data between Scanner or Report Center Engine and the STAT Guardian VMS database, the following credentials must be provided: (1) the engine making the database query must provide valid database credentials].

FDP_IFF.1.3 (4) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (4) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (4) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (4) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.16 FDP_IFF.1 Simple security attributes (5)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (5) The TSF shall enforce the [assignment: VULNERABILITY_UPDATE_SFP] based on the following types of subject and information security attributes: [assignment: (1) identification and authentication of web server (2) identification and authentication of the user credentials].

FDP_IFF.1.2 (5) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the import of vulnerability update data from the Harris Corporate Web Server into the Scanner or Report Center engine, the following credentials must be provided: (1) The requesting engine will verify the trusted-party signed certificate of the Harris Corporate Web Server (2) The requesting engine must provide user credentials to the web server].

FDP_IFF.1.3 (5) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (5) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (5) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (5) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.17 FDP_IFF.1 Simple security attributes (6)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (6) The TSF shall enforce the [assignment: SCAN_SFP] based on the following types of subject and information security attributes: [assignment: (1) identification and authentication of the user credentials for authenticated target machines].

FDP_IFF.1.2 (6) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the transfer of vulnerability data between Scanner Engine and authenticated targets, the following credentials must be provided: (1) username/password credentials for Windows targets (2) SSH public key for POSIX targets, or in the absence of public key, username/password credentials (3) SNMP community strings for Net Device targets].

FDP_IFF.1.3 (6) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (6) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (6) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (6) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.18 FDP_IFF.1 Simple security attributes (7)

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (7) The TSF shall enforce the [assignment: REMEDIATION_DATA_SFP] based on the following types of subject and information security attributes: [assignment: (1) identification and authentication of the user credentials for Remediation Database].

FDP_IFF.1.2 (7) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: For the transfer of remediation data between the PatchLink Server database and the Scanner Engine, the following credentials must be provided: (1) username/password credentials for remediation database].

FDP_IFF.1.3 (7) The TSF shall enforce the [assignment: no additional information flow control SFP rules].

FDP_IFF.1.4 (7) The TSF shall provide the following [assignment: no additional SFP capabilities]

FDP_IFF.1.5 (7) The TSF shall explicitly authorize an information flow based on the following rules: [assignment: none].

FDP_IFF.1.6 (7) The TSF shall explicitly deny an information flow based on the following rules: [assignment: none].

5.1.2.19 FDP_ITC.1 Import of user data without security attributes

Hierarchal to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [assignment: VULNERABILITY_UPDATE_SFP, SCAN_SFP, and REMEDIATION_DATA_SFP] when importing user data, controlled under the SFP from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: no additional importation control rules].

5.1.2.20 FDP_ITT.1 Basic internal transfer protection

Hierarchal to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FDP_ITT.1.1 The TSF shall enforce the [assignment: GUI_SFP, VULNERABILITY_DATA_SFP, REPORT_CENTER_SFP] to prevent the [selection: *disclosure, modification*] of user data when it is transmitted between physically separated parts of the TOE.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchal to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: one]] unsuccessful authentication attempts occur related to [assignment: log on to STAT Guardian VMS].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: log the failure status, user name, and time of failure to an event log.].

5.1.3.2 FIA_ATD.1 User attribute definition

Hierarchal to: No other components

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: user name, authentication data, assigned user group].

5.1.3.3 FIA_UAU.2 User authentication before any action

Hierarchal to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

5.1.3.4 FIA_UID.2 User identification before any action

Hierarchal to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of security functions behavior

Hierarchal to: No other components

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *disable, enable, modify the behavior of]* the functions [assignment: user and group management functions] to [assignment: members of the Administrator Users group].

5.1.4.2 FMT_MSA.1 Management of security attributes (1)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (1) The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, GUI_SFP] to restrict the ability to [selection: *modify*] the security attributes [assignment: a user’s password] to [assignment: the individual user or members of the Administrator Users group].

5.1.4.3 FMT_MSA.1 Management of security attributes (2)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (2) The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, REPORT_CENTER_SFP] to restrict the ability to [selection: *delete*, *modify,* [assignment: add]] the security attributes [assignment: the remote Report Center's SHA-1 thumbprint] to [assignment: members of the Advanced Scan, Advanced Remediate, Manager Users and Administrator Users groups].

5.1.4.4 FMT_MSA.1 Management of security attributes (3)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (3) The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, COMMAND_CENTER_SFP] to restrict the ability to [selection: *delete*, *modify,* [assignment: add]] the security attributes [assignment: the remote Scanner's SHA-1 thumbprint] to [assignment: members of the Administrator Users groups].

5.1.4.5 FMT_MSA.1 Management of security attributes (4)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (4) The TSF shall enforce the [assignment: VULNERABILITY_DATA_SFP] to restrict the ability to [selection: *delete, modify,* [assignment: add]] the security attributes [assignment: STAT Guardian VMS Database credentials] to [assignment: members of Administrator Users group or STAT Guardian VMS Database administrators].

5.1.4.6 FMT_MSA.1 Management of security attributes (5)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (5) The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, VULNERABILITY_UPDATE_SFP] to restrict the ability to [selection: *delete, modify*, [assignment: add]] the security attributes [assignment: web server credentials (username, password)] to [assignment: members of Manager Users, or Administrator Users groups].

5.1.4.7 FMT_MSA.1 Management of security attributes (6)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (6) The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, SCAN_SFP] to restrict the ability to [assignment: add] the security attributes [assignment: target user credentials (Windows username/password, POSIX Public Key or username/password, SNMP community string)] to [assignment: members of Scan Users, Advanced Scan Users, Manager Users, or Administrator Users groups].

5.1.4.8 FMT_MSA.1 Management of security attributes (7)

Hierarchal to: No other components

Dependencies: FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 (7) The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, SCAN_SFP] to restrict the ability to [selection: *delete, modify*] the security attributes [assignment: target user credentials (Windows username/password, POSIX Public Key or username/password, SNMP community string)] to [assignment: members of Advanced Scan Users, Manager Users, or Administrator Users groups].

5.1.4.9 FMT_MSA.2 Secure security attributes

Hierarchal to: No other components

Dependencies: ADV_SPM.1 Informal TOE security policy model

FDP_ACC.1 Subset access control

FDP_IFC.1 Subset Information Flow control

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.4.10 FMT_MSA.3 Static attribute initialization

Hierarchal to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: GUARDIAN_RBAC_SFP, GUI_SFP, VULNERABILITY_DATA_SFP, VULNERABILITY_UPDATE_SFP, SCAN_SFP, REMEDIATION_DATA_SFP] to provide [selection: [assignment: no]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: members of no user group] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The TSF does not allow default values for security attributes defined in the security functional policies. The TOE user is explicitly prompted to enter a secure attribute value (described in FMT_MSA.1) prior to allowing any inbound or outbound communication.

5.1.4.11 FMT_MTD.1 Management of TSF data (1)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (1) TSF shall restrict the ability to [selection: *modify*] the [assignment: user's password] to [assignment: the individual user or members of the Administrator Users group].

5.1.4.12 FMT_MTD.1 Management of TSF data (2)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (2) The TSF shall restrict the ability to [selection: *delete, modify,* [assignment: add]] the [assignment: remote Report Center's SHA-1 thumbprint] to [assignment: members of the Advanced Scan, Advanced Remediate, Manager Users and Administrator Users groups].

5.1.4.13 FMT_MTD.1 Management of TSF data (3)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (3) The TSF shall restrict the ability to [selection: *delete, modify,* [assignment: add]] the [assignment: remote Scanner's SHA-1 thumbprint] to [assignment: members of the Administrator Users groups].

5.1.4.14 FMT_MTD.1 Management of TSF data (4)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (4) The TSF shall restrict the ability to [selection: *delete*, *modify*, [assignment: add]] the [assignment: STAT Guardian VMS Database credentials] to [assignment: members of Administrator Users group or STAT Guardian VMS Database administrators].

5.1.4.15 FMT_MTD.1 Management of TSF data (5)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (5) The TSF shall restrict the ability to [selection: *delete*, *modify*, [assignment: add]] the [assignment: web server credentials (username, password)] to [assignment: members of Manager Users, or Administrator Users groups].

5.1.4.16 FMT_MTD.1 Management of TSF data (6)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (6) The TSF shall restrict the ability to [selection: [assignment: add]] the [assignment: target user credentials (Windows username/password, POSIX Public Key or username/password, SNMP community string)] to [assignment: members of Scan Users, Advanced Scan Users, Manager Users, or Administrator Users groups].

5.1.4.17 FMT_MTD.1 Management of TSF data (7)

Hierarchal to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MTD.1.1 (7) The TSF shall restrict the ability to [selection: *delete*, *modify*] the [assignment: target user credentials (Windows username/password, POSIX Public Key or username/password, SNMP community string)] to [assignment: members of Advanced Scan Users, Manager Users, or Administrator Users groups].

5.1.4.18 FMT_REV.1 Revocation

Hierarchal to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [selection: *users*, [Assignment: user groups]] within the TSC to [assignment: members of the Administrator Users group].

FMT_REV.1.2 The TSF shall enforce the rules [assignment: no other rules].

5.1.4.19 FMT_SMF.1 Specification of Management Functions

Hierarchal to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: create, delete, modify, and view role based access rules that permit or deny information flows].

5.1.4.20 FMT_SMR.1 Security roles

Hierarchal to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: Administrator Users, Manager Users, Scan Users, Advanced Scan Users, Remediate Users, Advanced Remediate Users, and Reports Users].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchal to: No other components.

Dependencies: No dependencies.

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

5.1.5.2 FPT_RVM.1 Non-bypassability of the TSP

Hierarchal to: No other components.

Dependencies: No dependencies.

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.

5.2 SECURITY REQUIREMENTS FOR IT ENVIRONMENT

The STAT Guardian VMS product relies upon the external IT environment (including the underlying operating system) to provide some of the security features of the product. The following section lists Security Functional Requirements (SFRs) partially or fully implemented by the IT environment. Table 5.2 details IT Environment Security Functional Requirements fulfilled by the IT environment:

Table 5.2 IT Environment Security Functional Requirements (SFR)

Class	**Component**	**Component Description**
FAU: Security Audit	FAU_GEN.1E	Audit data generation
	FAU_GEN.2E	User identity association
	FAU_SAR.1E	Audit review
	FAU_SAR.2E	Restricted audit review
	FAU_SAR.3E	Selectable audit review
FDP: User Data Protection	FDP_ACC.1E	Subset access control
	FDP_ACF.1E	Security attribute based access control
FIA: Identification and Authentication	FIA_UAU.2E	User authentication before any action
	FIA_UID.2E	User identification before any action
FMT: Security management	FMT_MSA.1E	Management of security attributes
	FMT_MSA.2E	Secure security attributes
	FMT_MSA.3E	Static attribute initialization
	FMT_MTD.1E	Management of TSF data
	FMT_SMF.1E	Specification of Management Functions
	FMT_SMR.1E	Security roles
FPT: Protection of the TSF	FPT_SEP.1E	TSF domain separation
	FPT_STM.1E	Reliable timestamps

5.2.1 Security Audit (FAU)

Table 5.2.1 details audit requirements fulfilled by the IT environment:

Table 5.2.1 IT Environment Auditable Events

Component	**Event**	**Details**
FAU_GEN.1E	Start-up and shutdown of audit functions	Start up and shutdown of Windows Event Log. Provided by operating system.
FAU_SAR.1E	Reading of information from the audit records	All attempts to view Windows Event Log data. Provided by operating system.
FDP_ACF.1E	Successful requests to perform an operation on an object covered by the SFP.	Modifications to operating system ACLs on TOE files, directories, and registry objects. Provided by operating system.
FIA_UAU.2E	All use of the authentication mechanism	Log all login attempts to the operating system. Provided by operating system.
FIA_UID.2E	All use of the user identification mechanism, including the user identity provided	All login attempts to the operating system. Provided by operating system.
FMT_MSA.2E	All offered and rejected values for a security attribute	Success or failure of authentication to operating system. Provided by operating system.
FMT_SMF.1E	Use of management functions	Success or failure of attempts to access management functions. Provided by operating system.
FMT_SMR.1E	Modifications to the group of users that are part of a role	Administrative adds or removes a user from a Windows user group. Provided by operating system.
FPT_STM.1E	Changes to the time	All modifications to the Windows System Clock. Provided by operating system.

5.2.1.1 FAU_GEN.1E Audit data generation

Hierarchal to: No other components.

Dependencies: FPT_STM.1E Reliable timestamps

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

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection: *minimal*] level of audit; and
- [Assignment: Use of STAT Guardian VMS component events in addition to the audit capabilities of the underlying operating system]

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

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

- For each audit event type, based on the auditable event definitions of the functional components included in the ST, [Assignment: the additional information specified in the details column of Table 5.2.1 Auditable Events].

5.2.1.2 FAU_GEN.2E User identity association

Hierarchal to: No other components

Dependencies: FAU_GEN.1E Audit data generation
FIA_UID.1E Timing of identification

FAU_GEN.2.1E The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_SAR.1E Audit review

Hierarchal to: No other components

Dependencies: FAU_GEN.1E Audit data generation

FAU_SAR.1.1E The TSF shall provide [assignment: authorized operating system users] with the capability to read [Assignment: date and time of the event, type of event, subject identity, and the outcome of the event (success or failure)] from the audit records.

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

5.2.1.4 FAU_SAR.2E Restricted Audit review

Hierarchal to: No other components

Dependencies: FAU_SAR.1E Audit review

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

5.2.1.5 FAU_SAR.3E Selectable audit review

Hierarchal to: No other components

Dependencies: FAU_SAR.1E Audit review

FAU_SAR.3.1E The TSF shall provide the ability to perform [selection: *sorting*] of audit data based on [assignment: date, event source].

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.1E Subset access control

Hierarchal to: No other components.

Dependencies: FDP_ACF.1E Security attribute based access control

FDP_ACC.1.1E The TSF shall enforce [assignment: OS_RBAC_SFP] on [assignment: TOE files, directory, and registry objects].

5.2.2.2 FDP_ACF.1E Security attribute based access control

Hierarchal to: No other components.

Dependencies: FDP_ACC.1E Subset access control

FMT_MSA.3E Static attribute initialization

FDP_ACF.1.1E The TSF shall enforce the [assignment: OS_RBAC_SFP] to objects based on the [assignment: operating system user identity, Windows group membership].

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

[assignment: The operating system shall limit the ability to access, modify, and/or delete TOE file, directory, and registry objects to those users explicitly authorized in the Access Control Lists (ACLs).]

FDP_ACF.1.3E The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: A member of the Windows Administrators group may always assign ACLs to himself.]

FDP_ACF.1.4E The TSF shall explicitly deny access of subjects to objects based on the

[assignment: The operating system shall deny access of TOE file, directory, and registry objects to operating system users not explicitly granted by Access Control Lists (ACLs).].

5.2.3 Identification and Authentication (FIA)

5.2.2.1 FIA_UAU.2E User authentication before any action

Hierarchal to: FIA_UAU.1E

Dependencies: FIA_UID.1E Timing of identification

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

5.2.2.2 FIA_UID.2E User identification before any action

Hierarchal to: FIA_UID.1E

Dependencies: No dependencies.

FIA_UID.2.1E The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of the user.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MSA.1 Management of security attributes (1) E

Hierarchal to: No other components

Dependencies: FDP_ACC.1E Subset access control

FMT_SMF.1E Specification of Management Functions

FMT_SMR.1E Security roles

FMT_MSA.1.1 (1) The TSF shall enforce the [assignment: OS_RBAC_SFP] to restrict the ability to [selection: *change_default, query, modify, delete*] the security attributes [assignment: ACLs on TOE files, directory, and registry objects] to [assignment: members of Windows Administrators group or Windows Guardian Users groups].

5.2.4.2 FMT_MSA.1 Management of security attributes (2) E

Hierarchal to: No other components

Dependencies: FDP_ACC.1E Subset access control

FMT_SMF.1E Specification of Management Functions

FMT_SMR.1E Security roles

FMT_MSA.1.1 (2) E The TSF shall enforce the [assignment: GUI_SFP] to restrict the ability to [selection: *delete*, *modify,* [assignment: add]] the security attributes [assignment: the Scanner or Report Center engine's SHA-1 thumbprint] to [assignment: members of the Windows Administrators or Windows Guardian Users groups].

Application Note: STAT Guardian VMS uses the SHA-1 signature of the engine's self-signed certificate to authenticate the TOE to the user. When the user selects "Accept Always", the STAT Guardian VMS GUI stores this value in the Windows Registry. Because the user is not yet authenticated to the TOE at this point, the security of this SHA-1 thumbprint is maintained by the Windows operating system. The security of this security attribute is maintained through the use of Windows ACLs and audit policy settings.

5.2.4.3 FMT_MSA.2E Secure security attributes

Hierarchal to: No other components

Dependencies: ADV_SPM.1 Informal TOE security policy model

FDP_ACC.1E Subset access control

FMT_MSA.1E Management of security attributes

FMT_SMR.1E Security roles

FMT_MSA.2.1E The TSF shall ensure that only secure values are accepted for security attributes.

5.2.4.4 FMT_MSA.3E Static attribute initialization

Hierarchal to: No other components.

Dependencies: FMT_MSA.1E Management of security attributes

FMT_SMR.1E Security roles

FMT_MSA.3.1E The TSF shall enforce the [assignment: OS_RBAC_SFP] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2E The TSF shall allow the [assignment: members of the Windows Administrators or Windows Guardian Users groups] to specify alternative initial values to override the default values when an object or information is created.

5.2.4.5 FMT_MTD.1 Management of TSF data (1) E

Hierarchal to: No other components.

Dependencies: FMT_SMF.1E Specification of Management Functions

FMT_SMR.1E Security roles

FMT_MTD.1.1 (3) E The TSF shall restrict the ability to [selection: *change_default, delete, modify,* [assignment: add]] the [assignment: ACLs on TOE files, directories, and registry keys] to [assignment: members of Windows Administrators or Windows Guardian Users groups].

5.2.4.6 FMT_MTD.1 Management of TSF data (2) E

Hierarchal to: No other components.

Dependencies: FMT_SMF.1E Specification of Management Functions

FMT_SMR.1E Security roles

FMT_MTD.1.1 (1) E The TSF shall restrict the ability to [selection: *query*, [assignment: add]] the [assignment: audit data] to [assignment: members of the Windows Users group].

5.2.4.7 FMT_MTD.1 Management of TSF data (3) E

Hierarchal to: No other components.

Dependencies: FMT_SMF.1E Specification of Management Functions

FMT_SMR.1E Security roles

FMT_MTD.1.1 (2) E The TSF shall restrict the ability to [selection: *delete*] the [assignment: audit data] to [assignment: members of the Windows Administrators group].

5.2.4.8 FMT_MTD.1 Management of TSF data (4) E

Hierarchal to: No other components.

Dependencies: FMT_SMF.1E Specification of Management Functions

FMT_SMR.1E Security roles

FMT_MTD.1.1 (3) E The TSF shall restrict the ability to [selection: *delete, modify*, [assignment: add]] the [assignment: Scanner or Report Center engine's SHA-1 thumbprint] to [assignment: members of the Windows Administrators or Windows Guardian Users groups].

Application Note: STAT Guardian VMS uses the SHA-1 signature of the engine's self-signed certificate to authenticate the TOE to the user. When the user selects "Accept Always", the STAT Guardian VMS GUI stores this value in the Windows Registry. Because the user is not yet authenticated to the TOE at this point, the security of this SHA-1 thumbprint is maintained by the Windows operating system. The security of this security attribute is maintained through the use of Windows ACLs and audit policy settings.

5.2.4.9 FMT_SMF.1E Specification of Management Functions

Hierarchal to: No other components.

Dependencies: No dependencies

FMT_SMF.1.1E The TSF shall be capable of performing the following security management functions: [assignment: add, modify, and delete operating system users and assign operating system users to Windows user groups].

5.2.4.10 FMT_SMR.1E Security roles

Hierarchal to: No other components.

Dependencies: FIA_UID.1E Timing of identification

FMT_SMR.1.1E The TSF shall maintain the roles: [assignment: Windows Users group, Windows Guardian Users group, Windows Administrators group].

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

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_SEP.1E TSF domain separation

Hierarchal to: No other components.

Dependencies: No dependencies.

FPT_SEP.1.1E The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2E The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2.5.2 FPT_STM.1E Reliable timestamps

Hierarchal to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1E The TSF shall be able to provide reliable timestamps for its own use.

5.3 TOE SECURITY FUNCTIONAL POLICIES

5.3.1 Access Control (OS_RBAC_SFP)

The host operating system enforces Role-Based Access Control (RBAC) of TOE files, directories, and registry keys. OS_RBAC_SFP restricts access to these TOE objects to members of the Windows Administrators or Windows Guardian Users groups. This policy is enforced by Windows Access Control Lists (ACLs) that are applied either at the time of install or during configuration of a secure TOE. A member of the Windows Administrators group may always grant himself ACLs to a protected TOE object.

5.3.2 Access Control (GUARDIAN_RBAC_SFP)

The GUARDIAN_RBAC_SFP assures that only policy-authorized individuals have access to certain STAT Guardian VMS functions. The TOE maintains a set of default user groups that define a subset of privileges, or STAT Guardian VMS functions, members of that group may perform upon the TOE. Only members of the Administrators User group may add users and assign them to user groups. All TOE components support enforcement of the GUARDIAN_RBAC_SFP.

5.3.3 STAT Guardian VMS GUI to/from Scanner Engine or Report Center Engine (GUI_SFP)

All communication between the STAT Guardian VMS GUI and a Scanner or Report Center Engine is secured via mutually authenticated HTTPS. Mutual authentication prevents spoofing or man-in-the-middle attacks. Under the evaluated configuration, the TOE will permit information flow under the following conditions: (1) The user manually verifies and then accepts the SHA-1 checksum of the service’s certificate displayed by the GUI And (2) The Engine verifies that the user credentials presented by the GUI are valid user credentials.

5.3.4 Data Aggregation with STAT Report Center (REPORT_CENTER_SFP)

STAT Scanners or Report Centers transmit vulnerability and/or remediation data to a remote Report Center for data aggregation. The REPORT_CENTER_SFP assures that the data is secured via authenticated HTTPS. Prior to transmitting data to the remote Report Center engine, the transmitting engine must verify the SHA-1 thumbprint of the remote Report Center engine.

5.3.5 Distributed Scanning with STAT Report Center (COMMAND_CENTER_SFP)

The STAT Command Center provides an additional distributed capability for enterprise-wide scanning and remediation. The COMMAND_CENTER_SFP assures that the data is secured via authenticated HTTPS. Prior to transmitting data to the remote Scanner engine, the transmitting engine must verify the SHA-1 thumbprint of the remote Scanner engine. The Scanner engine must verify the Scanner user credentials transmitted from the Report Center.

5.3.6 Scanner Engine or Report Center Engine to/from STAT Guardian VMS Database (VULNERABILITY_DATA_SFP)

The TOE stores vulnerability data, remediation data, and user credentials and settings in a MSDE or SQL Server database. The TOE secures all transfers of user and TSF data to/from the STAT Guardian VMS database by requiring successful authentication between Scanner Engine or Report Center Engine and the database. Every command sent to the database provides either the credentials of the logged in user or the credentials of the Engine service. The database verifies the user’s identity and access privileges before executing a stored procedure on that user’s behalf.

5.3.7 Scanner Engine to/from the Harris Corporate web server (VULNERABILITY_UPDATE_SFP)

Automatic vulnerability updates imported into STAT Guardian from the Harris Corporate website are secured via HTTPS. The TOE will accept a vulnerability update file from the web server if the following conditions are met: (1) The HTTPS protocol verifies the web server's trusted third party signed certificate. (2) The Scanner Engine provides a licensed Premier Site user's credentials to the web server.

5.3.8 Authenticated Scanning of Windows, POSIX, and SNMP targets (SCAN_SFP)

The Scanner Engine supports multiple means of assessing vulnerabilities on remote network targets. The SCAN_SFP applies to authenticated scanning only. STAT Guardian VMS also supports methods of scanning that do not require credentials: port scanning, null session scanning. The SCAN_SFP enforces user authentication for authenticated scanning: username/password authentication for Windows targets, SSH public key or username/password authentication for POSIX targets, and SNMP authentication for Network Device targets.

5.3.9 Scanner Engine to/from PatchLink Remediation database (REMEDIATION_DATA_SFP)

The STAT Patch and Remediation allows the Scanner engine to interface with a PatchLink Update Server in order to perform agent-based vulnerability scans and remediation. The REMEDIATION_DATA_SFP pertains to all imported and exported data that occurs between these two servers. The Scanner Engine exchanges data with the PatchLink Update Server via a direct ODBC connection to its database. Since in the evaluated configuration the two servers are co-located on the same box, the Scanner Engine implicitly authenticates to the PatchLink database using the Scanner Engine service's local Administrative account.

5.4 TOE SECURITY ASSURANCE REQUIREMENTS

The following are the set of security assurance requirements drawn from the CC Part 3 for the TOE's assurance claim of EAL 2 Augmented. Table 5.4 summarizes the TOE Assurance classes, components, and component descriptions.

Table 5.4 TOE Assurance Components

Class	Component	Component Description
ACM: Configuration Management	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.1	TOE CM coverage
ADO: Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing-sample
AVA: Vulnerability Assessment	AVA_MSU.1	Examination of Guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.4.1 Configuration Management (ACM)

5.4.1.1 ACM_CAP.4 Generation support and acceptance procedures

Dependencies: ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.6C The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.

ACM_CAP.4.7C The CM system shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.8C The CM Plan shall describe how the CM system is used.

ACM_CAP.4.9C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.10C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.11C The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.12C The CM system shall support the generation of the TOE.

ACM_CAP.4.13C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.1.2 ACM_SCP.1 TOE CM coverage

Dependencies: ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.1.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements:

ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 Delivery and Operation (ADO)

5.4.2.1 ADO_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.3 Development (ADV)

5.4.3.1 ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.4.3.2 ADV_HLD.1 Descriptive high-level design

Dependencies: ADV_FSP.1 Informal functional specification

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.3.3 ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4 Guidance Documents (AGD)

5.4.4.1 AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe 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.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4.2 AGD_USR.1 User guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5 Life Cycle Support (ALC)

5.4.5.1 ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.4.5.2 ALC_FLR.3 Systematic flaw remediation

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.3.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation of evidence elements:

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE user's reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.3.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.3.9C The flaw remediation guidance shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

Evaluator action elements:

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5.3 ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.6 Tests (ATE)

5.4.6.1 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.1 Informal functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.6.2 ATE_FUN.1 Functional testing

Dependencies: No dependencies.

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.6.3 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.7 Vulnerability Assessment (AVA)

5.4.7.1 AVA_MSU.1 Examination of Guidance

Dependencies: ADO_IGS.1 Installation, generation, and start-up procedures

ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.4.7.2 AVA_SOF.1 Strength of TOE security Function evaluation

Dependencies: ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D The developer shall perform strength of TOE security function analysis for each mechanism identified in the ST as having strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.4.7.3 AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE SUMMARY SPECIFICATION

This section describes the security functions and assurance measures of the TOE that meet the TOE security requirements. The SOF-basic claim applies to the following security functions: F.IAUSER, F.IAGUI, F.IAREPORTCTR, F.IACMDCTR, and F.IADATABASE.

6.1 TOE SECURITY FUNCTIONS

The TOE Security Functions are listed and described in Table 6.1.

Table 6.1 TOE Security Functions

F.AUDIT	STAT Guardian VMS is responsible for generating audit records for security-related events. Security event records are stored in two locations: the STAT Guardian VMS database and the Windows Event Log. The STAT Guardian VMS database is configured to log all successful and unsuccessful database login attempts to the MSDE database log. Remaining security event records generated by STAT Guardian VMS are stored in the Windows Event Log. The IT Environment is responsible for providing the means of reviewing these event records. When configured in accordance with the *STAT Guardian VMS Installation and Security Guide*, the IT Environment protects these event logs from unauthorized modification or deletion. A complete list of audited events is contained in *Table 5-2. TOE Auditable Events*
F.ROLE	The TOE maintains the following list of user groups or roles: Scan Users, Advanced Scan Users, Remediate Users, Advanced Remediate Users, Reports Users, Manager Users, and Administrator Users. Users may belong to one or more user groups. Each user group defines a set of privileges, or functions, members of that group are allowed to perform on the TOE. The TOE also ensures that a user's access to user and TSF data is restricted by his/her group privileges.
F.MANAGEROLES	The TOE provides management functions that allow members of the Guardian Administrator Users group to manage STAT Guardian users and user groups. Member of the Guardian Administrator Users group may create, modify, delete users and assign them to groups. STAT Guardian Administrators may also create new and modify existing user groups.
F.DISPSCANDATA	The TOE has the capability to display vulnerability data collected from remote network targets via the STAT Guardian VMS GUI. Vulnerability data may include: scan jobs, vulnerabilities, ports, users, shares, and services. A user's access to vulnerability data is limited by his/her group privileges.

F.DISPREMDATA	The TOE has the capability to display remediation data collected from a remote PatchLink Server via the STAT Guardian VMS GUI. Remediation data may include: agents, agent vulnerabilities, agent status, agent groups, and scheduled remediation. A user's access to remediation data is limited by his/her group privileges.
F.DISPREPORTS	The TOE provides functions to generate and display reports on vulnerability and remediation data via the STAT Guardian VMS GUI. A user's ability to generate and view reports is limited by his/her group privileges.
F.IAUSER	The TOE identifies and authenticates STAT Guardian users before allowing access to TOE functions and data. When users authenticate to the GUI or Database, they must present authorized user credentials. These credentials are then checked against a list of authorized users maintained in the STAT Guardian VMS database. All logon attempts are logged in by the STAT Guardian VMS database.
F. IAGUI	The TOE mutually identifies and authenticates the GUI to the Engine (Scanner or Report Center) and the Engine to the GUI to prevent spoofing or man-in-the-middle style attacks. Prior to sending user credentials to the engine, the GUI displays the SHA-1 thumbprint of the engine's self-signed certificate to the user. It is the user's responsibility to verify the SHA-1 thumbprint in order to verify the identity of the engine. The GUI then transmits the user's credentials to the engine. The engine verifies the user credentials against a list of authorized users in the database before allowing any action on the part of the user. The data transmitted between TOE components is protected via HTTPS.
F.IAREPORTCTR	The TOE provides the capability to aggregate vulnerability and remediation data using the STAT Report Center. When a Scanner Engine or Report Center Engine transmits data to a remote Report Center engine, the transmitting engine identifies and authenticates the receiving engine before it transmits sensitive data. To use this feature, the user is required to provide the SHA-1 signature of the receiving Report Center engine. The transmitting engine will verify this signature prior to transmitting user data to the Report Center Engine. The data transmitted between TOE components is protected via HTTPS.

F.IACMDCTR	The TOE allows STAT Report Centers configured with STAT Command Center to perform distributed scanning. In order to spawn a Scanning job on a remote Scanner, the Report Center must mutually identify and authenticate to that remote scanner. First, the Report Center engine must verify the SHA-1 thumbprint of the remote Scanner prior to transmitting data. Once the identity of the remote Scanner is confirmed, the Command Center transmits the job request and user credentials to the remote Scanner. The Scanner engine will then verify that the provided credentials correspond to a properly privileged Scanner account prior to executing the received job. The data transmitted between TOE components is protected via HTTPS.
F.IADATABASE	The Scanner and Report Center engines store and retrieve TOE and user data to/from the STAT Guardian VMS database. All database transactions use authenticated ODBC, either with the SQL credentials of the logged-in user or with the windows credentials of the engine service. In the evaluated configuration, this connection is secured via shared memory because the TOE components are co-located on the same machine.
F.IMPVULNUPDATE	Periodically new software/firmware vulnerabilities are released and the TOE vulnerability configuration must be updated. The TOE supports the automatic download of new vulnerability updates directly from the Harris Corporate website. Vulnerability Updates are downloaded over mutually authenticated HTTPS. The HTTPS protocol ensures that the website's Verisign signed certificate is verified before transmitting the user's credentials and license key to the web server.
F.IMPSCANDATA	Although the TOE supports a variety of scanning techniques: authenticated scanning, null session scanning, and port scanning, the TOE only assures the results of authenticated scanning. Authenticated scanning requires the STAT Scanner has authenticated the user to the target machine before collecting vulnerability information.
F.IMPREMDATA	The STAT Scanner engine with STAT Patch and Remediation imports remediation data on agents, agent groups, and agent vulnerabilities from the remote PatchLink Server. The connection between the STAT Scanner engine and the remote PatchLink Server database is via ODBC. In the evaluated configuration, the ODBC connection is implicitly authenticated with the Engine service's local Administrator credentials.
F.EXPREMDATA	The STAT Guardian VMS GUI also supports agent-based scanning and remediation in conjunction with PatchLink Update Server. The STAT Scanner engine with STAT Patch and Remediation supports functions to organize agents into agent groups, perform agent based scanning, and remediate targets. In order to support these functions, the Scanner engine must export data to the remote PatchLink Server database. In the evaluated configuration, the ODBC connection is implicitly authenticated with the Engine service's local Administrator credentials.

6.2 TOE ASSURANCE MEASURES

The TOE assurance measures are described in Table 6.2.

Table 6.2 TOE Assurance Measures

M.ID	A TOE CM reference database is maintained at the central development location. The TOE CM reference database incorporates a version identifier displayable to the user. Each development version reference and its corresponding documentation are tagged with a unique version label within the CM system.

M.CMSYST	CM documentation includes a configuration list describing all components, connections, interfaces, and required settings of the TOE. CM documentation is direct evidence that all of the configuration items are effectively maintained under a CM system and effectively describes the configuration identification plan. The CM system is designed with systemic measures permitting only authorized changes to existing configuration items. The CM acceptance plan describes the in-place process to accept modified or newly created configuration items as part of the TOE configuration. All modification to configuration items are assigned a new, unique identifier within the CM
M.AUTHCON	All instances of the TOE are labeled with unique standardized reference version numbers to ensure that users of the TOE are aware of which instance of the TOE they are using. All possible changes to composition of the TOE, whether or not they result in actual changes subject to evaluation requirements for the TOE are identified with unique reference version numbers. No unauthorized modifications can be made to the TOE under the CM system. Developer CM documentation, including configuration list and CM plan is available to the evaluator.
M.AUTHPRES	Documentation for all instances of the TOE labeled with unique standardized reference version numbers to ensure that users of the TOE are aware of which instance of the TOE they are using are available for evaluation. The CM method ensures all possible changes to composition of the TOE, whether or not they result in actual changes subject to evaluation requirements for the TOE are identified with unique reference version numbers are documented according to the CM Plan. No unauthorized modifications are made to the TOE under the CM system without descriptions and addition to the CM database. Developer CM documentation, including configuration list and CM plan is available to the evaluator.
M.GETTOE	The developer uses a process ensuring the customer receives only an unmodified and complete TOE. This process is documented and controlled with unique identification of all configuration items. All newly created item or modification to an existing item is fully traceable in the CM system.
M.SETUP	The developer provides documentation for procedures used for secure delivery, installation, generation and start-up of the TOE.
M.CMSPEC	An internally consistent high-level design, functional specification and product description are provided. The high-level design documentation identifies the underlying hardware, firmware and software required by the TSF. The high-level design also identifies all interfaces to the subsystems of the TSF that are externally visible to TCP/IP communication originating outside the TOE. The functional specification describes the purpose and use of all external TSF interfaces with effects, exceptions and error message details. The product description defines the TSF to a level of detail such that a TSF can be generated without requiring further design decisions.
M.TRACE	The developer provides correspondence mapping such that the security functionality detailed in the TOE functional specification is upwards traceable to the ST and downwards traceable to the TOE high-level design.

M.DOCS	Administrators are provided documentation describing administrative and security functions, warnings and error messages, and TSF privilege configurations. This documentation also describes assumptions regarding user behavior relevant to the secure operation of the TOE and all security parameters under the control of the administrator. Each type of security relevant event relative to the administrative functions performed is provided as well as a description of all relevant security requirements. This guidance document lists all implementation and security assumptions for the intended environment and identifies all TOE modes of operation.
M.DEVSEC	Development security documentation describes the physical, procedural and personnel security measures necessary to protect confidentiality and integrity of the TOE design and its implementation in a development environment.
M.FLAW	Procedures are documented for accepting and acting upon user reports of security flaws and requests for correction of flaws.
M.LIFE	A life-cycle model is used to develop and maintain the TOE. Documentation is provided that describes this model.
M.TEST	A correctly configured TOE is tested to confirm the TOE operates as specified. Documentation is provided corresponding to each test identified in the test documentation to the TSF as described in the functional specification. Test documentation including test plans, test procedure descriptions, expected results, and results from testing is provided.
M.VULN	Documentation is provided showing the strength of TOE security function analysis performed on specific mechanisms in the TOE. This also shows methods that a user could use to violate the TSP, and that analyzed vulnerabilities cannot be exploited in the intended environment.

7 PP CLAIMS

The TOE does not claim conformance with any Protection Profile (PP).

8 RATIONALE

This section provides the rationale for the satisfaction of all security requirements and security objectives claimed in this Security Target.

8.1 SECURITY OBJECTIVES RATIONALE

This section demonstrates how TOE and IT Environment Security Objectives address each assumption, threat and policy described in the TOE Security Environment in Section 3. Table 8.1.1 maps previously stated assumptions, threats and policies to TOE and environmental security objectives. Table 8.1.2 Security Objective Rationale further explains coverage for each assumption, threat and policy.

Table 8.1.1 Security Environment vs. Objectives

	O.ADMIN	O.AUDITS	O.AUTHCOMP	O.AUTHUSER	O.EXPORT	O.IMPORT	O.ROLES	OE.BACKUP	OE.DOMAIN	OE.EVTLOG	OE.GOODUSER	OE.NETWORK	OE.OSAUTH	OE.OSCONFIG	OE.PHYSICAL	OE.TOECONFIG
A.BACKUP								X								
A.NETWORK												X				
A.NOEVIL											X			X		X
A.OSCONFIG									X	X	X			X		
A. PHYSICAL															X	
A.TOECONFIG	X							X			X					X
A.TRAIN											X					
T.DATABASE		X	X	X			X	X		X		X	X	X	X	X
T.ELEVATE		X		X			X			X						
T.OS		X							X	X		X	X	X	X	
T.SNIFF			X	X	X	X						X	X			
T.SPOOF			X	X	X	X						X	X			
P.PASSWORD	X													X		X
P.ROLES	X						X									

Table 8.1.2 Security Objectives Rationale

A.BACKUP	**The organization operating the TOE has good backup and recovery procedures allowing the TOE to be recovered to a secure configuration after a hardware failure.** The OE.BACKUP objective ensures that appropriate backup and recovery procedures exist.

A.NETWORK	**TOE assets reside in a secure networked environment.** The OE.NETWORK objective ensures that the network on which the TOE resides is appropriately configured and secure.
A.NOEVIL	**TOE users are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by TOE documentation.** The OE.GOODUSER objective ensures that only authorized, trained, and security-screened individuals are granted access to the TOE. The OE.OSCONFIG objective ensures that the operating system on which the TOE is installed has been properly installed configured and security hardened. The OE.TOECONFIG objective ensures that the TOE is properly installed and configured in accordance with guidance documentation.
A.OSCONFIG	**The host operating system has been securely installed and configured in accordance with guidance documentation.** The OE.DOMAIN objective ensures that the operating system is protected from unauthorized tampering. The OE.EVTLOG ensures that the operating system provides a secure repository for storing security related events. The Windows Event Log will be protected from unauthorized tampering. The OE.GOODUSER objective ensures that only authorized, trained, and security-screened individuals are granted access to the operating system. The OE.OSCONFIG objective ensures that the operating system including operating system components used by the TOE (Windows Event Log, System Time, and Registry) has been securely installed and configured with the appropriate privileges. Windows user credentials conform to local and domain password restrictions as well as organizational password security policies.
A.PHYSICAL	**TOE assets, hardware and software, are physically secure and only authorized personnel have physical access to these resources.** The OE.PHYSICAL objective ensures that only authorized personnel have physical access to the TOE.

A.TOECONFIG	**The TOE has been securely installed and configured in accordance with guidance documentation.** The O.ADMIN objective ensures that TOE contains a set of administrative functions that allow effective management of operational and security objectives. The OE.BACKUP objective ensures that a proper backup and recovery procedure exist for the TOE and its data. The OE.GOODUSER objective ensures that only authorized, trained, and security-screened individuals are granted access to the TOE. The OE.TOECONFIG objective ensures that the TOE is properly installed and configured in accordance with guidance documentation. TOE user credentials conform to SQL Server database password restrictions as well as organizational password security policies.
A.TRAIN	**Assigned personnel will possess experience and/or appropriate training in supporting and maintaining all aspects of the TOE and the encompassing IT security environment.** The OE.GOODUSER objective ensures that only authorized, trained, and security-screened individuals are granted access to the TOE.

T.DATABASE	**An unauthorized user may gain access over the STAT Guardian database by bypassing a database security mechanism and use this access to elevate his/her privileges over STAT Guardian VMS functions and/or data.** The O.AUDITS objective ensures that all successful and unsuccessful database login attempts are logged to the STAT Guardian VMS Database. The O.AUTHCOMP objective ensures that TOE components must be properly identified and authenticated to the database before allowing execution of any other TOE functions. The O.AUTHUSER objective ensures that users must be properly identified and authenticated to the database before allowing execution of any other TOE functions. The O.ROLES objective ensures that TOE users only access stored procedures and data as specifically granted by their user group. The OE.BACKUP objective ensures that a proper backup and recovery procedure exist for the TOE and its data should a breach occur. The OE.EVTLOG ensures that only TOE Administrators or database administrators have the privilege to delete audit data. The OE.NETWORK objective ensures that the network on which the TOE resides is reasonably secure. The OE.PHYSICAL objective ensures that only authorized personnel have physical access to the TOE. The OE.OSAUTH objective ensures that users must be properly identified and authenticated to the operating system before allowing access to TOE. The OE.OSCONFIG objective ensures that the operating system on which the TOE is installed is appropriately security hardened to prevent unauthorized access. The OE.TOECONFIG objective ensures that the TOE is properly installed and configured in accordance with guidance documentation.
T.ELEVATE	**An authorized TOE user may attempt to execute functions and/or view data for which he/she has no authorized privileges.** The O.AUDITS objective ensures that security related events are logged to the STAT Guardian VMS Database. The O.AUTHUSER objective ensures that users must be properly identified and authenticated to the database before allowing execution of any other TOE functions. The O.ROLES objective ensures that TOE users only access stored procedures and data as specifically granted by their user group. The OE.EVTLOG ensures that only TOE Administrators or database administrators have the privilege to delete audit data.

T.OS	**An unauthorized user may attempt to gain access over the operating system by bypassing a security mechanism and use this access to elevate his/her privileges over STAT Guardian VMS functions and/or data.** The O.AUDITS objective ensures that all security related events are logged to the STAT Guardian VMS Database. The OE.DOMAIN ensures that the host operating system on which the TOE resides provides domain separation. The OE.EVTLOG ensures that only TOE Administrators or database administrators have the privilege to delete audit data. The OE.NETWORK objective ensures that the network on which the TOE resides is reasonably secure. The OE.OSAUTH objective ensures that users must be properly identified and authenticated to the operating system before allowing access to TOE. The OE.OSCONFIG objective ensures that the operating system on which the TOE is installed is appropriately security hardened to prevent unauthorized access. The OE.PHYSICAL objective ensures that only authorized personnel have physical access to the TOE.
T.SNIFF	**A networked attacker may attempt to gain unauthorized access to STAT Guardian VMS data by interrupting or monitoring communications between TOE components and between TOE components and networked targets.** The O.AUTHCOMP objective ensures the confidentiality and integrity of all user data transferred between TOE components. The O.AUTHUSER objective ensures that users must be properly identified and authenticated before allowing access to TOE. The O.EXPORT objective ensures the confidentiality of all user data exported to external IT products. The O.IMPORT objective ensures the confidentiality of all user data imported from external IT products. The OE.NETWORK objective ensures that the network on which the TOE resides is reasonably secure. The OE.OSAUTH objective ensures that users must be properly identified and authenticated to the operating system before allowing access to TOE.

T.SPOOF	**A networked attacker may attempt to view, modify or delete STAT Guardian VMS data by impersonating a TOE component or external IT product.** The O.AUTHUSER objective ensures that users must be properly identified and authenticated before allowing access to TOE. The O.AUTHCOMP objective ensures the confidentiality and integrity of all user data transferred between TOE components. The O.EXPORT objective ensures the confidentiality of all user data exported to external IT products. The O.IMPORT objective ensures the confidentiality of all user data imported from external IT products. The OE.NETWORK objective ensures that the network on which the TOE resides is reasonably secure. The OE.OSAUTH objective ensures that users must be properly identified and authenticated to the operating system before allowing access to TOE.
P.PASSWORD	**The TOE Administrator shall enforce all Organizational password security policies when assigning user credentials to TOE users.** The O.ADMIN objective ensures that TOE contains a set of administrative functions that allow effective management of operational and security objectives. The OE.OSCONFIG objective ensures that the operating system including operating system components used by the TOE (Windows Event Log, System Time, and Registry) has been securely installed and configured with the appropriate privileges. Windows user credentials conform to local and domain password restrictions as well as organizational password security policies. The OE.TOECONFIG objective ensures that the TOE is properly installed and configured in accordance with guidance documentation. TOE user credentials conform to SQL Server database password restrictions as well as organizational password security policies.
P.ROLES	**Organizational role-based access control policies shall determine which individuals are authorized as TOE users and a list of privileges that user shall be permitted.** The O.ADMIN objective ensures that TOE contains a set of administrative functions that allow effective management of operational and security objectives. The O.ROLES objective ensures that users may only access those STAT Guardian VMS functions that they are explicitly granted by an administrator

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 TOE Security Functional Requirements Rationale

Table 8.2.1.1 provides a mapping from TOE Security Functional Requirements to TOE Security Objectives. Table 8.2.1.2 contains a discussion of how each TOE Security Objective is addressed by the corresponding Security Functional Requirements.

Table 8.2.1.1 TOE SFRs vs. Security Objectives Mapping

	O.ADMIN	O.AUDITS	O.AUTHCOMP	O.AUTHUSER	O.EXPORT	O.IMPORT	O.ROLES
FAU_GEN.1		X					
FAU_GEN.2		X					
FDP_ACC.1	X						X
FDP_ACC.2	X						X
FDP_ACF.1	X						X
FDP_ETC.1					X		
FDP_IFC.1 (1)			X				
FDP_IFC.1 (2)			X				
FDP_IFC.1 (3)			X				
FDP_IFC.1 (4)			X				
FDP_IFC.1 (5)						X	
FDP_IFC.1 (6)						X	
FDP_IFC.1 (7)					X	X	
FDP_IFF.1 (1)			X				
FDP_IFF.1 (2)			X				
FDP_IFF.1 (3)			X				
FDP_IFF.1 (4)			X				
FDP_IFF.1 (5)						X	
FDP_IFF.1 (6)						X	
FDP_IFF.1 (7)					X	X	
FDP_ITC.1						X	
FDP_ITT.1			X				
FIA_AFL.1		X					
FIA_ATD.1	X						
FIA_UAU.2				X			
FIA_UID.2				X			

	O.ADMIN	O.AUDITS	O.AUTHCOMP	O.AUTHUSER	O.EXPORT	O.IMPORT	O.ROLES
FMT_MOF.1	X						
FMT_MSA.1 (1)	X						X
FMT_MSA.1 (2)	X						X
FMT_MSA.1 (3)	X						X
FMT_MSA.1 (4)	X						X
FMT_MSA.1 (5)	X						X
FMT_MSA.1 (6)	X						X
FMT_MSA.1 (7)	X						X
FMT_MSA.2	X						X
FMT_MSA.3	X						X
FMT_MTD.1 (1)	X						X
FMT_MTD.1 (2)	X						X
FMT_MTD.1 (3)	X						X
FMT_MTD.1 (4)	X						X
FMT_MTD.1 (5)	X						X
FMT_MTD.1 (6)	X						X
FMT_MTD.1 (7)	X						X
FMT_REV.1	X						
FMT_SMF.1	X						
FMT_SMR.1	X						X
FPT_ITT.1			X				
FPT_RVM.1			X	X	X	X	

Table 8.2.1.2 Evidence of Coverage for TOE Security Objectives

O.ADMIN	**The TOE must include a set of administrative functions that allow effective management of TOE operational and security functions.** The TOE GUARDIAN_RBAC_SFP ensures that access STAT Guardian VMS functions is restricted to authorized TOE users in accordance with assigned privileges based on user group. [FDP_ACC.1, FDP_ACC.2, FDP_ACF.1, FMT_SMR.1] The TOE allows members of the Administrator users group to create users and user groups, assign users to user groups, modify user group privileges, and delete users and user groups using the STAT Guardian VMS GUI. [FDP_ACF.1, FIA_ATD.1, FMT_MOF.1, FMT_REV.1, FMT_SMF.1] The TOE allows authorized users to modify security attributes (user credentials, target credentials, web server credentials, etc.) using the STAT Guardian VMS GUI. [FMT_MSA.1 (1)-(7), FMT_MSA.2, FMT_MSA.3, FMT_MTD.1 (1)-(7)]
O.AUDITS	**The TOE must record security-related events to a secure location.** The TOE shall ensure that all security-related events are reported to a secure event log maintained by the IT Environment. [FAU_GEN.1, FAU_GEN.2] The TOE shall record both successful and unsuccessful login attempts to the STAT Guardian VMS Database. [FIA_AFL.1]
O.AUTHCOMP	**The TOE must identify and authenticate TOE components prior to allowing intra-TSF communications.** TOE Information Flow Control policies (GUI_SFP, REPORT_CENTER_SFP, COMMAND_CENTER_SFP, and VULNERABILITY_DATA_SFP) ensure that TOE Components are successfully identified and authenticated prior to allowing intra-TSF communications. [FDP_IFC.1 (1)-(4), FDP_IFF.1 (1)-(4), FDP_ITT.1, FPT_ITT.1, FPT_RVM.1]
O.AUTHUSER	**The TOE must identify and authenticate TOE users prior to allowing users to execute any functions upon the TOE.** Users shall be correctly identified and authenticated before performing any other functions on the TOE. [FIA_UAU.2, FIA_UID.2, FPT_RVM.1]
O.EXPORT	**The TOE must ensure confidentiality of user data exported to external IT components.** TOE Information Flow Control policies (REMEDIATION_DATA_SFP) ensure that TOE Components and external IT components are successfully identified and authenticated prior to allowing export of user data. [FDP_IFC.1(7), FDP_IFF.1(7), FDP_ETC.1, FPT_RVM.1]

O.IMPORT	**The TOE must ensure confidentiality of user data imported from external IT components.** TOE Information Flow Control policies (SCAN_SFP, VULNERABILITY_UPDATE_SFP, and REMEDIATION_DATA_SFP) ensure that TOE Components and external IT components are successfully identified and authenticated prior to allowing import of user data. [FDP_IFC.1(5)–(7), FDP_IFF.1 (5)-(7), FDP_ITC.1, FPT_RVM.1]
O.ROLES	**The TOE must enforce Role-based access control on STAT Guardian VMS functions.** The TOE GUARDIAN_RBAC_SFP ensures that access STAT Guardian VMS functions is restricted to authorized TOE users in accordance with assigned privileges based on user group. [FDP_ACC.1, FDP_ACC.2, FDP_ACF.1, FMT_SMR.1] The TOE ensures that only secure security attribute values are accepted as authentication data and that those security attributes may be modified by authorized users [FMT_MSA.1(1)-(7), FMT_MSA.2, FMT_MSA.3, FMT_MTD.1 (1)-(7)] TOE shall restrict the ability to modify TSF data to authorized users only. [FMT_MSA.1 (1)-(7), FMT_MTD.1 (1)-(7)]

8.2.2 IT Environment Security Functional Requirements Rationale

Table 8.2.2.1 provides a mapping from Security Functional Requirements satisfied by the IT Environment to IT Environment Security Objectives. Table 8.2.2.2 contains a discussion of how each IT Environment Security Objectives are addressed by IT Environment Security Functional Requirements, configuration step or organizational security policy.

Table 8.2.2.1 IT Environment SFRs vs. Security Objectives Mapping

	OE.BACKUP	OE.DOMAIN	OE.EVTLOG	OE.GOODUSER	OE.NETWORK	OE.OSAUTH	OE.OSCONFIG	OE.PHYSICAL	OE.TOECONFIG
FAU_GEN.1E			X						
FAU_GEN.2E			X						
FAU_SAR.1E			X						
FAU_SAR.2E			X						
FAU_SAR.3E			X						
FDP_ACC.1E							X		
FDP_ACF.1E							X		
FIA_UAU.2E						X			
FIA_UID.2E						X			
FMT_MSA.1 (1)E							X		
FMT_MSA.1 (2)E									X
FMT_MSA.2E							X		X
FMT_MSA.3E							X		X
FMT_MTD.1 (1)E							X		
FMT_MTD.1 (2)E							X		
FMT_MTD.1 (3)E							X		
FMT_MTD.1 (4)E									X
FMT_SMF.1E							X		
FMT_SMR.1E							X		
FPT_SEP.1E		X							
FPT_STM.1E							X		

Table 8.2.2.2 Evidence of Coverage for IT Environment Security Objectives

OE.BACKUP	**Good backup and recovery procedures exist for the TOE and its data.** This environment security objective is trivially satisfied by stated assumptions about the IT environment in the *STAT Guardian VMS Installation and Security Guide*.
OE.DOMAIN	**The host operating system will provide domain separation and ensure that the TOE cannot be tampered with.** The host operating system provides domain separation. [FPT_SEP.1E]
OE.EVTLOG	**The host operating system on which the TOE is installed must provide a secure repository for security-related events.** The operating system is responsible for generating audit events in the case of startup or shutdown of audit functions. [FAU_GEN.1E] All generated events shall contain data and time of the event, type of event, subject identity, and success or failure of the event. [FAU_GEN.2E] The IT Environment provides two tools for viewing and/or managing security-related events generated by the TOE: SQL Server Enterprise Manager and the Windows Event Log. [FAU_SAR.1E] Both tools restrict unauthorized user access to event logs. [FAU_SAR.2E] Both tools allow authorized users to sort event records by date and event source. [FAU_SAR.3E]
OE.GOODUSER	**Personnel authorized to install, configure, administer, operate and/or maintain the TOE are non-malicious and have been trained in the use of the TOE.** This environment security objective is trivially satisfied by stated assumptions about the IT environment in the *STAT Guardian VMS Installation and Security Guide*.
OE.NETWORK	**The network on which the TOE components reside must be appropriately configured and secured to avoid disclosure of sensitive data.** This environment security objective is trivially satisfied by stated assumptions about the IT environment in the *STAT Guardian VMS Installation and Security Guide*.
OE.OSAUTH	**The user must be successfully authenticated to the host operating system before allowing any access to the TOE.** Operating system users must be successfully identified and authenticated before any other action on behalf of that user may occur. [FIA_UAU.2E, FIA_UID.2E]

OE.OSCONFIG	**The administrative user responsible for installation of the TOE must ensure that hosts on which TOE components will be installed have been properly configured and security hardened. Operating System components used by the TOE (Windows Event Log, System Time, Registry) are secured from unauthorized use and/or modification. OS user credentials must comply with organizational password security policies.** If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide*, the SQL Server audit logs and Windows Event Log are protected from unauthorized tampering. [FMT_MTD.1(2)E, FMT_MTD.1(3)E] If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide*, TOE files, directories and registry keys are protected from unauthorized tampering with Windows ACLs. [FMT_MSA.1(1)E, FMT_MSA.2E, FMT_MSA.3E, FMT_MTD.1(1)E] The Windows operating system provides the Windows Administrators user group. If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide*, members of this group have Full Control permissions to all TOE files, directories, and registry keys. [FDP_ACC.1E, FDP_ACF.1E, FMT_SMR.1E] The Windows operating system provides the Windows Users user group. If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide*, members of this group have no permissions to TOE files, directories, and registry keys. [FDP_ACC.1E, FDP_ACF.1E, FMT_SMR.1E] *STAT Guardian VMS Installation and Security Guide* contains detailed instructions for creating a Windows Guardian Users user group. If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide*, members of this group have Full Control permissions to all TOE files, directories, and registry keys. [FDP_ACC.1E, FDP_ACF.1E, FMT_SMR.1E] If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide,* Windows operating system ensures that only members of the Windows Administrators group or Windows Guardian Users Group may modify ACLs on TOE files, directories and registry keys [FMT_SMF.1E] If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide*, the Windows operating system prevents non-administrators from tampering with the System Clock. [FPT_STM.1E]

OE.PHYSICAL	**The physical environment in which the TOE resides must be secured from unauthorized access.** This environment security objective is trivially satisfied by stated assumptions about the IT environment in the *STAT Guardian VMS Installation and Security Guide*.
OE.TOECONFIG	**The administrative user responsible for the TOE must ensure that the TOE is installed and configured in accordance with guidance documentation. TOE user credentials must comply with organizational password security policies.** The SHA-1 of the engine's self-signed certificate is stored in the Windows registry. If configured in accordance with guidance in the *STAT Guardian VMS Installation and Security Guide* this registry key is secured via ACLs and audit policy settings. [FMT_MSA.1(2)E, FMT_MSA.2E, FMT_MSA.3E, FMT_MTD.1(4)E]

8.2.3 Rationale for Satisfying TOE Functional Requirement Dependencies

Table 8.2.3 identifies the TOE SFRs and their immediate dependencies, and also indicates whether the ST explicitly addresses each dependency.

Table 8.2.3 TOE Security Functional Requirement Dependencies

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	YES
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACC.2	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	YES
FDP_IFC.1	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	YES
FDP_ITC.1	FDP_IFC.1, FMT_MSA.3	YES
FDP_ITT.1	FDP_IFC.1	YES
FIA_AFL.1	FIA_UAU.1	YES
FIA_ATD.1	-	YES
FIA_UAU.1*		YES
FIA_UAU.2	FIA_UID.1	YES
FIA_UID.1**	-	YES
FIA_UID.2	FIA_UID.1	YES
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	YES
FMT_MSA.1	FDP_ACC.1, FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	YES
FMT_MSA.2***	FDP_ACC.1 FDP_IFC.1, FMT_MSA.1, FMT_SMR.1, ADV_SPM.1	YES
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	YES
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	YES
FMT_REV.1	FMT_SMR.1	YES
FMT_SMF.1	-	YES
FMT_SMR.1	FIA_UID.1	YES
FPT_ITT.1	-	YES
FPT_RVM.1	-	YES

* Derived from FIA_AFL.1. Although not included in this ST, FIA_UAU.1 is implicitly included because it is hierarchal to FIA_UAU.2.

** Derived from FAU_GEN.1, and FIA_UAU.1 through FIA_AFL.1. Although not included in this ST, FIA_UID.1 is implicitly included because it is hierarchal to FIA_UID.2.

*** The FMT_MSA.2 security functional requirement is dependent on ADV_SPM.1 Informal TOE security policy model. This requirement is trivially satisfied by the security policy descriptions provided in Section 5.3.2. It should therefore not be necessary to provide a separate document for the TOE security policy model.

8.2.4 Rationale for Satisfying IT Environment Functional Requirement Dependencies

Table 8.2.4 identifies the IT Environment SFRs and their immediate dependencies, and also indicates whether the ST explicitly addresses each dependency.

Table 8.2.4 IT Environment Security Functional Requirement Dependencies

Functional Component	Dependency	Included
FAU_GEN.1E	FPT_STM.1E	YES
FAU_GEN.2E	FAU_GEN.1E, FIA_UID.1E	YES
FAU_SAR.1E	FAU_GEN.1E	YES
FAU_SAR.2E	FAU_SAR.1E	YES
FAU_SAR.3E	FAU_SAR.1E	YES
FDP_ACC.1E	FDP_ACF.1E	YES
FDP_ACF.1E	FDP_ACC.1E, FMT_MSA.3E	YES
FIA_UAU.1E*	-	YES
FIA_UAU.2E	FIA_UID.1E	YES
FIA_UID.1E**	-	YES
FIA_UID.2E	FIA_UID.1E	YES
FMT_MSA.1E	FDP_ACC.1E, FMT_SMR.1E, FMT_SMF.1E	YES
FMT_MSA.2E***	FDP_ACC.1E, FMT_MSA.1E, FMT_SMR.1E, ADV_SPM.1	YES
FMT_MSA.3E	FMT_MSA.1E, FMT_SMR.1E	YES
FMT_MTD.1E	FMT_SMF.1E, FMT_SMR.1E	YES
FMT_SMF.1E	-	YES
FMT_SMR.1E	FIA_UID.1E	YES
FPT_SEP.1E	-	YES
FPT_STM.1E	-	YES

* Derived from FIA_AFL.1E. Although not included in this ST, FIA_UAU.1E is implicitly included because it is hierarchal to FIA_UAU.2E.

** Derived from FAU_GEN.1E, and FIA_UAU.1E through FIA_AFL.1E. Although not included in this ST, FIA_UID.1E is implicitly included because it is hierarchal to FIA_UID.2E.

*** The FMT_MSA.2E security functional requirement is dependent on ADV_SPM.1 Informal TOE security policy model. This requirement is trivially satisfied by the security policy descriptions provided in Section 5.3.2. It should therefore not be necessary to provide a separate document for the TOE security policy model.

8.2.5 Rationale for Satisfying Assurance Requirement Dependencies

Table 8.2.5 identifies the Security Assurance Requirements and their immediate dependencies, and also indicates whether the ST explicitly addresses each dependency.

Table 8.2.5 Security Assurance Requirement Dependencies

Functional Component	**Dependency**	**Included**
ACM_CAP.4	ALC_DVS.1	YES
ACM_SCP.1	ACM_CAP.3	YES
ADO_DEL.1	-	YES
ADO_IGS.1	AGD_ADM.1	YES
ADV_FSP.1	ADV_RCR.1	YES
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1	YES
ADV_RCR.1	-	YES
AGD_ADM.1	ADV_FSP.1	YES
AGD_USR.1	ADV_FSP.1	YES
ALC_DVS.1	-	YES
ALC_FLR.3	-	YES
ALC_LCD.1	-	YES
ATE_COV.1	ADV_FSP.1, ATE_FUN.1	YES
ATE_FUN.1	-	YES
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	YES
AVA_MSU.1	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1	YES
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	YES
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	YES

8.2.6 Strength of Function Rationale

A typical attacker in the intended environment for the TOE is assumed to have a low level of sophistication, but may have knowledge of vulnerabilities and access to attack methods that are in the public domain. The purpose of the attacks could be (1) to gain access to the host operating system resources, (2) to gain access to one or more of the TOE components or distributed external IT products with which the TOE communicates, (3) to monitor or disrupt communications between TOE components and/or external IT components. The attack potential, which is applicable for AVA_SOF.1 calculations, is LOW. Any residual vulnerability may only be exploited by an attacker of moderate or high attack potential. The strength of function claim is therefore SOF-BASIC.

A strength of function claim applies only to those security functions that utilize security attributes that may be exploited via probabilistic or permutational mechanisms (e.g. password or hash functions). STAT Guardian VMS uses two such security attributes: a Guardian user's username and password credentials and a Guardian engine's SHA-1 thumbprint. Thus, the SOF-basic claim applies to two categories of security functions: security functions that use the password security attribute (F.IAUSER, F.IAGUI, F.IACMDCTR, F.IADATABASE) and security functions that use an engine's SHA-1 thumbprint (F.IAGUI, F.IAREPORTCTR, F.IACMDCTR). This claim is discussed further in the *STAT Guardian VMS Strength of Function Analysis*.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

This section illustrates how TOE Security Functions and Assurance Measures satisfy all TOE Security Functional Requirements and Assurance Requirements claimed in the Security Target.

8.3.1 Security Function Rationale

Table 8.3.1.1 maps TOE Security Functional Requirements to TOE Security Functions. Table 8.3.1.2 contains a discussion of how Security Functional Requirement is addressed by TOE Security Functions.

Table 8.3.1.1 TOE SFRs vs. TOE Security Functions Mapping

	F.AUDIT	F.ROLE	F.MANAGEROLES	F.DISPSCANDATA	F.DISPREMDATA	F.DISPREPORTS	F.IAUSER	F.IAGUI	F.IAREPORTCTR	F.IACMDCTR	F.IADATABASE	F.IMPVULNUPDATE	F.IMPSCANDATA	F.IMPREMDATA	F.EXPREMDATA
FAU_GEN.1	X														
FAU_GEN.2	X														
FDP_ACC.1		X		X	X	X									
FDP_ACC.2		X		X	X	X									
FDP_ACF.1		X	X	X	X	X									
FDP_ETC.1															X
FDP_IFC.1 (1)								X							
FDP_IFC.1 (2)									X						
FDP_IFC.1 (3)										X					
FDP_IFC.1 (4)											X				
FDP_IFC.1 (5)												X			
FDP_IFC.1 (6)													X		
FDP_IFC.1 (7)														X	X
FDP_IFF.1 (1)								X							
FDP_IFF.1 (2)									X						
FDP_IFF.1 (3)										X					
FDP_IFF.1 (4)											X				
FDP_IFF.1 (5)												X			
FDP_IFF.1 (6)													X		
FDP_IFF.1 (7)														X	X
FDP_ITC.1												X	X	X	
FDP_ITT.1								X	X	X	X				
FIA_AFL.1	X														
FIA_ATD.1			X												
FIA_UAU.2							X								
FIA_UID.2							X								

	F.AUDIT	F.ROLE	F.MANAGEROLES	F.DISPSCANDATA	F.DISPREMDATA	F.DISPREPORTS	F.IAUSER	F.IAGUI	F.IAREPORTCTR	F.IACMDCTR	F.IADATABASE	F.IMPVULNUPDATE	F.IMPSCANDATA	F.IMPREMDATA	F.EXPREMDATA
FMT_MOF.1			X												
FMT_MSA.1 (1)			X					X							
FMT_MSA.1 (2)		X							X						
FMT_MSA.1 (3)		X								X					
FMT_MSA.1 (4)			X								X				
FMT_MSA.1 (5)		X										X			
FMT_MSA.1 (6)		X											X		
FMT_MSA.1 (7)		X											X		
FMT_MSA.2		X	X					X	X	X	X	X	X		
FMT_MSA.3		X	X					X	X	X	X	X	X		
FMT_MTD.1 (1)			X					X							
FMT_MTD.1 (2)		X							X						
FMT_MTD.1 (3)		X								X					
FMT_MTD.1 (4)			X								X				
FMT_MTD.1 (5)		X										X			
FMT_MTD.1 (6)		X											X		
FMT_MTD.1 (7)		X											X		
FMT_REV.1			X												
FMT_SMF.1			X												
FMT_SMR.1		X	X	X	X	X									
FPT_ITT.1								X	X	X	X				
FPT_RVM.1				X	X	X	X	X	X	X	X	X	X	X	X

Table 8.3.1.2 Evidence of Requirements vs. Security Function Mapping

FAU_GEN.1	**Audit data generation** The F.AUDIT function generates audit records for security events. Each audit record contains date and time of event, type of event, subject identity, and success/failure of the event. The IT environment ensures that startup and shutdown of audit functions is logged to the Windows event log.
FAU_GEN.2	**User identity association** The F.AUDIT function ensures that each audit record contains the identity of the user that caused the event.
FDP_ACC.1	**Subset Access Control** The F.ROLE function ensures that access to STAT Guardian VMS functions is restricted based on user role. The F.DISPSCANDATA, F.DISPREMDATA, and F.DISPREPORTS functions ensure that only users with authorized privileges may view STAT Guardian VMS data.
FDP_ACC.2	**Complete Access Control Enforcement of Subjects & Objects** The F.ROLE function ensures that access to STAT Guardian VMS functions is restricted based on user role. The F.DISPSCANDATA, F.DISPREMDATA, and F.DISPREPORTS functions ensure that only users with authorized privileges may view STAT Guardian VMS data.
FDP_ACF.1	**Security Attribute based access control** The F.ROLE function ensures that access to STAT Guardian VMS functions is restricted based on user role. The F.MANAGEROLES function ensures that only members of the Administrator Users group may assign a user to a role. A member of the Administrator Users group may assign roles to himself. The F.DISPSCANDATA, F.DISPREMDATA, and F.DISPREPORTS functions ensure that only users with authorized privileges may view STAT Guardian VMS data.
FDP_ETC.1	**Export of user data without security attributes** The F.EXPREMDATA allows authorized users to export user data from the Scanner engine to a remote PatchLink server.
FDP_IFC.1 (1)	**Information Flow Control** The F.IAGUI function enforces the GUI_SFP information flow control security functional policy.
FDP_IFC.1 (2)	**Information Flow Control** The F.IAREPORTCTR function enforces the REPORT_CENTER_SFP information flow control security functional policy.

FDP_IFC.1 (3)	**Information Flow Control** The F.IACMDCTR function enforces the COMMAND_CENTER_SFP information flow control security functional policy.
FDP_IFC.1 (4)	**Information Flow Control** The F.IADATABASE function enforces the VULNERABILITY_DATABASE_SFP information flow control security functional policy.
FDP_IFC.1 (5)	**Information Flow Control** The F.IMPVULNUPDATE function enforces the VULNERABILITY_UPDATE_SFP information flow control security functional policy.
FDP_IFC.1 (6)	**Information Flow Control** The F.IMPSCANDATA function enforces the SCAN_SFP information flow control security functional policy.
FDP_IFC.1 (7)	**Information Flow Control** The F.IMPREMDATA function enforces the REMEDIATION_DATABASE_SFP information flow control security functional policy. The F.EXPREMDATA function enforces the REMEDIATION_DATABASE_SFP information flow control security functional policy.
FDP_IFF.1 (1)	**Simple security attributes** The F.IAGUI enforces the GUI_SFP information flow control security functional policy.
FDP_IFF.1 (2)	**Simple security attributes** The F.IAREPORTCTR function enforces the REPORT_CENTER_SFP information flow control security functional policy.
FDP_IFF.1 (3)	**Simple security attributes** The F.IACMDCTR function enforces the COMMAND_CENTER_SFP information flow control security functional policy.
FDP_IFF.1 (4)	**Simple security attributes** The F.IADATABASE function enforces the VULNERABILITY_DATABASE_SFP information flow control security functional policy.
FDP_IFF.1 (5)	**Simple security attributes** The F.IMPVULNUPDATE function enforces the VULNERABILITY_UPDATE_SFP information flow control security functional policy.

FDP_IFF.1 (6)	**Simple security attributes** The F.IMPSCANDATA function enforces the SCAN_SFP information flow control security functional policy.
FDP_IFF.1 (7)	**Simple security attributes** The F.IMPREMDATA function enforces the REMEDIATION_DATABASE_SFP information flow control security functional policy. The F.EXPREMDATA function enforces the REMEDIATION_DATABASE_SFP information flow control security functional policy.
FDP_ITC.1	**Import of User Data without security attributes** The F.IMPVULNUPDATE function allows authorized users to download automatic vulnerability updates from the Harris Corporate Web Site. The F.IMPSCANDATA function allows authorized users to gather vulnerability data from remote targets. The F.IMPREMDATA function allows authorized users to import agent and remediation data from a remote PatchLink server.
FDP_ITT.1	**Basic internal transfer protection** The F.IAGUI enforces the GUI_SFP information flow control security functional policy. The F.IAREPORTCTR function enforces the REPORT_CENTER_SFP information flow control security functional policy. The F.IACMDCTR function enforces the COMMAND_CENTER_SFP information flow control security functional policy. The F.IADATABASE function enforces the VULNERABILITY_DATABASE_SFP information flow control security functional policy.
FIA_AFL.1	**Authentication failure handling** F.AUDIT ensures that every failed logon attempt is logged to the STAT Guardian VMS database.
FIA_ATD.1	**User attribute definition** F.MANAGEROLES ensures that the TOE maintains users, user credentials, and user groups.
FIA_UAU.2	**User authentication before any action** F.IAUSER ensures that each user is successfully authenticated to the GUI prior to allowing any actions on behalf of that user.
FIA_UID.2	**User identification before any action** F.IAUSER ensures that each user is successfully identified to the GUI prior to allowing any actions on behalf of that user.

FMT_MOF.1	**Management of security functions** F.MANAGEROLES ensures that only members of the Administrator User group may enable, disable, or modify the behavior of user and group management functions.
FMT_MSA.1 (1)	**Management of security attributes** The F.MANAGEROLES and F.IAGUI ensure that only an individual user or members of the Administrator User group may modify a user's password.
FMT_MSA.1 (2)	**Management of security attributes** The F. ROLES and F.IAREPORTCTR ensure that only members of the Advanced Scan Users, Adv Remediate Users, Manager Users, and Administrator User group may add, delete, or modify a remote Report Center's SHA-1 thumbprint.
FMT_MSA.1 (3)	**Management of security attributes** The F. ROLES and F.IACMDCTR ensure that only members of the Administrator User group may add, delete, or modify a remote Scanner's SHA-1 thumbprint.
FMT_MSA.1 (4)	**Management of security attributes** The F.MANAGEROLES and F.IADATABASE ensure that only members of the Administrator User group or STAT Guardian VMS Database administrators may add, delete, or modify STAT Guardian VMS Database credentials
FMT_MSA.1 (5)	**Management of security attributes** The F. ROLES and F.IMPVULNUPDATE ensure that only members of the Manager Users or Administrator User group may add, delete, or modify web server credentials.
FMT_MSA.1 (6)	**Management of security attributes** The F. ROLES and F.IMPSCANDATA ensure that only members of the Scan Users, Advanced Scan Users, Manager Users, and Administrator User groups may add target credential sets.
FMT_MSA.1 (7)	**Management of security attributes** The F. ROLES and F.IMPSCANDATA ensure that only members of the Advanced Scan Users, Manager Users, and Administrator User groups may modify or delete target credential sets.
FMT_MSA.2	**Secure Security Attributes** The F.MANAGEROLES, F.ROLE, F.IAGUI, F.IAREPORTCTR, F.IACMDCTR, F.IADATABASE, F.IMPVULNUPDATE, and F.IMPSCANDATA ensure that only secure values are accepted for security attributes.

FMT_MSA.3	**Static Attribute Initialization** The F.MANAGEROLES, F.ROLE, F.IAGUI, F.IAREPORTCTR, F.IACMDCTR, F.IADATABASE, F.IMPVULNUPDATE, and F.IMPSCANDATA ensure that a TOE user is explicitly prompted to enter a secure attribute value (described in FMT_MSA.1) prior to allowing any inbound or outbound communication.
FMT_MTD.1 (1)	**Management of TSF data** The F.MANAGEROLES and F.IAGUI ensure that only an individual user or members of the Administrator User group may modify a user's password.
FMT_MTD.1 (2)	**Management of TSF data** The F. ROLES and F.IAREPORTCTR ensure that only members of the Advanced Scan Users, Adv Remediate Users, Manager Users, and Administrator User group may add, delete, or modify a remote Report Center's SHA-1 thumbprint.
FMT_MTD.1 (3)	**Management of TSF data** The F. ROLES and F.IACMDCTR ensure that only members of the Administrator User group may add, delete, or modify a remote Scanner's SHA-1 thumbprint.
FMT_MTD.1 (4)	**Management of TSF data** The F.MANAGEROLES and F.IADATABASE ensure that only members of the Administrator User group or STAT Guardian VMS Database administrators may add, delete, or modify STAT Guardian VMS Database credentials.
FMT_MTD.1 (5)	**Management of TSF data** The F. ROLES and F.IMPVULNUPDATE ensure that only members of the Manager Users or Administrator User group may add, delete, or modify web server credentials.
FMT_MTD.1 (6)	**Management of TSF data** The F. ROLES and F.IMPSCANDATA ensure that only members of the Scan Users, Advanced Scan Users, Manager Users, and Administrator User groups may add target credential sets.
FMT_MTD.1 (7)	**Management of TSF data** The F. ROLES and F.IMPSCANDATA ensure that only members of the Advanced Scan Users, Manager Users, and Administrator User groups may modify or delete target credential sets.
FMT_REV.1	**Revocation of rules restrictions** F.MANAGEROLES ensures that only members of the Administrator User group have the ability to revoke a user's security attributes.

FMT_SMF.1	**Specification of management functions** F.MANAGEROLES ensures that the TOE allows members of Administrator User group to view, add, delete, and modify user group privileges that permit or deny information flows.
FMT_SMR.1	**Security roles** The F.ROLE and F.MANAGEROLES functions ensure that the TOE maintains the following user roles: Administrator User, Manager Users, Scan Users, Advanced Scan Users, Remediate Users, Advanced Remediate Users, and Reports Users. The F.DISPSCANDATA, F.DISPREMDATA, and F.DISPREPORTS functions ensure that only users with authorized privileges may view STAT Guardian VMS data.
FPT_ITT.1	**Basic internal TSF data transfer protection** The F.IAGUI, F.IAREPORTCTR, F.IACMDCTR, F.IADATABASE functions ensure that the TOE protects TSF data from unauthorized disclosure or modification.
FPT_RVM.1	**Non-bypassability of the TSP within the TOE** The F.IAUSER, F.IAGUI, F.IAREPORTCTR, F.IACMDCTR, F.IADATABASE, F.IMPVULNUPDATE, F.IMPSCANDATA, F.IMPREMDATA and F.EXPREMDATA functions ensure that TOE users, TOE components, and external IT components must be successfully identified and authenticated before TSC is allowed to proceed. The F.DISPSCANDATA, F.DISPREMDATA, and F.DISPREPORTS functions ensure that only users with authorized privileges may view STAT Guardian VMS data.

8.3.2 Assurance Measures Rationale

STAT Guardian VMS is designed to limit use of the TOE and its data to authorized users. Through the effective use of security policies and functions TOE protects its data from unauthorized disclosure and/or modification. STAT Guardian VMS is an effective and secure tool for vulnerability detection and remediation for most commercial and government environments.

An assurance level of EAL 2+, Structurally Tested, was selected as the threat to security is considered to be from unsophisticated network attackers. An evaluation at this level provides a moderate level of independently assured security via a thorough investigation of the TOE and its development.

Table 8.3.2.1 Assurance Measures vs. Assurance Functions Mapping maps the assurance measures to the assurance requirements. Table 8.3.2.2 Evidence of Assurance Measures vs. Assurance Functions Mapping discusses how each assurance requirement is addressed by the corresponding assurance measure.

Table 8.3.2.1 Assurance Measures vs. Assurance Functions Mapping

	M.ID	M.CMSYST	M.AUTHCON	M.AUTHPRES	M.GETTOE	M.SETUP	M.CMSPEC	M.TRACE	M.DOCS	M.DEVSEC	M.FLAW	M.LIFE	M.TEST	M.VULN
ACM_CAP.4	X	X	X	X										
ACM_SCP.1		X			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					
ALC_DVS.1										X				
ALC_FLR.3											X			
ALC_LCD.1												X		
ATE_COV.1													X	
ATE_FUN.1													X	
ATE_IND.2													X	
AVA_MSU.1														X
AVA_SOF.1														X
AVA_VLA.1														X

Table 8.3.2.2 Evidence of Assurance Measures vs. Assurance Functions Mapping

ACM_CAP.4	**Generation support and acceptance procedures** M.ID, M.CMSYST, M.AUTHCON and M.AUTHPRES satisfy the requirements for supporting the generation of unique TOE reference versions and providing change acceptance procedures.
ACM_SCP.1	**TOE CM coverage** M.GETTOE and M.CMSYST satisfy the requirement for providing a CM system with documentation.
ADO_DEL.1	**Delivery procedures** M.SETUP satisfies the requirements for documenting procedures for secure delivery of a configuration controlled TOE.
ADO_IGS.1	**Installation, generation, and start-up procedures** M.SETUP satisfies the requirements for documenting procedures for secure installation, generation, and start-up procedures for the TOE.
ADV_FSP.1	**Informal functional specification** M.CMSPEC satisfies the requirements for providing a functional specification.
ADV_HLD.1	**Descriptive high-level design** M.CMSPEC satisfies the requirements for providing the high-level design of the TSF.
ADV_RCR.1	**Informal correspondence demonstration** M.TRACE satisfies the requirements for providing an information correspondence demonstration.
AGD_ADM.1	**Administrator guidance** M.DOCS satisfies the requirements for providing administrator guidance.
AGD_USR.1	**User guidance** M.DOCS satisfies the requirements for providing user guidance.
ALC_DVS.1	**Identification of security measures** M.DEVSEC satisfies the requirements for producing development security documentation.
ALC_FLR.3	**Systematic flaw remediation** M.FLAW satisfies the requirements for documenting the procedures for flaw remediation.
ALC_LCD.1	**Developer defined life-cycle model** M.LIFE satisfies the requirements for documenting the established life-cycle model.

ATE_COV.1	**Evidence of coverage** M.TEST satisfies the requirements for providing evidence of test coverage.
ATE_FUN.1	**Functional testing** M.TEST satisfies the requirements for documenting the results of the functional testing.
ATE_IND.2	**Independent testing –sample** M.TEST satisfies the requirements for providing the TOE for testing.
AVA_MSU.1	**Examination of guidance** M.VULN satisfies the requirements for providing guidance documentation.
AVA_SOF.1	**Strength of TOE security function evaluation** M.VULN satisfies the requirements for providing strength of function claims for mechanisms.
AVA_VLA.1	**Developer vulnerability analysis** M.VULN satisfies the requirements for analyzing the TOE for vulnerabilities.