StillSecure VAM™ V5.5

Security Target V1.6

December 13, 2006

Developed by

CYGNACOM SOLUTIONS

Suite 5200 West♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: StillSecure VAM V5.5

ST Title: StillSecure VAM V5.5 Security Target

ST Version: Version 1.6

ST Authors: Debra Baker

ST Date: December 13, 2006

Assurance Level: EAL2

Strength of Function: SOF-basic

Registration: <To be filled in upon registration>

Keywords: Vulnerability Management and Remediation, Automated Patch Management, Access Control, Identification, Authentication, Security Target, Reports, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for StillSecure VAM V5.5. StillSecure VAM is a vulnerability management system that identifies, manages, and manages the remediation of network security vulnerabilities. StillSecure VAM manages the vulnerability remediation process from end-to-end, allowing an authorized administrator to quickly and systematically fix the vulnerabilities. Updated hourly with the most current vulnerability signatures, VAM scans for vulnerabilities using scheduled and on-demand scans. The vulnerabilities that are found during scans are managed by VAM's Vulnerability Repair Workflow. VAM tracks all scanning and remediation activities and delivers a range of reports for auditors, managers, and IT staff members.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Acronym definitions and references are provided in sections 9 and 10.

1.5 Acronyms

Table 1-1 Acronyms

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
FAU	Security Audit
FBI	Federal Bureau of Investigation
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	User Console
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IT	Information Technology
SANS	SysAdmin, Audit, Network, Security (Institute)
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol

1.6 References

Table 1-2 References

Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-002, Version 2.2, January 2004.
StillSecure VAM 5.5 Installation Guide (rev-a), June 23, 2006
StillSecure VAM 5.5 Users' Guide (rev-c), October 27, 2006

1.7 Terminology

Table 1-3 Customer Specific Terminology

Term	Definition
Audit data	Audit data is the data logged in the audit trail. Audit trails are logs maintained by StillSecure that track the vulnerabilities, work flow, actions taken of StillSecure users, and actions of the system itself.
Autodiscovery™	The process that detects and profiles devices on the targeted network. VAM runs Autodiscovery on a regular schedule to ensure all devices are accounted for and to alert you of any new devices that may require vulnerability scanning.
Custom scan policy	A user-defined scan policy, whereby the user manually selects the scan rules to apply to a device and sets the schedule of when the scan policy is run. For example, an authorized user might create a custom scan policy if there are a number of similar devices that are to be scanned in a specific way.
Device	A device is a host, router, switch, hub, or bridge which resides on a network. The device provides the TOE system data (traps and information) about the targeted network.
Device importance levels	A device is assigned one of three importance levels: high, medium, or low. Based on a device's importance level, VAM sets the repair schedule for vulnerabilities found on that device (i.e., high = short repair schedule; low = longer repair schedule). The VAM interface and reports display devices grouped and prioritized by device importance.
Distributed scanning	Enables VAM to scan remote networks and to scale to very large network environments. Distributed scanning is an integral part of Remote VAM and can be deployed within Sever VAM installations. There are two primary reasons to deploy distributed scanners: • Scaling-increase the number of scannable devices and the number of scans that can be performed • Scanning remote networks-scan portions of your network bounded by firewalls and access control lists Scan data generated by distributed scanners is securely sent to the central VAM repository, where it is consolidated and securely stored.
Groups	Allows an authorized administrator to organize the devices and the IT personnel responsible for their maintenance and management. Groups are optional. Targeted networks containing a modest number of devices may not need multiple groups; the single Default group automatically created during installation may be sufficient.

Term	Definition
Intelliscan™	An intelligent scan that automatically selects and applies the Scan rules appropriate for each device. Intelliscan eliminates the need for an authorized user to determine which scan rules to apply to each individual device.
Onboard Scanner	The onboard scanner is used to collect the System Data from the devices on the target network.
Port scans	VAM performs two types of port scans: TCP and UDP. TCP port scans generally run quickly when scanning a device. UDP port scans, on the other hand, can take a long time to complete because of how some devices respond when multiple UDP ports are scanned. To ensure efficient scanning, VAM provides three UDP port scans: (1) common UDP ports, (2) UDP ports 1-1000, and (3) UDP ports 1-65535. The common UDP ports scan is the quickest since it has the fewest ports to scan, whereas the UDP ports 1-65535 port scan can take more than 24 hours to perform on some devices. Scheduled scan policies use combinations of these different types of port scans.
SANS Top 20 Internet Security Vulnerabilities scan policy	A Scheduled scan policy that scans devices for the vulnerabilities on the SANS Top 20 Internet Security Vulnerabilities list. As the SANS/FBI organization updates their list of the most commonly exploited vulnerabilities, this scan policy is automatically updated during rule updates to reflect the changes.
Scan policy	A collection of Scan rules that tests devices for vulnerabilities. VAM installs with five Scheduled scan policies: Hourly+, Daily+, Weekly+, Monthly+, and SANS Top 20 Internet Security Vulnerabilities. Each Scheduled scan policy (except SANS Top 20 Internet Security Vulnerabilities) includes an Intelliscan™, which runs at the frequency indicated by the policy's name, plus additional port scans, which run on variable schedules. Attributes of scan policies include the number and types of scan rules included and the frequency the rules are run.
Scan rule	Tests a device for a specific security vulnerability. Applying a scan rule to a device yields one of two results: (1) a successful pass of that scan or (2) a scan rule violation, which results in VAM initiating the Vulnerability Repair Workflow process for that vulnerability.
SMS	Microsoft Systems Management Server (SMS) 2003 provides a means to manage software updates for Microsoft platform devices. Repair vulnerabilities via patch management with SMS; assign repairs to SMS and let VAM manage the repair process, removing the vulnerability from the workflow when the patch has installed successfully.
System data	The TCP and UDP port scan information and ICMP information collected from devices on the target network.
Target network	The domain of network and host traffic to be analyzed by the TOE.

Term	Definition
Vulnerability Repair Workflow™	The highly automated process of managing the repair of vulnerability from the time it is found through its repair. There are five states that vulnerability can be assigned as it progresses through the workflow. VAM automatically assigns vulnerabilities to the individuals responsible for repairs and schedules repair due dates based on the Device importance level.
Workflow state	The status of a vulnerability as it progresses through the Vulnerability Repair Workflow. The seven workflow states are: 1. Found 2. Confirmed 3. Under repair 4. Pending repair verification 5. SMS repairs in progress 6. Repaired 7. Ignored
Workflow roles	The roles assigned to individuals taking part in the Vulnerability Repair Workflow. Each workflow role has specific responsibilities. The four workflow roles are: • **Confirmer** – confirms that found vulnerabilities are legitimate; assigns repairers to vulnerabilities. • **Primary repairer** – fixes vulnerabilities that VAM has found. • **Secondary repairer** – fixes vulnerabilities that VAM has found. • **Owner** – the individual ultimately responsible for a given device.

Table 1-4 CC Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

2 TOE DESCRIPTION

2.1 Product Type

StillSecure VAM is a vulnerability management system that identifies, manages, and manages the remediation of network security vulnerabilities. StillSecure VAM systematically and regularly scans for network security vulnerabilities. Its automated scans run on a regular, customizable schedule. The vulnerabilities found during scans are tracked and managed by VAM's exclusive Vulnerability Repair Workflow. VAM logs all scanning and repair activities and delivers a range of detailed reports targeted at auditors, managers, and IT staff members.

2.2 How VAM Works

Once VAM is installed and configured the following sequence of activities will occur:

1. Map - The first step in the process is to map the target network. Before VAM can scan for vulnerabilities, it needs to discover and map the devices in the target network. This is accomplished with Autodiscovery, which an authorized administrator runs during the configuration process or via an On-demand scan. VAM's Autodiscovery is run on a regular schedule. Autodiscovery identifies and inventories all devices on the network down to the OS and application level. Autodiscovery uses TCP and UDP port scans and ICMP information to map out the target network.

2. Scan - The second step is to scan devices for vulnerabilities. Once Autodiscovery is complete, an authorized administrator assigns each device discovered to an appropriate Scheduled scan policy, or runs an On-demand scan. Scanning can occur individually for each device or can be accomplished for multiple devices simultaneously. VAM installs with five Scheduled scan policies:

- Hourly,
- Daily,
- Weekly,
- Monthly, and
- SANS Top 20 Internet Security Vulnerabilities.

The recommended approach is to assign devices to scan policies based on how frequently a device should be scanned. Devices deemed mission-critical can be scanned hourly or daily, while less critical devices can be scanned weekly or monthly. VAM also lets an authorized administrator create custom scan policies to meet any unique scanning needs. Once an authorized administrator has assigned a device to a scan policy, VAM automatically scans the device during the next scheduled scan. An authorized administrator can also manually initiate the scan if need be. VAM's Intelliscan feature automatically determines all appropriate scans to apply to each device based on device type, operating system, services, ports, and installed applications. As a result, scanning efficiency is maximized with a minimal impact on target network resources. Distributed scanners (DS) add remote scanning capabilities and load balancing to a VAM installation. The VAM Central server (CS) communicates with each DS and provides secure, centralized management of all scanning activities and data. The DS is not part of the evaluated configuration.

3. Repair - The third step is to manage identified vulnerabilities as they progress through the repair process. The scans that an authorized administrator runs in the previous step generate a list of vulnerabilities for devices on the target network. Some vulnerabilities may be critical and need immediate attention; others may be minor and can be ignored. VAM's Vulnerability Repair Workflow feature lets an authorized administrator assign, track, and manage repairs from the time a vulnerability is discovered until its repair has been verified by VAM. VAM is automatically updated as

often as hourly with the latest vulnerability Scan rules, ensuring up-to-date protection against newly discovered threats.

The workflow automatically assigns vulnerabilities to the responsible individuals and prioritizes repair schedules based on the affected device's importance. The Vulnerability Repair Workflow automatically:

- Notifies appropriate staff when new vulnerabilities are found.
- Assigns tasks based on group settings and permissions.
- Confirms vulnerabilities so unnecessary work isn't performed.
- Assigns and tracks vulnerabilities, showing who is responsible, the scheduled repair date, and the progress of repairs.
- Dynamically creates, maintains, and updates the repair schedule in Gantt chart format.
- Performs verification scans on reported repairs.
- Compiles a complete device history for meeting compliance and auditing requirements.

4. Report – The final step is reporting results. VAM lets an authorized administrator create reports on all vulnerability detection and repair activities that occur over a given period of time.

Generated on a corporate, division, or workgroup level, VAM reports provide concise security status information and detail responsibilities for updates and repairs. Report types include:

- **Executive status report –** highlights how the most important vulnerabilities are being addressed; designed for management, auditors, and regulators.
- **Vulnerability details –** breaks down all existing vulnerabilities by device, specifying repair schedules and responsibilities.
- **Vulnerability frequency (current) –** provides details on each type of vulnerability currently existing on the target network.
- **SANS Top 20 Internet Security Vulnerabilities –** breaks down existing SANS Top 20 Internet Security Vulnerabilities by device, device group, time period, and severity.
- **SANS Top 20 Internet Security Vulnerabilities (csv) –** breaks down existing SANS Top 20 Internet Security Vulnerabilities by device, device group, time period, and severity in a comma-separated list.
- **Patch summary –** shows status of SMS patches.
- **Ignored vulnerabilities –** shows vulnerabilities that have been ignored globally, and on specific devices.

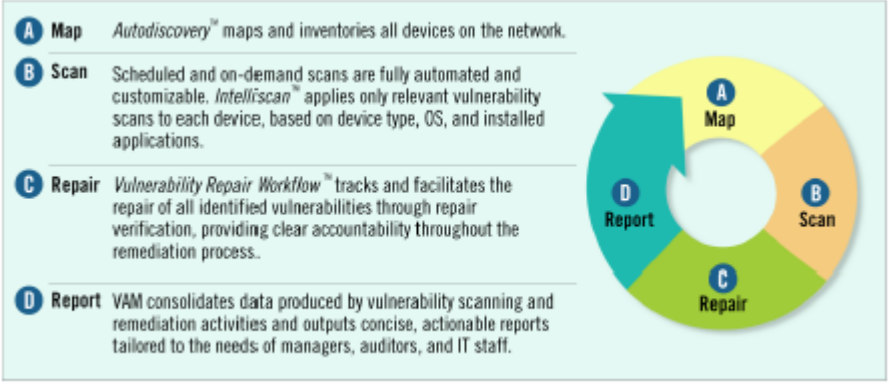

Figure 2-1 The VAM Process

2.3 StillSecure VAM Components

The evaluated product is comprised of the Server VAM, Desktop VAM, Remote VAM, and a User Console. VAM consists of three individual modules (Server VAM, Desktop VAM, and Remote VAM), each targeting a specialized scanning need. VAM modules integrate seamlessly. All products can be installed on a single server and managed through a single User Console (This how the evaluated product will be tested). The scan results, reports, and repair tasks generated by VAM modules can be rolled up into a single display or viewed individually by module, giving authorized administrators the flexibility needed to efficiently find and repair network vulnerabilities.

2.3.1 Server VAM

Server VAM safeguards the target network infrastructure. Server VAM is optimized for scanning servers, routers, switches, and other mission critical, network infrastructure devices.

2.3.2 Desktop VAM

Desktop VAM cost-effectively secures the back-door to the target network. Optimized for desktops, laptops, and printers, Desktop VAM secures the target network's desktop environment. Desktop VAM scans vulnerabilities on Microsoft and Apple operating systems for workstations, laptops, and other peripheral devices that are notorious for providing back-door entry into corporate networks. It also tracks and secures any mobile devices that are transient on the target network.

2.3.3 Remote VAM

Remote VAM locks down the exposed target network perimeter. Remote VAM performs automated, external penetration tests on Internet-visible devices. By assessing the external security posture, Remote VAM provides a “hacker’s eye view” of the target network, and allows the authorized administrator to focus on vulnerabilities that represent immediate threats to the organization.

2.3.4 User Console

StillSecure VAM has a web based User Console through which all StillSecure VAM functions are managed. Users access the User Console via a standard web browser, such as Internet Explorer or Netscape Communicator.

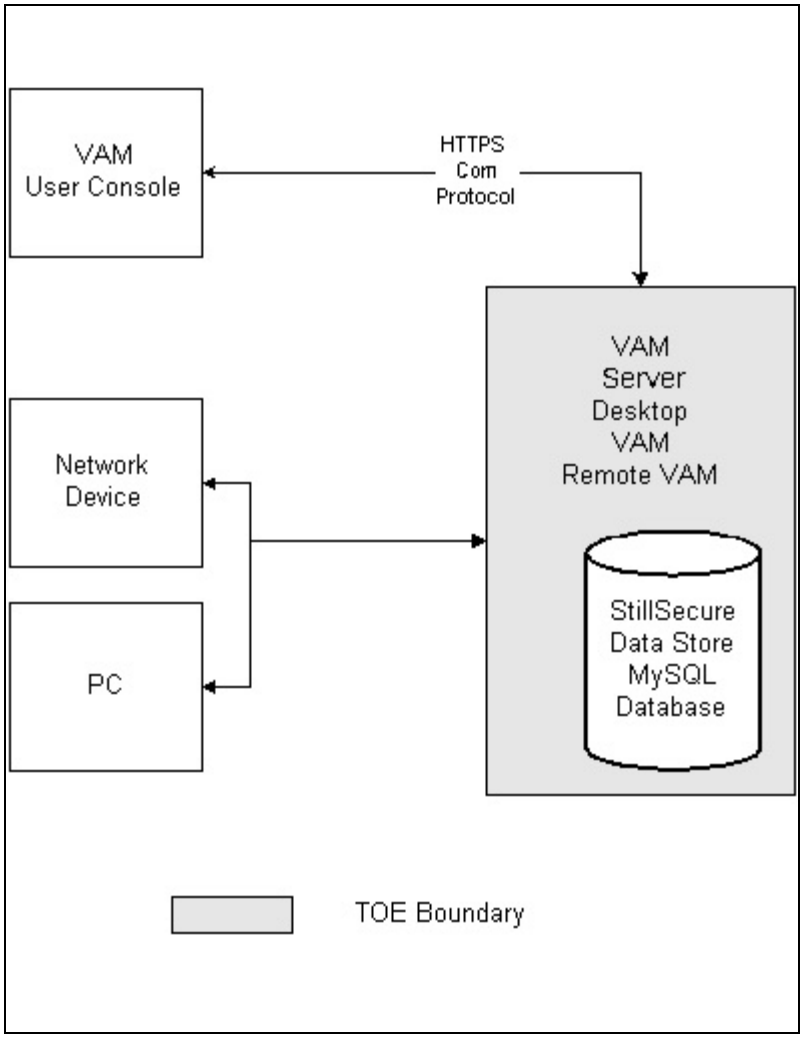

Figure 2-2 StillSecure VAM TOE Boundary

2.4 TSF Physical Boundary and Scope of the Evaluation

The TOE includes the following software only components:

- StillSecure VAM V5.5, includes all modules of the product:
  - Server VAM
  - Desktop VAM
  - Remote VAM
  - User Console

The TOE will be evaluated on the following operating system platform(s):

The evaluated configuration will be tested on a single server deployment that includes the following:

- StillSecure Server VAM, Desktop VAM, Remote VAM running on Linux RedHat Enterprise 4 on the same physical machine.
- The StillSecure VAM User Console will be presented on a separate machine running Internet Explorer 6.0 on a XP SP2 workstation.

The evaluated configuration will have the StillSecure VAM configured so that the strict passwords setting is activated as well as the expiration of the login password.

The TOE does not include the following IT Environment Components:

- Hardware platform(s) for all product components
- Operating System platform(s) for all product components
- Cryptographic module(s): SSL implementation on all platforms
- Transport standards HTTP, HTTPS, and FTP implementations
- Network or other connectivity: (Trusted Ethernet network)
- Third party relational database (MySQL) and its interface
- Internet Browser (ex. Internet Explorer, Netscape Communicator)
- Distributed Scanners

2.5 Logical Boundary

The logical boundary of the TOE will be broken down into the following security class features which are further described in sections 5 and 6. StillSecure VAM provides the following security features:

- **Security audit** - StillSecure VAM provides its own internal auditing capabilities separate from those of the Operating System. StillSecure VAM provides the ability to search and view its own audit records.
- **Identification and authentication** - StillSecure VAM provides user identification and authentication through the use of user accounts and the enforcement of password policies.
- **Security management** - StillSecure VAM provides security management through the use of the User Console. . The TOE provides multiple administrative roles (FMT_SMR.1).
- **Partial protection of the TSF**- StillSecure VAM partially protects its programs and data from unauthorized access through its own interfaces.
- **Vulnerability System** – The TOE provides several features that map, scan, manage remediation, and report on vulnerabilities of the devices on the target network.
  - **Map and Scan** – Using Autodiscovery, which uses onboard scanners to map the network. (VUL_SDC_EXP.1) The TOE is able to find all devices on the target network using ICMP pings with port and service scanners. Once the network is mapped, the onboard scanners scan for vulnerabilities of the devices on the target network.
  - **Repair** – Once the vulnerabilities have been mapped, the TOE provides a workflow process through its User Console to aid authorized users (FMT_SMR.1) in managing the patches and software updates that are necessary in correcting the found vulnerabilities. (FMT_MTD.1)
  - **Report** – The TOE provides reporting functionality to aid the authorized users in managing the found vulnerabilities and workflow process (VUL_DRS_EXP.1)

2.6 TOE Security Environment

It is assumed that there will be no untrusted users or software on the StillSecure VAM Server host. StillSecure VAM relies upon the underlying operating system and platform to provide reliable time stamps and to protect the StillSecure VAM Server host from other interference or tampering. StillSecure VAM relies on a Web Server to provide web services. The TOE environment is one where

the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE security environment can be categorized as follows:

- **Protection of TSF** - StillSecure VAM relies on the underlying OS to provide security capabilities for the TOE's protection. For the TOE's own protection the OS includes requirements that relate to the integrity of the TSF. These include TSF domain separation, reliable time-stamp, and Non-bypassability of the TSP.
- **Relational Database** - The Relational database provides the following:
  - Ensures data security with logins and passwords
  - Audit log storage and retrieval
- **Operating System and Hardware** –

  The OS and Hardware is being relied on for execution of the software, disk storage, and reliable time stamps.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

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

Table 3-1 Assumptions for the IT Environment

Item	Assumption Name	Description
1	A.AdmTra	Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords. However, administrators and operators are capable of error.
2	A.Env	Administrators will ensure that the environment has adequate facility to provide disk storage and other capabilities for the TOE's protection.
3	A.Low	The attack potential on the TOE is assumed to be low.
4	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the StillSecure VAM Server host which hosts the Server VAM, Desktop VAM, and Remote VAM modules.
5	A.Physical	Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access.
6	A.ProtectComm	Those responsible for the TOE will ensure the communications between the User Console and StillSecure VAM Server host are secure.
7	A.Users	It is assumed that authorized users will protect their authentication data.

Application Note: A.ProtectComm provides for a secure communications between the User Console and StillSecure VAM Server host. This can be accomplished by the following:

1. *SSL secure channel between the User Console and StillSecure VAM Server host*
2. *The User Console is located on the same machine as the StillSecure VAM Server host*
3. *There is a direct connection between the User Console and StillSecure VAM Server host on a secure network or via a serial cable or crossover ethernet cable.*

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE must counter the following threats to security:

Table 3-2 Threats

Item	Threat	Threat Description
1	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.
2	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.
3	T.Vul	The TOE may fail to notify the identified vulnerabilities or inappropriate activity based on association of system data received from all devices on the target network.
4	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access

Item	Threat	Threat Description
		to resources protected by the TOE.
5	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
6	T.Tamper	An attacker may attempt to modify TSF programs and data.
7	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 TOE Objectives

Item	Objective	Objective Description
1.	O.Access	The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles.
2.	O.Admin	The TOE will include a set of functions that allow effective management of its functions and data.
3.	O.Audit	The TOE will record audit records for data accesses and use of the TOE functions and will ensure protection of the audit storage.
4.	O.IDAuth	The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data.
5.	O.IDScan	The TOE will collect and store system data from the devices on the target network and will send an alarm upon the detection of a potential security violation.
6.	O.PartialNonBypass	The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
7.	O.PartialSelfProtection	The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure, through its own interfaces.
8.	O.PasswordQual	The TOE will be able to specify password quality parameters such as password expiration, minimum length, and password compositions.
9.	O.ProtectAuth	The TOE will provide protected authentication feedback and will force re-authentication after a configurable number of unsuccessful authentication attempts.
10.	O.Revoke	The TOE will allow administrators to revoke privileges of users.
11.	O.Roles	The TOE will support multiple roles.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 IT Environment Objectives

Item	Environment Objective	Environment Objective Description
12.	OE.AuditProtect	The IT environment will ensure the protection of the audit storage.
13.	OE.NonBypass	The IT environment will ensure that its protection mechanisms cannot be bypassed.
14.	OE.PartialSelfProtection	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
15.	OE.Time	The underlying operating system will provide reliable time stamps.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

Table 4-3 Non-IT Environment Objectives

Item	Non-IT Environment Objective	Non-IT Environment Objective Description
16.	ON.Install	Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security.
17.	ON.Low	Those responsible for the TOE will ensure that the TOE is in an environment where there is only a low attack potential.
18.	ON.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the StillSecure VAM Server host.
19.	ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
20.	ON.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
21.	ON.ProtectComm	Those responsible for the TOE will protect communications between the User Console and StillSecure VAM Server host are secure.
22.	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
23.	ON.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, explicit functional components derived from the CC Part 2, and assurance components from Part 3 of the CC.

5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, section 4.4.1.3.2 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "-*" refers to all iterations of a component.
- *Explicitly Stated Requirements* will be noted with a "_EXP" added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *NIAP and International Interpretations* have been reviewed. Relevant Interpretations are included and are noted in Interpretation Notes. Interpretation Notes are denoted by *italicized text.* The original CC text modified by the interpretation is not denoted nor explained.
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.2 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and explicit components derived from Part 2 of the CC, summarized in the Table 5-1 below.

Table 5-1 Functional Components

No.	Component	Component Name
1.	FAU_GEN.1	Audit data generation
2.	FAU_SAR.1	Audit review
3.	FAU_SAR.2	Restricted audit review
4.	FAU_SAR.3	Selectable audit review
5.	FAU_STG_EXP.1-1	Protected audit trail storage
6.	FIA_AFL.1	Authentication failure handling
7.	FIA_ATD.1	User attribute definition
8.	FIA_SOS.1	Verification of secrets
9.	FIA_UAU.2	User authentication before any action
10.	FIA_UAU.7	Protected authentication feedback
11.	FIA_UID.2	User identification before any action
12.	FMT_MTD.1	Management of TSF data
13.	FMT_REV.1	Revocation
14.	FMT_SMR.1	Security roles
15.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
16.	FPT_SEP_EXP.1-1	TSF domain separation
17.	VUL_SDC_EXP.1	System data collection
18.	VUL_ARP_EXP.1	Security alarms
19.	VUL_DRS_EXP.1	Data reporting

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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

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

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

c) **[*the following auditable events:***

- ***all workflow state changes for each vulnerability on the system***
- ***all found vulnerabilities***

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: **[*none*]**

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*the User with Admin permission*]** with the capability to read **[*all audit information*]** from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches*]** of audit data based on **[*device name, device IP address, name of repairer, discovering scanner name, workflow state, by time of workflow state change, and vulnerability name. The audit data can be sorted (ordered) by vulnerability count per device, device name, device importance, vulnerability severity level, and name of repairer*]**.

Dependencies: FAU_SAR.1 Audit review

FAU_STG_EXP.1-1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion initiated through its own TSFI.

FAU_STG_EXP.1.2-1 The TSF shall be able to prevent unauthorised modifications to the audit records in the audit trail initiated through its own TSFI.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when **[*an administrator configurable positive integer within 0 to 2.1 billion*]** unsuccessful authentication attempts occur related to **[*administrator and user login attempts*]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[*disable the administrator and user accounts until the account is reactivated by a user with Admin permission*]**.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **[*User Account Name;***
- ***Assigned Permissions (Admin, Write, Read, Disabled);***
- ***Assigned workflow roles (Confirmer, Repairer, and Owner);***
- ***Password***
- ***Assigned Groups*]**

Dependencies: No dependencies.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[*the rules of the password policy:***

- ***The minimum number of alphabetic characters required is 8;***
- ***One character has to be uppercase, a number, or a special character;***
- ***Expire the login password after a configurable number of days*.]**

Dependencies: No dependencies.

Application Note: When the strict passwords setting is activated the above password policy rules will be enforced.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only **[*a display of the typed in user name and asterisks for the password for password-based authentication*]** to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies.

5.2.3 Class FMT: Security Management (FMT)

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[*change_default, query, modify, delete, clear, [and other operations as specified in Table 5-2*]]** the **[*TSF Data as specified in Table 5-2*]** to **[*the role as specified as Authorized Role in Table 5-2*].**

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Table 5-2 Management of TSF Data

Security Function	Operation	TSF data	Authorized Role	Notes
Security Audit	Query	all audit data	User with Admin permission	
Security Audit	Query	audit data	Users with Read Permission (based on group or vulnerabilities assigned to them); Users with Write Permission (based on group or vulnerabilities assigned to them)	
Identification and Authentication	Query, add, modify, disable and delete	user account name	User with Admin permission	User with Admin permission manages user accounts
Identification and Authentication	Create and modify	password	User with Admin permission; User with Write Permission; User with Read Permission	
Security Management	Query and assign	permissions	User with Admin permission	The assigned permission are Admin, Write, Read, Disabled
Security Management	Query and assign users to	workflow roles	User with Admin permission	
Security Management	Modify workflow roles	workflow roles	User with Write Permission, User with Admin permission	Security Management
Security Management	Query, create, modify, and delete scan policies	scan policies	User with Admin permission	

Security Function	Operation	TSF data	Authorized Role	Notes
Security Management	Query, create, and modify scan policies of the assigned group	scan policies	User with Write Permission	
Security Management	Configure device profiles	device profiles	User with Admin permission; User with Write Permission;	Configuring device profiles entails assigning devices to scan policies, specifying allowed ports, and editing device names.
Security Management	modify device profiles; query devices that are in the users assigned groups.	device profiles	User with Admin permission; User with Write Permission;	
Security Management	Query, discard, and specify a vulnerability to be ignored forever	vulnerability	User with Admin permission; User with Write Permission (based on the group assigned to them);	
Security Management	Query, add, edit, and delete; Add devices to a group/ delete devices from a group; Add users to a group/ remove users from a group	groups	User with Admin permission	
Vulnerability System	Query, run	All reports	User with Admin permission	
Vulnerability System	Query, run	Assigned reports other than the executive status report	User with Write permission (based on the group assigned to them)	
Vulnerability System	Query	All reports	User with Write permission; User with Read permission	When a write user or read user queries all reports, only devices to which they have permission and which are in the assigned group will be reported.
Vulnerability System	Run	scan policies	User with Write permission (based on group assigned to them)	

FMT_REV.1 Revocation

Hierarchical to: No other components.

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [***users***] within the TSC to [***User with Admin Permission***].

FMT_REV.1.2 The TSF shall enforce the rules [***at the next login attempt***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*User with Admin permission, User with write permission, User with Read Permission*].**

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

Dependencies: FIA_UID.1 Timing of identification

5.2.4 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_ EXP.1-1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_ EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_ EXP.1.2-1 The TSF, when invoked by the underlying host OS, shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.5 Class VUL: Vulnerability System

VUL_SDC_EXP.1 System data collection

Hierarchical to: No other components

VUL_SDC_EXP.1.1 The TOE shall be able to collect the following information from the devices on the target network: see column 1 of Table 5-3.

VUL_SDC_EXP.1.2 At a minimum, the TOE shall collect and record the following information:

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

b) The additional information specified in the Details column of Table 5-3 System Data.

Table 5-3 System Data

Devices	Data Details
Devices (host, router, switch, hub, bridge, desktops, laptops, printers and other peripheral devices)	Open Ports
	Services
	Vulnerability Data
	ICMP information

VUL_SDC_EXP.1.3 The TOE shall scan all devices on the network for known vulnerabilities.

Dependencies: No dependencies

VUL_ARP_EXP.1 Security alarms

Hierarchical to: No other components.

VUL_ARP_EXP.1.1 The TSF shall take **[*action to send a notification via e-mail*]** upon detection of a potential security violation.

Dependencies: VUL_SDC_EXP.1 System data collection

VUL_DRS_EXP.1 Data reporting

Hierarchical to: No other components

VUL_DRS_EXP.1.1 The TSF shall be able to report collected system data using automatically generated reports.

VUL_DRS_EXP.1.2 The TSF shall be capable of generating user defined reports.

VUL_DRS_EXP.1.3 The TSF shall be capable of generating the following reports:

- Executive status report – highlights how the most important vulnerabilities are being addressed; designed for upper management, auditors, and regulators.
- Vulnerability details – breaks down all existing vulnerabilities by device, specifying repair schedules and responsibilities.
- Vulnerability frequency - current – provides details on each type of currently existing vulnerability.
- SMS Patch summary – Keeps the authorized administrators and users up-to-date on what vulnerabilities have been assigned to SMS, when they were assigned, and what the repair status is.
- Ignored vulnerabilities – Shows which vulnerabilities are ignored, both globally and on a per-device basis.

Dependencies: No dependencies.

5.2.6 Strength of Function

The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_SOS.1. The SOF claim for FIA_SOS.1 is SOF-basic. The strength of the “secrets” mechanism is consistent with the objectives of authenticating users (O.IDAuth). In addition, O.PasswordQual is consistent with the SOF-basic claim. Strength of Function shall be demonstrated for the non-certificate based authentication mechanisms to be SOF-basic, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential.

5.3 Security requirements for the IT Environment

StillSecure VAM requires that the operating system platform provide reliable time stamps. StillSecure VAM requires that the operating system provides TSF domain separation and Non-Bypassability.

Table 5-4 Functional Components for the IT environment

No.	Component	Component Name
1.	FAU_STG_EXP.1-2	Protected audit trail storage
2.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
3.	FPT_SEP_EXP.1-2	TSF domain separation
4.	FPT_STM.1	Reliable time stamps

5.3.1 Class FAU: Security Audit

FAU_STG_EXP.1-2 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-2 The IT Environment shall protect the stored audit records in the TSF audit trail from unauthorised deletion initiated through the IT Environment's Interfaces.

FAU_STG_EXP.1.2-2 The IT Environment shall be able to prevent unauthorised modifications to the audit records in the TSF audit trail initiated through the IT Environment's Interfaces.

Dependencies: FAU_GEN.1 Audit data generation

5.3.2 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-2 The IT environment shall ensure that the Operating System's Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP.1.1-2 The IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP_EXP.1.2-2 The IT environment shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-5.

Table 5-5 EAL2 Assurance Components

Component	Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

Section 6 describes the specific security functions that meet the criteria of the security class features that are described in section 2.4. The following sections describe the IT Security Functions of the TOE. These security functions satisfy the TOE security functional requirements. Table 6-1 includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. In sections 6, 7, and 8, the TOE and all its software modules and components will be mutually referred to as StillSecure VAM.

Table 6-1 Security Functional Requirements mapped to Security Functions

Item	SFRs	Security Class	Security Functions	Sub-functions
1	FAU_GEN.1	Security audit	Security Audit	AU-1
2	FAU_SAR.1	Security audit	Security Audit	AU-2
3	FAU_SAR.2	Security audit	Security Audit	AU-3
4	FAU_SAR.3	Security audit	Security Audit	AU-4
5	FAU_STG_EXP.1-1	Security audit	Security Audit	AU-5
6	FIA_AFL.1	Identification and authentication	Identification and Authentication	IA-1
7	FIA_ATD.1	Identification and authentication	Identification and Authentication	IA-2
8	FIA_SOS.1	Identification and authentication	Identification and Authentication	IA-3
9	FIA_UAU.2	Identification and authentication	Identification and Authentication	IA-4
10	FIA_UAU.7	Identification and authentication	Identification and Authentication	IA-5
11	FIA_UID.2	Identification and authentication	Identification and Authentication	IA-6
12	FMT_MTD.1	Security management	Security Management	SM-1
13	FMT_REV.1	Security management	Security Management	SM-2
14	FMT_SMR.1	Security management	Security Management	SM-3
15	FPT_RVM_EXP.1-1	Protection of the TSF	Manage User Access	MUA-1
16	FPT_SEP_EXP.1-1	Protection of the TSF	Manage User Access	MUA-2
17	VUL_SDC_EXP.1	Vulnerability System	Vulnerability System	VUL-1
18	VUL_ARP_EXP.1	Vulnerability System	Vulnerability System	VUL-2
19	VUL_DRS_EXP.1	Vulnerability System	Vulnerability System	VUL-3

6.1.2 Security Audit Function

AU-1 Audit data generation (FAU_GEN.1)

StillSecure provides an audit trail function. Audit trails are logs maintained by StillSecure that track the vulnerabilities, work flow, actions taken of StillSecure users, and actions of the system itself.

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

- ***Start-up and shutdown of the audit functions***
- ***all workflow state changes for each vulnerability on the system***
- ***all found vulnerabilities***

The audit logs are stored in the on board MySQL database, which is password protected (remote users are disallowed) and firewalled (the MySQL connection port is protected from outside requests by the on board iptables firewall). The machine hosting the MySQL database will be physically located in a secure location. All system, database, and application passwords are encrypted. The encryption is outside the scope of the TOE.

AU-2 Audit review (FAU_SAR.1)

StillSecure provides the user with Admin permission with the capability to read all audit information from the audit records. The audit records are provided in a manner suitable for the user to interpret the information. All work flow state changes for each vulnerability are viewable in the repair schedule. Admin users can view all vulnerabilities in the repair schedule.

AU-3 Restricted audit review (FAU_SAR.2)

The TSF prohibits all users read access to the audit records, except those users that have been granted explicit read-access.

AU-4 Selectable audit review (FAU_SAR.3)

StillSecure VAM provides the ability to perform searches of audit data based on device name, device IP address, name of repairer, discovering scanner name, workflow state, by time of workflow state change, and vulnerability name. The audit date can be sorted (ordered) by vulnerability count per device, device name, device importance, vulnerability severity level, and name of repairer.

AU-5 Protected audit trail storage (FAU_STG_EXP.1-1)

The TSF is able to protect stored audit records from unauthorized deletion as well as prevent unauthorized modifications to the audit records

The audit logs are stored in the on board MySQL database, which is password protected (remote users are disallowed) and firewalled (the MySQL connection port is protected from outside requests by the on board iptables firewall). The machine hosting the MySQL database will be physically located in a secure location. All system, database, and application passwords are encrypted. The encryption is outside the scope of the TOE.

Normal authorization controls that apply within the User Console, as well as the database password protection and on board firewall prevent unauthorized users from modifying or deleting the audit data.

6.1.3 Identification and Authentication

IA-1 Authentication failure handling (FIA_AFL.1)

Users with the Admin permission are able to configure a lockout of an administrator and user after a set number of unsuccessful login attempts. The user and administrator accounts will remain locked until the account is reactivated by an authorized user with Admin permissions.

IA-2 User attribute definition (FIA_ATD.1)

The TSF maintains the following user security attributes:

- User Account Name;
- Assigned Permissions (Admin, Write, Read, Disabled);
- Assigned workflow roles (Confirmer, Repairer, and Owner);
- Password
- Assigned group

Assigned Permissions are described below:

Admin permission

The Admin permission is assigned to users responsible for managing the VAM installation. Admin users have unrestricted access to all VAM functions and belong to all groups. In addition to having all possible Write permissions (described below), Admin users have authority to:

- Configure the system (access to all configuration screens)
- Create, add, modify, disable and delete user accounts; Create and modify passwords
- Query and assign permissions. The assigned permissions are Admin, Write, Read and Disabled.
- Query, add, edit and delete groups; add devices to a group/delete devices from a group; add users to a group/remove users from a group.
- Query and assign a user with write permission to workflow roles
- Query, create, modify and delete scan policies
- Configure device profiles (assign devices to scan policies, specify allowed ports, edit device names), modify device profiles and query devices that are in the users assigned group
- Query, discard and specify a vulnerability to be ignored forever.
- Query all audit data
- Generate all reports

Write permission

The Write permission is assigned to users who participate in the vulnerability repair workflow. All write-permission users can see devices based on what workflow role has been assigned globally, by device, or by a specific vulnerability. Write users are only allowed to view information pertaining to the groups to which they belong. All Write-permission users can act as confirmers, repairers or owners in the vulnerability repair workflow. (see Table 6-2 for more information),. Users with write permission can generate limited set of reports for the devices they are assigned:

Additional permissions can be individually assigned to Write users, depending on their responsibilities and authority. These optional write permissions allow users to:

- Modify planned repair dates
- Reassign repair tasks
- Query, discard and specify a vulnerability to be ignored forever
- Query, create and modify scan policies
- Configure and modify device profiles, create, modify passwords
- Query devices that are in the user's assigned groups

- Query and assign users to workflow roles, modify workflow roles
- Query audit data of the group
- Query all reports
- Run scan policies

The optional write permissions are individually selected for each write-permission user on the Accounts tab.

Read permission

Assign Read permission to users, such as executives and managers, who need to view the information stored and maintained in VAM. Read users are only permitted to view information pertaining to the groups to which they belong. They are permitted to view all information in the main VAM window and query all reports but cannot access VAM configuration tabs.

Disabled permission

User accounts assigned a Disabled status have no access permissions whatsoever; their accounts are maintained in VAM, but the user is prohibited from logging onto the system. Disabled accounts can be re-activated at any time by the user with admin permission, simply by assigning one of the three permissions (admin, write or read permissions).

Workflow roles

These are the roles assigned to the individuals taking part in the vulnerability repair workflow. This is usually a user with Write Permission. Each workflow role has specific responsibilities. They are:

Table 6-2 Workflow Roles

Workflow Role	Description
Confirmer	Confirmers verify that vulnerabilities found by VAM are legitimate. Confirmers assign repairers to discovered vulnerabilities. When vulnerability is found on a device, VAM requests that the default confirmer confirm the new vulnerability as the first step in the workflow process. .
Repairer	Repairers fix vulnerabilities that have been found on devices in the target network. A primary and secondary repairer can be assigned. When a vulnerability is found on a device and has been confirmed by the confirmer (if a confirmer has been specified), the primary repairer is automatically assigned to fix the vulnerability as the next step in the Vulnerability Repair Workflow process.
Owner	An owner can be assigned to devices on the target network. While not used in the vulnerability repair workflow, the owner label can associate individuals with the devices under their purview. The owner of a device can also be overridden on the Device profile.

IA-3 Verification of secrets (FIA_SOS.1)

The TSF provides a mechanism to verify that secrets meet the rules of the password policy. A user with Admin permission can activate strict passwords in the TOE by setting the strict passwords variable to 1 as described in the Administrator guide. Once the strict password setting has been activated, the password policy is as follows:

- The minimum number of alphabetic characters required is 8;
- One character has to be uppercase, a number, or a special character.

In addition, a user with the Admin permission can expire the login password after a configurable number of days. This also becomes part of the password policy since users are expected to create new passwords after a given number of days.

IA-4 User authentication before any action (FIA_UAU.2)

StillSecure VAM provides a password mechanism to authenticate administrators and users before they are able to access the TOE. If the administrator or user enters an incorrect password, the administrator or user cannot log in.

IA-5 Protected authentication feedback (FIA_UAU.7)

StillSecure VAM provides only a display of the typed in user name and asterisks for the password for password-based authentication to the user while the authentication is in progress.

IA-6 User identification before any action (FIA_UID.2)

StillSecure VAM identifies users before they are able to access the TOE. Users are identified by their user name.

6.1.4 Security Management

SM-1 Management of TSF Data (FMT_MTD.1)

Users with Admin permission have full access to the User Console and are able to manage all TSF data as specified in Table 5-2 in section 5.2.

Users with Write permission are able to manage TSF data as specified in Table 5-2.

Users with Read permission have read-only access to specific TSF data as specified in Table 5-2.

Security functions and the authorized roles required to execute them are listed in Table 5-2 in Section 5.2.

SM-2 Revocation (FMT_REV.1)

The TOE allows authorized users to revoke security attributes associated with the individual users within the TSC. Users with Admin Permission can revoke the security attributes associated with individual users. When a user account is assigned a Disabled status by the administrator, that user has no access permissions whatsoever and that user is prohibited from logging onto the system. These rules will be enforced at the next login attempt.

SM-3 Security Roles (FMT_SMR.1)

The TOE maintains the following trusted roles:

- User with Admin Permission
- User with Write Permission
- User with Read Permission

A user with write permission participates in the Vulnerability repair flow. All write-permission users can act as confirmers, repairers or owners in the vulnerability repair flow.

6.1.5 Manage User Access

MUA-1 Non-bypassability (FPT_RVM_EXP.1-1)

The TSF ensures that TOE security functions are partially non-bypassable. Since this is a software-only TOE, it also relies on the underlying OS to provide non-bypassability. The TOE ensures that security protection enforcement functions are invoked and succeed before each function within the TOE's scope of control is allowed to proceed. StillSecure VAM identifies users before they are

able to access the TOE. The TOE provides a password mechanism to authenticate users before they are able to access the TOE.

MUA-2 TSF domain separation (FPT_SEP_EXP.1-1)

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. Since this is a software-only TOE, it also relies on the underlying OS to provide TSF domain separation.

StillSecure VAM 5.5's protected domain includes the StillSecure VAM software and all of its software components as specified in section 2.4 as being in the TOE Boundary. The TSF enforces separation between the security domains of subjects in the TSC. StillSecure VAM relies on the Operating System to provide security capabilities for the TOE's protection. The underlying assumption regarding the operation of the TOE is that it is maintained in a physically secure environment.

6.1.6 Vulnerability System

VUL-1 System Data Collection (VUL_SDC_EXP.1)

StillSecure VAM collects its own system data directly from the target network via the onboard scanners. The scanners identify and inventory all devices on the target network. The OS and applications for each device are identified when known.

Once Autodiscovery is complete, the second step is to scan devices and hosts for vulnerabilities. An authorized administrator assigns each device discovered to an appropriate scheduled scan policy, or runs an on-demand scan. Scanning can occur individually for each device or can be accomplished for multiple devices simultaneously.

VAM's Intelliscan feature automatically determines all appropriate scans to apply to each device based on device type, operating system, services, ports, and installed applications.

See Table 5-3 for a list of system data that is collected on the devices and hosts on the target network.

VUL-2 Security alarms (VUL_ARP_EXP.1)

The TSF shall take action to send a notification via e-mail upon detection of a potential security violation. StillSecure VAM sends notifications throughout the work flow process beginning with new vulnerabilities that are found. When new vulnerabilities are found, a notification via e-mail is sent to the user(s) with the Confirmer workflow role. Users with the workflow user roles (Confirmer, Repairer, and Owner) receive e-mails throughout the workflow process concerning their responsibilities. Separate from these e-mail notifications, additional e-mail notifications can be configured. VAM automatically notifies relevant authorities when events occur that require their attention. A user with Admin permissions can configure which notifications are sent. The events for which notifications can be sent are:

• **When a new device is discovered** – VAM sends notifications when Autodiscovery discovers devices not previously known to VAM.

• **When a workflow state is changed** – VAM can send notifications when the workflow *state* of a vulnerability changes.

• **When a vulnerability is ignored** – When a vulnerability on a device is selected to be ignored, an email notification can be sent to other email accounts.

VAM sends these email notifications to the email address associated with the user's VAM account. Additional email notifications can be sent to non-user email addresses, distribution lists, and pager email accounts. Notifications are assigned by group. Each group that is maintained in VAM can have a unique notification setup.

VUL-3 Data reporting (VUL_DRS_EXP.1)

StillSecure VAM is able to report collected system data using automatically generated reports. In addition, the TSF is capable of generating user defined reports and the following reports:

- Executive status report – highlights how the most important vulnerabilities are being addressed; designed for upper management, auditors, and regulators.
- Vulnerability details – breaks down all existing vulnerabilities by device, specifying repair schedules and responsibilities.
- Vulnerability frequency - current – provides details on each type of currently existing vulnerability.
- SMS Patch summary – Keeps the authorized administrators and users up-to-date on what vulnerabilities have been assigned to SMS, when they were assigned, and what the repair status is.
- Ignored vulnerabilities – Shows which vulnerabilities are ignored, both globally and on a per-device basis.

6.1.7 SOF Claims

The following IT Security Function is realized by probabilistic or permutational mechanisms:

- IA-3: Identification and Authentication

Within IA-3, the methods used to provide difficult-to-guess passwords are probabilistic. The SOF claim for all of these IT security functions is SOF-basic.

6.2 Assurance Measures

The TOE satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-3 Assurance Measures and How Satisfied

Component	Evidence Requirements	How Satisfied
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	VAM™ v5.5 StillSecure VAM Configuration Management Capabilities (rev-g), January 3, 2007
ADO_DEL.1	Delivery Procedures	VAM™ v5.5 StillSecure VAM Delivery Procedures (rev-e), December 8, 2006
ADO_IGS.1	Installation, generation, and start-up procedures	StillSecure VAM 5.5 Installation Guide (rev-a), June 23, 2006
ADV_FSP.1	Functional Specification	VAM™ v5.5 StillSecure VAM Functional Specification (rev-i), December 12, 2006
ADV_HLD.1	High-Level Design	VAM™ v5.5 High-level Design (rev-i), December 12, 2006
ADV_RCR.1	Representation Correspondence	VAM™ v5.5 Representation Correspondence (rev-i), December 12, 2006,
AGD_ADM.1	Administrator Guidance	StillSecure VAM 5.5 Installation Guide (rev-a), June 23, 2006

Component	Evidence Requirements	How Satisfied
		StillSecure VAM 5.5 Users' Guide (rev-c), October 27, 2006
AGD_USR.1	User Guidance	StillSecure VAM 5.5 Installation Guide (rev-a), June 23, 2006
		StillSecure VAM 5.5 Users' Guide (rev-c), October 27, 2006
ATE_COV.1	Test Coverage Analysis	Test Coverage Analysis 1.1
ATE_FUN.1	Test Documentation	StillSecure VAM™ V5.5 Test Procedures V0.3
ATE_IND.2	TOE for Testing	TOE for Testing
AVA_SOF.1	SOF Analysis	StillSecure VAM™ Strength of Function Analysis, Version 0.1, November 15, 2006
AVA_VLA.1	Vulnerability Analysis	StillSecure VAM™ V5.5 Vulnerability Report

7 PP Claims

The StillSecure VAM Security Target was not written to address any existing Protection Profile.

8 RATIONALE

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE and the IT Environment. Rationale is provided for each threat below the table.

Table 8-1 All Threats to Security Countered

Item	Threat Name	Security Objective
1	T.BadPassword	O.PasswordQual O.ProtectAuth
2	T.Bypass	O.PartialNonBypass OE.NonBypass
3	T.Vul	O.IDScan
4	T.Mismanage	O.Admin O.Revoke O.Roles
5	T.Privil	O.Access O.PartialSelfProtection OE.PartialSelfProtection O.IDAuth O.ProtectAuth ON.Operations ON.Physical
6	T.Tamper	O.Access O.IDAuth O.PartialNonBypass O.PartialSelfProtection OE.PartialSelfProtection OE.NonBypass O.Revoke
7	T.Undetect	O.Audit OE.AuditProtect OE.Time

T.BadPassword: Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE. T.BadPassword is countered by:

- O.PasswordQual: The TOE will be able to specify password quality parameters such as password expiration, minimum length, and password compositions. This objective enables the administrator to specify checks for bad password qualities.
- O.ProtectAuth: The TOE will provide protected authentication feedback and will force re-authentication after a configurable number of unsuccessful authentication attempts. When an authorized user account is typing in their password only asterisks will be seen on the screen. This will limit the ability to see what an authorized user account's password is.

T.Bypass: An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF. T.Bypass is countered by:

- O.PartialNonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TSF security functions.

T.Vul: The TOE may fail to notify the identified vulnerabilities or inappropriate activity based on association of system data received from all devices on the target network. T.Vul is countered by:

- O.IDScan: The TOE will collect and store system data from the devices on the target network and will send an alarm upon the detection of a potential security violation. This objective counters this threat by the TOE collecting system data from devices on the target network and sending an alarm upon the detection of a potential security violation.

T.Mismanage: Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- O.Admin: The TOE will include a set of functions that allow effective management of its functions and data. Administrative tools make it easier for administrators to correctly manage the TOE.
- O.Roles: The TOE will support multiple roles. Multiple roles can be used to enforce separation of duty, so that one administrator can catch errors made by another administrator.
- O.Revoke: The TOE will allow administrators to revoke privileges of users. This will limit the access of users.

T.Privil: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. T.Privil is countered by:

- O.Access: The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles. This objective addresses this threat by providing for levels of user permissions, so that some users have more access to functions than others. This objective builds upon the O.IDAuth objective by only permitting authorized user accounts to access TOE functions. In addition, this objective builds upon the O.Roles objective by providing multiple roles and levels of user access.
- O.PartialSelfProtection: The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing partial TOE self-protection and separation between users. In addition, the TOE will maintain separation between code executing on behalf of different user accounts.
- OE.PartialSelfProtection: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by the underlying Operating System providing partial protection to the TOE and its data.
- O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of user accounts prior to any TOE function access.
- O.ProtectAuth: The TOE will provide protected authentication feedback and will force re-authentication after a configurable number of unsuccessful authentication attempts. This objective provides for the password to not be displayed when an authorized user is typing in their password. This will limit the ability to see what an authorized user account holder's password is.
- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. This objective addresses this threat by making certain the TOE is managed and operated in a secure manner according to the TOE Guidance documentation.

- ON.Physical: Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective addresses this threat by making sure the parts of the TOE critical to enforcing the StillSecure VAM security are located in a physically secure area.

T.Tamper: An attacker may attempt to modify TSF programs and data. T.Tamper is countered by:

- O.Access: The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles. This objective addresses this threat by providing for levels of user permissions, so that some users have more access to functions than others. This objective builds upon the O.IDAuth objective by only permitting authorized user accounts to access TOE functions. In addition, this objective builds upon the O.Roles objective by providing multiple roles and levels of user access.
- O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of user accounts prior to any TOE function access.
- O.PartialNonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- O.PartialSelfProtection: The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing partial TOE self-protection and separation between users. In addition, the TOE will maintain separation between code executing on behalf of different user accounts.
- OE.PartialSelfProtection: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by the underlying Operating System providing partial protection to the TOE and its data.
- OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TOE security functions.
- O.Revoke: The TOE will allow administrators to revoke the privileges of the users. This will limit the access of users.

T.Undetect: Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered. T.Undetect is countered by:

- O.Audit: The TOE will record audit records for data accesses and use of the TOE functions and will ensure protection of the audit storage. This objective provides for the TOE to generate audit records in an audit trail. Since the TOE records data accesses and use of the TOE functions, violations to the security policy will be recorded. In addition, this objective provides for the protection of the audit trail storage.
- OE.AuditProtect: The IT environment will ensure partial protection of the stored audit records. This objective counters the threat by requiring the IT Environment to provide protection of the audit storage.
- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

Table 8-2 Reverse mapping of TOE Security Objectives to Threats

Item	Objective	Threat
1.	O.Access	T.Privil T.Tamper
2.	O.Admin	T.Mismanage

Item	Objective	Threat
3.	O.Audit	T.Undetect
4.	O.IDAuth	T.Privil T.Tamper
5.	O.IDScan	T.Vul
6.	O.PartialNonBypass	T.Bypass T.Tamper
7.	O.PartialSelfProtection	T.Privil T.Tamper
8.	O.PasswordQual	T.BadPassword
9.	O.ProtectAuth	T.Privil T.BadPassword
10.	O.Revoke	T.Mismanage T.Tamper
11.	O.Roles	T.Mismanage

8.1.2 Assumptions

Table 8-3 shows that all of the secure usage assumptions are addressed by either security objectives for the IT environment or Non-IT security objectives. Rationale for each assumption is provided below the table.

Table 8-3 All Assumptions Addressed

Item	Assumption	Objective
1	A.AdmTra	ON.Install ON.Operations ON.Person
2	A.Env	ON.Install
3	A.Low	ON.Low
4	A.NoUntrusted	ON.NoUntrusted
5	A.Physical	ON.Physical
6	A.ProtectComm	ON.ProtectComm
7	A.Users	ON.ProtectAuth

A.AdmTra: Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords. However, administrators and operators are capable of error. A.AdmTra is covered by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. This objective provides for secure installation and configuration of the TOE.
- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. The procedures will provide guidance to the administrators and users on setting passwords and how to securely operate the TOE. This objective provides for operation procedures to be in place.
- ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE.

A.Env: Administrators will ensure that the environment has adequate facility to provide disk storage and other capabilities for the TOE's protection. A.Env is covered by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes installing the TOE on the recommended Operating Systems and hardware according to the product's installation requirements and Guidance documentation. This objective provides for secure installation of the TOE.

A.Low: The attack potential on the TOE is assumed to be low. A.Low is covered by:

- ON.Low: Those responsible for the TOE will ensure that the TOE is in an environment where there is only a low attack potential. This objective provides protection by placing the TOE in a low attack potential environment.

A.NoUntrusted: It is assumed that there will be no untrusted users and no untrusted software on the StillSecure VAM Server host which hosts the Server VAM, Desktop VAM, and Remote VAM modules. A.NoUntrusted is covered by:

- ON.NoUntrusted: The administrator will ensure that there are no untrusted users and no untrusted software on the StillSecure VAM Server host. This objective provides for the protection of the TOE from untrusted software and users.

A.Physical: Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access. A.Physical is covered by:

- ON.Physical: Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software.

A.ProtectComm: Those responsible for the TOE will ensure the communications between the User Console and StillSecure VAM Server host are secure.

- ON.ProtectComm: Those responsible for the TOE will protect communications between the User Console and StillSecure VAM Server host are secure.

A.Users: It is assumed that users will protect their authentication data. A.Users is covered by:

- ON.ProtectAuth: The users will ensure that their authentication data is held securely and not disclosed to unauthorized persons. This objective provides for user account holders to protect their authentication data.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-4 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included below the table.

Table 8-4 All Objectives Met by Functional Components

Item	Objective	Security Functional Requirement
1.	O.Access	FAU_SAR.2 Restricted audit review FAU_STG_EXP.1-1 Protected audit trail storage FIA_AFL.1 Authentication failure handling FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action FMT_MTD.1 Management of TSF data FMT_REV.1 Revocation

Item	Objective	Security Functional Requirement
2.	O.Admin	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FIA_ATD.1 User attribute definition FMT_MTD.1 Management of TSF data VUL_DRS_EXP.1 Data reporting
3.	O.Audit	FAU_GEN.1 Audit data generation FAU_STG_EXP.1-1 Protected audit trail storage
4.	O.IDAuth	FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action
5.	O.IDScan	VUL_SDC_EXP.1 System data collection VUL_ARP_EXP.1 Security alarms
6.	O.PartialNonBypass	FPT_RVM_EXP.1-1 Non-bypassability of the TSP
7.	O.PartialSelfProtection	FPT_SEP_EXP.1-1 TSF domain separation
8.	O.PasswordQual	FIA_SOS.1 Verification of secrets
9.	O.ProtectAuth	FIA_UAU.7 Protected authentication feedback FIA_AFL.1 Authentication failure handling,
10.	O.Revoke	FMT_REV.1 Revocation
11.	O.Roles	FMT_SMR.1 Security roles

O.Access: The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles. O.Access is addressed by:

- FAU_SAR.2 Restricted audit review, which requires that access to audit data be restricted to authorized users.
- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion, and modifications to the audit log will be prevented.
- FIA_AFL.1 Authentication failure handling, which requires the TSF to detect when an administrator configured maximum number of unsuccessful authentication attempts occur related to administrator and user login attempts. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF will disable the administrator and user accounts until the account is reactivated by a user with Admin permission.
- FIA_UAU.2 User authentication before any action, which requires each user with a user account be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that each user with a user account to be successfully identified before allowing access to the TOE.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_REV.1 Revocation, which requires that the TSF restrict ability to revoke security attributes associated with the users to users with admin permission.

O.Admin: The TOE will include a set of functions that allow effective management of its functions and data. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that users with Admin permission be able to read all audit information from the audit records.
- FAU_SAR.3 Selectable audit review, which requires that the TSF will provide the ability to search audit data based on the specified criteria.

- FIA_ATD.1 User attribute definition, which requires the TSF to maintain a list of security attributes belonging to individual users. The list of security attributes are user account name, assigned permission, assigned workflow role, password and assigned group.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- VUL_DRS_EXP.1 Data Reporting, which requires the TOE to provide data reporting capabilities.

O.Audit: The TOE will record audit records for data accesses and use of the TOE functions and will ensure protection of the audit storage. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications to the audit log will be prevented.

O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAuth is addressed by:

- FIA_UAU.2 User authentication before any action, which requires each user account to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that each user with a user account to be successfully identified before allowing access to the TOE.

O.IDScan: The TOE will collect and store system data from the devices on the target network and will send an alarm upon the detection of a potential security violation.

- VUL_SDC_EXP.1 System data collection, which requires the TOE to collect system data from devices on the target network.
- VUL_ARP_EXP.1 Security Alarms, which requires the TOE to take action to send a notification via e-mail upon detection of a potential security violation.

O.PartialNonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.

- FPT_RVM_EXP.1-1 Non-bypassability of the TSP which requires that TSP enforcement functions are invoked and succeed before a security relevant function is allowed to proceed.

O.PartialSelfProtection: The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.

- FPT_SEP_EXP.1-1 TSF domain separation, which requires the TSF to provide a domain, that partially protects itself from interference and tampering by untrusted users. This requires that the TOE provide partial protection to maintain separation between code executing on behalf of different users.

O.PasswordQual: The TOE will be able to specify password quality parameters such as password expiration, minimum length, and password compositions. O.PasswordQual is addressed by:

- FIA_SOS.1 Verification of secrets, which requires that the TSF provide a mechanism to verify that passwords meet the rules of the password policy.

O.ProtectAuth: The TOE will provide protected authentication feedback and will force re-authentication after a configurable number of unsuccessful authentication attempts. O.ProtectAuth is addressed by:

- FIA_UAU.7 Protected authentication feedback, the TSF shall provide only a display of the typed in user account name and asterisks for the password for password authentication.
- FIA_AFL.1 Authentication failure handling, which requires that the TSF detect when an administrator configurable maximum number of unsuccessful attempts occurs related to administrator and user login attempts. The user account will be disabled once the defined number of unsuccessful login attempts occurs until the account is reactivated by a user with admin permission.

O.Revoke: The TOE will allow administrators to revoke privileges of users.

- FMT_REV.1 Revocation, which requires that the TSF restrict ability to revoke security attributes associated with the users to users with admin permission.

O.Roles: The TOE will support multiple roles. O.Roles is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple roles.

Table 8-5 Reverse mapping of TOE SFRs to TOE Security Objectives

Note: Table 8-5 has been included as a consistency check to show that each TOE SFR maps back to at least one TOE security objective

Item	Security Functional Requirement	Objective
1.	FAU_GEN.1	O.Audit
2.	FAU_SAR.1	O.Admin
3.	FAU_SAR.2	O.Access
4.	FAU_SAR.3	O.Admin
5.	FAU_STG_EXP.1-1	O.Access O.Audit
6.	FIA_AFL.1	O.ProtectAuth O.Access
7.	FIA_ATD.1	O.Admin
8.	FIA_SOS.1	O.PasswordQual
9.	FIA_UAU.2	O.Access O.IDAuth
10.	FIA_UAU.7	O.ProtectAuth
11.	FIA_UID.2	O.IDAuth O.Access
12.	FMT_MTD.1	O.Access O.Admin
13.	FMT_REV.1	O.Access O.Revoke
14.	FMT_SMR.1	O.Roles
15.	FPT_RVM_EXP.1-1	O.PartialNonBypass
16.	FPT_SEP_EXP.1-1	O.PartialSelfProtection
17.	VUL_SDC_EXP.1	O.IDScan
18.	VUL_ARP_EXP.1	O.IDScan
19.	VUL_DRS_EXP.1	O.Admin

8.2.2 Dependencies

Table 8-6 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT environment an "E" will be next to the reference number.

Table 8-6 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1.	FAU_GEN.1	Audit data generation	FPT_STM.1	23 E
2.	FAU_SAR.1	Audit review	FAU_GEN.1	1
3.	FAU_SAR.2	Restricted audit review	FAU_SAR.1	2
4.	FAU_SAR.3	Selectable audit review	FAU_SAR.1	2
5.	FAU_STG_EXP.1-1	Protected audit trail storage	FAU_GEN.1	1
6.	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	9 (H)
7.	FIA_ATD.1	User attribute definition	None	None
8.	FIA_SOS.1	Verification of secrets	None	None
9.	FIA_UAU.2	User authentication before any action	FIA_UID.1	11 (H)
10.	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	9 (H)
11.	FIA_UID.2	User identification before any action	None	None
12.	FMT_MTD.1	Management of TSF data	FMT_SMR.1	14
			FMT_SMF.1	See section 8.2.3
13.	FMT_REV.1	Revocation	FMT_SMR.1	14
14.	FMT_SMR.1	Security roles	FIA_UID.1	11 (H)
15.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None	None
16.	FPT_SEP_EXP.1-1	TSF domain separation	None	None
17.	VUL_SDC_EXP.1	System data collection	None	None
18.	VUL_ARP_EXP.1	Security alarms	VUL_SDC_EXP.1	17
19.	VUL_DRS_EXP.1	Data Reporting	None	None

Table 8-7 IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
20.	FAU_STG_EXP.1-2	Protected audit trail storage	FAU_GEN.1	1
21.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	None	None
22.	FPT_SEP_EXP.1-2	TSF domain separation	None	None
23.	FPT_STM.1	Reliable time stamps	None	None

8.2.3 Rationale why dependencies are not met

For FMT_MTD.1, Management of TSF data, FMT_SMF.1 Specification of Management Functions is not applicable for this TOE since all the management functions required by the TOE are implicit in the FMT components.

8.2.4 Strength of Function Rationale

A strength of function level of SOF-basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. As stated in section 6.1.4, IA-3 is a security function based on probabilistic methods. See section 5.2.6 for the objectives that SOF supports. The specific "strength" required of the methods used to provide difficult-to-guess passwords are defined in FIA_SOS.1 in section 5.2.

8.2.5 Assurance Rationale

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs builds on the others. For example, FAU_GEN.1 details the auditable events generated by the TSF. FAU_SAR.1 specifies which authorized users are able to read what audit information from the audit records. For example, FAU_SAR.1 states that the user with Admin permission is able to read all audit records from the audit records. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.3 gives the TOE the ability to perform searches of the audit event data. FAU_STG_EXP.1 provides for protected storage of the audit data. Audit records are generated for many events where other requirements are coming to bear, such as login, policy check failures, and management functions.

Login processing brings in elements of many requirements, but all in a complementary way. FIA_UID.2 wants the user identified before allowing any other operations and FIA_UAU.2 wants the user authenticated before allowing any other operations. FIA_SOS.1 defines the strength of the authentication. FIA_UAU.7 requires that feedback from authentication input be obscured. FIA_ATD.1 specifies the security attributes belonging to individual users. FIA_AFL.1 specifies that the administrator and user accounts will be disabled if an administrator configured maximum number of unsuccessful authentication attempts is surpassed.

The management requirements (FMT_) are related to many of the other requirements. FMT_MTD.1 specifies the management of TSF Data according to assigned roles. The roles that are listed in Table 5-2 are also defined in FMT_SMR.1. FMT_REV.1 specifies that, TSF will restrict the ability to revoke security attributes of the users to administrator. Since the system data that is collected by the TOE from the target network is TSF Data, the FDP_ACC.1 and FDP_ACF.1 requirements have been left out of the ST. FMT_MTD.1 describes the management of the TSF Data. In many cases, the other functions will enforce the settings made through the management functions. Installation functions (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions.

VUL_SDC_EXP.1 makes sure the TOE is able to collect the specified system data from the devices on the target network. VUL_ARP_EXP.1 requires the TSF to send a notification via e-mail upon detection of a potential security violation. VUL_DRS_EXP.1 makes sure the TOE is able to report collected system data using automatically generated reports.

8.2.7 Explicitly Stated Requirements Rationale

A refinement that adds additional detail and narrows the scope has to be iterated to meet the original scope of the SFR. FAU_STG_EXP.1, FPT_RVM_EXP.1 and FPT_SEP_EXP.1 had to be explicitly stated because it provides partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. Since the iteration of FAU_STG_EXP.1, FPT_RVM_EXP.1 and FPT_SEP_EXP.1 span both the TOE requirements and IT Environment, it must be explicitly stated. VUL_SDC_EXP.1, VUL_ARP_EXP.1, and VUL_DRS_EXP.1 had to be explicitly stated because the CC Part 2 does not have any Vulnerability related SFRs that can describe the functions of the TOE.

8.2.8 Requirements for the IT Environment

Table 8-8 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included below the table.

Table 8-8 All Objectives for the IT Environment map to Requirements in the IT environment

Objective	Requirement for the IT Environment	Component Title
OE.AuditProtect	FAU_STG_EXP.1-2	Protected audit trail storage
OE.NonBypass	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
OE.PartialSelfProtection	FPT_SEP_EXP.1-2	TSF domain separation
OE.Time	FPT_STM.1	Reliable time stamps

OE.AuditProtect: The IT environment will ensure the protection of the audit storage. OE.AuditProtect is addressed by:

- FAU_STG_EXP.1-2 Protected audit trail storage, which requires the IT environment to protect the stored records in the audit trail from unauthorized deletion and can prevent unauthorized modifications to the audit records in the audit trail. The TOE relies on the underlying OS, Relational Database to protect the audit trail storage.

OE.NonBypass: The IT environment will ensure that its protection mechanisms cannot be bypassed. OE.NonBypass is addressed by:

- FPT_RVM_EXP.1-2 Non-bypassability of the TSP, which requires that the IT Environment ensures the OS enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

OE.PartialSelfProtection: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. OE.PartialSelfProtection is addressed by:

- FPT_SEP_EXP.1-2 TSF domain separation, which requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment will enforce separation between security domains of subjects in the Operating System's Scope of Control.

OE.Time The underlying operating system will provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that time stamps be provided by the IT environment.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-9 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-9 Mapping of Functional Requirements to TOE Summary Specification

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
1.	FAU_GEN.1	Audit data generation	AU-1	Specifies the types of events to be audited and the information to be recorded in an audit record.
2.	FAU_SAR.1	Audit review	AU-2	Specifies who has the capability to read information from the audit records.
3.	FAU_SAR.2	Restricted audit review	AU-3	Specifies that only specific user accounts have read access to the audit records.
4.	FAU_SAR.3	Selectable audit review	AU-4	Specifies that the TOE provides the ability to perform searches of the audit data, based on various criteria.
5.	FAU_STG_EXP.1	Protected audit trail storage	AU-5	Specifies that the TOE is able to protect the stored audit records from unauthorized deletion and prevent modifications to the audit records.
6.	FIA_AFL.1	Authentication failure handling	IA-1	Specifies that the TOE detects when an administrator configured maximum number of unsuccessful authentication attempts occur related to administrator and user login attempts. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE disables the administrator and user accounts until the account is reactivated by a user with Admin permission.
7.	FIA_ATD.1	User attribute definition	IA-2	Specifies the security attributes maintained for each user account.
8.	FIA_SOS.1	Verification of secrets	IA-3	Specifies that user account passwords meet the rules of the password policy.
9.	FIA_UAU.2	User authentication before any action	IA-4	Specifies that the TOE requires each user account to successfully authenticate with a password before being allowed any other actions.
10.	FIA_UAU.7	Protected authentication feedback	IA-5	Specifies that the TOE displays only the typed in user account name and asterisks for the password during password authentication.
11.	FIA_UID.2	User identification before any action	IA-6	Specifies that the TOE requires each user to identify himself/herself before being allowed to perform any other actions.

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
12.	FMT_MTD.1	Management of TSF data	SM-1	Specifies that the TOE restricts the ability to access data.
13.	FMT_REV.1	Revocation	SM-2	
14.	FMT_SMR.1	Security roles	SM-3	Specifies the roles maintained in the TOE.
15.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	MUA-1	Specifies that the StillSecure VAM's security policy enforcement functions are invoked and succeed before each function is allowed to proceed.
16.	FPT_SEP_EXP.1-1	TSF domain separation	MUA-2	Specifies that the StillSecure VAM maintains a security domain for its own execution and enforces separation between security domains of the users.
17.	VUL_SDC_EXP.1	System data collection	VUL-1	Specifies that the TOE collects its own system data directly from the target network
18.	VUL_ARP_EXP.1	Security alarms	VUL-2	Specifies the TSF will send a notification via e-mail upon detection of a potential security violation.
19.	VUL_DRS_EXP.1	Data Reporting	VUL-3	Specifies that the TOE is able to generate reports on collected system data.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-10.

Table 8-10 Assurance Measures Rationale

Component	Evidence Requirements	How Satisfied	Rationale
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	StillSecure VAM Configuration Management Capabilities (rev-f)	• CM Proof - Shows the CM system is being used. • Configuration Item List(s) - is comprised of a list of the source code files and version numbers - is comprised of a list of design documents with version numbers - is comprised of test documents with version numbers - user and administrator documentation with version numbers
ADO_DEL.1	Delivery Procedures	StillSecure VAM Delivery Procedures (rev-e)	Provides a description of all procedures that are necessary to maintain security when distributing TOE software to the user's site. - Applicable across all phases of delivery from packaging, storage, distribution
ADO_IGS.1	Installation, generation, and start-up procedures	StillSecure VAM 5.5 Installation Guide (rev-a) StillSecure VAM 5.5 Users Guide (rev-c) StillSecure VAM QuickStart card	Provides detailed instructions on how to install the TOE.
ADV_FSP.1	Functional Specification	StillSecure VAM Functional Specification (rev-l)	Provides rationale that the TSF is fully represented Describes the TSF interfaces and TOE functionality
ADV_HLD.1	High-Level Design	StillSecure VAM High Level Design (rev-i)	Describes the TOE subsystems and their associated security functionality

Component	Evidence Requirements	How Satisfied	Rationale
ADV_RCR.1	Representation Correspondence	StillSecure VAM Representation Correspondence (rev-i)	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. Functional specification and high-level design.
AGD_ADM.1	Administrator Guidance	StillSecure VAM 5.5 Installation Guide (rev-a), June 23, 2006 StillSecure VAM 5.5 Users' Guide (rev-c), October 27, 2006	Describes how to administer the TOE securely.
AGD_USR.1	User Guidance	StillSecure VAM 5.5 Installation Guide (rev-a), June 23, 2006 StillSecure VAM 5.5 Users' Guide (rev-c), October 27, 2006	Describes the secure use of the TOE.
ATE_COV.1	Test Coverage Analysis	StillSecure VAM Test Coverage Analysis V1.0	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_FUN.1	Test Documentation	StillSecure VAM Test Plan V0.1 StillSecure VAM Test Cases V2.1	Test documentation includes test plans and procedures and expected and actual results.
ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
AVA_SOF.1	SOF Analysis	StillSecure VAM SOF V0.1	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	Vulnerability Analysis	StillSecure VAM Vulnerability Report V1.1	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.