AhnLab

EPP, EDR 1.0 and V3 Endpoint Security 9.0

Security Target

Version 1.2

August 2019

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	29 Jul 2019	L Turner	Release for certification
1.1	8 Aug 2019	L Turner	Update TOE environment
1.2	26 Aug 2019	L Turner	Update TOE environment

Table of Contents

1 Introduction 5

1.1 Overview 5
1.2 Identification 5
1.3 Conformance Claims 5
1.4 Terminology 5

2 TOE Description 7

2.1 Type 7
2.2 Usage 7
2.3 Security Functions 8
2.4 Physical Scope 8
2.5 Logical Scope 9

3 Security Problem Definition 11

3.1 Threats 11
3.2 Organizational Security Policies 11
3.3 Assumptions 11

4 Security Objectives 12

4.1 Objectives for the Operational Environment 12
4.2 Objectives for the TOE 12

5 Security Requirements 13

5.1 Conventions 13
5.2 Extended Components Definition 13
5.3 Functional Requirements 15
5.4 Assurance Requirements 23

6 TOE Summary Specification 24

6.1 Secure Management 24
6.2 Security Dashboard 25
6.3 Malware Detection & Response 26
6.4 Threat Detection & Response 27

7 Rationale 31

7.1 Security Objectives Rationale 31
7.2 Security Requirements Rationale 32

List of Tables

Table 1: Evaluation identifiers 5
Table 2: Terminology 5
Table 3: Threats 11
Table 4: Organizational Security Policies 11
Table 5: Assumptions 11
Table 6: Security Objectives for the Operational Environment 12
Table 7: Security Objectives 12
Table 8: Extended Components 13
Table 9: Summary of SFRs 15
Table 10: Assurance Requirements 23
Table 11: Security Objectives Mapping 31
Table 12: Suitability of Security Objectives 31
Table 13: Security Requirements Mapping 33

Table 14: Suitability of SFRs 33
Table 15: Dependency Rationale 34

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the AhnLab EPP, EDR 1.0 and V3 Endpoint Security 9.0 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 EPP, EDR 1.0 and V3 Endpoint Security 9.0 See section 2.4 for software build numbers.
Security Target	AhnLab EPP, EDR 1.0 and V3 Endpoint Security 9.0: Security Target, v1.1

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

1.4 Terminology

Table 2: Terminology

Term	Definition
ASD	AhnLab Smart Defense
CC	Common Criteria
EAL	Evaluation Assurance Level
EDR	AhnLab Endpoint Detection and Response solution
Endpoint	Host on the network protected by AhnLab.
Endpoint User	User of an endpoint system.
EPP	AhnLab Endpoint Protection Platform
ESA	AhnLab Endpoint Security Assessment solution

Term	Definition
ES	Endpoint Security
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
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.
STIX	Structured Threat Information eXpression
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 console and agent to efficiently operate and manage multiple endpoint security solutions. The TOE includes two of these endpoint security solutions: AhnLabV3 (anti-virus) and AhnLab EDR (behavioral threat detection and response).

2.2 Usage

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

a) **AhnLab EPP Management Manager.** EPP is a management platform that is used to efficiently operate and manage multiple AhnLab endpoint security solutions. These endpoint security solutions are deployed as agents via the EPP. EPP provides a web-based user interface for TOE administration, definition of policies and review of a configurable security dashboard.

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

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

d) **AhnLab EDR.** The EDR server[1] and agent provide behavioural threat detection and response capabilities.

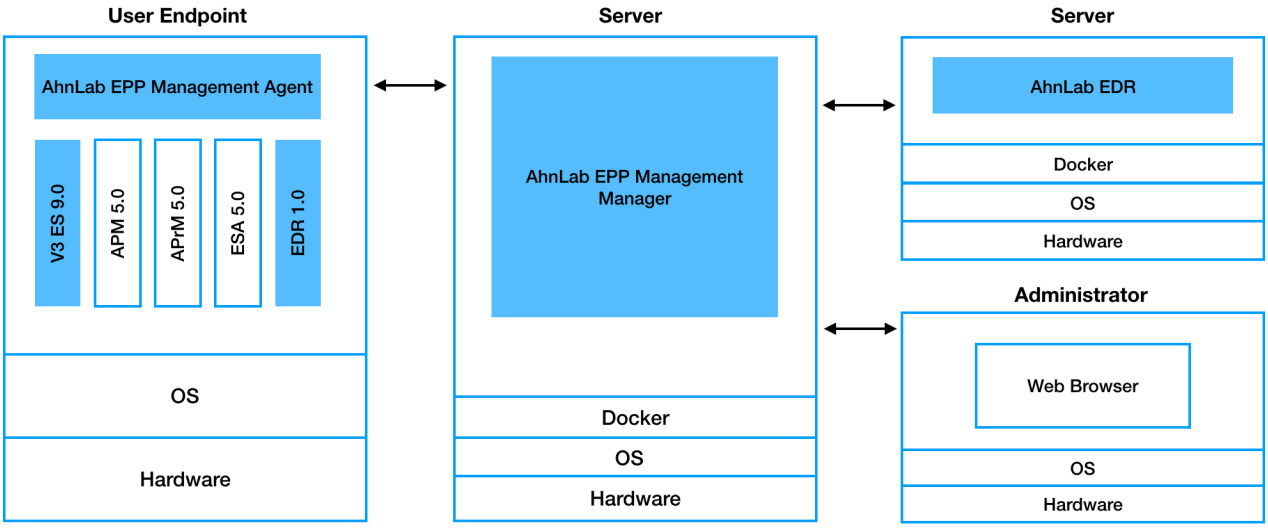


Figure 1: TOE components

[1] The EDR server component is an EPP Management Manager server configured to be in EDR mode. This enables offload of EDR related analysis from the primary EPP Management Manager server.

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 EPP Patch Management

      (2) AhnLab Privacy Management

      (3) AhnLab ESA

      (4) AhnLab EDR

      (5) AhnLab V3 Endpoint Security

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) Reputation-based malware detection

   iii) Behavior-based malware detection

   iv) Repair, quarantine and/or deletion of infected files

   v) Content filtering (blocking malicious websites)

d) **Threat Detection & Response.** The EDR TOE component provides the following behavioral threat detection and response functionality:

   i) Detect suspicious file, process, system, network or registry behavior.

   ii) Generate process trees of suspicious behavior to allow analysts to visualize relationships between suspicious systems, files and processes.

   iii) Respond to detected suspicious behavior - Block Network, Collect Artifact, Terminate Process and Search for/Collect Files.

2.4 Physical Scope

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

a) AhnLab EPP Management Manager 1.0.2.16 / EDR Manager 1.0.2.16 on:

   i) Docker 18.09 / CentOS 7

b) AhnLab EPP Management Agent 1.0.2.10(861) on:

   i) Windows 7, 8, 8.1 and 10

   ii) Windows Server 2008 SP2, 2008 R2, 2012, 2012 R2 and 2016

iii) macOS Sierra (10.12) and High Sierra (10.13)

c) AhnLab EDR Agent 1.0.2.10(861) on:

i) Windows 7, 8 and 10

ii) Windows Server 2008 SP2, 2008 R2, 2012, 2012 R2 and 2016

d) AhnLab V3 Endpoint Security 9.0.56.1 (Build 1418) on:

i) Windows 7, 8, 8.1 and 10

8 Users obtain the TOE via download from AhnLab.

2.4.1 Guidance Documents

9 The TOE includes the following guidance documents:

a) AhnLab EPP, EDR 1.0 and V3 Endpoint Security 9.0 Common Criteria Guide (PDF), v1.0

b) AhnLab EPP Management Help (HTML), https://help.ahnlab.com/epp/1.0.2/en_us/start.htm

c) AhnLab V3 Endpoint Security Help (HTML), https://help.ahnlab.com/V3_ES_90/en_us/start.htm

2.4.2 Non-TOE Components

10 The TOE requires the following components in the environment:

a) **NTP Server.** Time server.

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

c) **ASD Cloud Server.** The ASD cloud server (cloud service provided by AhnLab).

d) **Supported Operating Systems.** The supported OS software identified in section 2.4.

11 The EPP Management Manager operates with the following AhnLab endpoint security solutions in the TOE environment:

a) AhnLab EPP Patch Management 5.0

i) AhnLab EPP Patch Management Manager 5.0

ii) AhnLab EPP Patch Management Agent 5.0

b) AhnLab Privacy Management 5.0

i) AhnLab Privacy Management Manager 5.0

ii) AhnLab Privacy Management Agent 5.0

c) AhnLab ESA 1.0

i) AhnLab ESA Manager 1.0

ii) AhnLab ESA Agent 1.0

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) V3 Network Intrusion Prevention

b) V3 Device Control

c) V3 Safe Experience

3 Security Problem Definition

3.1 Threats

Table 3: Threats

Identifier	Description
T.MALWARE	Attackers compromise an endpoint via malware.
T.APT	Attackers use advanced techniques and/or zero-day exploits via unknown entry points to affect a prolonged compromise of an endpoint.
T.MGMT	Attackers compromise or disable the TOE via its management interfaces.

3.2 Organizational Security Policies

Table 4: Organizational Security Policies

Identifier	Description
OSP.DASHBOARD	The TOE must provide a configurable dashboard that allows administrators to review security relevant analytical data.

3.3 Assumptions

Table 5: 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.
A.COMMS	The IT environment will protecte network communications between TOE components and between the TOE and administrators.
A.CLOUD	The AhnLab Cloud Server in the IT environment will provide malware analysis services for TOE submitted artifacts.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: 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.
OE.COMMS	The IT environment shall provide protected network communications between TOE components and between the TOE and administrators.
OE.CLOUD	The AhnLab Cloud Server[2] in the IT environment shall provide malware analysis services for TOE submitted artifacts.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.MALWARE	The TOE shall detect and respond to known and suspected malware on protected endpoints.
O.APT	The TOE shall detect and facilitate analysis of suspicious behaviour on protected endpoints; and allow administrators to specify response actions to be taken.
O.MGMT	The TOE shall authenticate administrators, restrict access according to role and record a log of their actions.
O.FILTER	The TOE shall filter known malicious websites.
O.DASHBOARD	The TOE shall provide a configurable dashboard that allows administrators to review security relevant analytical data.

[2] Also referred to as AhnLab Smart Defense (ASD)

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

Table 8: Extended Components

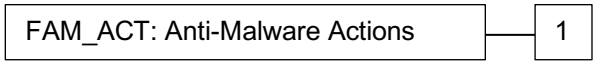
Class / Component	Title	Rationale
Class: FAM	Anti-Malware	No existing CC Part 2 classes or components address anti-malware requirements.
FAM_ACT.1	Anti-Malware Actions	
FAM_ALR.1	Anti-Malware Alerts	
FAM_SCN.1	Ani-Malware Scanning	

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

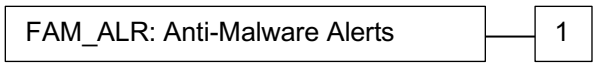
FAM_ACT.1.1 Upon detection of [selection: *memory-based, file-based*] malware, the TSF shall: [assignment: *list of actions*].

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

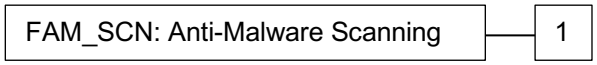
FAM_ALR.1.1 Upon detection of malware, the TSF shall generate the following alerts: [assignment: *list of alert types and destinations*].

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.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FAM_ACT.1	Anti-Malware Actions
FAM_ALR.1	Anti-Malware Alerts
FAM_SCN.1	Anti-Malware Scanning
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAA.3	Simple Attack Heuristics
FDP_IFC.1	Subset information flow control

Requirement	Title
FDP_IFF.1	Simple security attributes
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
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

5.3.1 Anti-Malware (FAM)

FAM_ACT.1 Anti-Malware Actions

Hierarchical to: No other components.

Dependencies: FAM_SCN.1

FAM_ACT.1.1 Upon detection of [memory-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 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 EPP Management Manager 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, reputation, behavior].

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

5.3.2 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~~ [*allow the Administrator:*

- *Block Network*
- *Collect Artifact*
- *Terminate Process*
- *Collect Files*

] 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*
EPP Agent event	*IP Address, Computer Name, Last Logged in User, Department, Content (description of event).*

Event	*Additional Details*
Task History	*Task, Status, Contents, Error*
Malware Infection	*Agent ID, IP Address, Computer Name, Last Logged in User, Department, Malware Name, Infected File Path, Hash Value, Status, Scan Type, Owner, Accessed Computer, Infected Computer*
Scan/Real-time Scan	*Agent ID, IP Address, Computer Name, Last Logged in User, Department, Contents, Details*
V3 Update	*Agent ID, IP Address, Computer Name, Last Logged in User, Department, Contents, Details*
EDR History	*Agent ID, Type, Hash Value, Process Name, Process Path, Target, Target File Path, Description*
Administrator Event	*Administrator ID, Administrator IP Address, Description*
Update	*Server Name, Server IP Address, Category, Description*
Agent Installation File	*Installation File Name, Description*

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.3 Simple Attack heuristics

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [

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

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

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [*system activity collected by agents deployed on protected endpoints*].

FAU_SAA.3.3 The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

5.3.3 User Data Protection (FDP)

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*Content Filtering SFP*] on [

- *Subjects: Endpoints*
- *Information: HTTP traffic*
- *Operations: HTTP operations*].

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

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

FDP_IFF.1.1 The TSF shall enforce the [*Content Filtering SFP*] based on the following types of subject and information security attributes: [

- *Endpoint attributes:*
  - *Agent Identifier*
- *HTTP traffic attributes:*
  - *URL*].

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: [*permitted by default*].

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

FDP_IFF.1.4 The TSF shall explicitly allow an information flow based on the following rules: [*URL references an explicitly allowed website per Administrator configuration*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*URL matches filtered website per Administrator configuration of the Content Filter for:*

- *Malicious sites*
- *Phishing sites*
- *Potentially unwanted sites*
- *Administrator defined site*].

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 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.

5.3.5 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 [*Content Filter SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Content Filter Rules*] to [*Super Admin* and *Endpoint User*].

FMT_MSA.3 Static attribute initialization

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 [*Content Filter 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 [*Super Admin, Policy Admin, Endpoint 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 EDR*
    - *Detection settings / status*
    - *Response settings / status*

- *Manage V3*
  - *Scan settings / status*
  - *Content filter settings*
  - *Infected file response settings*].

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*
- *Group Admin*
- *License Admin*
- *Security 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.

5.4 Assurance Requirements

28 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
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

29 The TOE enables secure management of its functions.

6.1.1 FAU_GEN.1

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

6.1.2 FAU_GEN.2

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

6.1.3 FIA_UAU.2

32 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.

6.1.4 FIA_UAU.5

33 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.

6.1.5 FIA_UID.2

34 TOE users are identified by a username at login.

6.1.6 FMT_MSA.1

35 The following users roles are able to modify the content filter settings:

a) Super Admin

b) Policy Admin

c) Endpoint User (implied role for V3 Agent user)

6.1.7 FMT_MSA.3

36 The TOE uses restrictive default values for content filtering by enabling the following filtering rules by default:

a) Malicious sites filtering

b) Phishing sites filtering

6.1.8 FMT_SMF.1

37 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 EDR

   i) Detection settings / status

   ii) Response settings / status

f) Manage V3

   i) Scan settings / status

   ii) Content filter settings

g) Infected file response settings

h) View Process Trees

38 The management capabilities are further described at:
http://help.ahnlab.com/epp/1.0.1/en_us/start.htm

6.1.9 FMT_SMR.1

39 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 Dashboard and 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 EDR license, Detection menu will not be activated. A license admin can check his or her account information, and specify a Security Admin.

e) **Group 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.

40 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

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

6.2.1 FMT_SMF.1

42 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.

43 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

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

6.3.1 FAM_ACT.1

45 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

6.3.2 FAM_ALR.1

46 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

47 A log of alerts is also sent to the EPP Management Manager (Agent Log). These alert logs contain details such as:

a) Agent ID

b) IP Address

c) Computer Name

d) Last Logged in User

e) Malware Name

f) Infected File Path

g) Hash Value

h) Status

6.3.3 FAM_SCN.1

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

49 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.

50 The following detection methods are used by the TOE:

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

b) **Reputation based detection.** Uses AhnLab Smart Defense reputation scores to detect objects that are reputed to be malware.

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

51 When **Cloud-based Protection** is enabled, suspicious objects may be sent to the AhnLab Cloud Server for analysis using a combination of the above methods.

6.3.4 FDP_IFC.1

52 TOE agents enforce content filtering rules on HTTP (web) requests from protected endpoints as described below.

6.3.5 FDP_IFF.1

53 TOE administrators can configure content filtering rules as follow:

a) **Block malicious sites.** Filters web sites that AhnLab has identified as malicious.

b) **Block phishing sites.** Filters web sites that AhnLab has identified as phishing sites.

c) **Block potentially unwanted sites.** Filters web sites that AhnLab has identified as suspicious.

d) **Administrator defined filter.** Explicitly allow or deny access to web sites designated by the administrator.

6.4 Threat Detection & Response

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

6.4.1 FAU_ARP.1

55 When behavioral threats are detected (as described below), the TOE is capable of the following responses:

a) **Block Network.** TOE agent components block outgoing network packets from the endpoint. If it is a TCP session, a reset packet is sent to terminate the session.

b) **Collect Artifact.** TOE agent components collect log information, history information, timeline, registry and additional information and report this to the EPP server for analysis by TOE administrators.

c) **Terminate Process.** TOE agent components collects the file that generated the detected behavior, and ends the created process.

d) **Collect Files.** TOE agent components search for the specified files, collects and submits them to the EPP server for analysis.

6.4.2 FAU_SAA.3

56 The TOE detects behavioral threats based on the following suspicious behaviors:

a) System: Suspicious system behavior:

i) Loads drivers: Driver loading has been detected in the system. If the detected process and loaded driver are whitelisted or digitally signed, it will not be logged.

ii) Performs injection: Injection has been detected in the system.

iii) Writes to child process memory: If the target process and child process are whitelisted, it will not be logged.

iv) Writes to other process memory: If the target process and other process are whitelisted, it will not be logged.

v) Opens physical memory object: Attempt to open the physical memory object has been detected in the system.

b) File: Suspicious file behavior:

i) Creates a file. Files created by an untrusted process within the last 5 minutes and ZIP files will be logged.

ii) Creates an executable file. If the target file and created executable file are whitelisted or digitally signed, it will not be logged.

iii) Downloads an executable file. If the downloaded executable file is whitelisted or digitally signed, it will not be logged.

iv) Deletes an executable file. If the target file and created executable file are whitelisted, it will not be logged.

v) Renames an executable file. File renamed by trustedinstaller.exe in System32 will not be logged.

vi) Modifies an executable file. If the target file and modified are whitelisted or digitally signed, it will not be logged.

vii) Replicates itself. If the target file is whitelisted or digitally signed, it will not be logged.

viii) Deletes itself. If the target file is whitelisted, it will not be logged.

ix) Renames itself. If the target file and renamed file are whitelisted, it will not be logged.

x) Changes system files.

xi) Changes the Hosts file.

xii) Creates an Autorun.inf file.

xiii) Registers a scheduled task. (Excluded if the current process is whitelisted.)

xiv) Writes data to the MBR.

xv) Downloads data files. Downloaded Non-PE file will be logged – zip, jar, hwp, doc, xls, ppt and msi.

xvi) Opens document files. If the target file is whitelisted or accessed known programs (word.exe, excel.exe or hwp.exe), it will not be logged. First initial to open the target document file will be logged.

xvii) Accesses multiple document files (jpg, doc and hwp). If the target file accesses document files (jpg, doc and hwp), and modifies the files 5 times, renames the files 10 times and removes the files 15 times, it will be logged. If all of the above processes are whitelisted and the files are external files, it will not be whitelisted.

xviii) Changes file properties. If the target file is whitelisted, it will not be logged.

c) Process: Suspicious process behavior:

i) Creates a new process. If the target process and created process are whitelisted or digitally signed, it will not be logged.

ii) Runs abnormal execution of process. Svchost.exe, csrss.exe, wininit.exe, winlogon.exe, services.exe and explorer.exe of Windows will not be logged.

iii) Executes a suspicious process. Winlogon.exe, logonui.exe, userinit.exe, WgaTray.exe and svchost.exe of Windows, and whitelisted and digitally signed target process and created process will not be logged.

iv) Loads DLLs. Whitelisted DLLs will not be logged. Packet.dll and Sysdm.cpl loaded by non-whitelisted process will be logged.

v) Loads suspicious DLL.

d) Registry: Suspicious registry behavior. Common OS registry behavior will not be logged. Only the changes in the registry in specified path will be detected.

i) Registers an autorun: Registers the process under the Runonce key to autorun at startup. E.g.) HKU\S-xxx\Software\Microsoft\Windows\CurrentVersion\Runonce

ii) Registers a screen saver file (*.SCR)

iii) Registers an autorun program in registry. (e.g. HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File ExecutionOptions\FlashPlayerUpdateService.exe)

iv) Registers Internet Explorer browser helper object: Registers Internet Explorer browser helper object. E.g.) HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser HelperObjects\{xxx}

v) Registers Internet Explorer toolbar.

vi) Changes Internet Explorer search settings.

vii) Changes Internet Explorer start page.

viii) Changes Internet Explorer advanced settings: Changes Internet Explorer advanced settings. E.g.) HKU\S-1-5-21-152636949-826243119-599685761-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings

ix) Changes Internet Explorer security settings.

x) Changes Internet Explorer extensions.

xi) Changes Internet Explorer pop-up settings.

xii) Attempts to change the security level.

xiii) Configures program concealment.

xiv) Changes WinSock2 communication settings.

xv) Changes security zone level for Internet options.

xvi) Changes autorun setting of CD/USB drives.

xvii) Changes shell folder.

xviii) Sets to change file name on system startup. If set by Windows process, it will not be logged.

xix) Registers recursive autorun.

xx) Registers abnormal autorun.

xxi) Registers itself in Service.

xxii) Registers itself in the screen saver.

xxiii) Registers itself on the Internet Explorer toolbar.

xxiv) Changes network connection properties.

e) Network: Suspicious network behavior.

i) Connects to network. After the first connection to HTTP, random connections will be logged. Each HTTPS, Mail Port, overseas IP and TCP connection will be logged one time.

ii) Abnormal network packets. If suspicious behavior is detected, it will be logged once only. If the target process is whitelisted, it will not be logged.

57 The TOE EDR component may also use Indicator of Compromise (IOC) defined patterns to identify suspicious behaviours. IOC files define signs of malicious activity in STIX format.

7 Rationale

7.1 Security Objectives Rationale

58 Table 11 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 11: Security Objectives Mapping

	T.MALWARE	T.APT	T.MGMT	OSP.DASHBOARD	A.ADMIN	A.USER	A.PHYSICAL	A.TIME	A.COMMS	A.CLOUD
O.MALWARE	X									
O.APT	X	X								
O.MGMT			X							
O.FILTER	X									
O.DASHBOARD				X						
OE.ADMIN					X					
OE.USERS						X				
OE.PHYSICAL							X			
OE.TIME								X		
OE.COMMS									X	
OE.CLOUD										X

59 Table 12 provides the justification to show that the security objectives are suitable to address the security problem.

Table 12: 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
	O.APT. Mitigates the threat of unknown malware by detecting suspicious behaviour and allowing relevant analysis and response. **O.FILTER.** Mitigates the threat of downloading malware from known malicious websites.
T.APT	**O.APT.** Mitigates this threat by requiring that the TOE detect suspicious behaviour, which is indicative of a compromise by attackers, and allowing further analysis and response.
T.MGMT	**O.MGMT.** Mitigates this threat by preventing unauthorized access via authentication, limiting access to functions based on role and auditing administrative actions to allow any unauthorized actions to be detected.
OSP.DASHBOARD	**O.DASHBOARD.** Upholds the stated policy by requiring the TOE to implement the required functionality.
A.ADMIN	**OE.ADMIN.** Upholds the assumption by restating it as an objective for the operational environment.
A.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.
T.TIME	**OE.TIME.** Upholds the assumption by restating it as an objective for the operational environment.
A.COMMS	**OE.COMMS.** Upholds the assumption by restating it as an objective for the operational environment.
A.CLOUD	**OE.CLOUD.** Upholds the assumption by restating it as an objective for the operational environment.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

60 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 13: Security Requirements Mapping

	O.MALWARE	O.APT	O.MGMT	O.FILTER	O.DASHBOARD
FAM_ACT.1	X				
FAM_ALR.1	X				
FAM_SCN.1	X				
FAU_ARP.1		X			
FAU_GEN.1			X		
FAU_GEN.2			X		
FAU_SAA.3		X			
FDP_IFC.1	X			X	
FDP_IFF.1	X			X	
FIA_UAU.2			X		
FIA_UAU.5			X		
FIA_UID.2			X		
FMT_MSA.1			X		
FMT_MSA.3			X		
FMT_SMF.1			X		X
FMT_SMR.1			X		

Table 14: 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). **FDP_IFC.1** requires filtering of malicious sites (protect). **FDP_IFF.1** requires filtering of malicious sites (protect).
O.APT	**FAU_ARP.1** requires response capability for behavioral threats (respond). **FAU_SAA.3** requires behavioural detection capabilities (detect).
O.MGMT	**FAU_GEN.1** requires auditing of security relevant events. **FAU_GEN.2** requires inclusion of identity in audit events. **FIA_UAU.2** requires authentication of users. **FIA_UAU.5** requires multiple authentication mechanisms. **FIA_UID.2** requires identification of users. **FMT_MSA.1** requires management of security attributes. **FMT_MSA.3** requires restrictive default values for security attributes. **FMT_SMF.1** requires specification of management functions. **FMT_SMR.1** requires specification of security roles.
O.FILTER	**FDP_IFC.1** requires filtering of HTTP. **FDP_IFF.1** requires filtering of HTTP.
O.DASHBOARD	**FMT_SMF.1** requires user-defined dashboard capability.

Table 15: Dependency Rationale

SFR	Dependency	Rationale
FAM_ACT.1	FAM_SCN.1	Met
FAM_ALR.1	FAM_SCN.1	Met
FAM_SCN.1	None.	-
FAU_ARP.1	FAU_SAA.1	Not met. FAU_SAA.3 is used as the basis for security alarms instead.
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

SFR	Dependency	Rationale
FAU_SAA.3	None	-
FDP_IFC.1	FDP_IFF.1	Met
FDP_IFF.1	FDP_IFC.1	Met
	FMT_MSA.3	Met
FIA_UAU.2	FIA_UID.1	Met
FIA_UAU.5	None	-
FIA_UID.2	None	-
FMT_MSA.1	FDP_ACC.1, or FDP_IFC.1	Met
	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