Invincea, Inc.

Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0

Security Target

April 2015

Document prepared by

Document History

Version	Date	Author	Description
1.0	7 March 2014	L Turner	Initial release for evaluation.
1.1	6 May 2014	L Turner	Updates to align with development documents.
1.2	13 May 2014	L Turner	Updates to address OR1.
1.3	14 May 2014	L Turner	Additional updates to address OR1.
1.4	23 June 2014	L Turner	Updates to address certifier OR1.
1.5	12 August 2014	L Turner	Remove host based firewall and proxy support.
1.6	25 September 2014	L Turner	Update to address OR3.
1.7	14 November 2014	L Turner	Update to align with test findings.
1.8	29 January 2014	L Turner	Update to address CB OR2.
1.9	21 April 2015	L Turner J Rutherford	Update form factors to specify virtual appliance.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 Invincea FreeSpace™ is an anti-malware and threat intelligence solution that provides a secure container for users to run the most common web browsers and document applications within. The secure container keeps malware from executing or installing on the host machine. Malware is detected by Invincea's behavior based threat detection. Upon detection, the secure container is destroyed and a clean container is recreated to ensure the end user machine is not compromised. Invincea FreeSpace™ integrates with the Invincea Management Server, which manages client configuration and software versions and which collects any threats that were detected on an end user machine.

2 This Security Target (ST) defines the Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0
Security Target	Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0 Security Target, v1.9

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 4

b) CC Part 2 extended

c) CC Part 3 conformant

d) Evaluation Assurance Level (EAL) 2 augmented (ALC_FLR.1)

1.4 Terminology

Table 2: Terminology

Term	Definition
CC	Common Criteria
CLI	Command Line Interface
EAL	Evaluation Assurance Level
FreeSpace Host	An architectural concept referring to all components of Invincea FreeSpace™ that exist outside of the secure container.
FreeSpace Guest	An architectural concept referring to the components of Invincea

Term	Definition
	FreeSpace™ that comprise the virtual domain which isolates operating system resources from malicious code. Synonymous with: secure container, secure virtual container.
Host	A computer. Distinct from FreeSpace Host.
IMS	Invincea Management Server
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality
WebUI (WebMin)	Web User Interface (Web Administration) – third party interface to perform basic appliance / OS configuration in place of CLI commands. This interface is not included in the scope of evaluation.

2 TOE Description

2.1 Type

4 The TOE is an anti-malware and threat intelligence solution.

2.2 Usage

5 The TOE is comprised of two software components:

a) **Invincea FreeSpace™.** A software application that is installed on end user machines.

b) **Invincea Management Server (IMS).** A virtual appliance used to manage client configuration and software versions and collect information on threats detected on end user machines.

6 Usage of each of these components is further described in the following sections.

2.2.1 Invincea FreeSpace™

7 Invincea FreeSpace™ provides a secure container for users to run the most common web browsers and document applications within. By running these applications in a secure container, users are protected from malicious attacks that may come via a website or infected document. Invincea FreeSpace™ supports the following web browsers and document applications:

a) Internet Explorer

b) Mozilla Firefox

c) Google Chrome

d) Browser plugins: Java Runtime Container, Adobe Flash, Apple QuickTime and Microsoft Silverlight

e) Adobe Reader and Adobe Acrobat: PDF files

f) Microsoft Word: DOC, DOCX and other MS Word files

g) Microsoft Excel: XLS, XLSX and other MS Excel files

h) Microsoft PowerPoint: PPT, PPTX and other MS PowerPoint files

8 Invincea FreeSpace™ has the following key features:

a) **Invincea WebRedirector.** The Invincea WebRedirector controls which websites are viewed in a user's unprotected web browser versus a protected browser in the Invincea secure container. Users and/or administrators can specify which sites are trusted.

b) **Document Protection.** Users and/or administrators are able to specify the file types and applications that should be opened in the secure container. There is also an option to only open documents originating from the internet in the secure container.

c) **Application Border.** Applications running in the Invincea secure container contain a customizable border color that outlines application windows opened within the secure container. This is to help the user distinguish between the unprotected applications and those running in the secure container.

d) **Download Protection.** Users and/or administrators are able to block unsafe file types to from being downloaded by a protected browser, including executables that do not contain a valid digital signature.

e) **Threat Detection.** Invincea FreeSpace™ has a built in detection engine that detects unsafe behavior within the secure container. When a suspicious activity is detected, Invincea FreeSpace™ indicates a restore needs to be completed to return the secure container to a clean state.

f) **Restore.** The Restore option is used to restore the Invincea secure container to a clean state if suspicious activity has been detected or if the container needs to be reset for any other reason.

g) **Incident Reporting.** Detected threats may be reported to an Invincea Management Server.

9 Invincea FreeSpace™ may be installed in the following ways:

a) **Default Installation.** In this scenario Invincea FreeSpace™ is installed in a default state directly onto an end user machine with all configuration options under full control of the end user.

b) **Custom Installation.** Invincea FreeSpace™ ships with a set of configuration files that can be modified to better suit each company's environment. Administrators may disable user modifiable preferences and configure the above mentioned features according to organizational requirements. Invincea offers the option for administrators to lock down Invincea preferences so they cannot be changed by end users.

2.2.2 Invincea Management Server

10 The Invincea Management Server is Linux software that provides a modular system for integration with Invincea FreeSpace™ clients. It is available and tested in the virtual appliance form factor.

11 The Invincea Management Server supports the following modules:

a) **Administration Module.** Provides a graphical interface for administrators to manage IMS users and view logs.

b) **Threats Module.** Allows administrators to view and analyze incident reports submitted by Invincea FreeSpace™ clients. Requires license to activate.

c) **Configuration Module.** Allows for centralized management of the Invincea FreeSpace™ clients, managing both configuration files and software versions. Requires license to activate.

12 Administrators may perform appliance configuration via Command Line Interface (CLI). Administrators use the IMS functions via a web based user interface referred to as the IMS Console.

2.3 Security Functions

13 The TOE provides the following security functions:

a) **Secure Container.** The TOE provides a virtual domain (the security container) to execute web browsers and document applications within to isolate host operating system resources from malicious code. The secure container may be restored to a clean state at any time or in response to detected threats.

b) **Threat Detection.** The TOE implements a behavioral threat detection engine that monitors the secure container for indicators of malicious activity.

c) **Threat Intelligence.** The TOE provides administrators with detailed information about threats encountered by protected clients. Requires deployment of the Invincea Management Server.

d) **Policy Enforcement.** The TOE allows the user and/or administrator to define policies directing the usage of the secure container based on trusted websites, document source and types, allowable download types and digital signatures. The TOE enforces the defined policies.

e) **Secure Administration.** TOE administrators are able to restrict the ability of users to alter client configuration. TOE administrators must authenticate to the Invincea Management Server which maintains a log of administrator actions.

f) **Protected Communications.** The TOE encrypts communications with administrators and between Invincea FreeSpace™ clients and the Invincea Management Server.

g) **Verifiable Updates.** The TOE uses digital signatures to verify updates to Invincea FreeSpace™ and the Invincea Management Server.

h) **Self Protection.** The TOE implements a packet filter firewall on the Invincea Management Server to help protect against network based attacks.

2.4 Physical Scope

14 The TOE is comprised of the following software:

a) Invincea FreeSpace™ (a Microsoft Windows application)

b) Invincea Management Server (a virtual appliance) with Threats Module and Configuration Module licenses

2.4.1 Guidance Documents

15 The TOE includes the following guidance documents:

a) Invincea FreeSpace™ Administrator's Guide 4.0

b) Invincea FreeSpace™ User Guide v4.0

c) Invincea Management Server – Installation and Configuration Guide v2.0

d) Invincea FreeSpace™ v4.0 / Invincea Management Service v2.0 Common Criteria Addendum

2.4.2 Non-TOE Components

16 The TOE operates with the following components in the environment:

a) **Client Platform.** Invincea FreeSpace™ is a software application that in the evaluated configuration, runs on the following platforms:

i) Microsoft Windows 7 32 and 64-bit

ii) Microsoft Windows 8.1 32 and 64-bit

b) **Virtual Computing Platform.** The Invincea Management Sever virtual appliance supports the following virtual platforms (or equivalent):

i) VMware vSphere 4.0 or later

ii) VMware Workstation 7.1.0 or later

2.5 Logical Scope

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

18 The SSH and WebUI (WebMin) IMS appliance administration interfaces are excluded from the scope of evaluation.

19 Invincea FreeSpace™ supports Microsoft Windows XP however this configuration is excluded from the scope of evaluation.

20 The TOE must be configured in accordance with the guidance document: *Invincea FreeSpace™ v4.0 / Invincea Management Service v2.0 Common Criteria Addendum*.

3 Security Problem Definition

3.1 Threats

21 Table 3 identifies the threats addressed by the TOE.

Table 3: Threats

Identifier	Description
T.MALICOUS_CODE	Attackers compromise a user's computer via malicious code embedded in a website or document.
T.IMS_ATTACK	Attackers compromise the Invincea Management Server via a network based attack.
T.DATA_LOSS	Attackers exfiltrate data from a user's computer.
T.USER_ALTER	Non-administrative users attempt to alter client configuration options.
T.COMMS	Attackers compromise the confidentiality or integrity of communication between TOE components or between the TOE and administrators.
T.UPDATE	Attackers compromise the integrity of TOE updates.

3.2 Organizational Security Policies

22 Table 4 identifies the Organizational Security Policies (OSPs) that are addressed by the TOE.

Table 4: OSPs

Identifier	Description
OSP.WEB_REDIRECTOR	The TOE must allow users and administrators to specify websites that are trusted and do not require TOE protection.
OSP.DOWNLOAD_TYPE	The TOE must allow users and administrators to specify file types that will be blocked from downloading.
OSP.DOWNLOAD_SIGNED	The TOE must allow users and administrators to prevent download of executable files that do not have a valid digital signature.
OSP.DOCUMENT_TYPE	The TOE must allow users and administrators to specify document types that require TOE protection.
OSP.DOCUMENT_LOCAL	The TOE must allow users and administrators to disable TOE protection for documents which are created locally.

Identifier	Description
OSP.ADMIN_AUTH	The TOE must ensure that administrators are authenticated when accessing server components.
OSP.ADMIN_AUDIT	The TOE must ensure that an audit log of administrative actions performed at server components is maintained.
OSP.THREAT_INTEL	The TOE must allow clients to submit incident reports to the server.

3.3 Assumptions

23 Table 5 identifies the assumptions related to the TOE's environment.

Table 5: Assumptions

Identifier	Description
A.ADMIN	Administrators are trusted and follow guidance.
A.USER	Users are trusted and follow guidance.
A.IMS	The Invincea Management Server is deployed in a physically secure environment on a trusted network.
A.INSTALL_STATE	It is assumed that there is no pre-existing compromise of the host.
A_CAPI	Microsoft Windows provides cryptographic services to Invincea FreeSpace™.

4 Security Objectives

4.1 Objectives for the Operational Environment

24 Table 6 identifies the objectives for the operational environment.

Table 6: Operational environment objectives

Identifier	Description
OE.ADMIN	TOE administrators shall be trustworthy and shall follow guidance.
OE.USERS	TOE users shall be trustworthy and follow guidance.
OE.IMS	The Invincea Management Server shall be deployed in a physically secure environment on a trusted network.
OE.INSTALL_STATE	The host shall be in a known good state (not compromised).
OE.CAPI	Microsoft Windows shall provide cryptographic services to Invincea FreeSpace™.

4.2 Objectives for the TOE

25 Table 7 identifies the security objectives for the TOE.

Table 7: Security objectives

Identifier	Description
O.CONTAINER	The TOE shall provide a secure container for users to run web browsers and document applications within. The secure container shall isolate critical system resources from code executing within the container.
O.DETECT	The TOE shall detect suspicious activity within the secure container and respond according to an administrator defined policy.
O.RESTORE	The TOE shall destroy the secure container when directed by the user or by an administrator defined policy.
O.WEB	The TOE shall ensure that only websites that have been designated by users or administrators as trusted can be opened outside of the secure container.
O.DOWNLOADS	The TOE shall block downloads within the secure container based on file type and digital signatures as configured by users or administrators.

Identifier	Description
O.DOCUMENTS	The TOE shall ensure that documents are opened in the secure container based on file type and source (local or internet) as configured by users or administrators.
O.USER_RESTRICT	TOE administrators shall be able to restrict the ability of users to alter client configuration.
O.THREAT_INTEL	The TOE shall collect incident reports if so configured.
O.SECURE_ADMIN	The TOE shall authenticate Invincea Management Server administrators and record a log of their actions.
O.SECURE_COMMS	The TOE shall encrypt communications with administrators and between distributed components.
O.IMS_FIREWALL	The TOE shall protect the Invincea Management Server component from network attack by implementing a traffic filter firewall.
O.TRUSTED_UPDATE	The TOE shall provide the ability to verify the integrity of software updates.

5 Security Requirements

5.1 Conventions

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

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

5.2 Extended Components Definition

27 Table 8 identifies the extended components which are incorporated into this ST.

Table 8: Extended Components

Component	Title	Rationale
FDP_SVC.1	Secure Virtual Container	No existing CC Part 2 SFRs address the creation of virtual domain / container. Since the purpose of the secure virtual container is to protect user data from malicious code, a new family was created within the User Data Protection (FDP) class.

5.2.1 Secure Virtual Container (FDP_SVC)

5.2.1.1 Family Behavior

28 This family provides requirements that address the protection of user data from malicious code by means of a secure virtual container. A secure virtual container isolates critical resources of the underlying host from code executing within the container and allows monitoring of activities within the container.

5.2.1.2 Component Leveling

29 FDP_SVC.1 Virtual container addresses protection of user data from malicious code by means of a secure virtual container and enabling monitoring of activities within the container.

5.2.1.3 Management: FDP_SVC.1

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

a) Management of policies used to invoke usage of the secure virtual container

5.2.1.4 Audit: FDP_SVC.1

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

a) None

FDP_SVC.1 Secure Virtual Container

Hierarchical to: No other components.

Dependencies: None

FDP_SVC.1.1 The TSF shall maintain a virtual container for execution of [assignment: *list of processes or applications to be run inside the container*].

FDP_SVC.1.2 The TSF shall isolate the following host resources from being affected by code executing within the container: [assignment: *list of host resources to be protected from malicious code]*.

FDP_SVC.1.3 The TSF shall invoke the virtual container according to the following rules: [assignment: *list of rules*].

FDP_SVC.1.4 The TSF shall reset the virtual container to a known good state upon the following conditions: [assignment: *list of conditions*].

FDP_SVC.1.5 The TSF shall enable monitoring of the following activities within the container: [assignment: *list of activities to be monitored*]

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FAU_ARP.1	Security Alarms
FAU_GEN.1	Security Audit
FAU_GEN.2	User Identity Association
FAU_SAA.4	Complex Attack Heuristics
FAU_SAR.1	Audit Review
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FDP_IFC.1(1)	Subset Information Flow Control (Policy Enforcement)
FDP_IFF.1(1)	Simple Security Attributes (Policy Enforcement)

Requirement	Title
FDP_IFC.1(2)	Subset Information Flow Control (IMS Firewall)
FDP_IFF.1(2)	Simple Security Attributes (IMS Firewall)
FDP_SVC.1	Secure Virtual Container
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	User Identification Before Any Action
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MSA.1(1)	Management of Security Attributes (Policy Enforcement)
FMT_MSA.1(2)	Management of Security Attributes (IMS Firewall)
FMT_MSA.3(1)	Static Attribute Initialization (Policy Enforcement)
FMT_MSA.3(2)	Static Attribute Initialization (IMS Firewall)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable Time Stamps
FTA_SSL.4	User-Initiated Termination
FTP_TRP.1	Trusted path

5.3.1 Security Audit (FAU)

FAU_ARP.1 Security Alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take **the following actions depending on the configured preferences:**

- *Notify the user*
- *Terminate suspect process*
- *Remove suspect documents on detection*
- *Remove downloads from a suspect session*

- *Clear all browsing data from a suspect session*
- *Restore the secure container:*
  - *After a specified period of time (default 30 seconds), or*
  - *Prompt the user to restore*
- *Generate a local log entry*
- *Submit an incident report to the IMS subsequent to restore*

upon detection of a potential security violation.

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	Location
Logged in	IP address	IMS Activity Log
Logged out	n/a	IMS Activity Log
Change password	Username of user whose password was changed.	IMS Activity Log
Create user	Username of new user	IMS Activity Log
Delete user	Username of deleted user	IMS Activity Log
Locked user	n/a	IMS Activity Log
Unlocked user	n/a	IMS Activity Log
Change user permissions (flags)	Username of user whose flags were changed	IMS Activity Log
Deleted incident	n/a	IMS Activity Log
Incident	Source Number of changes Analysis – list of suspicious actions	IMS Incidents

Event	Additional Details	Location
	Event Tree – process, file, registry and network events Timeline – timeline of suspicious actions Geography – suspected locations of suspicious events Configuration - host system identification details, running applications and versions, running dlls	
Incident Detected	n/a	FreeSpace log file: inv.log

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: *the following events when not consistent with known application behavior:*

- *Unexpected thread creation.*
- *Unexpected process launches.*
- *Reflective DLL injection*
- *Module loads from Universal Naming Convention (UNC) paths*

and the following signature events: *none* 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: *WinAPI calls within the secure container*.

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 *Administrators* with the capability to read *incident reports and the IMS Activity Log* 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.

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *listed in the table below* and specified cryptographic key sizes *listed in the table below* that meet the following: *standards listed in the table below*.

Algorithm	Key Size	Standards
Triple DES (CBC)	168	DRNG: ANSI X9.31
AES (CBC)	256	DRNG: ANSI X9.31
RSA	1024, 2048	DRNG: ANSI X9.31

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwrite the memory occupied by keys with "zeros"* that meets the following: *none*.

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform *cryptographic operations shown in the table below* in accordance with a specified cryptographic algorithm *shown in the table below* and cryptographic key sizes *shown in the table below* that meet the following: *standards shown in the table below*.

Operation	Algorithm	Key Size	Standards and Certs*
Symmetric encryption and decryption	Triple DES (CBC)	168	FIPS 46-3 Certs. #1226, #1227, #1231, and #1232
	AES (CBC)	256	FIPS 197 Certs. #1888, #1887, #1889, #1895, #1893, and #1894
Digital signature generation and verification	RSA	1024 2048	FIPS 186-3 Certs. #964, #965, #969, and #970
Message digest	SHA-1	N/A	FIPS 180-3 Certs. #1658, #1659, #1663, and #1664
Message authentication	HMAC	96 160	FIPS 198 Certs. #1129, #1130, #1134, and #1135

*Cryptographic Algorithm Validation Program (CAVP) certificates

5.3.3 User Data Protection (FDP)

FDP_IFC.1(1) Subset information flow control (Policy Enforcement)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the *FreeSpace SFP* on

- *Subjects: Host Browser, Host Document Application, Protected Browser, Protected Document Application*
- *Information: URL, Document, File*
- *Operations: Visit URL, open document, download file*

FDP_IFC.1(2) Subset information flow control (IMS Firewall)

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the *IMS Firewall SFP* on

- *Subjects: Network Device, IMS*
- *Information: IP Packets*
- *Operations: Receive Packet, Send Packet*

FDP_IFF.1 (1) Simple security attributes (Policy Enforcement)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the *FreeSpace SFP* based on the following types of subject and information security attributes: *subjects, information and attributes shown in the table below.*

Entity	Type	Attributes
Host Browser	Subject	Trusted Sites List
Host Document Application	Subject	Protected Applications List (file extensions) Only open documents originating from the internet (enabled / disabled)
Protected Browser*	Subject	Trusted Sites List Block unsafe extensions (enabled / disabled) Block unsigned executables (enabled / disabled) Unsafe Extensions List (file extensions)
Protected Document	Subject	Protected Applications List (file extensions)

Entity	Type	Attributes
Application*		Only open documents originating from the internet (enabled / disabled)
URL	Information	URL
Document	Information	File Extension Source (local / internet)
File	Information	Extension Signature (valid / invalid)

*Executed within the secure container specified by FDP_SVC.1.

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

- *Visit URL:*
  - *If URL is trusted (on the Trusted Sites List) then view URL in Host Browser*
  - *If URL is untrusted (not on the Trusted Sites List) then view URL in Protected Browser*
- *Open document:*
  - *If Document is unprotected (File Extension is not on the Protected Applications List) then open Document in the Host Document Application*
  - *If Document is protected (File Extension is on the Protected Applications List) then open Document in the Protected Document Application, subject to the following rule:*
  - *If 'Only open documents originating from the internet' is enabled then:*
    - *Where Document Source is local, open Document in the Host Document Application*
    - *Where Document Source is internet, open Document in the Protected Document Application*
- *Download file:*
  - *If Protected Browser 'Block unsafe file extensions' is enabled, block the download if the file download extension is on the Unsafe Extensions List.*
  - *If Protected browser 'Block unsigned executables' is enabled and the File Extension is an executable then block the download if the File Signature is invalid.*
  - *Otherwise allow downloads.*

FDP_IFF.1.3 The TSF shall enforce the*: no additional rules.*

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *no additional rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *no additional rules*.

FDP_IFF.1(2) Simple security attributes (IMS Firewall)

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the *IMS Firewall SFP* based on the following types of subject and information security attributes *subjects, information and attributes shown in the table below.*

Entity	Type	Attributes
Network Device	Subject	Presumed Address (represented by IP Packet)
IMS	Subject	Interface (Eth0 etc.) Connection State (New, Established, Related, Invalid) Inbound Rules* Outbound Rules* *Rules defined by: • Action: Accept, Drop • Condition: If / and logic statements comprised of IP Packet attributes and IMS attributes (if the logic statement evaluates to true then the associated action is performed).
IP Packet	Information	Source IP Address Destination IP Address Source Port Destination Port Protocol Protocol Flags

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

- *Receive Packet:*

    - *IMS Inbound Rules determine if a packet is received (Accept) or not (Drop).*
- *Send Packet*
    - *IMS Outbound Rules determine if a packet is transmitted (Accept) or not (Drop).*

FDP_IFF.1.3 The TSF shall enforce the *no additional rules*.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *no additional rules.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *no additional rules*.

FDP_SVC.1 Secure Virtual Container

Hierarchical to: No other components.

Dependencies: None

FDP_SVC.1.1 The TSF shall maintain a virtual container for execution of:

- *Supported browsers and plugins (section 2.2.1)*
- *Supported document applications(section 2.2.1)*

FDP_SVC.1.2 The TSF shall isolate the following host resources from being affected by code executing within the container:

- *File System*
- *Registry*
- *Running Processes*

FDP_SVC.1.3 The TSF shall invoke the virtual container according to the following rules: *Protected Browser and Protected Document Application rules specified by FDP_IFF.1(1)*.

FDP_SVC.1.4 The TSF shall reset the virtual container to a known good state upon the following conditions:

- *User initiated restore*
- *Scheduled restore*
- *In response to a detected threat as specified in FAU_ARP.1*

FDP_SVC.1.5 The TSF shall enable monitoring of the following activities within the container:

- *Process execution*
- *File writes*
- *Registry writes*
- *Network listeners*

- *Successful network connections*

5.3.4 Identification and Authentication (FIA)

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

Application note: This is related to administrator authentication to the IMS.

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**~~ **IMS** shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note: This is related to administrator authentication to the IMS.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The ~~**TSF**~~ **IMS** shall provide *bullets (•) or no feedback* to the user while the authentication is in progress.

Application note: This is related to administrator authentication to the IMS. Bullets are shown when entering a password at the IMS console. No feedback is given when entering a password at the CLI.

5.3.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to <u>disable, enable, modify the behaviour of</u> the functions *specified at FMT_SMF.1* to *Authorized Users and Administrators*.

FMT_MSA.1 (1) Management of security attributes (Policy Enforcement)

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 *FreeSpace SFP* to restrict the ability to change_default, query, modify, delete the security attributes *listed at FDP_IFF.1(1)* to *Authorized Users and Administrators*.

FMT_MSA.1 (2) Management of security attributes (IMS Firewall)

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 *IMS Firewall SFP* to restrict the ability to change_default, query, modify, delete the security attributes *inbound rules and outbound rules* to *Administrators*.

FMT_MSA.3 (1) Static attribute initialization (Policy Enforcement)

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 *FreeSpace SFP* to provide permissive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the *Authorized Users and Administrators* to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3 (2) Static attribute initialization (IMS Firewall)

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 *IMS Firewall 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 *Administrators* 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 Invincea FreeSpace™ client TSF attributes and preferences*
- *Manage IMS TSF attributes and system settings*
- *Initiate trusted updates*

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:

- *Administrator (IMS)*
- *CMS Modify (IMS)*
- *TDS Modify (IMS)*
- *Authorized User (FreeSpace implied role)*

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

Application Note: Regarding *Authorized Users:* Invincea FreeSpace™ is configured through a set of locally stored files. These files are only available to users with administrative privileges on the host machine – any such user is considered an *Authorized User.* In addition, users are *Authorized Users* for those client attributes and preferences that have been flagged as 'user modifiable' in the configuration files.

5.3.6 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.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.3.7 TOE Access (FTA)

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The **~~TSF~~ IMS** shall allow user-initiated termination of the user's own interactive session.

5.3.8 Trusted Path/Channels (FTP)

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 *remote access to the IMS*.

5.4 Assurance Requirements

32 The TOE security assurance requirements are summarized in Table 10 commensurate with EAL2+ (ALC_FLR.1).

Table 10: 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

Assurance Class	Components	Description
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.1	Basic Flaw Remediation
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 Container

33 The TOE provides a virtual domain (the secure container) to execute web browsers and document applications within to isolate host operating system resources from malicious code. The secure container may be restored to a clean state at any time, in accordance with a defined schedule or in response to detected threats.

Table 11: Secure Container SFRs

SFR	Fulfilment
FDP_SVC.1	Invincea FreeSpace™ creates a selectively virtualized filesystem and Windows registry hive which is accessible to the FreeSpace Guest (secure container). Invincea FreeSpace™ uses a combination of user-mode DLLs, kernel drivers and Windows executables to effectively create a separate FreeSpace Host and FreeSpace Guest. TOE components reside on both the FreeSpace Host and FreeSpace Guest and communicate via TCP. Protected browsers and document applications are launched as child processes of the FreeSpace Guest. The TOE intercepts WinAPI calls from FreeSpace Guest processes which enables monitoring of process, file and network activity, provides isolation between FreeSpace Guest and FreeSpace Host running processes and allows enforcement of threat detection policies. In order to restore the FreeSpace Guest to a known good state, the virtualized filesystem and Windows registry are deleted and re-created and FreeSpace Guest components are restarted. A restore may be performed at the request of the user, in response to a detected threat, or in accordance with a defined schedule.

6.2 Threat Detection

34 The TOE implements a behavioral threat detection engine that monitors the secure container for indicators of malicious activity.

Table 12: Threat Detection SFRs

SFR	Fulfilment
FDP_SVC.1	Invincea FreeSpace™ intercepts WinAPI calls from FreeSpace Guest processes which are inspected by the threat detection engine.
FAU_SAA.4	The threat detection engine implements a whitelist of known application behaviour and will trigger when the following events occur: • Unexpected thread creation. • Unexpected process launches. • Reflective DLL injection • Module loads from Universal Naming Convention (UNC) paths

SFR	Fulfilment
	A trigger indicates that a potential threat has been detected.

FAU_ARP.1	The response to a detected threat is configurable and includes the following options:
	• **Notify the user.** When this option is enabled the user receives a notification that a threat has been detected. An additional menu item can also be displayed in the system tray menu. The user may select the "Suspect Activity Details" option to view further information regarding the activity. This may be coupled with a prompt to restore per below (restore the secure container).
	• **Terminate suspect process.** When this option is enabled the TOE terminates suspect processes as soon as they are detected.
	• **Remove suspect documents on detection.** When this option is enabled the TOE deletes documents that are located on the end user PC if a threat is detected within the document. This document will be permanently deleted. The user will be notified if this occurs. An example of this option would be the user opening a PDF on their desktop that contained malicious content. This file would be deleted from the desktop and a restore of the secure container would be executed (or prompted).
	• **Remove downloads from a suspect session.** When this option is enabled the TOE immediately remove any files downloaded during a session that is deemed infected from the host machine. The user will be notified of the deleted files at the time of infection. An example of this option would be if the user downloaded three PDF documents with the protected browser and then browsed to a malicious site. These three documents would be removed from the location that they were downloaded to.
	• **Clear all browsing data from a suspect session.** This option allows for the TOE to clear all secure container browsing data (additional bookmarks, changes to browser settings, history, cookies, etc.) during a suspect session (when a suspicious activity alert is displayed). If the option is not checked, then the browsing history and data will remain intact when the restore happens, even if they have been modified by the attack (such as changing the home page to something malicious or adding in malicious bookmarks).
	• **Restore the secure container** (refer to section 6.1):
	  ○ After a specified period of time (default 30 seconds), or
	  ○ Prompt the user to restore
	• **Generate a local log entry** (see FAU_GEN.1 below)
	• **Submit an incident report** to the IMS subsequent to restore (see section 6.3)

FAU_GEN.1	Invincea FreeSpace™ generates a log entry in the local 'inv.log' file.

6.3 Threat Intelligence

35 The TOE provides administrators with detailed information about threats encountered by protected clients. Requires deployment of the Invincea Management Server.

Table 13: Threat Intelligence SFRs

SFR	Fulfilment
FDP_SVC.1	Invincea FreeSpace™ monitors / records the following from within the Guest: process execution, file writes, registry writes, network listeners, successful network connections. This allows the actions of detected threats and actions leading to threat to be recorded for later inspection.

FAU_ARP.1	When configured to do so, Invincea FreeSpace™ will submit incident reports to the IMS. These are XML files that record:
	• **Source.** URL or File location of the triggering event.
	• **Date/Time.** The date/time that the event occurred and time of all actions during the threat.
	• **Analysis.** Record of all actions during the threat, including:
	  ○ Executables Written (and details)
	  ○ Processes Launched (and details)
	  ○ Connections Opened (and details)
	  ○ System Changes (and details)
	  ○ URLs visited (and details)
	• **Configuration Data.** Additional details to aid forensic analysis such as running applications and versions, running dlls and host system and identification details.

FAU_GEN.1	Per FAU_ARP.1 above, the clients submit incident reports to the IMS.
FAU_SAR.1	The IMS allows administrators to view incident reports and summary information.

6.4 Policy Enforcement

36 The TOE allows the user and/or administrator to define policies directing the usage of the secure container based on trusted websites, document source and types, allowable download types and digital signatures. The TOE enforces the defined policies.

Table 14: Policy Enforcement SFRs

SFR	Fulfilment
FDP_IFC.1(1) FDP_IFF.1(1)	**WebRedirector** The Invincea WebRedirector controls which websites are viewed in a user's unprotected web browser versus a protected browser in the Invincea secure container. When a user attempts to access a website in the unprotected browser that is not considered "trusted" the WebRedirector will reopen the requested page in an Invincea protected browser to ensure a safe browsing experience. The WebRedirector also ensures that trusted websites can be opened in an unprotected browser by the same process. The WebRedirector is implemented as plugins in the web browsers. Users may disable the WebRedirector plugins however are trusted not to do so. Users and administrators are able to specify trusted sites (however users may be restricted per section 6.5). **Document Protection** Invincea FreeSpace™ enables administrators and users (users may be restricted per section 6.5) to enable or disable document protection for protected applications. By disabling document protection for an application, the associated file types for that application will no longer open inside the secure container. An additional option is: 'Only open documents originating from the internet'. This option will allow only documents that originate from the internet to be opened in an Invincea protected document application. Documents which are created locally will be opened outside of the secure container. When not selected, all documents will be opened in the secure container (for document types that Invincea FreeSpace™ is default program). **Downloads** Invincea FreeSpace™ provides the ability to configure additional options on how files are handled when downloaded as follows: • **Block unsafe file extensions from downloading.** This option allows the TOE to stop any blacklisted file types from being downloaded by a protected browser. The following is the default list of file types that will be blocked by enabling this option (can be modified by an administrator): bas, bat, chm, cmd, com, cpl, crt, dll, exe, hlp, hta, inf, ins, isp, msc, msi, msp, mst, pif, reg, scr, sct, shb, shs, sys, vb, vbe, vbs, wsc, wsf, wsh • **Block executable downloads that are not digitally signed.** This option allows the TOE stop any executable without digital signature from being downloaded. Executable downloads that are digitally signed will be downloaded. The TOE makes use of the Microsoft CryptoAPI to confirm the validity of digital signatures.

SFR	Fulfilment
FMT_MSA.1(1) FMT_MSA.3(1)	The default Invincea FreeSpace™ settings are generally permissive as follows: • Browser protection is enabled • Document protection is enabled • Only open documents originating from the internet is disabled • Block unsafe file extensions is disabled • Block unsigned executables is disabled An *Administrator* or *Authorized User* can modify these defaults via configuration files.

6.5 Secure Administration

37 TOE administrators are able to restrict the ability of users to alter client configuration. TOE administrators must authenticate to the Invincea Management Server which maintains a log of administrator actions.

Table 15: Secure Administration SFRs

SFR	Fulfilment
FAU_GEN.1	Invincea FreeSpace™ maintains the following logs: • inv.log file contains details of detected threats The IMS maintains the following logs: • IMS activity log for administrative functions • Incident reports received from Invincea FreeSpace™ clients • IMS sites log for changes to sites trusted by clients
FAU_GEN.2	The IMS activity log contains user identifiers for applicable events.
FAU_SAR.1	The administrator may view, filter, search and export the IMS Activity Log from the IMS Console.
FIA_UAU.2 FIA_UID.2	The IMS implements the following administrative interfaces which prompt for username and password: • IMS Console • CLI No actions may be performed until administrators are successfully authenticated.
FIA_UAU.7	Passwords are not echoed back to the IMS user during authentication. Only characters such as bullets (•) are echoed.

SFR	Fulfilment
FMT_MOF.1	The IMS implements password based access control to ensure that only *Administrators* are able to disable, enable or modify the configuration of the IMS. Invincea FreeSpace™ is configured through a set of locally stored files. These files are only available to users with administrative privileges on the host machine – any such user is considered an *Authorized User* and is able to disable, enable, modify the configuration of Invincea FreeSpace™ on that host. Certain attributes within the configuration files include a 'user modifiable' flag. When this flag is enabled, Invincea FreeSpace™ users can see and modify that attribute / setting at the user interface. Users are *Authorized Users* for those client attributes and preferences that have been flagged as 'user modifiable'. IMS *Administrators* are able to 'push' configuration changes via customized files to managed Invincea FreeSpace™ clients.
FMT_SMR.1	The IMS has a local user database. *Administrators* have full control over the IMS and managed Invincea FreeSpace™ client configuration. In addition to the *Administrator* role, the IMS maintains the following roles: • **CMS Modify.** Has the ability to change limited IMS configuration settings. • **TDS Modify.** Has the ability to change threat related IMS settings. IMS users may have more than one role. All IMS users have full read access. The role of *Authorized User* is an implied role relevant to the Invincea FreeSpace™ client and refers to users with local administrative privileges. In addition, users are *Authorized Users* for those client attributes and preferences that have been flagged as 'user modifiable' in the configuration files.

SFR	Fulfilment
FMT_SMF.1	The IMS provides CLI and IMS Console (web based) interfaces to perform management functions. The CLI interface allows the following relevant management functions: • Network configuration • Certificate management (TLS) • Firewall configuration • IMS Software updates • System time configuration The IMS Console provides the following management functions: • Provides a graphical interface for administrators to review threat based information, such as top infected users, top infected hosts and more. • Allows administrators to view and analyze incident reports submitted by Invincea FreeSpace™ clients. • Allows for centralized management of the Invincea FreeSpace™ clients, managing both configuration files and software versions. Invincea FreeSpace™ is configured through a set of locally stored files: • **Preferences.xml** These preferences include most options found in the System Tray menu and the Preferences UI, server configuration information and other program configurations. This file can also be used to determine which preferences are available to the end user via the preferences UI. • **Custom_apps.xml** These settings include network and proxy settings, browser home page, user-agent strings and support for browser add-ons. Once set, these settings will become default values for the browser. • **Trustedsites.txt** This is a configuration file that can be used to allow certain websites to open in the unprotected browser, rather than in the protected browser. The TOE includes a sample file with some general sites and can be customized to suit each deployed environment. Both trustedsites.txt (the global white list) and trustedsites2.txt (the division based white list) can be included in the installation package. In addition to the above files, Invincea FreeSpace™ users interact with the TOE via the user interface, system tray and in response to message prompts such as those prompting to restore the secure container.
FPT_STM.1	The IMS uses an internal system clock provided by the underlying Linux based operating system. Invincea FreeSpace™ makes use of the host system clock. In each case the TOE will reliably apply a timestamp to generated audit logs based on these time sources.

SFR	Fulfilment
FTA_SSL.4	IMS *Administrators* may log out of the IMS at any time to terminate an interactive session.

6.6 Protected Communications

38 The TOE encrypts communications with administrators and between Invincea FreeSpace™ clients and the Invincea Management Server.

Table 16: Protected Communications SFRs

SFR	Fulfilment
FCS_CKM.1 FCS_CKM.4 FCS_COP.1	Cryptographic operations are relevant to the IMS only. Invincea FreeSpace™ makes use of the Microsoft CryptoAPI provided by the environment. The IMS makes use of the following FIPS 140-2 validated module to perform the cryptographic operations specified at FCS_CKM.1, FCS_CKM.4 and FCS_COP.1: • Red Hat Enterprise Linux OpenSSL (openssl 1.0.0-20.el6 and dracut-fips 004-248.el6_3.1) Cert #1758 configured in accordance with the Security Policy for this module. Invincea affirms equivalency between the tested OS and CentOS 6.6 implemented by the TOE. Security Policy: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1758.pdf

FPT_ITT.1	Communications between the IMS and Invincea FreeSpace™ are protected via TLS. The TOE's TLS implementation has the following characteristics:
	• TLS v1.0
	• Supported ciphersuites:
	  ○ TLS_RSA_WITH_AES_128_CBC_SHA
	  ○ TLS_RSA_WITH_AES_256_CBC_SHA
	  ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	  ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA

FTP_TRP.1	Communication between the IMS and remote administrators is protected via TLS for IMS Console access (over HTTPS). The TOE uses the same implementation of TLS for HTTPS connections as described above at FPT_ITT.1.

6.7 Verifiable Updates

39 The TOE uses digital signatures to verify updates to Invincea FreeSpace™.

Table 17: Verifiable Updates SFRs

SFR	Fulfilment

SFR	Fulfilment
FCS_COP.1	Software update files are digitally signed with Invincea, Inc. code signing key - X.509 / RSA 2048 bit key. The IMS verifies digital signatures prior to installing updates and aborts if signature verification fails.
FMT_SMF.1	IMS *Administrators* are able to manage Invincea FreeSpace™ client software updates from the IMS Console. Invincea FreeSpace™ *Authorized Users* are able to update client software via the Preferences UI.

6.8 Self Protection

40 The TOE implements a packet filter firewall on the IMS to help protect against network based attacks.

Table 18: Self Protection SFRs

SFR	Fulfilment
FDP_IFC.1(2) FDP_IFF.1(2)	The IMS implements a Linux Firewall (IPTables). The firewall can be configured via the CLI interface. Details on the usage of IPTables can be found at: https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-IPTables.html
FMT_MSA.1(2) FMT_MSA.3(2)	The default settings for the IMS firewall are restrictive. Only those ports necessary for the IMS to function are open. An IMS *Administrator* may change these settings via CLI.

7 Rationale

7.1 Security Objectives Rationale

41 Table 19 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 19: Security Objectives Mapping

	T.MALICOUS_CODE	T.IMS_ATTACK	T.DATA_LOSS	T.USER_ALTER	T.COMMS	T.UPDATE	OSP.WEB_REDIRECTOR	OSP.DOWNLOAD_TYPE	OSP.DOWNLOAD_SIGNED	OSP.DOCUMENT_TYPE	OSP.DOCUMENT_LOCAL	OSP.ADMIN_AUTH	OSP.ADMIN_AUDIT	OSP.THREAT_INTEL	A.ADMIN	A.USERS	A.IMS	A.INSTALL_STATE	A.CAPI
O.CONTAINER	X		X																
O.DETECT	X																		
O.RESTORE	X																		
O.WEB							X												
O.DOWNLOADS								X	X										
O.DOCUMENTS										X	X								
O.USER_RESTRICT				X															
O.THREAT_INTEL														X					
O.SECURE_ADMIN												X	X						
O.SECURE_COMMS					X														
O.IMS_FIREWALL		X																	
O.TRUSTED_UPDATE						X													
OE.ADMIN															X				
OE.USERS																X			
OE.IMS		X															X		
OE.INSTALL_STATE																		X	

	T.MALICOUS_CODE	T.IMS_ATTACK	T.DATA_LOSS	T.USER_ALTER	T.COMMS	T.UPDATE	OSP.WEB_REDIRECTOR	OSP.DOWNLOAD_TYPE	OSP.DOWNLOAD_SIGNED	OSP.DOCUMENT_TYPE	OSP.DOCUMENT_LOCAL	OSP.ADMIN_AUTH	OSP.ADMIN_AUDIT	OSP.THREAT_INTEL	A.ADMIN	A.USERS	A.IMS	A.INSTALL_STATE	A.CAPI
OE.CAPI																			X

42 Table 20 provides the justification to show that the security objectives are suitable to address the security problem.

Table 20: Suitability of Security Objectives

Element	Justification
T.MALICOUS_CODE	**O.CONTAINER.** The secure container insulates the user's computer from the actions of malicious code that is delivered via a website or document. **O.DETECT.** Executed malicious code will be detected based on the actions that the code attempts to perform within the security container and the TOE will react based on an administrator defined policy. **O.RESTORE.** The secure container can be destroyed and restored as directed by the user or administrator defined policy (such as in response to detecting malicious code). Doing so removes the effects of any malicious code within the container.
T.IMS_ATTACK	**O.IMS_FIREWALL.** The traffic filter firewall adds a layer of defence to reduce the network reachable ports available to attackers. **OE.IMS.** Placement of the IMS within a trusted network provides a layer of defence against external network attacks.
T.DATA_LOSS	**O.CONTAINER.** Any malicious code that executes within the secure container is prevented from reading or exfiltrating user data from the host file system.
T.USER_ALTER	**O.USER_RESTRICT.** TOE administrators are able to configure the TOE to prevent users from altering the configuration.
T.COMMS	**O.SECURE_COMMS.** The TOE prevents confidentiality or integrity compromise by using encryption to protect communication between TOE components and between the TOE and administrators.

Element	Justification
T.UPDATE	**O.TRUSTED_UPDATE.** The TOE protects against a compromise to the integrity of TOE updates by providing the ability to verify updates.
OSP.WEB_REDIRECTOR	**O.WEB.** The TOE provides the ability for users and administrators to specify websites that are trusted and do not require TOE protection.
OSP.DOWNLOAD_TYPE	**O.DOWNLOADS.** The TOE provides the ability for users and administrators to specify file types that will be blocked from downloading.
OSP.DOWNLOAD_SIGNED	**O.DOWNLOADS.** The TOE provides the ability for users and administrators to prevent download of executable files that do not have a valid digital signature.
OSP.DOCUMENT_TYPE	**O.DOCUMENTS.** The TOE provides the ability for users and administrators to specify document types that require TOE protection.
OSP.DOCUMENT_LOCAL	**O.DOCUMENTS.** The TOE provides the ability for users and administrators to disable TOE protection for documents which are created locally.
OSP.ADMIN_AUTH	**O.SECURE_ADMIN.** The TOE requires administrators to authenticate to the Invincea Management Server.
OSP.ADMIN_AUDIT	**O.SECURE_ADMIN.** The TOE generates an audit log of administrative actions performed at the Invincea Management Server.
OSP.THREAT_INTEL	**O.THREAT_INTEL.** The TOE is able to collect incident reports from clients if deployed with the Invincea Management Server and configured to collect incident reports.
A.ADMIN	**OE.ADMIN.** TOE administrators are trustworthy and follow guidance.
A.USER	**OE.USER.** TOE users are trustworthy and follow guidance.
A.IMS	**OE.IMS.** The Invincea Management Server is deployed in a physically secure environment on a trusted network.
A.INSTALL_STATE	**OE.INSTALL_STATE.** For installations that do not use Internet Isolation there is no pre-existing compromise of the host.
A.CAPI	**OE.CAPI.** Microsoft Windows provides the crypto API for Invincea FreeSpace™.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

43 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.1 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 21: Security Requirements Mapping

	O.CONTAINER	O.DETECT	O.RESTORE	O.WEB	O.DOWNLOADS	O.DOCUMENTS	O.USER_RESTRICT	O.THREAT_INTEL	O.SECURE_ADMIN	O.SECURE_COMMS	O.IMS_FIREWALL	O.TRUSTED_UPDATE
FAU_ARP.1		X	X					X				
FAU_GEN.1								X	X			
FAU_GEN.2									X			
FAU_SAA.4		X										
FAU_SAR.1								X	X			
FCS_CKM.1										X		
FCS_CKM.4										X		
FCS_COP.1										X		X
FDP_IFC.1(1)				X	X	X						
FDP_IFF.1(1)				X	X	X						
FDP_IFC.1(2)											X	
FDP_IFF.1(2)											X	
FDP_SVC.1	X	X	X	X	X	X		X				
FIA_UAU.2									X			
FIA_UAU.7									X			

	O.CONTAINER	O.DETECT	O.RESTORE	O.WEB	O.DOWNLOADS	O.DOCUMENTS	O.USER_RESTRICT	O.THREAT_INTEL	O.SECURE_ADMIN	O.SECURE_COMMS	O.IMS_FIREWALL	O.TRUSTED_UPDATE
FIA_UID.2									X			
FMT_MOF.1							X		X			
FMT_MSA.1(1)				X	X	X	X					
FMT_MSA.1(2)											X	
FMT_MSA.3(1)				X	X	X	X					
FMT_MSA.3(2)											X	
FMT_SMF.1							X		X			X
FMT_SMR.1							X		X			
FPT_ITT.1										X		
FPT_STM.1									X			
FTA_SSL.4									X			
FTP_TRP.1										X		

Table 22: Suitability of SFRs

Objectives	**SFRs**
O.CONTAINER	**FDP_SVC.1** requires the TOE to provide a secure container for supported web browsers and document applications which isolates critical system resources from code executing within the container.
O.DETECT	**FAU_ARP.1** requires the TOE to respond to potential security violations. **FAU_SAA.4** requires the TOE to detect potential security violations. **FDP_SVC.1** requires the TOE to provide monitoring of system activity to enable detection of potential security violations.
O.RESTORE	**FAU_ARP.1** requires the TOE to respond to a potential security violation by automatically restoring the virtual container or prompting

Objectives	SFRs
	the user to restore depending on the administrator defined policy. **FDP_SVC.1** requires the TOE to be able to reset the virtual container to a known good state upon specified conditions.
O.WEB	**FDP_IFC.1(1)** and **FDP_IFF.1(1)** together specify the rules for web redirection. **FDP_SVC.1** requires the TOE to invoke the secure container according to the specified web redirection rules. **FMT_MSA.1(1)** and **FMT_MSA.3(1)** specify rules for secure initialization and management of the attributes related to web redirection.
O.DOWNLOADS	**FDP_IFC.1(1)** and **FDP_IFF.1(1)** together specify the rules for download restrictions. **FDP_SVC.1** requires the TOE to provide the secure container within which download restrictions are enforced. **FMT_MSA.1(1)** and **FMT_MSA.3(1)** specify rules for secure initialization and management of the attributes related to download restrictions.
O.DOCUMENTS	**FDP_IFC.1(1)** and **FDP_IFF.1(1)** together specify the rules for protecting document application. **FDP_SVC.1** requires the TOE to invoke the secure container according to the specified protected document application rules. **FMT_MSA.1(1)** and **FMT_MSA.3(1)** specify rules for secure initialization and management of the attributes related to protected documents.
O.USER_RESTRICT	**FMT_MOF.1** specifies restrictions on which roles can modify management functions. **FMT_MSA.1(1)** and **FMT_MSA.3(1)** specify restrictions on which roles can modify policy enforcement security attributes. **FMT_SMF.1** specifies the management functions. **FMT_SMR.1** specifies the security roles.
O.THREAT_INTEL	**FAU_ARP.1** requires the FreeSpace™ client to submit an incident report in response to a potential security violation if so configured by the administrator. **FAU_GEN.1** requires the IMS to record the incident reports. **FAU_SAR.1** requires the IMS to provide administrators with the ability to read incident reports. **FDP_SVC.1** requires the virtual container to monitor the system activities that are included in the **incident** report.
O.SECURE_ADMIN	**FAU_GEN.1** requires the IMS to log administrative actions.

Objectives	SFRs
	FAU_GEN.2 requires the IMS to include usernames in audit records. **FAU_SAR.1** requires the IMS to provide administrators with the ability to read specified audit records. **FIA_UAU.2** requires the IMS to authenticate administrators. **FIA_UAU.7** requires protected feedback during authentication. **FIA_UID.2** requires the IMS to identify administrators. **FMT_MOF.1** specifies the security roles with access to management functions. **FMT_SMF.1** specifies the management functions. **FMT_SMR.1** specifies the security roles. **FPT_STM.1** requires the IMS to provide reliable timestamps for audit records. **FTA_SSL.4** requires the IMS to allow administrators to log off / terminate a session.
O.SECURE_COMMS	**FCS_CKM.1** specifies requirements for key generation. **FCS_CKM.4** specifies requirements for key destruction. **FCS_COP.1** specifies encryption/decryption and message digest requirements used to protect communications. **FPT_ITT.1** requires protection of communication between separate parts of the TOE (i.e. between the IMS and FreeSpace™ client). **FTP_TRP.1** requires protection of communication with remote administrators.
O.IMS_FIREWALL	**FDP_IFC.1(2)** and **FDP_IFF.1(2)** together specify the information flow control policy for the IMS firewall. **FMT_MSA.1(2)** and **FMT_MSA.3(2)** specify the rules for secure initialization and management of IMS firewall attributes.
O.TRUSTED_UPDATE	**FCS_COP.1** specifies digital signature requirements used for verification of updates. **FMT_SMF.1** requires that the TOE be capable of initiating trusted updates.

7.3 TOE Summary Specification Rationale

44 Table 23 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 23: Map of SFRs to TSS Security Functions

	Secure Container	Threat Detection	Threat Intelligence	Policy Enforcement	Secure Administration	Protected Communications	Verifiable Updates	Self Protection
FAU_ARP.1		X	X					
FAU_GEN.1		X	X		X			
FAU_GEN.2					X			
FAU_SAA.4		X						
FAU_SAR.1			X		X			
FCS_CKM.1						X		
FCS_CKM.4						X		
FCS_COP.1						X	X	
FDP_IFC.1(1)				X				
FDP_IFF.1(1)				X				
FDP_IFC.1(2)								X
FDP_IFF.1(2)								X
FDP_SVC.1	X	X	X					
FIA_UAU.2					X			
FIA_UAU.7					X			
FIA_UID.2					X			
FMT_MOF.1					X			
FMT_MSA.1(1)				X				
FMT_MSA.1(2)								X

FMT_MSA.3(1)				X				
FMT_MSA.3(2)								X
FMT_SMF.1					X		X	
FMT_SMR.1					X			
FPT_ITT.1						X		
FPT_STM.1					X			
FTA_SSL.4					X			
FTP_TRP.1						X		