SentinelOne™

Singularity Complete

Security Target

Version 1.7

December 2022

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Description
0.1	20 June 2021	Initial draft for client review.
0.2	7 October 2021	Updated client comments. 2nd draft for client review. Initial draft for evaluation.
1.0	19 November 2021	Addressed evaluator ORs.
1.1	23 November 2021	Addressed evaluator ORs.
1.2	7 March 2022	Modified for EAL updates.
1.3	11 March 2022	Addressed evaluator ORs.
1.4	10 May 2022	Addressed ORs.
1.5	21 July 2022	Updated TOE version and evaluated platforms.
1.6	13 October 2022	Updated macOS endpoint version.
1.7	8 December 2022	Addressed ORs.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the SentinelOne Singularity Complete Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE components work together to provide a next-generation endpoint security platform for threat management and response.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	SentinelOne Singularity Complete (Version S, Build #30) See section 2.4 for software versions and build numbers.
Security Target	SentinelOne Singularity Complete Security Target, v1.7

1.3 Conformance Claims

3 This ST supports the following conformance claims:

- CC version 3.1 Release 5
- CC Part 2 extended
- CC Part 3 conformant
- EAL 2+ ALC_FLR.2

1.4 Terminology

Table 2: Terminology

Term	Definition
AI	Artificial Intelligence
BT	Bluetooth
CC	Common Criteria
CIDR	Classless Inter-Domain Routing
DB	Database
EAL	Evaluation Assurance Level
Endpoint	Host on the network protected by SentinelOne.
Endpoint User	User of an endpoint system.

Term	Definition
EPP	Endpoint Protection Platform
Feature Extraction	Is the process of identifying different components of a file. For example, identifying the file imports debugger functions, kernel exceptions, etc.
Malware	A harmful program that infiltrates a user’s system. Computer viruses, worms, spyware and Trojans are common malware.
ML	Machine Learning
PP	Protection Profile
RBAC	Role Based Access Control
Remote Memory	Refers to cross process memory operations on a single endpoint.
SaaS	Software as a Service
SFP	Security Function Policy
ST	Security Target
S1	SentinelOne
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
XDR	Extended Detection and Response
2FA	Two-Factor Authentication

2 TOE Description

2.1 Type

4 The TOE is an endpoint security platform that provides a single integrated management server and agent to efficiently operate and manage multiple endpoint security solutions. Using advanced Artificial Intelligence (AI), the TOE provides Malware detection and mitigation and external device discovery and control.

2.2 Usage

5 The TOE includes the components outlined in red in Figure 1, which are used as follows:

- **SentinelOne Singularity Management Console.** SentinelOne Singularity Management Console is the front-end interface to efficiently operate and manage the Singularity XDR Platform endpoint security solution. Singularity Management Console provides a web-based user interface for TOE administration, definition of policies, and review of a configurable security dashboard.
- **SentinelOne Singularity Agent.** The SentinelOne Singularity Agent, installed on endpoints, is used to facilitate the security solution by collecting endpoint data and enforcing protection and response policies. It provides connectivity between the protected endpoints and the management server.

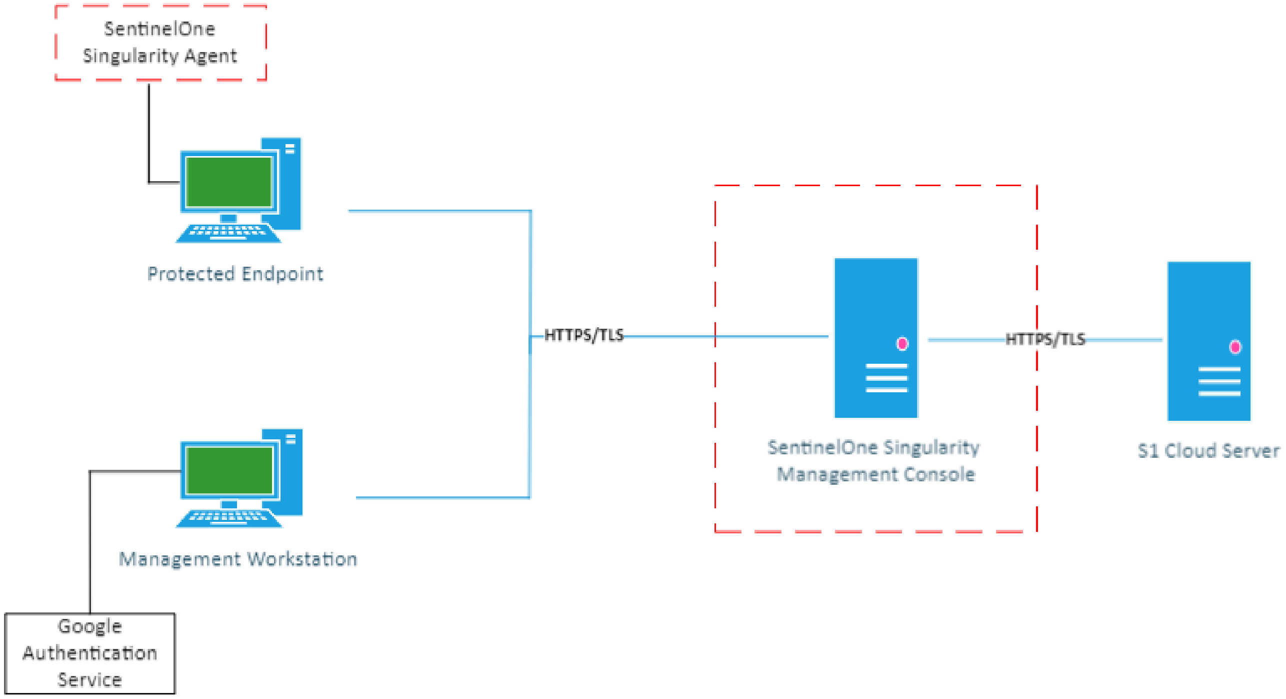
SentinelOne Singularity Agent
Protected Endpoint
HTTPS/TLS
HTTPS/TLS
SentinelOne Singularity Management Console
S1 Cloud Server
Management Workstation
Google Authentication Service

Figure 1: TOE components

2.3 Security Functions

6 The TOE provides the following security functions:

- **Secure Management.** The TOE enables secure management of its functions and endpoint security solutions via:
  - i) Identification and authentication of administrative users
  - ii) Role Based Access Control (RBAC)
  - iii) Audit of management actions and security related events
  - iv) Management of Agents, policies, and mitigation actions
- **Security Dashboard.** TOE administrators can view the threat landscape, agent information and statistics via configurable dashboards.
- **Malware Detection & Response.** The malware detection and response component provides the following detection and response functionality:

  Detection
  - i) AI/ML-based feature extraction and static file analysis
  - ii) Signature-based malware detection
  - iii) Reputation-based malware detection
  - iv) Behavior-based attack detection

  Response
  - i) Process termination
  - ii) Quarantine and/or deletion of infected files
  - iii) File and system restoration
  - iv) Network quarantine
  - v) Blacklisting
- **Device Control**. The Device Control TOE component provides the following external device control functionality:
  - i) Device identification
  - ii) Apply Block and Allow policy enforcement for BT devices
  - iii) Apply Block, Read Only and Read/Write rules for USB devices
- **Protected Communications**. The TOE protects communications between remote administrators and the management server, between the management server and endpoint agents, and between the management server and the S1 cloud server.

2.4 Physical Scope

7 The physical boundary of the TOE is the SentinelOne Singularity Complete software executing on supported non-TOE operating systems as follows:

- Singularity Complete Management Console (Version S, Build #30)
  i) Ubuntu 18.04
- Linux Sentinel Agent 22.1 GA (Build 22.1.2.7):
  i) RHEL 8.3
  ii) Ubuntu 20.04
  iii) Amazon Linux 2 (Kernel version 4.14)
  iv) SLES 15.4.12.14-150.58-default
- Windows Sentinel Agent 21.7.5 SP2 (Build 21.7.5.1080):
  i) Windows 10
  ii) Windows Server 2019
  iii) Windows Server 2012R2
- macOS Sentinel Agent 21.12.2 GA (Build 21.12.2.6003):
  i) macOS 11.6

8 Once registered with SentinelOne, customers are provided access to the support portal and a file share, where all TOE software components may be downloaded. The following files must be downloaded in the evaluated configuration:

Management Console: sentinel_mgmt_S_GA_SP2_30_UBUNTU_RH.tar.gz

Linux Sentinel Agent: SentinelAgent_Linux_22_1_2_7_x86_64-release-22.1.2.rpm/deb

(Note: .deb files are for Ubuntu Agent distributions and .rpm are for all other Linux platforms)

Windows Sentinel Agent: SentinelInstaller-x64_windows_64bit_v21_7_5_1080.exe

macOS Sentinel Agent: Sentinel-Release-21-12-2-6003_macos_v21_12_2_6003.pkg

9 The TOE is installed and configured at the customer site by SentinelOne Support personnel.

2.4.1 Minimum Hardware Requirements

10 The following table identifies the minimum hardware requirements for the TOE components in the evaluated configuration:

Table 3: Minimum Hardware Requirements

Component	Minimum Hardware Requirement
Management Console	CPU: 4 Cores Memory: 8GB IOPS: 1K Disk Space: 500GB
Windows Agent	• 1 GHz CPU • 1 GB of RAM • 2 GB free disk space
Linux Agent	• 2 GHz Dual-core CPU • 4 GB of RAM • 25 GB free disk space
macOS Agent	• 1 GHz CPU • 1 GB of RAM • 2 GB free disk space

2.4.2 Guidance Documents

11 The TOE includes the following guidance documents:

- SentinelOne Singularity Complete Common Criteria Guide, v1.4
  - PDF available upon customer request.
- SentinelOne Singularity Online Help
  - Available in HTML delivered with the TOE and accessed via the management console.

2.4.3 Non-TOE Components

12 The TOE requires the following components in the environment:

- **Management Workstation**. Workstation with internet access required to access and manage the TOE.
- **S1 Cloud Server**. Malware analysis server (provided by SentinelOne).
- **Authenticator Service.** Google Authentication Service required for two-factor authentication (2FA).
- **Supported Operating Systems.** The supported OS software identified in section 2.4 running on general purpose hardware.

2.5 Logical Scope

13 The logical scope of the TOE comprises the security functions defined in section 2.3.

2.5.1 Excluded Functions

14 The following functions are outside of the logical TOE scope (and have not been evaluated):

- Firewall Control
- Agent Proxying
- Binary Vault
- Singularity Marketplace
- Cloud (SaaS) Deployment
- Use of Active Directory, LDAP, and SSO authentication

2.5.2 Excluded Interfaces

15 The following interfaces are excluded from the evaluated configuration:

- **Remote Shell**. The Remote Shell provides remote script execution and allows authorized administrators to run scripts to collect data and respond to events on endpoints remotely. Remote shell is disabled by default and can only be enabled by an administrator assigned the Global role. This feature must first be enabled Globally, and then again enabled for individual users. It is not used in the evaluated configuration.

3 Security Problem Definition

3.1 Threats

Table 4: Threats

Identifier	Description
T.MALWARE	Attackers may compromise an endpoint via malware.
T.APPLICATION	Attackers may compromise an endpoint by executing malicious software.
T.APT	Attackers use advanced techniques and exploits to affect a prolonged compromise of an endpoint.
T.DEVICE	Malicious files may breach and compromise an endpoint through physical device access.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.MGMT	Attackers compromise or disable the TOE via its management interfaces.

3.2 Organizational Security Policies

Table 5: Organizational Security Policies

Identifier	Description
OSP.DASHBOARD	Administrators shall make use of the configurable TOE dashboard to review security relevant analytical data and take appropriate action.

3.3 Assumptions

Table 6: Assumptions

Identifier	Description
A.ADMIN	Administrators are trusted and follow guidance.
A.AUTH	The authentication service in the IT environment will provide two-factor authentication codes for administrators.
A.CLOUD	The S1 Cloud Server in the IT environment will provide malware analysis services for TOE submitted artifacts.
A.USER	Non-administrative users of endpoints are trusted and follow guidance.
A.PHYSICAL	TOE components are protected from unauthorized physical access.
A.TIME	The IT environment will provide a reliable time source.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 7: Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	TOE administrators shall be trustworthy and shall follow guidance.
OE.AUTH	The authentication service in the IT environment shall provide two-factor authentication codes for administrators.
OE.CLOUD	The S1 Cloud Server in the IT environment shall provide malware analysis services for TOE submitted artifacts.
OE.USERS	Non-administrative users of endpoints shall be trustworthy and follow guidance.
OE.PHYSICAL	TOE components shall be protected from unauthorized physical access.
OE.TIME	The IT environment shall provide a reliable time source.

4.2 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
O.APPLICATION	The TOE shall collect and manage a filesystem inventory of protected endpoints and allow or deny execution of files.
O.APT	The TOE shall detect and facilitate analysis of suspicious behaviour on protected endpoints and allow administrators to specify response actions to be taken.
O.DEVICE	The TOE shall manage the access and control of external devices connecting to endpoints.
O.MGMT	The TOE shall authenticate administrators, provide management capabilities, restrict access according to role and record a log of their actions.
O.MALWARE	The TOE shall detect and respond to known and suspected malware on protected endpoints.
O.DASHBOARD	The TOE shall provide a configurable dashboard that allows administrators to review security relevant analytical data.
O.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators, between the management server and agents, and between the management server and the S1 cloud server.

5 Security Requirements

5.1 Conventions

16 This document uses the following font conventions to identify the operations defined by the CC:

- **Assignment.** Indicated with italicized text.
- **Refinement.** Indicated with bold text and strikethroughs.
- **Selection.** Indicated with underlined text.
- **Assignment within a Selection:** Indicated with italicized and underlined text.
- **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

17 Table 9 identifies the extended components which are incorporated into this ST.

Table 9: Extended Components

Class / Component	Title	Rationale
Class: FAM	Anti-Malware	No existing CC Part 2 classes or components address anti-malware requirements.
FAM_ACT.1	Anti-Malware Actions	
FAM_SCN.1	Anti-Malware Scanning	
Class: FDC	External Device Control	No existing CC Part 2 classes or components address IPS requirements.
FDC_DET.1	External Device Detect	
FDC_ACT.1	External Device Actions	
Class: FIA	Identification & Authentication	No existing CC Part 2 classes or components address X.509 certificate requirements.
FIA_X509.1	X509 Certificate Validation	
FIA_X509.2	X509 Certificate Authentication	

5.2.1 Anti-Malware Actions (FAM_ACT)

5.2.1.1 Family Behavior

18 This family defines requirements for actions to be taken on malware detection.

5.2.1.2 Component Leveling

19 FAM_ACT.1 Addresses actions to be taken on malware detection.

5.2.1.3 Management: FAM_ACT.1

20 The following actions could be considered for the management functions in FMT:

- Configuration of actions.

5.2.1.4 Audit: FAM_ACT.1

21 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Action taken in response to detection of malware.

FAM_ACT.1 Anti-Malware Actions

Hierarchical to: No other components.

Dependencies: FAM_SCN.1

FAM_ACT.1.1 Upon detection of malware, the TSF shall: [assignment: *list of actions*].

5.2.2 Anti-Malware Scanning (FAM_SCN)

5.2.2.1 Family Behavior

22 This family defines requirements for malware scanning.

5.2.2.2 Component Leveling

23 FAM_SCN.1 Addresses malware scanning.

5.2.2.3 Management: FAM_SCN.1

24 The following actions could be considered for the management functions in FMT:

- Configuration of scanning parameters.

5.2.2.4 Audit: FAM_SCN.1

25 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- None

FAM_SCN.1 Anti-Malware Scanning

Hierarchical to: No other components.

Dependencies: No dependencies.

FAM_SCN.1.1 The TSF shall perform local filesystem scans for malware based upon [selection: known signatures, reputation, behavior, [assignment: *other file analysis types*]].

FAM_SCN.1.2 The TSF shall scan all system files when they are created, updated, or executed.

5.2.3 External Device Detect (FDC_DET)

5.2.3.1 Family Behavior

26 This family defines requirements for external device detection.

5.2.3.2 Component Leveling

27 FDC_DET.1 Addresses the detection of external devices connecting to managed endpoints.

5.2.3.3 Management: FDC_DET.1

28 The following actions could be considered for the management functions in FMT:

- None.

5.2.3.4 Audit: FDC_DET.1

29 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- None.

FDC_DET.1 External Device Detect

Hierarchical to: No other components.

Dependencies: No dependencies.

FDC_DET.1.1 The TSF shall detect when the following types of external devices connect to a managed endpoint: [assignment: *list of external device types*].

5.2.4 External Device Actions (FDC_ACT)

5.2.4.1 Family Behavior

30 This family defines requirements for actions performed on external devices.

5.2.4.2 Component Leveling

FDC_ACT: External Device Actions
1

31 FDC_ACT.1 Addresses actions to be taken on external devices connecting to managed endpoints.

5.2.4.3 Management: FDC_ACT.1

32 The following actions could be considered for the management functions in FMT:

- Configuration of actions.

5.2.4.4 Audit: FDC_ACT.1

33 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Basic: Action taken in response to detection of an external device.

FDC_ACT.1 External Device Actions

Hierarchical to: No other components.

Dependencies: FDC_DET.1

FDC_ACT.1.1 Upon detection of an external device, the TSF shall: [assignment: *list of actions*].

5.2.5 X509 Certificate Validation (FIA_X509)

5.2.5.1 Family Behavior

34 This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules.

5.2.5.2 Component Leveling

FIA_X509: X509 Certificate Validation
1
2

35 FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the rules specified in the component.

36 FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates.

5.2.5.3 Management: FIA_X509.1, FIA_X509.2

37 The following actions could be considered for the management functions in FMT:

- None.

5.2.5.4 Audit: FIA_X509.1, FIA_X509.2

38 The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- None.

FIA_X509.1 X.509 Certificate Validation

Hierarchical to: No other components.

Dependencies: FIA_X509.2

FIA_X509.1.1 The TSF shall validate certificates in accordance with the following rules:

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certificate path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

FIA_X509.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509.2 X.509 Certificate Authentication

Hierarchical to: No other components.

Dependencies: FIA_X509.1

FIA_X509.2.1 The TSF shall use X.509v3 certificates to support authentication for [selection: DTLS, HTTPS, IPsec, TLS, SSH, [assignment: *other protocols],* no protocols], and [selection: code signing for system software updates [*assignment: other uses*], no additional uses].

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAM_ACT.1	Anti-Malware Actions
FAM_SCN.1	Anti-Malware Scanning
FDC_DET.1	External Device Detect
FDC_ACT.1	External Device Actions
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAA.4	Complex Attack Heuristics
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FIA_AFL.1	Authentication Failure Handling
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.5	Multiple Authentication Mechanisms
FIA_UID.2	User Identification Before Any Action
FIA_X509.1	X509 Certificate Validation
FIA_X509.2	X509 Certificate Authentication
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted Path

5.3.1 Anti-Malware (FAM)

FAM_ACT.1 Anti-Malware Actions

Hierarchical to: No other components.

Dependencies: FAM_SCN.1

FAM_ACT.1.1 Upon detection of malware, the TSF shall: [

- *Stop all processes related to the threat,*
- *Move the executable to a confined path and encrypt it,*
- *Delete all files and repair system changes created by the threat,*
- *Restore altered files,*
- *Block network connections to the infected endpoint,*
- *Add the threat to the Blacklist*

].

FAM_SCN.1 Anti-Malware Scanning

Hierarchical to: No other components.

Dependencies: No dependencies.

FAM_SCN.1.1 The TSF shall perform local filesystem scans for malware based upon [known signatures, reputation, behavior, [*matches against a known hash database, feature extraction, static file analysis*]].

FAM_SCN.1.2 The TSF shall scan all system files when they are created, updated, or executed.

5.3.2 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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) [*Auditable events listed in the table below*].

Event	*Additional Details*
Administrative Actions	Policy changes, Login/Logout, User Added Date, User Modified Date, User Deleted Date, Login Settings, Account Modification
Policy Updates/Events	User ID, Policy Name, Policy Details
Security Agent Events	Agent ID, Agent IP, Computer Name, Last Login User, Event Details
Malware Events	Agent ID, Agent IP, Computer Name, Malware Name, Event Details
Full Disk Scan	Agent ID, Agent IP, Computer Name, Details
Execution Control Events	Agent ID, Agent IP, Computer Name, Owner Process ID, File Name, File Path, File Hash, Provider, Signed by, File Size, Response Method, Event Details

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 (if applicable), 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, [*additional details specified in the above table*].

FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

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

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.4 Complex Attack heuristics

Hierarchical to: FAU_SAA.3 Simple attack heuristics

Dependencies: No dependencies.

FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [

- *Reconnaissance*
- *Resource Development*

- *Initial Access*
- *Execution*
- *Persistence*
- *Privilege Escalation*
- *Defense Evasion*
- *Credential Access*
- *Discovery*
- *Lateral Movement*
- *Collection*
- *Command and Control*
- *Exfiltration*
- *Impact*

] and the following signature events [

- *Suspicious system behavior*
- *Suspicious file behavior*
- *Suspicious process behavior*
- *Suspicious registry behavior*
- *Suspicious network behavior*

] that may indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.4.2 The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of [*system activity collected by agents deployed on protected endpoints*].

FAU_SAA.4.3 The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when system activity is found to match a signature event or event sequence that indicates a potential violation of the enforcement of the SFRs.

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

5.3.3 External Device Control (FDC)

FDC_DET.1 External Device Detect

Hierarchical to: No other components.

Dependencies: No dependencies.

FDC_DET.1.1 The TSF shall detect when the following types of external devices connect to a managed endpoint: [*USB Storage Device, Bluetooth Device*].

FDC_ACT.1 External Device Actions

Hierarchical to: No other components.

Dependencies: FDC_DET.1

FDC_ACT.1.1 Upon detection of an external device, the TSF shall: [

For USB Devices:

- *Allow Read and Write*
- *Allow Read Only*
- *Block*

For Bluetooth Devices:

- *Block or Allow*].

39 **Application Note**: USB device detection and actions are only supported on Windows and macOS endpoints. Bluetooth device detection and actions are only supported on Windows.

5.3.4 User Data Protection (FDP)

FDP_ACC.1 Subset Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*RBAC SFP*] on [

Subjects: Administrators

Objects: TSF Data

Operations: Configure and manage administrative accounts and agents, and anti-malware and external device policies].

FDP_ACF.1 Security Attribute Based Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute authorization

FDP_ACF.1.1 The TSF shall enforce the [*RBAC SFP*] on [

Subjects: Administrators

Subject Attributes: Role

Objects: TSF Data

Object Attributes: None].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the administrative user is able to access the TSF data and perform the operations associated with an administrative function if the role permits access to the function*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*users assigned the Admin role have full access to all TSF data*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules: [*no additional rules*]

5.3.5 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [[3]] unsuccessful authentication attempts occur related to [*management console login*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock out the user account for 30 minutes*].

FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [*password and (if configured) two-factor authentication (2FA)*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [

- *Password: valid username and password*
- *2FA: valid code must be entered*].

Application Note: A third party authentication service is used in the environment for 2FA.

FIA_UID.2 User Identification Before Any Action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

FIA_X509.1 X.509 Certificate Validation

Hierarchical to: No other components.

Dependencies: FIA_X509.2

FIA_X509.1.1 The TSF shall validate certificates in accordance with the following rules:

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certificate path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

FIA_X509.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509.2 X.509 Certificate Authentication

Hierarchical to: No other components.

Dependencies: FIA_X509.1

FIA_X509.2.1 The TSF shall use X.509v3 certificates to support authentication for [TLS], and [no additional uses].

5.3.6 Security Management (FMT)

FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*RBAC SFP*] to restrict the ability to [query, modify, delete] the security attributes [*authentication settings, administrator accounts, endpoint agents, external device control and anti-malware policies*] to [*administrative users assigned the appropriate role*].

FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*RBAC SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*authorized administrative user*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *Manage authentication settings (Management Console)*
- *Manage administrator accounts*
- *Manage agents (Agent Policy)*
- *Manage dashboard (User-defined Dashboard)*
- *Manage Blacklists*
- *Manage External Device detection and response Policies*
- *Manage Anti-Malware Policies*
- *Perform full disk scan*

].

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [

- *Admin*
- *IR Team*
- *SOC*
- *IT*
- *Viewer*
- *C-Level*
- *Endpoint User*].

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

Application Note: The Endpoint User role is an implied role applied to users of the endpoint.

5.3.7 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3.8 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*communication with the S1 Cloud Server*].

FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*TOE administration*]].

5.4 Assurance Requirements

40 The TOE security assurance requirements are summarized in Table 11 commensurate with EAL2 + (ALC_FLR.2).

Table 11: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-Enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Secure Management

41 The TOE enables secure management of its functions.

6.1.1 FAU_GEN.1

42 The TOE generates the audit events identified at FAU_GEN.1 which are stored in a local database.

6.1.2 FAU_GEN.2

43 The TOE includes user account names in audit events when applicable.

6.1.3 FAU_SAR.1

44 The TOE provides administrators with the ability to view all audit records.

6.1.4 FDP_ACC.1

45 The TOE enforces role-based access control on administrative access to security functions.

6.1.5 FDP_ACF.1

46 The TOE enforces role-based access control on administrative access to security functions.

6.1.6 FIA_AFL.1

47 By default, if a user attempts to log in to the Management Console unsuccessfully 3 times, the user is locked out of the Console for 30 minutes. Unsuccessful authentication encompasses incorrect username/password combinations, incorrect 2FA code, and timeout of 2FA code usage.

6.1.7 FIA_UAU.2

48 TOE users must be authenticated before any administrative functions become available. Users are authenticated by a username and password, and optionally a third party generated authentication code. Google Authentication Services are used in the evaluated configuration.

6.1.8 FIA_UAU.5

49 In addition to username and password authentication, the TOE can be configured to use an external authentication service. When configured, 2FA works as follows:

- User authenticates with username and password;
- TOE requests a 2FA code (generated by the authentication service);
- User must enter the 2FA code (within the allotted timeframe provided by the service) to successfully complete authentication.

6.1.9 FIA_UID.2

50 TOE users are identified by a username at login.

6.1.10 FMT_MSA.1

51 The TOE enforces role-based access control on administrative access to security functions. A description of access capabilities for each role are described in sections 6.1.12 and 6.1.13 below. A description of the user management permissions is provided in the online help under the *Role-Based Access Control* section.

6.1.11 FMT_MSA.3

52 The RBAC SFP is considered restrictive by default in that administrators do not have access to security functionality unless assigned a role.

6.1.12 FMT_SMF.1

53 The TOE management capabilities include:

- Managing authentication settings (Management Console)
- Managing administrator accounts
- Managing agents (Agent Policy)
- Managing dashboard (User-defined Dashboard)
- Managing Blacklists
- Managing External Device detection and response policies
- Managing Anti-Malware Policies
- Performing full disk scan

6.1.13 FMT_SMR.1

54 The TOE enforces role-based access control as follows:

- **Admin.** Use of all Management Console features.
- **IR Team.** Respond to threats, investigate breaches, and create incident response and root cause analysis reports.
- **SOC.** Mitigate and remediate threats and isolate endpoints.
- **IT.** Edit exclusions, blacklist items, and configure settings such as Notifications and Device Control.
- **C-Level.** Create, edit, and delete reports.
- **Viewer.** Can not run any actions.

55 An implied role of **Endpoint User** is also defined. This role applies to users of protected endpoints.

6.2 Security Dashboard

56 TOE administrators can view threat information and statistics via a configurable dashboard.

6.2.1 FMT_SMF.1

57 The TOE provides the management capability for a User-Defined Dashboard – to create a custom dashboard for each administrator account by adding and removing widgets. In a user-defined dashboard, statuses are displayed by category. The dashboard is able to display information such as:

- Threats: Types of threats, status, actions, time frame, etc.
- Endpoints: Endpoint agents by category (OS, Health, etc.).
- Applications: Applications by risk level.

6.3 Malware Detection & Response

58 The malware detection and response TOE component provides the functionality as described in the following sections.

6.3.1 FAM_ACT.1

59 The Malware Detection and Mitigation Policy can be set to “Protect” or “Detect”. If set to Detect, the TOE does not perform any mitigation actions and only sends alerts. If set to Protect, the TOE automatically performs the following mitigation actions when malware is detected:

- Stops all processes related to the threat.
- Moves the executable to a confined path and encrypts it.
- Deletes all files and repairs system changes created by the threat.
- Restores altered files.
- Blocks network connections to the infected endpoint.
- Adds the threat to the Blacklist (if not already on the list).

60 Mitigation actions are determined by the Protect Level configured for the policy. Administrators have the option to Kill & Quarantine, Remediate, and Rollback. By default, the Protect Level is hardcoded to Kill & Quarantine. If the policy Protect Level is set to Remediate or Rollback, and Threats is set to Protect, the Agent automatically implements the full Response Plan. The following responses can be automated in the policy:

- **Kill** – Stops all processes related to the threat.
- **Quarantine** – Moves the threat and the executable it created or changed to a confined path and encrypts them.
- **Remediate** – Deletes all files and system changes created by the threat.
- **Rollback** – Restores the endpoint to a saved VSS snapshot, undoing the changes made by the process and its associated assets.
- **Disconnect from Network** – The Agent can communicate only with the Management Console. The endpoint cannot communicate with other components on the network.

61 **Note**: The Rollback feature is only available on Windows Agents.

6.3.2 FAM_SCN.1

62 When the SentinelOne Agent is installed on an endpoint machine, the TOE performs a full disk scan for any known malware using the reputation engine, or any file that is determined as Suspicious or Malicious by the static AI engines. The static AI engines then monitor for new or changed files.

63 The TOE maintains both a Local and Global blacklist of all files that are identified as malicious or suspicious. Local blacklists are housed by the individual endpoint. The Global blacklist is stored and maintained on the management console. Files on the blacklist are defined by a SHA1 hash and can be created manually, or automatically via the Malware Detection feature.

64 When a user attempts to write or execute a file on a managed endpoint, the TOE performs a hash-based analysis and checks to determine if the file is on the local blacklist. If the file is not on the local blacklist, the Agent sends the hash to the management server. The management server then sends the hash to the S1 cloud server to perform additional malware analysis. If the analysis determines that the hash/file is suspicious or malicious, the TOE adds the hash/file to the Global blacklist. When the Global blacklist is updated, the management server automatically pushes local blacklist updates to the Agents.

65 If, under either scenario described above, the analysis determines that the file is not suspicious or on the blacklist, the TOE will allow execution of the file. If the analysis determines that the file is suspicious or on the blacklist, the TOE will block the file from executing.

66 The following malware detection methods are used by the TOE:

- **Signature based detection.** Uses patterns and hash values to detect known malware.
- **Reputation based detection.** Uses reputation scores to detect objects that are reputed to be malware.
- **Static AI based detection.** Uses an ML-based file scanner to detect unknown malware without a specific signature.
- **Behavior based detection.** Uses observation of suspicious file/process behavior patterns to detect objects that behave like malware.

6.4 Protected Communications

6.4.1 FPT_ITT.1

67 Communications between the Singularity Management Server and the endpoint agents are protected using TLSv1.2. The following cipher suites are supported in the evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

6.4.2 FTP_ITC.1

68 Communications between the Management Server and the S1 Cloud Server are protected using TLSv1.2 and TLSv1.3. The TOE periodically polls the S1 cloud server using HTTPS. The following cipher suites are supported in the evaluated configuration:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

6.4.3 FTP_TRP.1

69 Communications between the Management Server and remote administrators are protected using TLSv1.2. The supported cipher suites are identified in section 6.4.1.

6.4.4 FIA_X509.1 and FIA_X509.2

70 The TOE performs X.509 certificate validation as follows:

a) TLS client validation of server certificates (management server/agent and management server/S1 cloud communications);

b) When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates (such as the web server certificate presented by the TOE TLS web GUI).

71 Management Server X.509 certificates are verified and signed by a trusted CA before being loaded onto the TOE.

72 When the X.509 certificate is loaded onto the TOE, the TOE validates the following:

a) The certification path terminates with a trusted CA certificate;

b) All CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

73 The Singularity Agent performs TLS client validation of the management server X.509 certificate, checking for the following characteristics:

a) The certification path terminates with a trusted CA certificate;

b) All CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

74 The TOE does not support X.509 mutual authentication. Instead, a token is generated by the management console and passed as a parameter to the endpoint agent during registration. Once configured, the management console verifies the registration token passed by the agent after the TLS handshake is completed.

75 The management server performs TLS client validation of the S1 cloud server X.509 certificate, checking for the following characteristics:

a) The certification path terminates with a trusted CA certificate;

b) All CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

76 The management console, acting as the TLS client, does not present a client certificate. Instead, a cloud token provided by SentinelOne is added to the management console during installation. Once configured, the S1 cloud server verifies the cloud token passed by the management console after the TLS handshake is completed.

77 The TOE maintains a trust store where all certificates are stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope.

6.5 Threat Detection & Response

78 The TOE threat detection and response component provides the behavioral threat detection and response functionality described in the following sections.

6.5.1 FAU_SAA.4

79 The TOE detects malicious behavior based on the monitoring of the following events:

- Image execution:
  - i) Process Creation
  - ii) Module load into running processes
  - iii) Driver load
- Threads:
  - i) Every new thread creation
  - ii) Every “hijack” of existing thread
- File creation and modification:
  - i) Any modification of existing file
  - ii) Any creation of new files on the disk
- Registry key and value – creation and modification:
  - i) The creation and modification of a registry key under a monitored path
  - ii) The creation and modification of a registry value under a monitored path
- Network: TCP connection
  - i) Every TCP connection will be monitored with the used Ips and Ports
- Memory operations:
  - i) Every remote memory allocation
  - ii) Every remote memory write
  - iii) Every remote memory free
  - iv) Memory injections
- RPC calls:
  - i) Every relevant RPC call is monitored in order to do a proper event source attribution to system operations (WMI, COM objects etc)

80 The TOE uses the monitored events mentioned above in order to:

- Create a stateful model of the operating system and running objects
- Attribute every monitored event correctly
- Trigger on malicious events raised from the native monitoring described above. For example, writing a new registry key under the “run key” would trigger a persistence detection.

6.6 External Device Control

6.6.1 FDC_DET.1

81 The TOE can detect when external USB and Bluetooth devices connect to a managed endpoint.

6.6.2 FDC_ACT.1

82 The TOE can block and allow external USB and Bluetooth devices from connecting to a managed endpoint. Authorized administrators can create rules to define the Interface (type of device – USB or Bluetooth), Rule Type, Scope, and Action. In the evaluated configuration, the following rule parameters are supported:

83 For Bluetooth Devices:

- Interface – Bluetooth
- Rule Type – Device Hardware
- Scope – Global
- Action – Allow or Block

84 For USB Devices:

- Interface – USB
- Rule Type – Device Class
- Scope – Global
- Action – Allow Read & Write, Allow Read Only, Block

85 **Note**: USB device detection and actions are only supported on Windows and macOS endpoints. Bluetooth device detection and actions are only supported on Windows.

7 Rationale

7.1 Security Objectives Rationale

86 Table 12 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 12: Security Objectives Mapping

	T.APPLICATION	T.APT	T.DEVICE	T.EAVES	T.MALWARE	T.MGMT	OSP.DASHBOARD	A.ADMIN	A.AUTH	A.CLOUD	A.USER	A.PHYSICAL	A.TIME
O.APPLICATION	X												
O.APT		X											
O.DEVICE			X										
O.MALWARE					X								
O.MGMT						X							
O.PROTCOMMS				X									
O.DASHBOARD							X						
OE.ADMIN								X					
OE.AUTH									X				
OE.CLOUD										X			
OE.USERS											X		
OE.PHYSICAL												X	
OE.TIME													X

87

88 Table 13 provides the justification to show that the security objectives are suitable to address the security problem.

Table 13: Suitability of Security Objectives

Element	Justification
T.APPLICATION	**O.APPLICATION.** Mitigates this threat by requiring that the TOE collect an inventory of executable files on managed endpoints and allow or deny the running of these files.
T.APT	**O.APT.** Mitigates this threat by requiring that the TOE detect suspicious behaviour, which is indicative of a compromise by attackers, and allowing further analysis and response.
T.DEVICE	**O.DEVICE.** Mitigates this threat by requiring that the TOE detect connected external devices and apply allow and block policies.
T.EAVES	**O.PROTCOMMS.** Mitigates this threat by requiring that the TOE protect communications for remote administrators, between the management server and agents, and between the management server the S1 cloud server.
T.MALWARE	**O.MALWARE.** Mitigates the threat of malware by requiring that the TOE detect and respond to known and suspected malware.
T.MGMT	**O.MGMT.** Mitigates this threat by preventing unauthorized access via authentication, limiting access to functions based on role and auditing administrative actions to allow any unauthorized actions to be detected.
OSP.DASHBOARD	**O.DASHBOARD.** Upholds the stated policy by requiring the TOE to implement the required functionality.
A.ADMIN	**OE.ADMIN.** Upholds the assumption by restating it as an objective for the operational environment.
A.AUTH	**OE.AUTH.** Upholds the assumption by restating it as an objective for the operational environment.
A.CLOUD	**OE.CLOUD.** Upholds the assumption by restating it as an objective for the operational environment.
A.USER	**OE.USER.** Upholds the assumption by restating it as an objective for the operational environment.
A.PHYSICAL	**OE.PHYSICAL.** Upholds the assumption by restating it as an objective for the operational environment.
A.TIME	**OE.TIME.** Upholds the assumption by restating it as an objective for the operational environment.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

89 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 14: Security Requirements Mapping

	O.APPLICATION	O.APT	O.DEVICE	O.MALWARE	O.MGMT	O.DASHBOARD	O.PROTCOMMS
FAM_ACT.1	X	X		X			
FAM_SCN.1	X	X		X			
FDC_DET.1			X				
FDC_ACT.1			X				
FAU_GEN.1					X		
FAU_GEN.2					X		
FAU_SAA.4		X					
FAU_SAR.1					X		
FDP_ACC.1					X		
FDP_ACF.1					X		
FIA_AFL.1					X		
FIA_UAU.2					X		
FIA_UAU.5					X		
FIA_UID.2					X		
FIA_X509.1							X
FIA_X509.2							X
FMT_MSA.1					X		
FMT_MSA.3					X		
FMT_SMF.1		X			X	X	
FMT_SMR.1					X		

	O.APPLICATION	O.APT	O.DEVICE	O.MALWARE	O.MGMT	O.DASHBOARD	O.PROTCOMMS
FPT_ITT.1							X
FTP_ITC.1							X
FTP_TRP.1							X

Table 15: Suitability of SFRs

Objectives	SFRs
O.APPLICATION	**FAM_ACT.1** requires application response actions (respond). **FAM_SCN.1** requires scanning of filesystem inventory.
O.APT	**FAU_SAA.4** requires behavioral and system event detection capabilities (detect). **FAM_ACT.1** requires application response actions (respond) **FAM_SCN.1** requires scanning of filesystem inventory. **FMT_SMR.1** provides for endpoint policy management.
O.DEVICE	**FDC_DET.1** requires the detection of external devices connecting to managed endpoints. **FDC_ACT.1** requires external device response actions.
O.MALWARE	**FAM_ACT.1** requires malware response actions (respond). **FAM_SCN.1** requires scanning for malware (detect).

Objectives	SFRs
O.MGMT	**FAU_GEN.1** requires auditing of security relevant events. **FAU_GEN.2** requires inclusion of identity in audit events. **FAU_SAR.1** requires the ability to review the audit records. **FDP_ACC.1** requires access rules to management functions and data. **FDP_ACF.1** requires access rules to management functions and data. **FIA_AFL.1** locks user accounts for unsuccessful authentication attempts. **FIA_UAU.2** requires authentication of users. **FIA_UAU.5** requires multiple authentication mechanisms. **FIA_UID.2** requires identification of users. **FMT_MSA.1** requires management of security attributes. **FMT_MSA.3** requires restrictive default values for security attributes. **FMT_SMF.1** requires specification of management functions. **FMT_SMR.1** requires specification of security roles.
O.DASHBOARD	**FMT_SMF.1** requires user-defined dashboard capability.
O.PROTCOMMS	**FIA_X509.1** requires the validation of X.509 certificates used for TLS. **FIA_X509.2** requires the use of X.509 certificates for TLS authentication. **FPT_ITT.1** requires encrypted communications between the management server and endpoint agents. **FTP_ITC.1** requires encrypted communications between the management server and the S1 cloud server. **FTP_TRP.1** requires encrypted communications for remote administration.

Table 16: Dependency Rationale

SFR	Dependency	Rationale
FAM_ACT.1	FAM_SCN.1	Met
FAM_SCN.1	None.	-
FDC_DET.1	None.	
FDC_ACT.1	FDC_DET.1	Met
FAU_GEN.1	FPT_STM.1	The TOE makes use of the underlying operating system for time stamps.

SFR	Dependency	Rationale
FAU_GEN.2	FAU_GEN.1	Met
	FIA_UID.1	Met by FIA_UID.2
FAU_SAA.4	None.	-
FAU_SAR.1	FAU_GEN.1	Met
FDP_ACC.1	FDP_ACF.1	Met
FDP_ACF.1	FDP_ACC.1	Met
	FMT_MSA.3	Met
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.2
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2
FIA_UAU.5	None	-
FIA_UID.2	None	-
FIA_X509.1	FIA_X509.2	Met
FIA_X509.2	FIA_X509.1	Met
FMT_MSA.1	FDP_ACC.1, or FDP_IFC.1	Met by FDP_ACC.1
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.3	FMT_MSA.1	Met
	FMT_SMR.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_ITT.1	None	-
FTP_ITC.1	None	-
FTP_TRP.1	None	-