AhnLab

CPP 1.0

Security Target

Version 2.5

June 2022

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Description
1.0 – 1.9	2021	Evaluation versions.
2.0	22 Feb 2022	Release for certification.
2.1	11 Mar 2022	Update guidance version
2.2	22 Mar 2022	Update TOE and guidance version.
2.3	11 Apr 2022	Correction to Table 3.
2.4	11 May 2022	Add cc_220513 patch.
2.5	29 Jun 2022	Update TOE and guidance versions.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the AhnLab Cloud Platform Protection (CPP) 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	AhnLab CPP 1.0 See section 2.4 for software versions and build numbers.
Security Target	AhnLab CPP 1.0 Security Target, v2.5

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) EAL 2+ ALC_FLR.1

1.4 Terminology

Table 2: Terminology

Term	Definition
AC	Application Control
ASD	AhnLab Smart Defense
CC	Common Criteria
CPP	Cloud Protection Platform
EAL	Evaluation Assurance Level
Endpoint	Host on the network protected by AhnLab.
Endpoint User	User of an endpoint system.
IPS	Intrusion Prevention System

Term	Definition
IOC	Indicator of Compromise
Malware	A harmful program that infiltrates a user's system. Computer viruses, worms, spyware and Trojans are common malware.
PP	Protection Profile
RBAC	Role Based Access Control
Scan Type	AhnLab V3 malware scan types consisting of: • **Real-time Scan.** Continuous scanning of file i/o and memory. • **Intense Scan.** A file scan based on indexing. May be performed on-demand or as a scheduled scan. • **Smart Scan.** Selectively scans important folders, processes and boot area. Performed on start-up and on-demand. • **Diagnostic Scan.** Scans the most vulnerable areas for security threats. Performed on-demand.
TOE	Target of Evaluation
TSF	TOE Security Functionality
V3	AhnLab anti-virus program

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. The TOE includes three of these endpoint security solutions: AhnLab V3 Net (anti-virus), AhnLab Host IPS (network intrusion detection/prevention) and AhnLab Application Control.

2.2 Usage

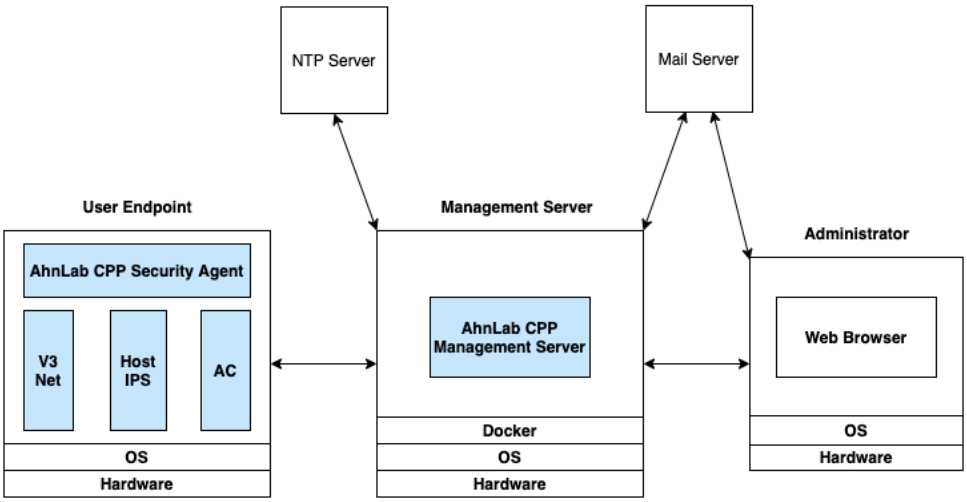


Figure 1: TOE components

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

a) **AhnLab CPP Management Server.** The CPP Management Server is a software application that is used to efficiently operate and manage multiple AhnLab endpoint security solutions. These endpoint security solutions are deployed as agents via the CPP Security Agent. The CPP Management Server provides a web-based user interface for TOE administration, definition of policies and review of a configurable security dashboard.

b) **AhnLab CPP Security Agent.** The CPP Security Agent, installed on endpoints (i.e. hosts), is used to provide connectivity between protected endpoints and the CPP management server, to deploy endpoint protection agents, and to facilitate monitoring and/or enforcement actions of the deployed AhnLab endpoint security solutions.

c) **AhnLab V3 Net.** The V3 Net agent provides malware detection and response capabilities.

d) **AhnLab Host IPS.** The Host IPS agent detects and blocks network intrusion attacks via signature-based detection.

e) **AhnLab Application Control.** The Application Control agent provides application whitelisting to only allow execution of trusted applications.

2.3 Security Functions

6 The TOE provides the following security functions:

a) **Secure Management.** The TOE enables secure management of its functions and AhnLab endpoint security solutions via:

   i) Identification and authentication of administrative users

   ii) Role Based Access Control

   iii) Audit of management actions

   iv) Management of AhnLab endpoint security solutions:

      (1) AhnLab CPP Management

      (2) AhnLab Host IPS

      (3) AhnLab Application Control

      (4) AhnLab V3 Net

b) **Security Dashboard.** TOE administrators are able to view threat information and statistics via configurable dashboards and threat process trees.

c) **Malware Detection & Response.** The V3 TOE component provides the following malware detection and response functionality:

   i) Signature-based malware detection

   ii) Behavior-based malware detection

   iii) Repair, quarantine, ignore and/or deletion of infected files

d) **Application Control.** The Application Control TOE component provides the following endpoint file discovery and execution control functionality:

   i) Endpoint file scanning

   ii) Whitelisting

   iii) File execution control and logging

e) **Host IPS**. The Host IPS TOE component provides the following network threat detection and response functionality:

   i) Signature-based intrusion detection and prevention

   ii) Incident logging and network traffic control

f) **Protected Communications**. The TOE protects communications between remote administrators and the Management Server, and between the Management Server and CPP Security Agents.

2.4 Physical Scope

7 The physical boundary of the TOE is the software executing on supported non-TOE operating systems as shown in Table 3.

Table 3: TOE Software

TOE Software	TOE Version	Non-TOE Operating Systems
AhnLab CPP Management Server	1.0.3.10-24 with cc_220513 patch	Docker 20.10/CentOS 7.8
AhnLab CPP Security Agent for Windows Server	1.0.9.7 (build 88)	Windows Server 2012 R2 Windows Server 2016 Windows Server 2019
AhnLab V3 Net for Windows Server	9.0.67.9 (build 1840)	
AhnLab Application Control for Windows Server	1.0.3.6 (build 678)	
AhnLab Host IPS for Windows Server	1.0.4.6 (build 484)	
AhnLab CPP Security Agent for Linux Server	1.0.6.4 (build 64)	CentOS 7.6 (kernel 3.10.0-957.el7.x86_64) RHEL 7.8 (kernel 3.10.0-1127.el7.x86_64) RHEL 8.2 (kernel 4.18.0-193.el8.x86_64) Ubuntu 20.04 (kernel 5.8.0-43-generic) Amazon Linux 2 (kernel 4.14.154-128.181.amzn2.x86_64)
AhnLab V3 Net for Linux Server	3.6.10.7(build 801)	
AhnLab Application Control for Linux Server	1.0.6.5 (build 1657)	
AhnLab Host IPS for Linux Server	1.0.6.4 (build 1153)	

8 Users may obtain all TOE software components via download from AhnLab. User should contact AhnLab to obtain the correct TOE software versions.

9 **Note**: The Amazon Linux 2 endpoint is deployed as an on-premises virtual machine in the evaluated configuration.

2.4.1 Guidance Documents

10 The TOE includes the following guidance documents:

a) AhnLab CPP 1.0 Common Criteria Guide (PDF), v1.9

b) AhnLab CPP Management Help (HTML),
https://help.ahnlab.com/cpp/1.0.3/en_us/start.htm

c) AhnLab V3 Net for Windows Server Help (HTML),
https://help.ahnlab.com/V3_Net_90/en_us/start.htm

d) AhnLab V3 Net for Linux Server Help (HTML),

https://help.ahnlab.com/V3Net/V3Net_Linux/en_US/start.htm

2.4.2 Non-TOE Components

11 The TOE requires the following components in the environment:

a) **Administrator Workstation**. Workstation required to access and manage the TOE.

b) **NTP Server.** Time server.

c) **Mail Server.** Email server required for OTP.

d) **Supported Operating Systems.** The supported OS software identified in section 2.4 running on general purpose hardware.

2.5 Logical Scope

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

2.5.1 Excluded Functions

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

a) CPP Firewall

b) V3 for VDI

c) V3 Net for Unix

d) Cloud Based Protection

e) Reputation based detection

f) ASD Whitelist

3 Security Problem Definition

3.1 Threats

Table 4: Threats

Identifier	Description
T.MALWARE	Attackers compromise an endpoint via malware.
T.APPLICATION	Attackers may compromise an endpoint by executing malicious software.
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.
T.NETWORK	Attackers may gain access to protected resources through network attacks.

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.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.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.MALWARE	The TOE shall detect and respond to known and suspected malware on protected endpoints.
O.APPLICATION	The TOE shall collect an inventory of executable software on managed endpoints and allow or deny execution of files.
O.MGMT	The TOE shall authenticate administrators, restrict access according to role and record a log of their actions.
O.NETWORK	The TOE shall analyze network traffic for suspicious behavior and allow or deny the flow of information.
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 and between server and agents.

5 Security Requirements

5.1 Conventions

14 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 adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

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

Table 9: Extended Components

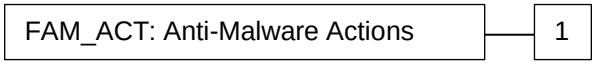
Class / Component	Title	Rationale
Class: FAM	Anti-Malware	No existing CC Part 2 classes or components address anti-malware requirements.
FAM_ACT.1	Anti-Malware Actions	
FAM_ALR.1	Anti-Malware Alerts	
FAM_SCN.1	Ani-Malware Scanning	
Class: FAC	Application Control	No existing CC Part 2 classes or components address application control requirements.
FAC_ACT.1	Application Control Actions	
FAC_SCN.1	Application Control Scanning	
Class: FIP	Intrusion Prevention	No existing CC Part 2 classes or components address IPS requirements.
FIP_ANL.1	IPS Analysis	
FIP_RCT.1	IPS React	

5.2.1 Anti-Malware Actions (FAM_ACT)

5.2.1.1 Family Behavior

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

5.2.1.2 Component Leveling



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

5.2.1.3 Management: FAM_ACT.1

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

a) Configuration of actions.

5.2.1.4 Audit: FAM_ACT.1

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

a) Basic: Action taken in response to detection of a malware.

FAM_ACT.1 Anti-Malware Actions

Hierarchical to: No other components.

Dependencies: FAM_SCN.1

FAM_ACT.1.1 Upon detection of [selection: *memory-based, process-based, file-based*] malware, the TSF shall: [assignment: *list of actions*].

5.2.2 Anti-Malware Alerts (FAM_ALR)

5.2.2.1 Family Behavior

20 This family defines requirements for delivering security alerts when malware is detected.

5.2.2.2 Component Leveling

21 FAM_ALR.1 Addresses alerts when malware is detected.

5.2.2.3 Management: FAM_ALR.1

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

a) Configuration of alerts.

5.2.2.4 Audit: FAM_ALR.1

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

a) None.

FAM_ALR.1 Anti-Malware Alerts

Hierarchical to: No other components.

Dependencies: FAM_SCN.1

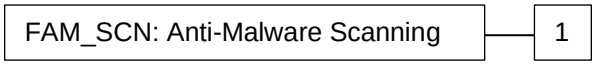
FAM_ALR.1.1 Upon detection of malware, the TSF shall generate the following alerts: [assignment: *list of alert types and destinations*].

5.2.3 Anti-Malware Scanning (FAM_SCN)

5.2.3.1 Family Behavior

24 This family defines requirements for malware scanning.

5.2.3.2 Component Leveling



25 FAM_SCN.1 Addresses malware scanning.

5.2.3.3 Management: FAM_SCN.1

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

a) Configuration of scanning parameters.

5.2.3.4 Audit: FAM_SCN.1

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

a) None

FAM_SCN.1 Anti-Malware Scanning

Hierarchical to: No other components.

Dependencies: No dependencies.

FAM_SCN.1.1 The TSF shall perform real-time, scheduled, and on-demand scans for malware based upon [selection: known signatures, reputation, behavior].

FAM_SCN.1.2 The TSF shall perform scheduled scans at the time and frequency configured by the Administrator.

5.2.4 Application Control Actions (FAC_ACT)

5.2.4.1 Family Behavior

28 This family defines requirements for application control.

5.2.4.2 Component Leveling

29 FAC_ACT.1 Addresses endpoint application control.

5.2.4.3 Management: FAC_ACT.1

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

a) Configuration of application whitelists.

5.2.4.4 Audit: FAC_ACT.1

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

a) Basic: Application control events and responses.

FAC_ACT.1 Application Control Actions

Hierarchical to: No other components.

Dependencies: FAC_SCN.1

FAC_ACT.1.1 Upon detection of an attempt to execute a runnable software file, the TSF shall perform the actions specified by the authorized administrator. Actions are administratively configurable on a per-Agent basis and consist of:

a) Allow execution of the file,

b) Block execution of the file,

c) [selection: [assignment: *list of other actions*], no other actions].

5.2.5 Application Control Scanning (FAC_SCN)

5.2.5.1 Family Behavior

32 This family defines requirements for application scanning.

5.2.5.2 Component Leveling

33 FAM_SCN.1 Addresses application scanning.

5.2.5.3 Management: FAC_SCN.1

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

a) Configuration of scanning parameters.

5.2.5.4 Audit: FAC_SCN.1

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

a) None

FAC_SCN.1 Application Control Scanning

Hierarchical to: No other components.

Dependencies: No dependencies.

FAC_SCN.1.1 The TSF shall perform real-time scans for running of unregistered software files.

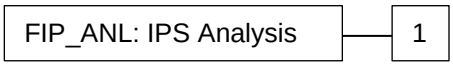
FAC_SCN.1.2 The TSF shall perform real-time scans for execution of runnable software.

5.2.6 IPS Analysis (FIP_ANL)

5.2.6.1 Family Behavior

36 This family defines requirements for network intrusion detection and prevention.

5.2.6.2 Component Leveling



37 FIP_ANL.1 Addresses network analysis.

5.2.6.3 Management: FIP_ANL.1

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

a) Configuration of IPS parameters.

5.2.6.4 Audit: FIP_ANL.1

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

a) Basic: Detection of events.

FIP_ANL.1 IPS Analysis

Hierarchical to: No other components.

Dependencies: No dependencies.

FIP_ANL.1.1 The TSF shall be able to apply a set of rules for analysing all inbound network traffic.

FIP_ANL.1.2 The TSF shall be able to apply a database of attack signatures representing the patterns of network intrusion attempts.

FIP_ANL.1.3 The TSF shall record within each analytical result at least the following information:

a) Date and detection time of the result, type of result, identification of the data source.

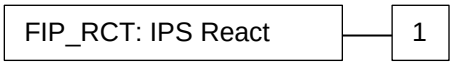
b) [assignment: *other additional information to be recorded*].

5.2.7 IPS React (FIP_RCT)

5.2.7.1 Family Behavior

40 This family defines requirements for actions to be taken when a network intrusion event is detected.

5.2.7.2 Component Leveling



41 FIP_RCT.1 Addresses the reaction to network attacks.

5.2.7.3 Management: FIP_RCT.1

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

a) Configuration of IPS parameters.

5.2.7.4 Audit: FIP_RCT.1

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

a) Basic: Reaction to network intrusion events.

FIP_RCT.1 IPS React

Hierarchical to: No other components.

Dependencies: FIP_ANL.1.

FIP_RCT.1.1 The TSF shall take [assignment: *list of actions*] when an intrusion event is detected.

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAC_ACT.1	Application Control Actions
FAC_SCN.1	Application Control Scanning
FAM_ACT.1	Anti-Malware Actions
FAM_ALR.1	Anti-Malware Alerts
FAM_SCN.1	Anti-Malware Scanning
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.3	Selectable Audit Review
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.5	Multiple Authentication Mechanisms
FIA_UID.2	User Identification Before Any Action
FIP_ANL.1	IPS Analysis
FIP_RCT.1	IPS React
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_TRP.1	Trusted Path

5.3.1 Application Control (FAC)

FAC_ACT.1 Application Control Actions

Hierarchical to: No other components.

Dependencies: FAC_SCN.1

FAC_ACT.1.1 Upon detection of an attempt to execute a runnable software file, the TSF shall perform the actions specified by the authorized administrator. Actions are administratively configurable on a per-Agent basis and consist of:

a) Allow execution of the file,

b) Block execution of the file,

c) [no other actions].

FAC_SCN.1 Application Control Scanning

Hierarchical to: No other components.

Dependencies: No dependencies.

FAC_SCN.1.1 The TSF shall perform real-time scans for running of unregistered software files.

FAC_SCN.1.2 The TSF shall perform real-time scans for execution of runnable software.

5.3.2 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 [memory-based, process-based, file-based] malware, the TSF shall: [

- *For file-based malware, perform the actions configured by the administrator, which may be:*
  - *Ignore: Does not repair or remove the infected file*
  - *Repair: Remove malware from an infected file*
  - *Quarantine: Quarantine files before attempting repair, If unable to repair then remove files*
  - *Remove: Removes the infected file without attempting to repair*
- *For process-based malware, terminate the process and delete the executable file.*
- *For memory-based malware, kill the infected thread*

]

Application Note: Actions are configured per scan type. Available actions are dependent on the scan type.

FAM_ALR.1 Anti-Malware Alerts

Hierarchical to: No other components.

Dependencies: FAM_SCN.1

FAM_ALR.1.1 Upon detection of malware, the TSF shall generate the following alerts: [*Malware alert log sent to CPP Management Server and malware alert displayed to the Endpoint User*].

FAM_SCN.1 Anti-Malware Scanning

Hierarchical to: No other components.

Dependencies: No dependencies.

FAM_SCN.1.1 The TSF shall perform real-time, scheduled, and on-demand scans for malware based upon [known signatures, behavior].

FAM_SCN.1.2 The TSF shall perform scheduled scans at the time and frequency configured by the Administrator.

5.3.3 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*
Security Agent Events	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Last Login User, Department, Details
Job History	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Last Login User, Department, Job, Status, Error

Event	*Additional Details*
Malware Infections	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Malware Name, Infection Path, Status, Scan Method
Scan/Real-Time Scan	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Last Login User, Department, Details
V3 Update	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Last Login User, Department, Details
HIPS Agent Events	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Function, Details
IPS Event	Log Received, Log Created, Detection Ended, Agent ID, Agent IP, Signature Name, Severity, Source IP, Source Port, Source Country, Destination IP, Destination Port, Destination Country, Network Direction, Session Direction, Packet Direction, Attack Attempt, No. of Packets, Response Method, Block Option, Packet Info
AC Agent Events	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Function, Details
Execution Control Events	Log Received, Log Created, Agent ID, Agent IP, Computer Name, Owner Process ID, File Name, File Path, File Hash, Provider, Signed by, File Size, Response Method, AC State, Reason

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_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 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.

FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filters*] of audit data based on [*date, Agent IP, Agent ID, computer name*].

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, agents, anti-malware, Host IPS, Application Control, and alerts].

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 Super 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_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) one-time password (OTP)*] 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 required;* • *OTP: valid OTP must be entered*].
Application Note:	OTP is emailed to the user once a valid username and password has been entered.

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.

5.3.6 Intrusion Prevention (FIP)

FIP_ANL.1 IPS Analysis

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIP_ANL.1.1	The TSF shall be able to apply a set of rules for analysing all inbound network traffic.
FIP_ANL.1.2	The TSF shall be able to apply a database of attack signatures representing the patterns of network intrusion attempts.
FIP_ANL.1.3	The TSF shall record within each analytical result at least the following information:

a) Date and detection time of the result, type of result, identification of the data source.

b) [*Log Received, Log Created, Detection Ended, Agent ID, Agent IP, Signature Name, Severity, Source IP, Source Port, Source Country, Destination IP, Destination Port, Destination Country, Network Direction, Session Direction, Packet Direction, Attack Attempt, No. of Packets, Response Method, Block Option, Packet Info*].

FIP_RCT.1 IPS React

Hierarchical to: No other components.

Dependencies: FIP_ANL.1.

FIP_RCT.1.1 The TSF shall take [*log the suspected detection of traffic and allow it pass, log the suspected detection of traffic and block*] when an intrusion event is detected.

5.3.7 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, security agents, Application Control settings, V3 settings, IPS settings*] 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 alerts (Notification Center)*
- *Manage dashboard (User-defined Dashboard)*
- *Manage Application Control*
    - *Scan settings / status*
    - *Application whitelists*
- *Manage Host IPS*
    - *Detection and response settings*
    - *Signature database*
- *Manage V3*
    - *Scan settings / status*
    - *Infected file response settings*.
- *View Process Trees]*.

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 [

- *Super Admin*
- *Policy Admin*
- *General Admin*
- *Department Admin*
- *License Admin*
- *Security Admin*
- *User-Defined Admin*
- *Endpoint User*].

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

Application Note: The TOE also supports custom roles with selected privileges. The Endpoint User role is an implied role applied to users of the endpoint.

5.3.8 Protection of the TSF

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.

5.3.9 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 [[*TOE administration*]].

5.4 Assurance Requirements

44 The TOE security assurance requirements are summarized in Table 11 commensurate with EAL2+ (ALC_FLR.1).

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.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 Management

45 The TOE enables secure management of its functions.

6.1.1 FAU_GEN.1

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

6.1.2 FAU_GEN.2

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

6.1.3 FAU_SAR.1

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

6.1.4 FAU_SAR.3

49 The TOE provides administrators with the ability to sort audit records.

6.1.5 FDP_ACC.1

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

6.1.6 FDP_ACF.1

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

6.1.7 FIA_UAU.2

52 TOE users must be authenticated before any administrative functions become available. Users are authenticated by a username and password, and optionally an OTP as described below.

6.1.8 FIA_UAU.5

53 In addition to username and password authentication, the TOE can be configured to use one-time passwords. When configured, OTP works as follows:

a) User authenticates with username and password;

b) TOE generates an OTP and emails it to the user (per email configured at user account creation);

c) User must enter the OTP within 10 minutes to successfully complete authentication.

6.1.9 FIA_UID.2

54 TOE users are identified by a username at login.

6.1.10 FMT_MSA.1

55 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.

6.1.11 FMT_MSA.3

56 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

57 The TOE management capabilities include:

a) Manage authentication settings (Management Console)

b) Manage administrator accounts

c) Manage agents (Agent Policy)

d) Manage dashboard (User-defined Dashboard)

e) *Manage Application Control*

- *Scan settings / status*
- *Application whitelists*

f) *Manage Host IPS*

- *Detection and response settings*
- *Signature database*

g) *Manage V3*

- *Scan settings / status*
- *Infected file response settings*].

h) View Process Trees

58 The management capabilities are further described at:

https://help.ahnlab.com/cpp/1.0.2/en_us/start.htm

6.1.13 FMT_SMR.1

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

a) **Super Admin.** A top-level admin with full control. Only a super admin has access to Settings.

b) **Policy Admin.** A policy admin has access to Management, but not Report.

c) **General Admin.** A general admin has access to Dashboard, Report and Log, where the admin can check the current status, logs and notifications, and view daily, weekly and monthly reports. There is no session timeout for a general admin, so the admin will not be automatically logged out.

d) **License Admin.** A license admin has privileges to features associated with the selected licensed product only. For example, if there is no Application Control license, the menu will not be activated. A license admin can check his or her account information, and specify a Security Admin.

e) **Department Admin.** A group admin has limited privileges to his or her department, with access to Management, Response and Report. A group admin can create a report on his or her department only.

f) **Security Admin.** A security admin is in charge of security, therefore can check detected malware and suspicious behaviors.

g) **User-Defined Admin**. A user-defined admin has access to specified features only.

60 An implied role of **Endpoint User** is also defined. This role applies to users of protected endpoints who have access to the V3 Agent user interface.

6.2 Security Dashboard

61 TOE administrators are able to view threat information and statistics via a configurable dashboard and process trees.

6.2.1 FMT_SMF.1

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

a) Top Malware Infected Agents: The agents with the most malware infection.

b) Top Malware: The most detected malware by period.

c) Top Suspicious Agents: The agents with the most suspicious behaviors.

d) Top Suspicious Binaries: The agents with the most suspicious binaries.

e) Top Suspicious Agents: The agents with the most suspicious behaviors by period.

63 The TOE also provides the capability to visualize threats as process trees to show the relation between process execution and suspicious behavior. The system name, process name, file name, registry and network are each displayed as an icon. The relation between these objects is indicated by an arrow and the order of behavior is shown in numbers.

6.3 Malware Detection & Response

64 The V3 TOE component provides malware detection and response functionality as described in the following sections.

6.3.1 FAM_ACT.1

65 Upon detection of malware, the TOE will respond with the administrator defined actions for the scan type. The actions that may be configured are:

a) Ignore: Does not repair or remove the infected file

b) Quarantine: Quarantine files before attempting repair, If unable to repair then remove files

c) Remove: Removes the infected file without attempting to repair

66 For process-based malware, administrators can configure whether to block or allow a process. If a process is registered as blocked, the TOE will terminate the process and delete the executable. If configured to allow, then the process is allowed to run without intervention.

6.3.2 FAM_ALR.1

67 When malware is detected, an alert is displayed to the Endpoint User. The content of the alert is dependent on the type of scan and the information available. Alerts contain details such as:

a) Name of the malware detected

b) Status of the malware

c) File path

d) Reputation score

e) Trust level

68 A log of alerts is also sent to the CPP Management Server (Agent Log). These alert logs contain details such as:

a) Log Received

b) Log Created

c) Agent ID

d) Agent IP

e) Computer Name

f) Malware Name

g) Infection Path

h) Status

i) Scan Method

6.3.3 FAM_SCN.1

69 The TOE V3 component performs anti-malware scanning in real-time, on-demand, and/or according to an administrator defined schedule.

70 The types of scans that may be performed are as follows:

a) **Smart Scan.** Smart Scan checks all files on local drives and automatically removes detected malware.

b) **Real-time Scan.** Continuously scans real-time I/O, boot record, memory, process and network drives for malware.

c) **Intense Scan.** Selects memory, process, boot record, critical system files and folders to scan for malware including email and compressed files.

71 The following detection methods are used by the TOE:

a) **Signature based detection.** Uses patterns and hash values to detect known malware.

b) **Behavior based detection.** Uses observation of suspicious file/process behavior patterns to detect objects that behave like malware.

6.4 Application Control

72 The Application Control TOE component provides application whitelisting and control functionality as described in the following sections.

6.4.1 FAC_ACT.1

73 The TOE can be configured to set the conditions of a file that must be met to allow the execution. The following Trusting Conditions can be set by an authorized administrator:

- **Valid Certificates**: This condition allows the execution of a file if it has a valid certification.
- **Signer Whitelist**: This condition allows the execution of a file if it is signed by a user permitted by the admin, without verifying the certificate.

- **Use File Supplier**: This condition allows the execution of a file if it is provided by a supplier permitted by the admin, without verifying the certificate.

6.4.2 FAC_SCN.1

74 The TOE may be configured in Simulation Mode which notifies administrators in case a file, that is not registered in the inventory policy, is executed during a specific time frame.

6.5 Intrusion Prevention

75 The Host IPS component provides network analysis and threat detection functionality as described in the following sections.

6.5.1 FIP_ANL.1

76 Authorized administrators have the ability to enable and configure IPS on the TOE. The TOE can be configured to analyze the network traffic and detect signature-based attacks, or the following:

- IP Fragmentation: Responds to attacks that bypass the signature-based defense feature by dismantling and transmitting malicious data from IP layer.
- TCP Segmentation: Responds to attacks that bypass the signature-based defense feature by dismantling and transmitting malicious data from TCP layer.
- URL Obfuscation: Responds to attacks that bypass signature-based defense feature by obfuscating and concealing malicious URL.

77 Administrators can choose to enable or disable the provided default signatures provided by AhnLab, or create custom signatures. The TOE generates a log for all IPS events.

6.5.2 FIP_RCT.1

78 IPS must be enabled on the TOE. When enabled, the IPS Operation Mode may be configured to either Detect or Block. If configured to only Detect, the TOE will log the suspected intrusion and allow the traffic to pass. If configured to Block, the TOE will log the suspected intrusion and block the traffic.

6.6 Protected Communications

6.6.1 FPT_ITT.1

79 Communications between the CPP Management Server and the CPP Security Agents are protected using TLSv1.2. The following cipher suites are supported in the evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

6.6.2 FTP_TRP.1

80 Communications between the CPP Management Server and remote administrators are protected using TLSv1.2. The supported cipher suites are identified in section 6.6.1.

7 Rationale

7.1 Security Objectives Rationale

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

Table 12: Security Objectives Mapping

	T.MALWARE	T.APPLICATION	T.EAVES	T.MGMT	T.NETWORK	OSP.DASHBOARD	A.ADMIN	A.USER	A.PHYSICAL	A.TIME
O.MALWARE	X									
O.APPLICATION		X								
O.MGMT				X						
O.NETWORK					X					
O.DASHBOARD						X				
O.PROTCOMMS			X							
OE.ADMIN							X			
OE.USERS								X		
OE.PHYSICAL									X	
OE.TIME										X

82 Table 12 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.MALWARE	**O.MALWARE.** Mitigates the threat of malware by requiring that the TOE detect and respond to known and suspected malware.

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.EAVES	**O.PROTCOMMS.** Mitigates this threat by requiring that the TOE encrypt communications for remote administrators and between the server and agents.
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.
T.NETWORK	**O.NETWORK.** Mitigates this threat by requiring that the TOE analyze incoming network traffic for know network attacks and denying or allow the flow of information.
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.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

83 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 14: Security Requirements Mapping

	O.MALWARE	O.APPLICATION	O.MGMT	O.NETWORK	O.DASHBOARD	O.PROTCOMMS
FAC_ACT.1		X				
FAC_SCN.1		X				
FAM_ACT.1	X					
FAM_ALR.1	X					
FAM_SCN.1	X					
FAU_GEN.1			X			
FAU_GEN.2			X			
FAU_SAR.1			X			
FAU_SAR.3			X			
FDP_ACC.1			X			
FDP_ACF.1			X			
FIA_UAU.2			X			
FIA_UAU.5			X			
FIA_UID.2			X			
FIP_ANL.1				X		
FIP_RCT.1				X		
FMT_MSA.1			X			
FMT_MSA.3			X			

	O.MALWARE	O.APPLICATION	O.MGMT	O.NETWORK	O.DASHBOARD	O.PROTCOMMS
FMT_SMF.1			X		X	
FMT_SMR.1			X			
FPT_ITT.1						X
FTP_TRP.1						X

Table 15: Suitability of SFRs

Objectives	SFRs
O.MALWARE	**FAM_ACT.1** requires malware response actions (respond). **FAM_ALR.1** requires alerts on malware detection (respond). **FAM_SCN.1** requires scanning for malware (detect).
O.APPLICATION	**FAC_ACT.1** requires application response actions (respond). **FAC_SCN.1** requires scanning for executable software (detect).
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. **FAU_SAR.3** requires the ability to sort of filter 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_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.

Objectives	SFRs
O.NETWORK	**FIP_ANL.1** requires network scanning for known attacks. **FIP_RCT.1** requires reactions to malicious network traffic.
O.DASHBOARD	**FMT_SMF.1** requires user-defined dashboard capability.
O.PROTCOMMS	**FPT_ITT.1** requires encrypted communications between the management server and endpoint agents. **FTP_TRP.1** requires encrypted communications for remote administration.

Table 16: Dependency Rationale

SFR	Dependency	Rationale
FAC_ACT.1	FAC_SCN.1	Met
FAC_SCN.1	None.	-
FAM_ACT.1	FAM_SCN.1	Met
FAM_ALR.1	FAM_SCN.1	Met
FAM_SCN.1	None.	-
FAU_GEN.1	FPT_STM.1	The TOE makes use of an NTP server for time stamps.
FAU_GEN.2	FAU_GEN.1	Met
	FIA_UID.1	Met by FIA_UID.2
FDP_ACC.1	FDP_ACF.1	Met
FDP_ACF.1	FDP_ACC.1	Met
	FMT_MSA.3	Met
FIA_UAU.2	FIA_UID.1	Met
FIA_UAU.5	None	-
FIA_UID.2	None	-
FIP_ANL.1	None.	-
FIP_RCT.1	FIP_ANL.1	Met

SFR	Dependency	Rationale
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_TRP.1	None	-