# AhnLab MDS

More security,
More freedom

샌드박스 기반의 지능형 위협 대응 솔루션

표준제안서


AhnLab

# CONTENTS





AhnLab

# 01
# 제안 배경

국내외 주요 지능형 공격 피해 사례

주요 지능형 공격 기법

주요 지능형 공격 유입 경로

최신 지능형 공격 트렌드

기존 보안 솔루션의 지능형 공격 대응 한계

지능형 공격 대응 방안 모색의 필요성

# 국내외 주요 지능형 공격 피해 사례

불특정 다수가 아닌 특정한 대상을 겨냥한 치밀하고 지능화된 공격(Advanced Persistent Threat, APT)이 지속적으로 증가하고 있습니다.
이러한 지능화된 공격은 주로 이메일, 웹, 엔드포인트를 통해 기업 및 기관에 유입, 막대한 피해를 야기하고 있습니다.

## 웹(네트워크) 기반 공격

개인정보
**8,000만 건** 유출

미국 유명 보험사

랜섬웨어
약 **4만 명** 감염

국내 유명 커뮤니티 사이트

## 이메일 기반 공격

개인정보
**5억 건** 유출

글로벌 포털 사이트

개인정보
**1,000만 건** 유출

국내 인터넷 쇼핑몰

## 엔드포인트 기반 공격

다수의
**중요 정보** 유출

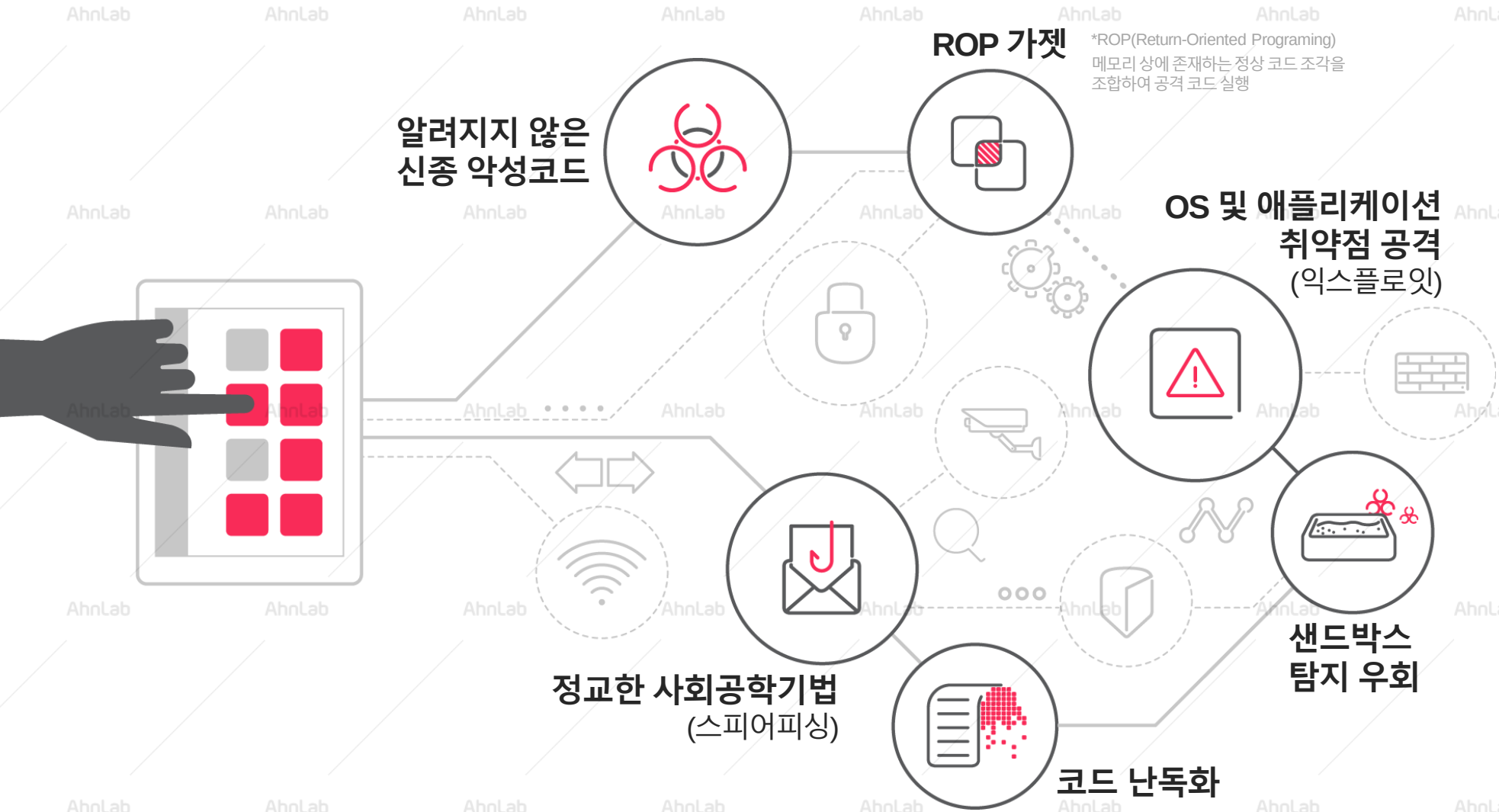
사회기반 시설

파일 암호화(랜섬)
**17,000달러**

미국 대형 병원

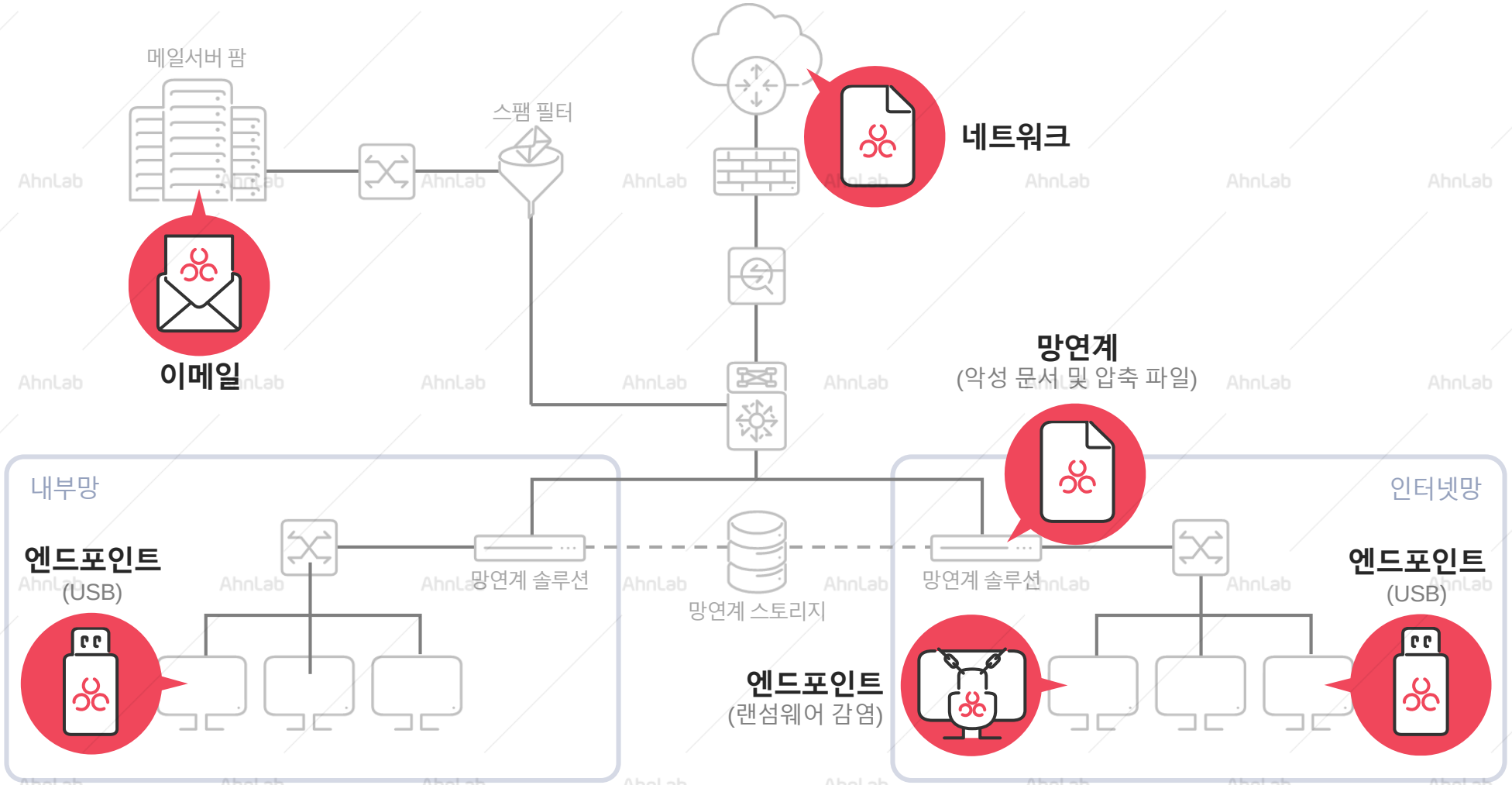
# 주요 지능형 공격 기법

지능형 공격은 보안 솔루션의 탐지를 피하기 위해 정교한 기술과 다양한 방식을 복합적으로 이용해 공격을 전개합니다.



# 주요 지능형 공격 유입 경로

정교하고 복합적인 기술을 이용한 지능형 공격은 네트워크, 이메일은 물론 망연계 구간 등 다양한 경로를 통해 지속적으로 침입을 시도합니다.
공격 경로면에서 직접 엔드포인트에 침투해 악성 행위를 수행하는 랜섬웨어 또한 지능형 위협의 일종으로 분류됩니다.



# 최신 지능형 공격 트렌드

최근 지능형 위협은 언제, 어디서, 어떤 목적으로, 어떤 경로를 통해 유입되는지 파악하기 어려울 만큼 다변화된 양상을 보이고 있습니다.
또한 공격 툴과 인프라 등을 제공하는 사이버 범죄의 서비스화(Crime as a Service)로 APT 공격이 증가할 것으로 전망됩니다.

| | 기존 APT | → 최신 APT |
|---|---|---|
| **공격 목적** | 정치적·사회적 목적 | 정치적•사회적 목적 + 금전적 목적 |
| **공격 주체** | 국가 주도(사이버전) | 국가, 스폰서십 + 해커 집단 |
| **공격 유입 경로** | 웹, 이메일 | 웹, 이메일 + 네트워크, 엔드포인트 직접 침투 |
| **악성코드** | 실행 파일(.exe) | 실행 파일 + 문서 파일, 스크립트 등 |

+

- 보안 솔루션 우회 기술 탑재
- 사이버 범죄 서비스화(Crime as a Service)

# 기존 보안 솔루션의 지능형 공격 대응 한계

지능형 공격이 지속적으로 고도화•다변화되면서
기존의 보안 솔루션만으로는 대응하기 쉽지 않기 때문에 공격 변화에 따른 다각화된 대응이 추가•보완되어야 합니다.

| 기존 보안솔루션 | 보완점 |
| --- | --- |
| **Firewall & NGFW**<br>네트워크 접근 통제 및<br>어플리케이션 통제를 통한 악성코드 유입 차단 | **허용된 주소, 프로토콜,<br>어플리케이션을 통한<br>악성코드 유입 차단 방안 필요** |
| **IPS**<br>네트워크 기반 룰을 통한<br>악성코드 유입 차단 | **파일 기반<br>악성코드 탐지 방안 필요** |
| **Spam Filter**<br>스팸/정크 메일 차단 및<br>시그니처 매칭을 통한 악성 첨부파일 차단 | **신•변종 악성 첨부파일, 압축 파일<br>및 본문 내 악성 URL에 대한 탐지<br>방안 필요** |
| **AV**<br>시그니처 매칭을 통한<br>악성코드 유입•실행 차단 | **신•변종 악성코드 및 랜섬웨어<br>탐지·차단 보완 필요** |

# 지능형 공격 대응 방안 모색의 필요성

지능형 공격에 효과적으로 대응하기 위해서는 최신 공격의 특성을 다각도로 고려하면서도 기존 보안 솔루션과 유기적으로 연계된 사이버 킬체인(Cyber Kill-Chain) 마련이 필요합니다.

## 공격 대상 정찰

치밀한 사전 준비

## Predict 사전 예측

공격 배후 세력 및
공격 전략 분석

## 사전 예방 Prevent

최신 글로벌 및 국내
보안위협 인텔리전스

## 공격 명령 및 제어

C&C 서버를 통한 악성코드 및 명령 전달

## 사이버 무기화

- 신종 악성코드
- 신규 취약점 익스플로잇

## Respond 대응

네트워크 및 엔드포인트
- 다단계 차단 기술

악성 이메일 차단(격리)
감염 의심 호스트 격리

## 탐지 Detect

멀티엔진 기반 탐지/분석
- 시그니처 기반
- 클라우드 평판 기반
- 샌드박스 분석

샌드박스 우회 악성코드 탐지/분석

## 다양한 경로를 통한 침입

웹, 이메일 첨부파일, 망연계 구간, SSL 트래픽, USB 등

# 02
# AhnLab MDS

AhnLab MDS 개요

단계별 지능형 위협 대응 프로세스

대응 프로세스 1 – 위협 수집

대응 프로세스 2 – 위협 탐지 및 분석

대응 프로세스 3 – 모니터링

대응 프로세스 4 – 영역별 위협 대응

# AhnLab MDS

**AhnLab MDS**는 다양한 공격 유입 경로별로 최적화된 대응 방안을 제공하는 **지능형 위협 대응 솔루션**입니다.
'수집-탐지/분석-모니터링-대응' 프로세스를 통해 랜섬웨어 및 신종 악성코드, 익스플로잇(exploit) 등 고도화된 공격에 효과적으로 대응합니다.

## 네트워크 기반 공격 대응

이상 트래픽 탐지 및 차단

## 엔드포인트 기반 공격 대응

악성코드 삭제 /실행 보류 | 의심 파일 추출 | 시스템 격리

## 이메일 기반 공격 대응

이메일 격리 기능 | 이메일 필터링 연계

## 망연계/ 파일 서버 대응

망연계 솔루션 연동 | 3rd party 솔루션 연계

### 수집

주요 경로를 통해
유입되는 위협 수집

### 탐지/분석

멀티엔진 기반의
다단계 분석 모듈 제공

### 모니터링

직관적인 위협 가시성
지속적인 위협 모니터링

### 대응

네트워크 에이전트 기반
위협 대응

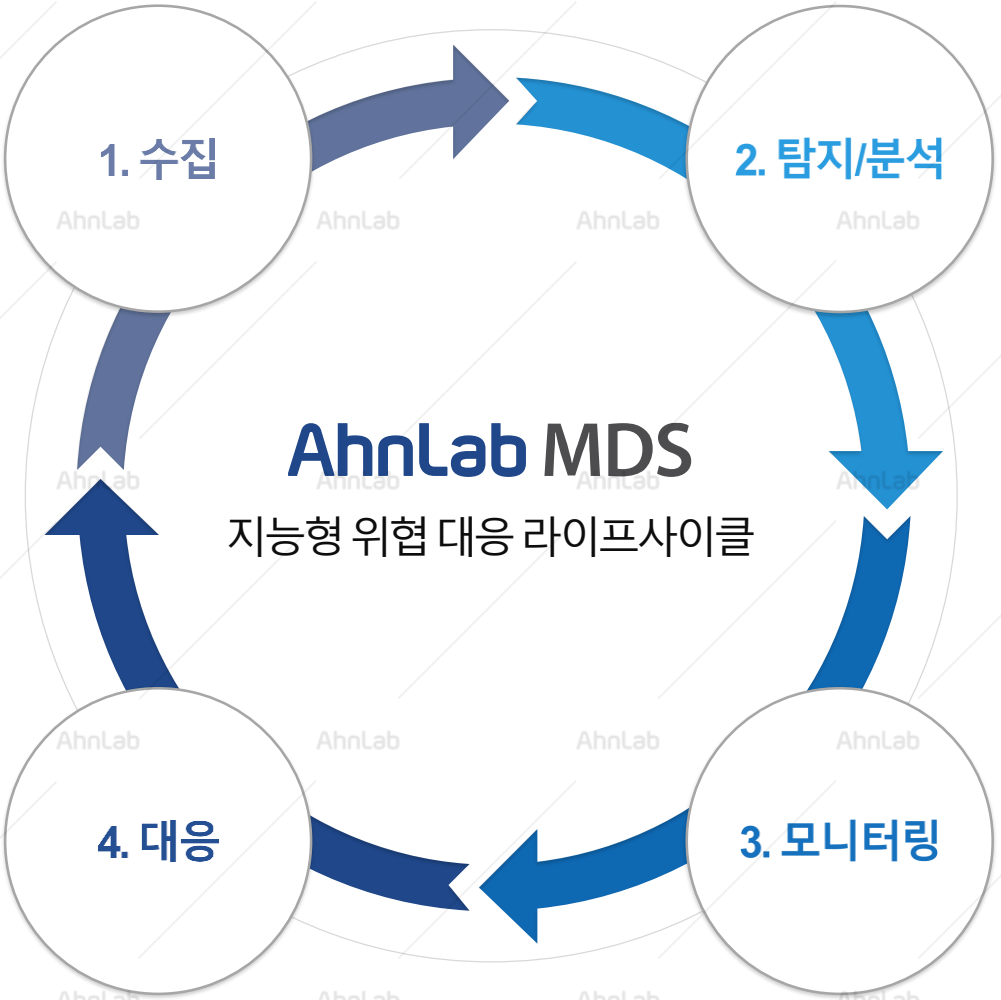
# 단계별 지능형 위협 대응 프로세스

AhnLab MDS는 지능형 위협의 라이프사이클을 중심으로 '수집-탐지/분석-모니터링-대응' 의 각 단계에서 능동적으로 탐지 및 대응합니다.

## 위협 수집

- 유입되는 위협 추출 및 수집 (파일, 트래픽, 이메일)

- 위협 수집 구간: 네트워크, 이메일, 엔드포인트 망연계, 파일 서버




## 탐지 및 분석

- 멀티엔진 기반의 알려진 위협 및 신/변종 위협 탐지

- 시그니처 엔진
- 평판 기반
- 행위 분석(샌드박스 기반)
- 사용자(관리자) 정의 기반

## 유입 경로별 대응

- 네트워크 대응 : 이상 트래픽 탐지 및 차단
- 이메일 대응 : 의심스러운 이메일 격리
- 엔드포인트 대응 : 악성코드 자동·수동 삭제 및 호스트 격리
- 망연계 대응 : 망간 전송 자료 실시간 분석

## 위협 가시성

- 위협 등급 체계 분류 및 대응 우선 순위 제공

# 대응 프로세스 1 – 위협 수집

AhnLab MDS는 네트워크 샌드박스 및 전용 에이전트를 통해 다양한 경로를 통해 유입되는 위협을 신속하게 수집합니다.
또한 다수의 제3자 솔루션과의 연동을 통한 위협 수집 및 분석을 지원하며, 온디멘드 분석 서비스를 제공합니다.

## 네트워크 대응

- HTTP, FTP, SMTP/POP3, SMB/CIFS 등을 통해 유입되는 실행/비실행 파일 수집

## 엔드포인트 대응

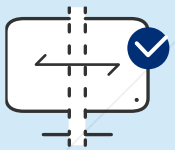
- 엔드포인트에 직접 유입되는 실행/비실행 파일 수집
  (USB 등 각종 저장매체, 암호화 트래픽)

## 온디멘드 분석

- 관리자가 직접 업로드하는 파일에 대한 분석 서비스 제공(핀포인트 검사)

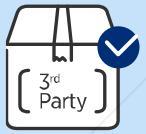
## 이메일 대응

- 스팸 차단 시스템과 API연동을 통한 이메일 수집
- 스팸 차단 시스템을 통과한 이메일 수집



## 망연계 영역 대응

- 망연계 솔루션과 공유폴더 연동을 통한 망간 전송 자료 수집
- 망연계 솔루션과 API 연동을 통해 전달되는 망간 전송 자료 수집



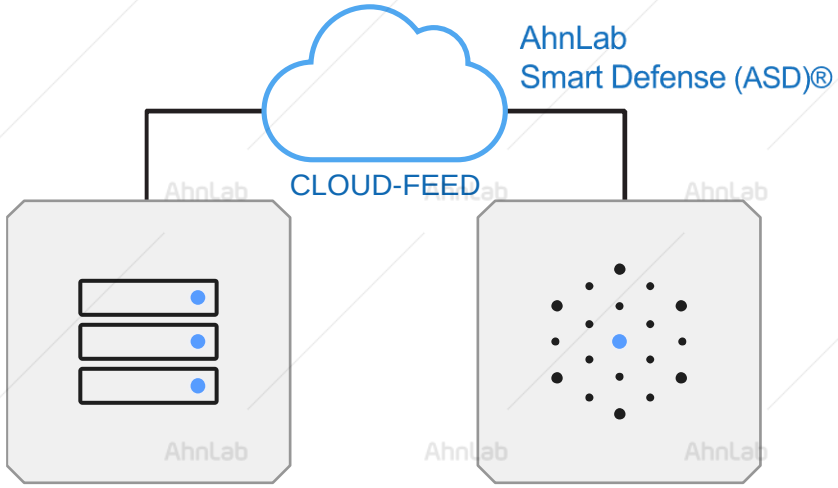

## 멀티 벤더(3rd party) 상호 연계

- 전용 API를 통해 타 솔루션이 전달하는 파일 분석

# 대응 프로세스 2 – 위협 탐지 및 분석

## 멀티엔진 분석

AhnLab MDS는 시그니처 기반, 평판 기반, 비시그니처(signature-less) 기반 등 멀티엔진을 기반으로 기존 방식의 위협(Known)부터 알려지지 않은(Unknown) 신•변종 위협까지 정확하고 효율적으로 탐지 및 분석합니다.




*ASD : 클라우드 컴퓨팅 기반의 악성코드 분석 시스템

### SIGNATURE -BASED

**로컬 ASD 엔진**

- 유해 사이트 탐지
- C&C 트래픽 탐지

VirusTotal API 연동(옵션)

### REPUTATION -BASED

**클라우드 피드**

- 클라우드(ASD) 기반 분석
- 평판 정보 및 화이트리스트 DB

### USER-DEFINED RULE

**YARA**
**MD5 HASH**
**IP/Domain**

### SIGNATURE -LESS

**Behavior analysis**
**Content analysis(DICA™)**

- 신•변종 실행형 악성코드 동적 분석
- 신•변종 비실행형 악성코드 분석

90%

**Black & White List** (Known 악성코드 탐지)

10%

**Gray List** (Unknown 악성코드 탐지)

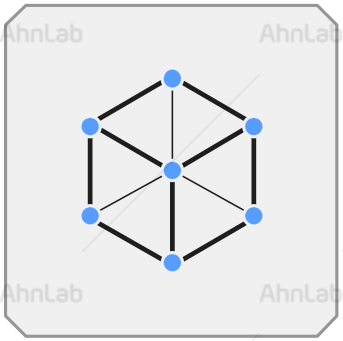
# 대응 프로세스 2 – 위협 탐지 및 분석

## 가상머신 기반 동적 분석

AhnLab MDS는 가상머신을 기반으로 동적 행위 분석과 동적 콘텐트 분석을 수행하여 알려지지 않은 신종 악성코드 기반의 고도화된 위협을 정밀하게 분석합니다.

### 동적 행위 분석 엔진
Dynamic Behavior Analysis

- 가상머신 기반으로 실행(PE)형 악성코드 행위 분석
- 운영체제 상의 의심스러운 행위 정보 모니터링
- 연관 파일 행위 및 평판 정보 종합 분석 및 악성 판정



SIGNATURE-LESS

Behavior analysis

Content analysis(DICA™)

### 동적 콘텐트 분석 엔진
Dynamic Intelligent Content Analysis

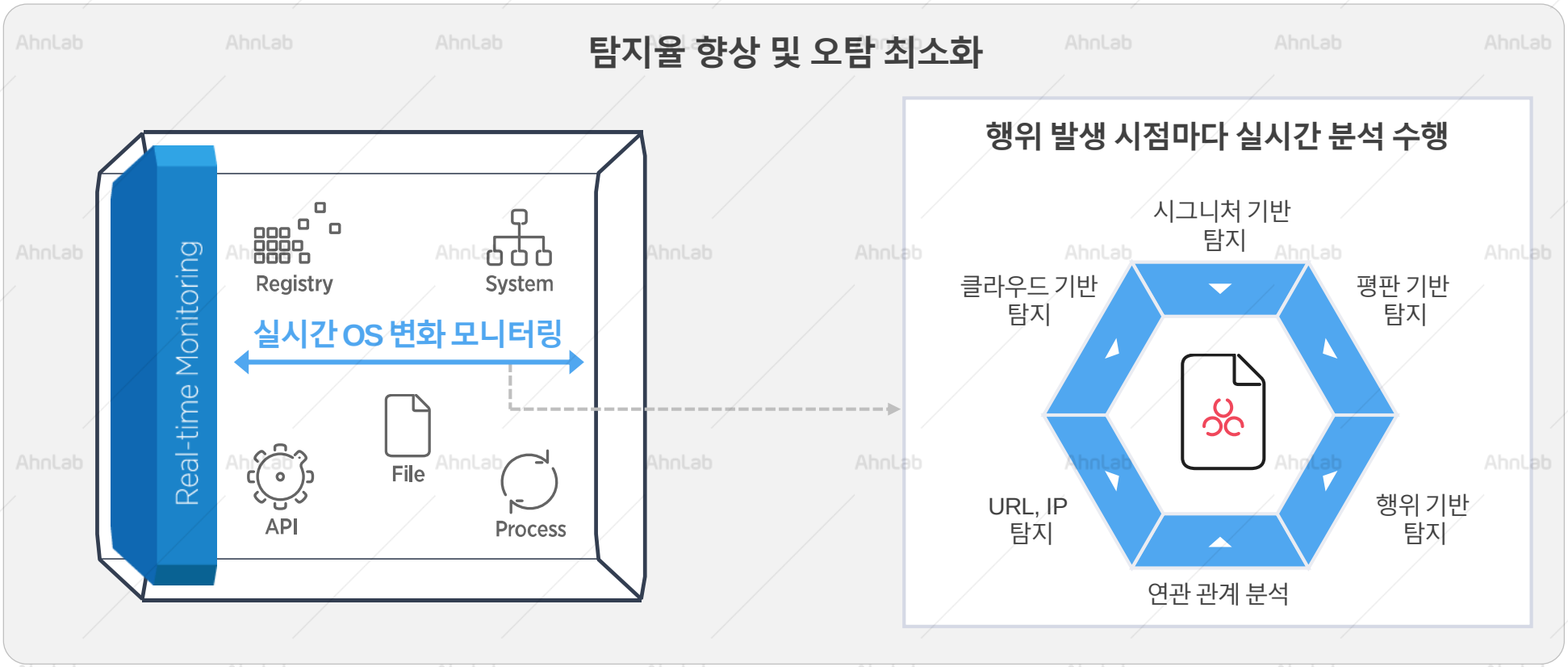
- 문서 등 비실행(non-PE)형 악성코드 정밀 분석
- 리버스 엔지니어링 기법의 메모리 분석
- 보안 취약점 공격 (exploit) 단계에서 악성 판정
- 악성 쉘코드의 실행 전 단계에서 악성 판정
  (행위 발생 여부와 관계없이 탐지 가능)

# 대응 프로세스 2 – 위협 탐지 및 분석

## 동적 행위 분석

AhnLab MDS의 행위 분석 엔진은 파일/프로세스/레지스트리/네트워크 변화를 실시간으로 분석하며, 모든 연관 파일의 행위 정보, 평판 정보 및 연관 정보를 종합적으로 분석해 오탐을 최소화합니다.

## 동적 행위 분석 Dynamic Behavior Analysis



# 대응 프로세스 2 – 위협 탐지 및 분석

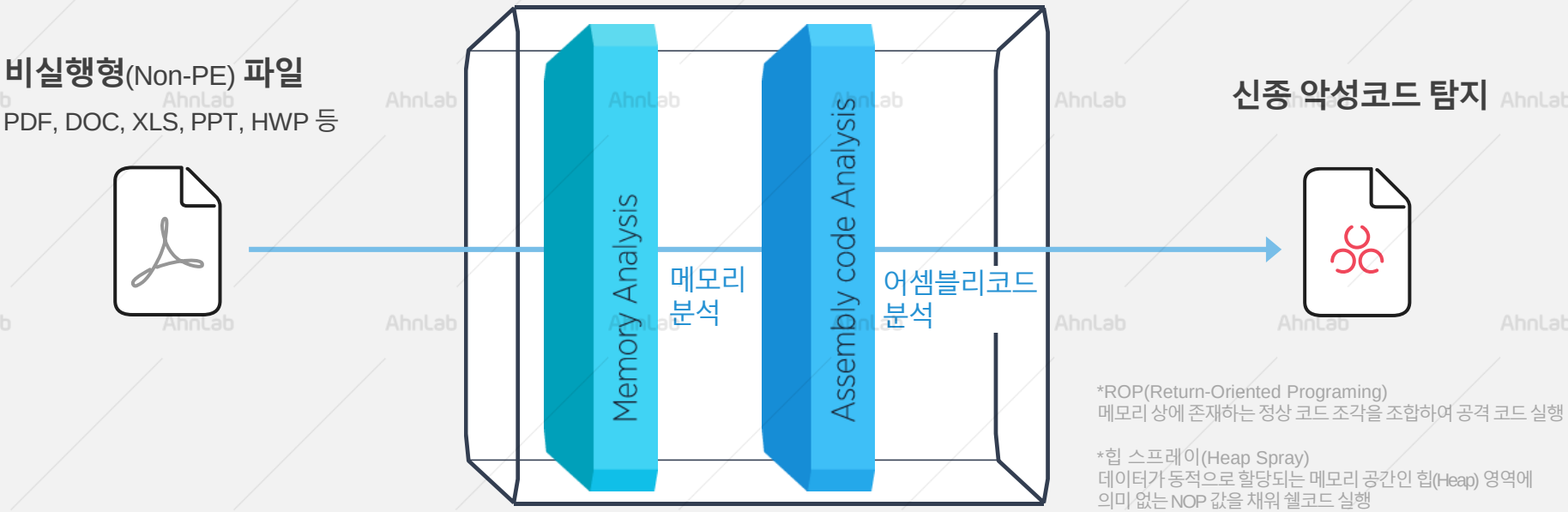
## 동적 콘텐트 분석

동적 콘텐트 분석(DICA) 엔진을 통해 MS오피스·PDF·한컴오피스 등의 취약점을 이용한 신종 비실행형(non-PE) 악성코드를 탐지합니다.
특히 버퍼오버플로우, ROP, 힙 스프레이 등의 공격 기법을 이용하는 악성코드에 대한 탐지가 가능합니다.

## 동적 콘텐트 분석 Dynamic Intelligent Content Analysis

DICA™

- 애플리케이션의 취약점 공격 단계(exploitation)에서 악성코드 탐지
- 제로데이(zero-day) 취약점을 이용한 신종 악성코드 탐지
- ROP 공격/ 힙 스프레이 공격




*ROP(Return-Oriented Programing)
메모리 상에 존재하는 정상 코드 조각을 조합하여 공격 코드 실행

*힙 스프레이(Heap Spray)
데이터가 동적으로 할당되는 메모리 공간인 힙(Heap) 영역에 의미 없는 NOP 값을 채워 쉘코드 실행

# 대응 프로세스 3 – 모니터링

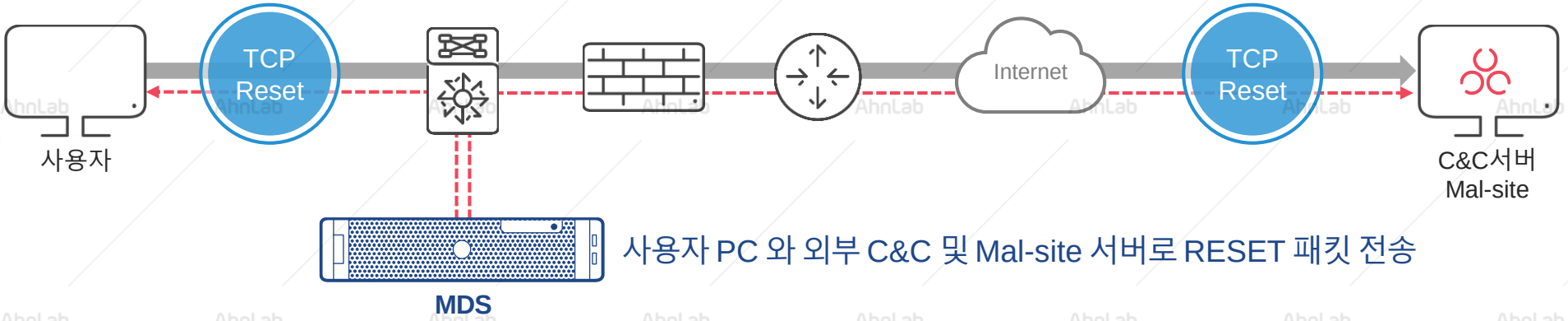
AhnLab MDS는 탐지 및 분석 결과에 따라 크게 3가지 등급으로 분류하고, '악성 등급'에 대해서는 위험도에 따라 다시 3단계로 분류합니다.
정상 파일을 포함한 총 10단계의 세분화된 분류 체계를 제공함으로써 효율적인 위협 대응에 기여합니다.


| 구분 | 위험도 | 분류 기준 | |
|---|---|---|---|
| 악성 등급 | High | 알려진 악성코드 (Known) | 알려지지 않은 신•변종 악성코드 (Unknown) |
| | Medium | | |
| | Low | | |
| 모니터링 등급 | Grey2 | 명확한 악성은 아니지만 악성일 가능성이 높기 때문의 주의해야 하는 이벤트 | |
| | Grey1 | 악성일 가능성은 낮지만 분석을 통해 확인이 필요한 이벤트 - 예시) 암호 압축 파일 탐지 등 | |
| 정상 등급 | Likely Normal | 분석 결과 정상으로 분류된 파일 | |
| | Normal | 정상 파일 | |

# 대응 프로세스 4 – 영역별 대응_네트워크

AhnLab MDS는 C&C 서버 접속 및 악성코드 배포 사이트(Malsite) 등 이상 트래픽에 대해 네트워크단에서의 차단 기능을 제공합니다.
(* 전용 에이전트 설치 여부와 상관없이 기본으로 제공되는 기능)

## 네트워크 레벨 차단 기능




## 네트워크 레벨에서의 차단 대상 이벤트

- C&C 트래픽 탐지 이벤트
- Malsite 접속 탐지 이벤트

## 네트워크 레벨 차단 방식

| 대상 프로토콜 | 차단 방식 |
|---|---|
| TCP | TCP RESET 패킷을 client-server 양측에 전송 |
| UDP | ICMP Unreachable 패킷을 client-server 양측에 전송 |

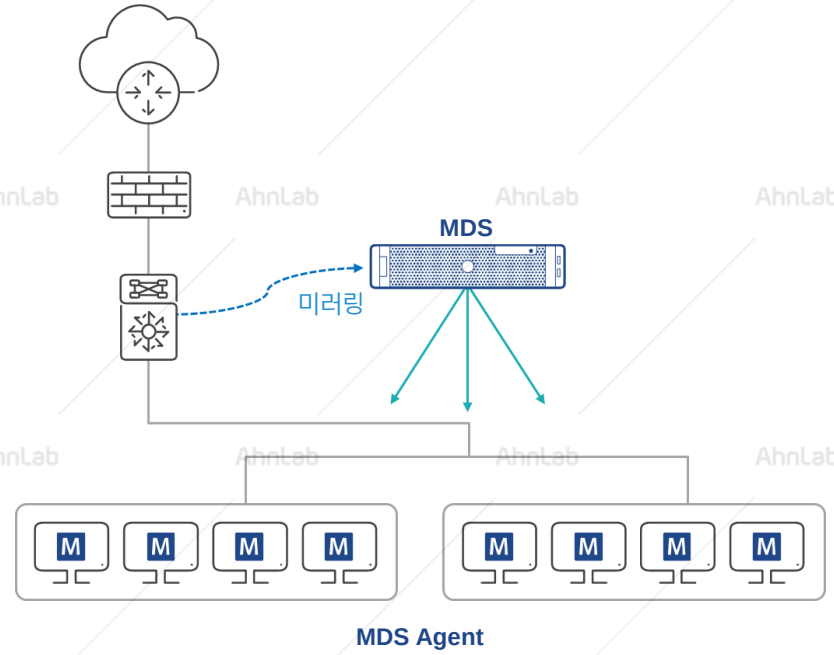
# 대응 프로세스 4 – 영역별 대응_네트워크 및 엔드포인트 연계

AhnLab MDS는 네트워크 샌드박스와 엔드포인트 전용 에이전트와의 연계를 통해 내부로 유입되는 위협에 대한 실질적인 대응이 가능합니다.

## 네트워크-엔드포인트 연계 위협 수집 및 대응

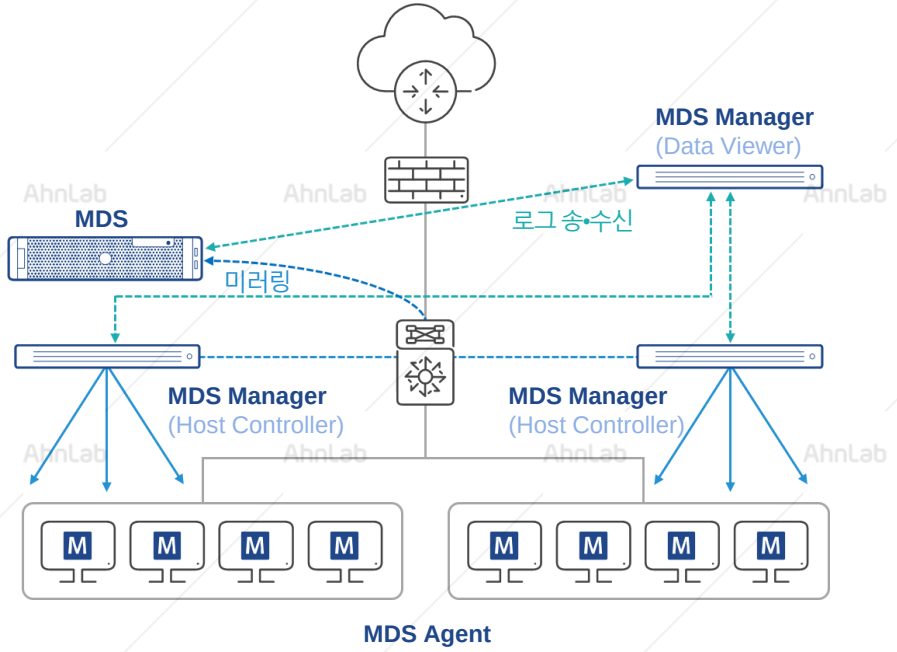
### 1 올인원(All-in-one)

단일 장비를 통한 탐지, 분석, 통합 로그 모니터링, 에이전트 관리




### 2 확장형

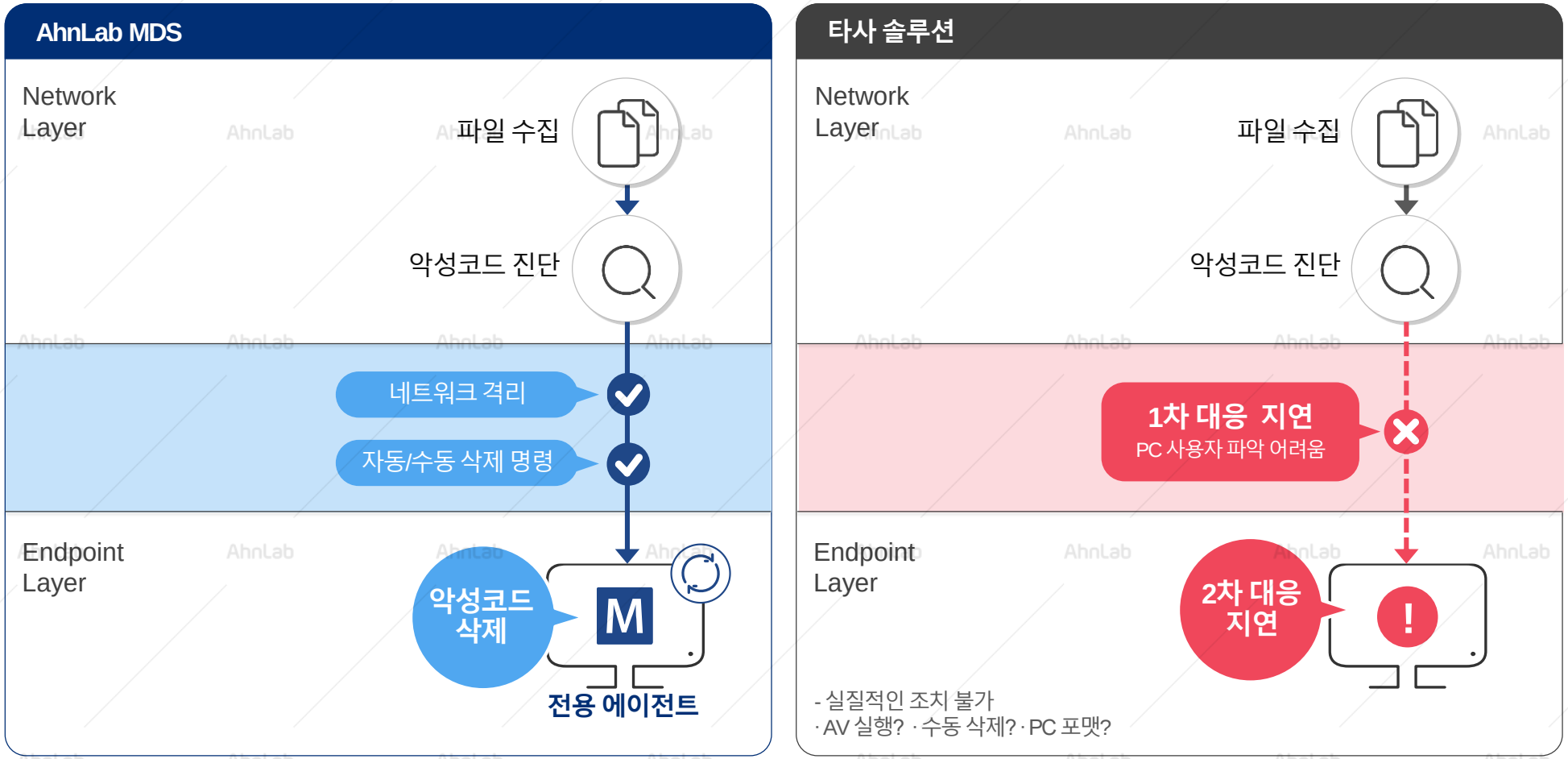
탐지 및 분석, 통합 로그 관리 및 모니터링, 에이전트 관리를 각각의 장비로 운영



# 대응 프로세스 4 – 영역별 대응_엔드포인트

AhnLab MDS는 전용 에이전트를 통해 탐지된 악성코드를  다운로드한 호스트를 네트워크에서 격리함으로써 위협의 내부 전파를 차단하며, 자동 및 수동 삭제를 통한 조치를 수행합니다.

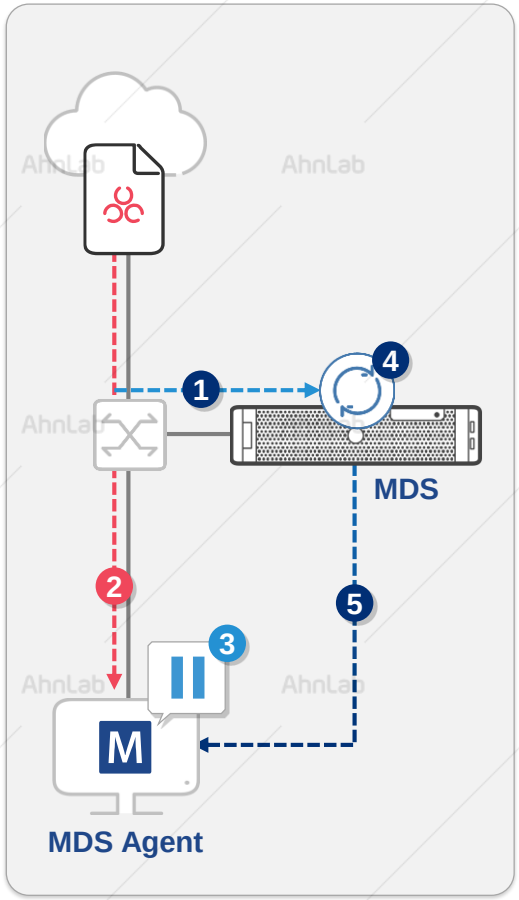
## AhnLab MDS vs 타사 솔루션 비교



# 대응 프로세스 4 – 영역별 대응_엔드포인트

## 실행 보류

전용 에이전트를 통한 "실행 보류(Execution Holding, EH)" 기능으로 악성 여부가 확인되지 않은 파일의 실행을 방지하며,
이를 통해 최초 감염(First Victim, Patient Zero)에 대한 피해 예방 및 대응도 가능합니다.




1 트래픽 미러링 및 분석 시작

2 PC내 파일 다운로드

분석 소요 시간

3 다운로드된 파일 실행 및 실행 보류 동작

4 분석 완료 및 악성 판정

5 삭제 명령 전달

대응 소요 시간

Execution Holding™

실행 보류 기능

'실행 보류' 기능 동작

정상 판정 → 실행 허용

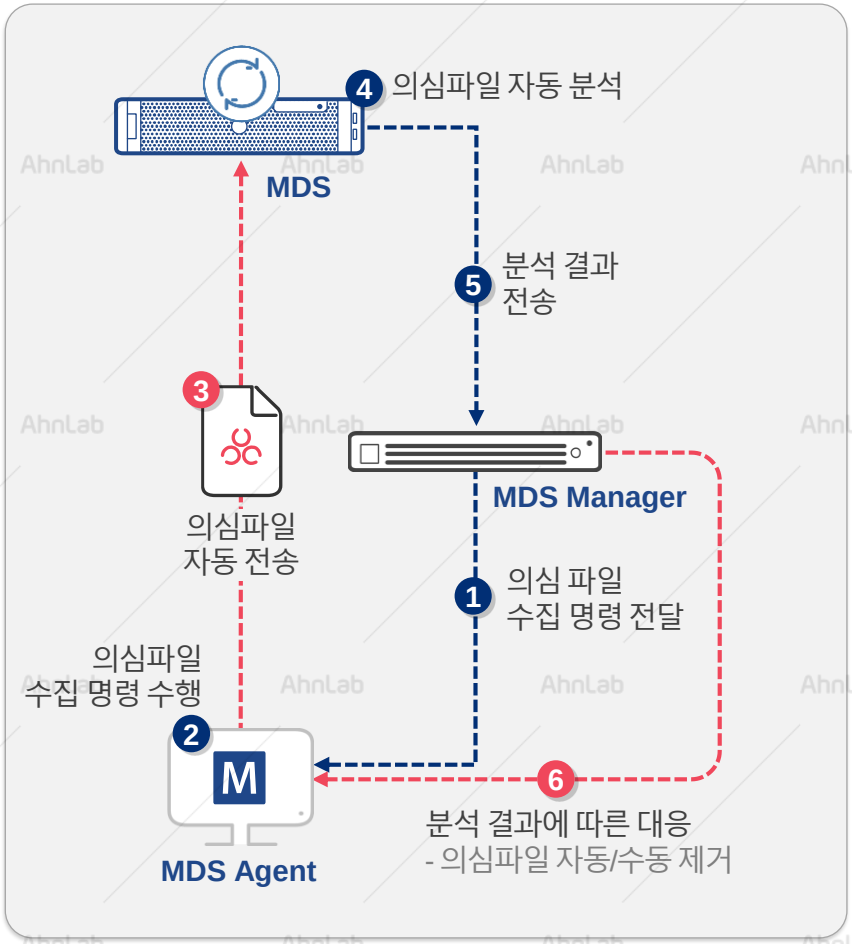
악성 판정 → 실행 보류

*잠재 악성코드 실행 차단*

# 대응 프로세스 4 – 영역별 대응_엔드포인트

## 의심파일 추출

AhnLab MDS는 전용 에이전트를 통해 머신러닝 기반의 "의심파일 추출" 기능을 제공합니다. 이를 통해 전체 엔드포인트 내의 의심 행위 발현 여부 검사부터 기존에 잠재되어 있는 의심 파일 수집 및 자동 분석, 대응(삭제)까지 가능합니다.




### 악성코드 감염 의심 호스트에서 악성 가능성이 있는 파일 검색 및 수집

**주요 추출 대상** (휘발성/비휘발성 데이터)

- 최근 실행된 프로그램 리스트
- 현재 실행 중인 프로세스 리스트
- 서비스 등록된 프로그램 리스트
- 자동실행 관련 레지스트리 등록 프로그램

### 전체 또는 일부 시스템을 대상으로 '의심파일 수집' 가능

### 탐지/분석 장비(MDS)가 관련 정보를 보유하고 있지 않은 파일의 경우, 상세 분석을 위해 MDS 장비로 전송

→ MDS의 분석 결과에 따라 대응 가능

# 대응 프로세스 4 – 영역별 대응_이메일

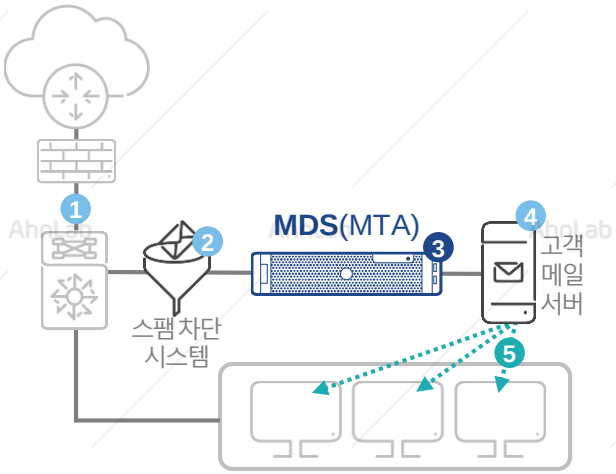
## 이메일 위협 수집

AhnLab MDS는 이메일을 통해 유입되는 악성 콘텐츠에 대한 수집, 탐지, 분석 및 차단이 가능하며, 고객사 내부의 메일 인프라 환경에 따라 다양한 구성 방식을 지원합니다.

- 다양한 구성 방식 제공
- 이메일 첨부파일에 주로 사용되는 문서 및 압축 파일 탐지/분석
- 이메일 본문 내 URL에 대한 동적 분석
- 암호화 압축 파일 분석 및 로깅 제공
- 위협 등급 체계에 따른 대응 우선 순위 제공
- 악성 메일 차단 시 경보 메일 발송 (메일 수신자, 보안 관리자)

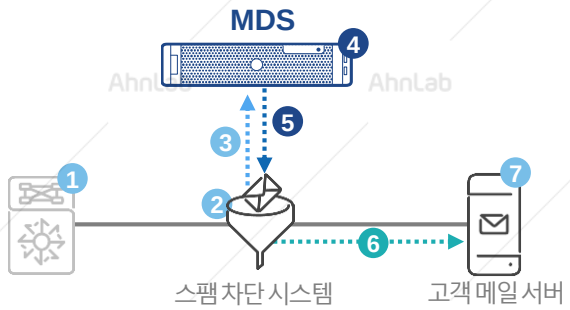
### 1 MDS MTA 모드

1. 이메일 수신
2. 스팸 메일 차단
3. 악성 메일 분석·탐지·격리·차단
4. 정상 이메일 전달
5. 안전한 메일 수신



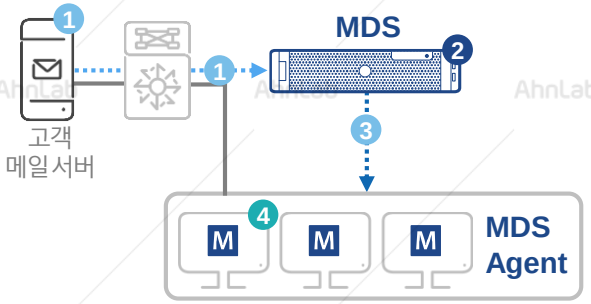

### 2 스팸 차단 시스템 연동

1. 이메일 수신
2. 스팸 메일 차단
3. 스팸 필터링 후 전송되는 메일 전달
4. 악성 메일 분석·탐지
5. 분석 결과 전달
6. 정상 메일만 고객 메일서버로 전송
7. 정상 이메일 전달




### 3 MDS 미러링/BCC 모드

1. BCC 이메일 전달 또는 이메일 트래픽 수집(미러링)
2. 악성 메일 분석·탐지
3. 악성 파일 조치 명령
4. 악성코드 삭제

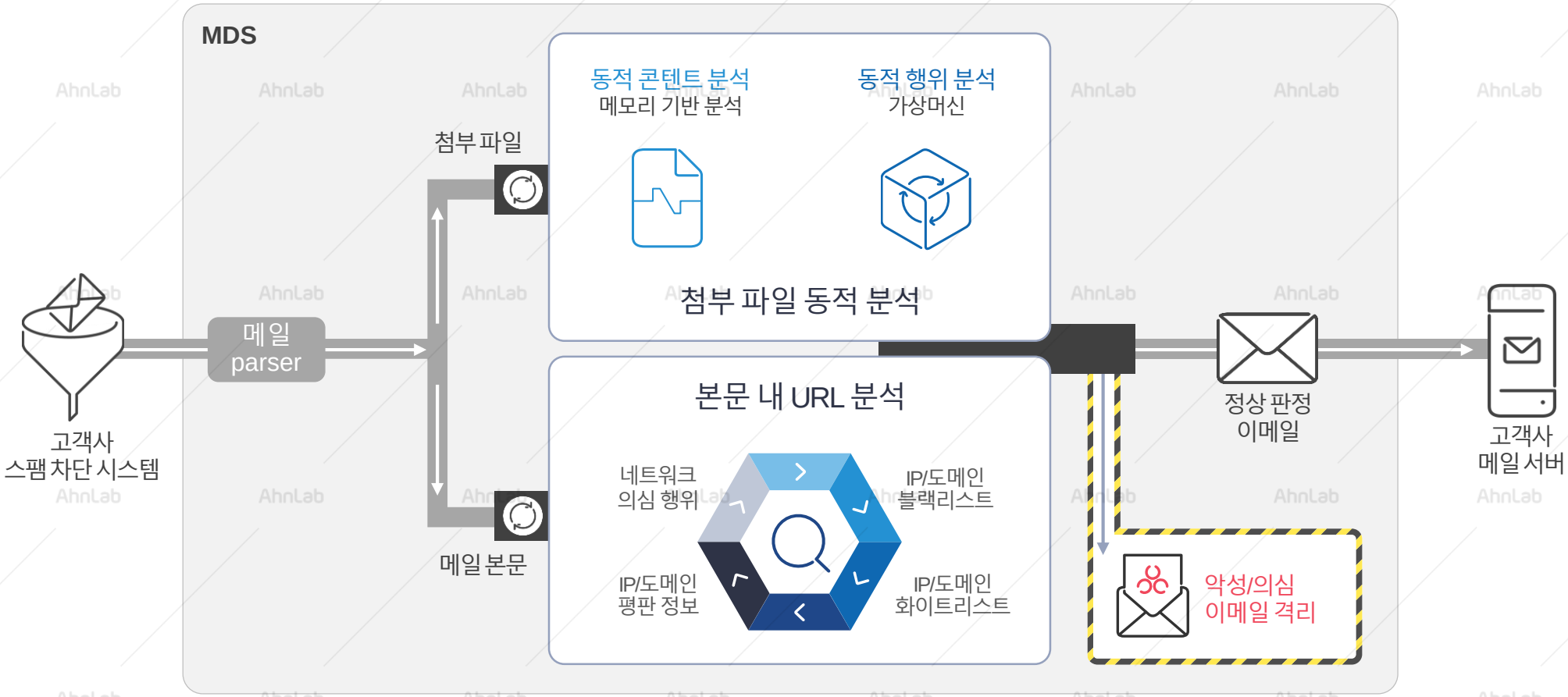


# 대응 프로세스 4 – 영역별 대응_이메일

## 이메일 분석

AhnLab MDS는 메일의 첨부 파일에 대한 가상머신 기반의 동적 분석뿐만 아니라 메일 본문 내의 악성 URL 및 스크립트(script)에 대해 블랙리스트/화이트리스트 및 평판 정보 기반의 다차원 분석을 수행합니다.

### 이메일 격리(MTA) 기능 – 상세 분석



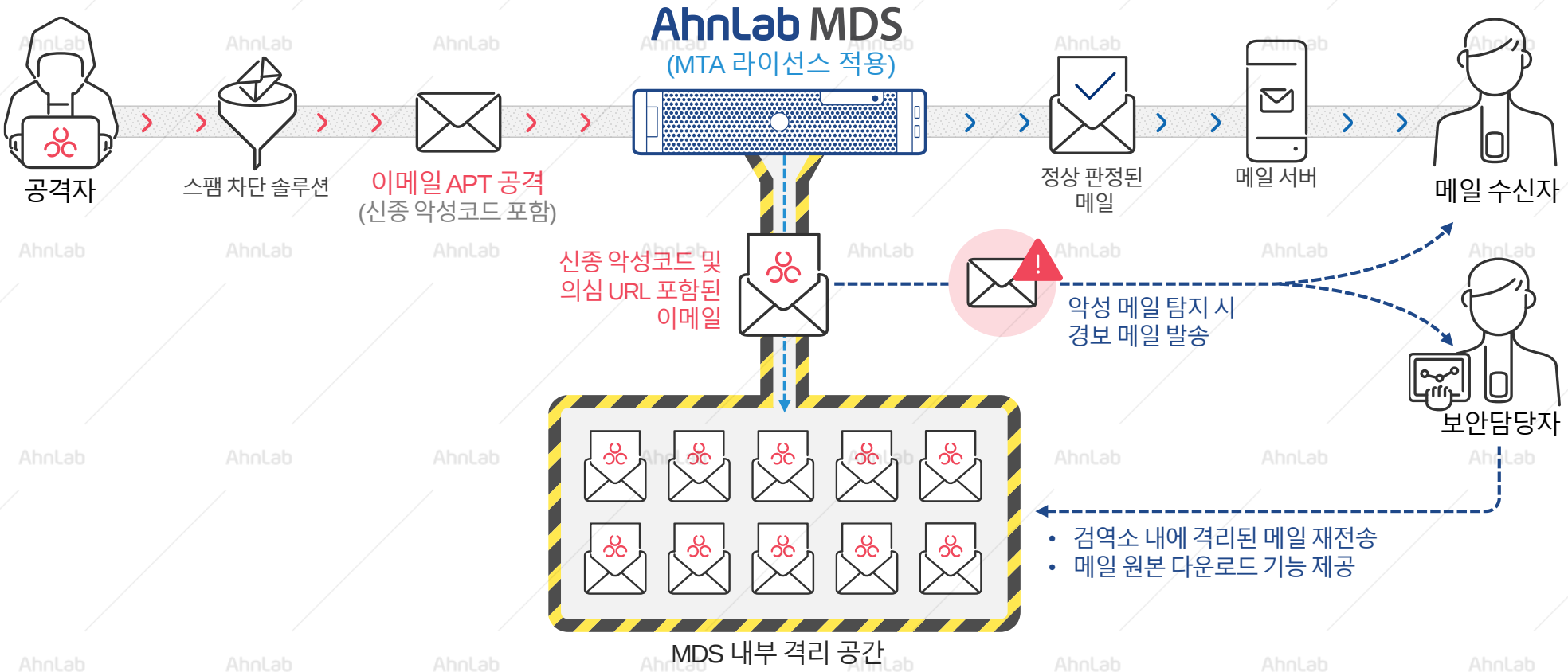
# 대응 프로세스 4 – 영역별 대응_이메일

## 이메일 격리

악성 또는 의심스러운 이메일을 탐지하고 자동 격리하며, 악성 메일 탐지 시 메일수신자 및 보안 관리자에게 경보 메일을 발송합니다.
격리된 이메일은 추가 분석을 위해 다운로드하거나 '관리자 명령'을 통해 격리 해지(수신자에게 메일 전송)할 수 있습니다.

이메일 격리(MTA) 및 경보 메일 발송

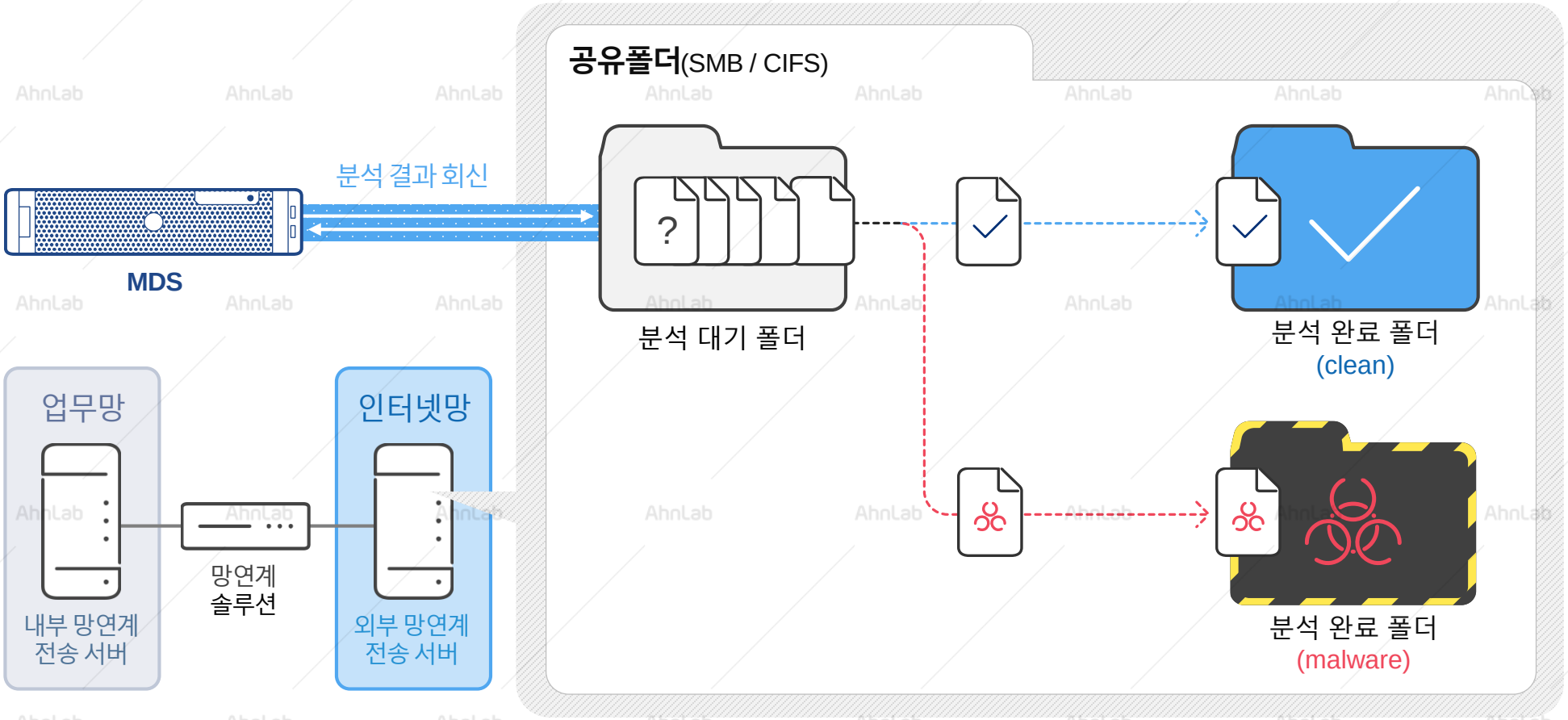
* MTA : Mail Transfer Agent



# 대응 프로세스 4 – 영역별 대응_망연계

AhnLab MDS는 공유폴더 스캔 기능을 통해서 망연계 솔루션을 거쳐서 유입되는 '신종 악성코드 의심 파일'에 대한 동적 분석 수행 후 안전한(Clean) 폴더와 악성 파일 격리 폴더로 이동시킵니다.

## 망연계 솔루션 연동 - 공유폴더 실시간 검사 기능 (다중 폴더 동시 검사 지원)

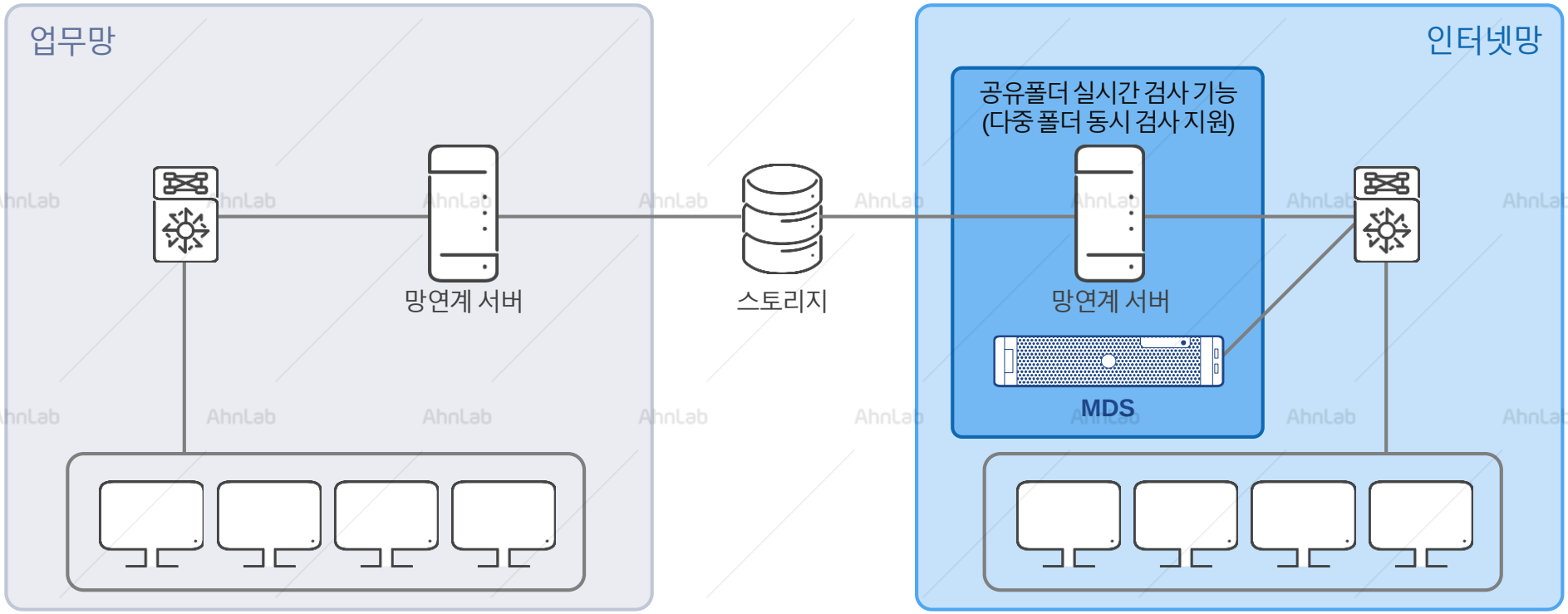


# 대응 프로세스 4 – 영역별 대응_망연계

AhnLab MDS는 망연계 시스템에 대한 공유폴더 연동 및 전용 API 연동 방식을 지원합니다. 망연계 시스템 연동을 통해 인터넷망과 업무망 사이에서 송•수신되는 대부분의 문서 파일, 압축 파일에 대한 신속하고 정확한 탐지 및 분석이 가능합니다.

## 망연계 시스템 연동 구성 (공유폴더 연동 및 API 연동)

- 다양한 망연계 연동 방식 제공
  - 공유폴더 연동 방식
  - 전용 API 를 통한 연동 방식
- 망간 송·수신되는 문서, 압축 파일에 대한 빠르고 정확한 탐지 및 분석
- 특정 공유 폴더 실시간/예약 검사
- 최대 1GB 파일 분석 가능
- 위협 등급 체계에 따른 대응 우선 순위 제공



# 03
# 특장점

특장점1 – 위협 가시성

특장점2 – 암호화 트래픽 대응

특장점3 – 행위 분석 우회 위협 탐지

특장점4 – 비용 효율성

특장점5 – V3 통합 에이전트 제공

특장점6 – 다양한 보안 솔루션 연동

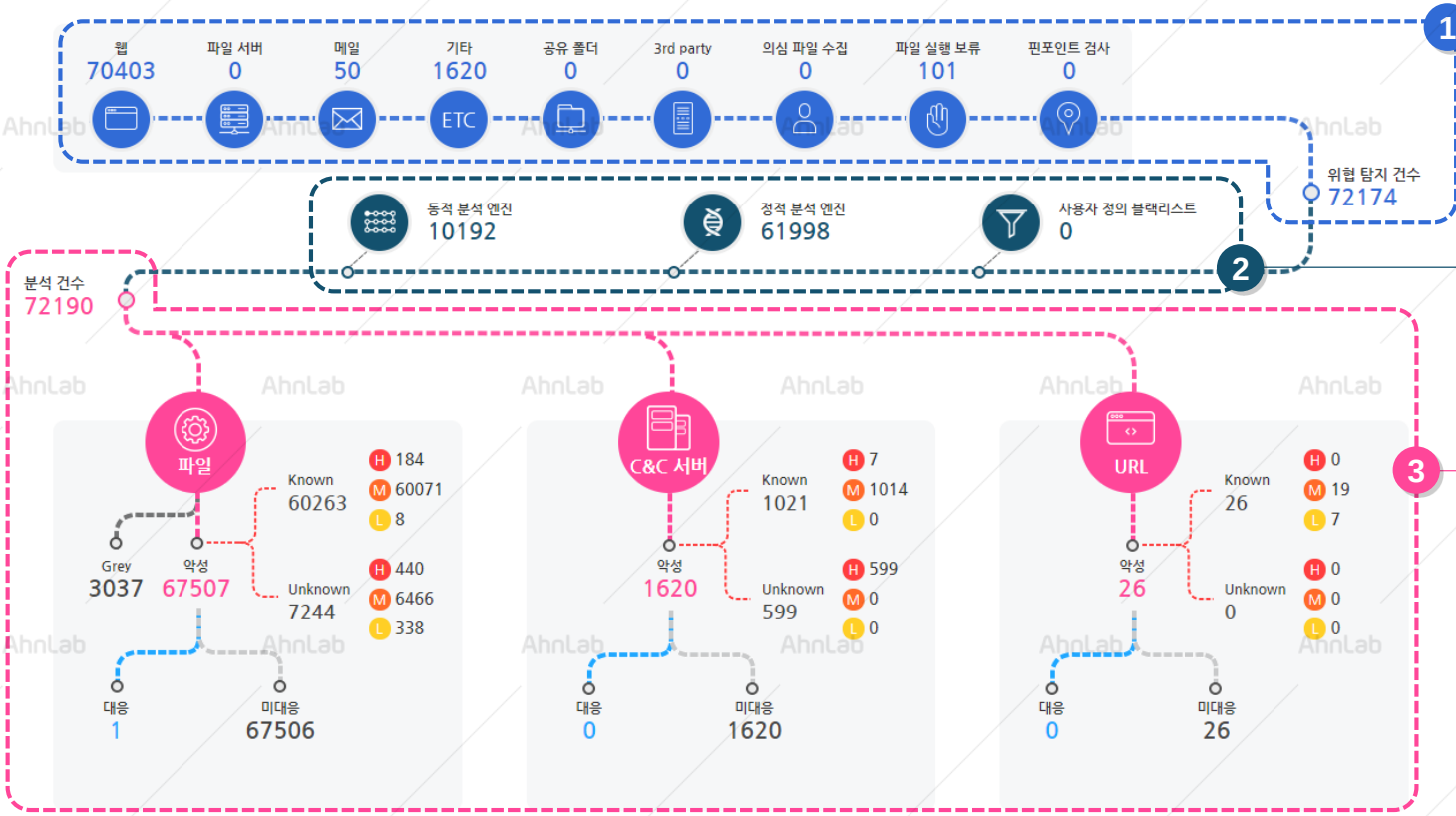
특장점7 – 상위 기관 배포 룰 연계

도입 효과

# 특장점1 – 위협 가시성(1/2)

AhnLab MDS는 내부로 유입된 위협의 종류, 유입 경로, 확산 정도 및 탐지된 위협에 대해 직관적인 위협 가시성을 제공합니다. 이를 통해 악성코드 확산 등 위협 현황을 파악하고 즉각적이며 실질적인 조치가 가능합니다.

## 대시보드를 통한 직관적인 위협 추이 제공




1

### 위협 탐지 현황

- 경로별 위협 탐지 현황
- 위협 수집 현황 및 상태
  (예: 실행 보류 등)

2

### 분석 현황

- 다중 엔진 기반의 분석 현황

3

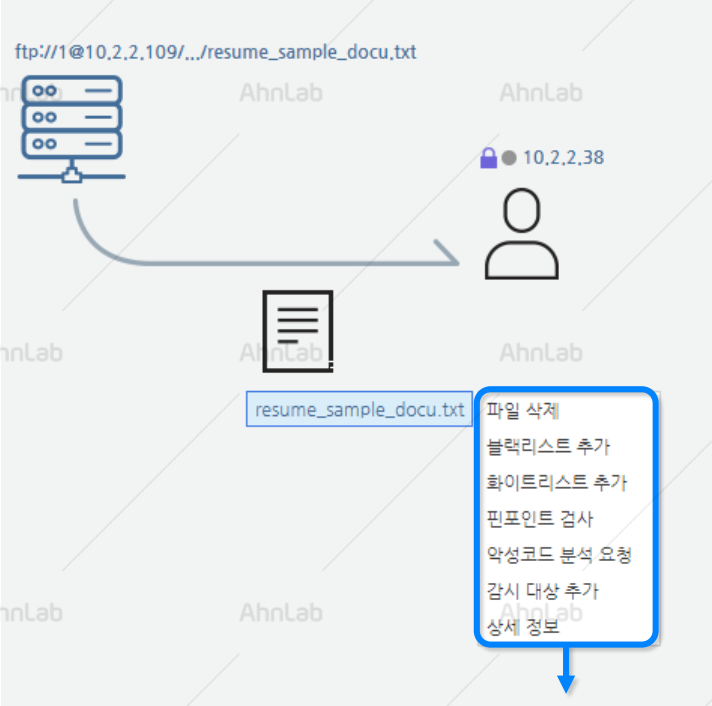
### 분석 결과

- Known/Unknown 위협 현황
- 대응/미대응 현황

# 특장점1 – 위협 가시성(2/2)

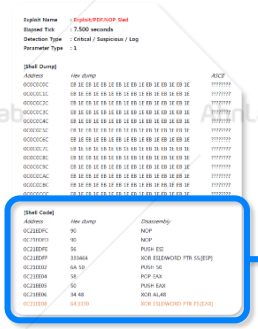
위협에 대해 상세한 '공격 흐름도'를 통해 위협의 종류, 행위 및 공격 단계에 따라 적절한 대응 및 조치가 가능합니다.
또한 동적 콘텐트 분석(DICA)를 통해 어셈블리코드 및 메모리 분석에 관한 상세하고 직관적인 리포트를 제공합니다.

## 공격 흐름도




분석 결과에 따른 조치 방안 제시
(삭제/격리/분석 요청/예외 처리 등)

## 어셈블리코드 분석 리포트

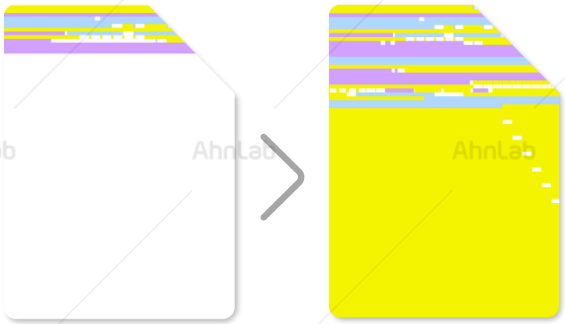


쉘코드 메모리 덤프 및 어셈블리코드

[Shell Code]

| *Address* | *Hex dump* | *Disassembly* |
|---|---|---|
| 0C21EDFC | 90 | NOP |
| 0C21EDFD | 90 | NOP |
| 0C21EDFE | 56 | PUSH ESI |
| 0C21EDFF | 333464 | XOR ESI,DWORD PTR SS:[ESP] |
| 0C21EE02 | 6A 50 | PUSH 50 |
| 0C21EE04 | 58 | POP EAX |
| 0C21EE05 | 50 | PUSH EAX |
| 0C21EE06 | 34 48 | XOR AL,48 |
| 0C21EE08 | 64:3330 | XOR ESI,DWORD PTR FS:[EAX] |

## 메모리 분석 리포트

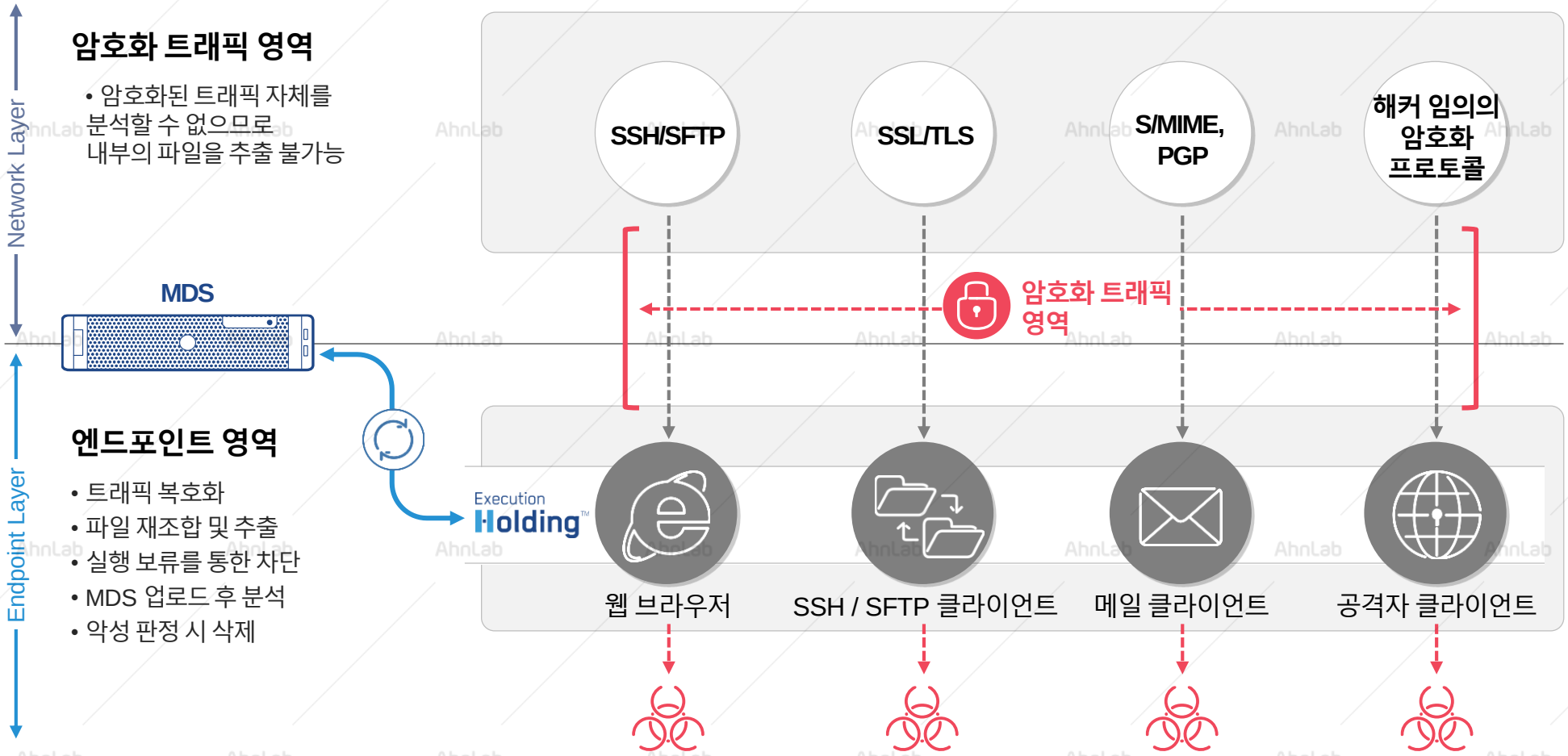


힙 스프레이 공격 전/후의
가상 메모리 사용 비교

# 특장점2 – 암호화 트래픽 대응

AhnLab MDS의 '실행 보류' 기능을 활용해 다양한 암호화 트래픽을 통해 유입되는 지능형 위협도 탐지 및 차단합니다.
즉, '암호화 트래픽 복호화 전용솔루션' 을 별도로 구축하지 않아도 대응이 가능합니다.

## 실행 보류(Execution Holding) 기능을 활용한 암호화 트래픽 대응

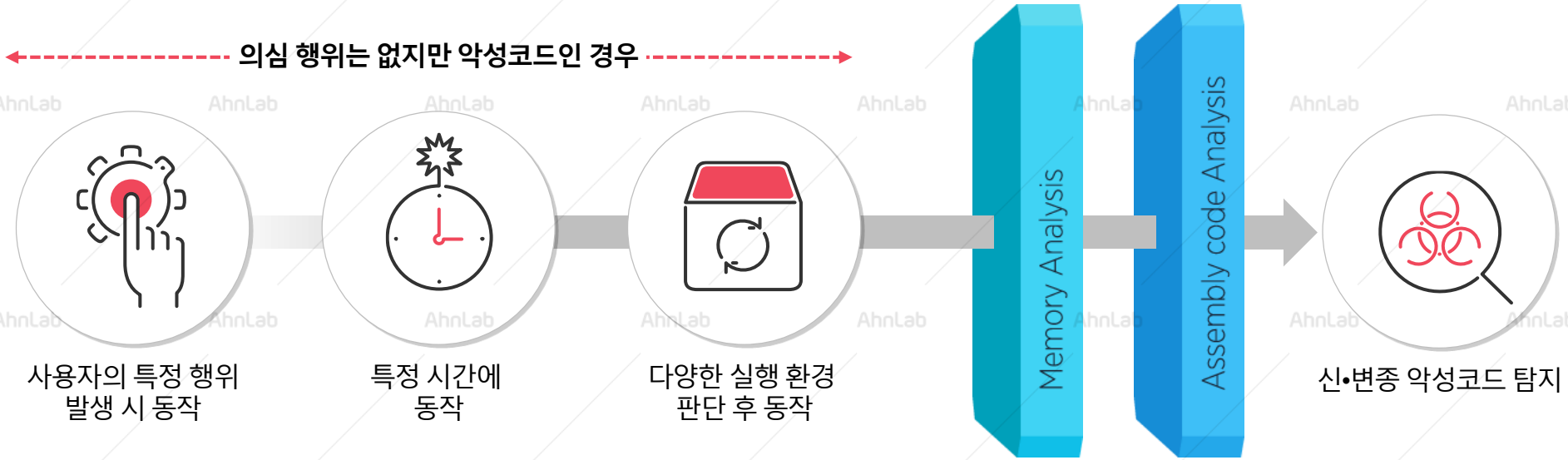


# 특장점3 – 행위 분석 우회 위협 탐지

최근 행위 기반 탐지를 우회하는 악성코드 에 의한 피해가 지속적으로 발생함에 따라 행위 기반 분석을 우회하는 신종 악성코드에 대한 탐지가 요구됩니다. AhnLab MDS는 동적 행위 분석과 동적 콘텐트 분석 엔진을 통해 행위 분석을 우회하는 신종 악성코드를 탐지하고 있습니다.

- 동적 콘텐트 분석을 통해 행위 발생 여부와 상관없이 신종 익스플로잇 및 악성코드 탐지
- 다양한 가상머신(VM) 우회 기법을 탐지하는 자체 알고리즘 및 특화된 룰셋 탑재
- 실행형 및 비실행형 행위 분석 우회 악성코드 탐지

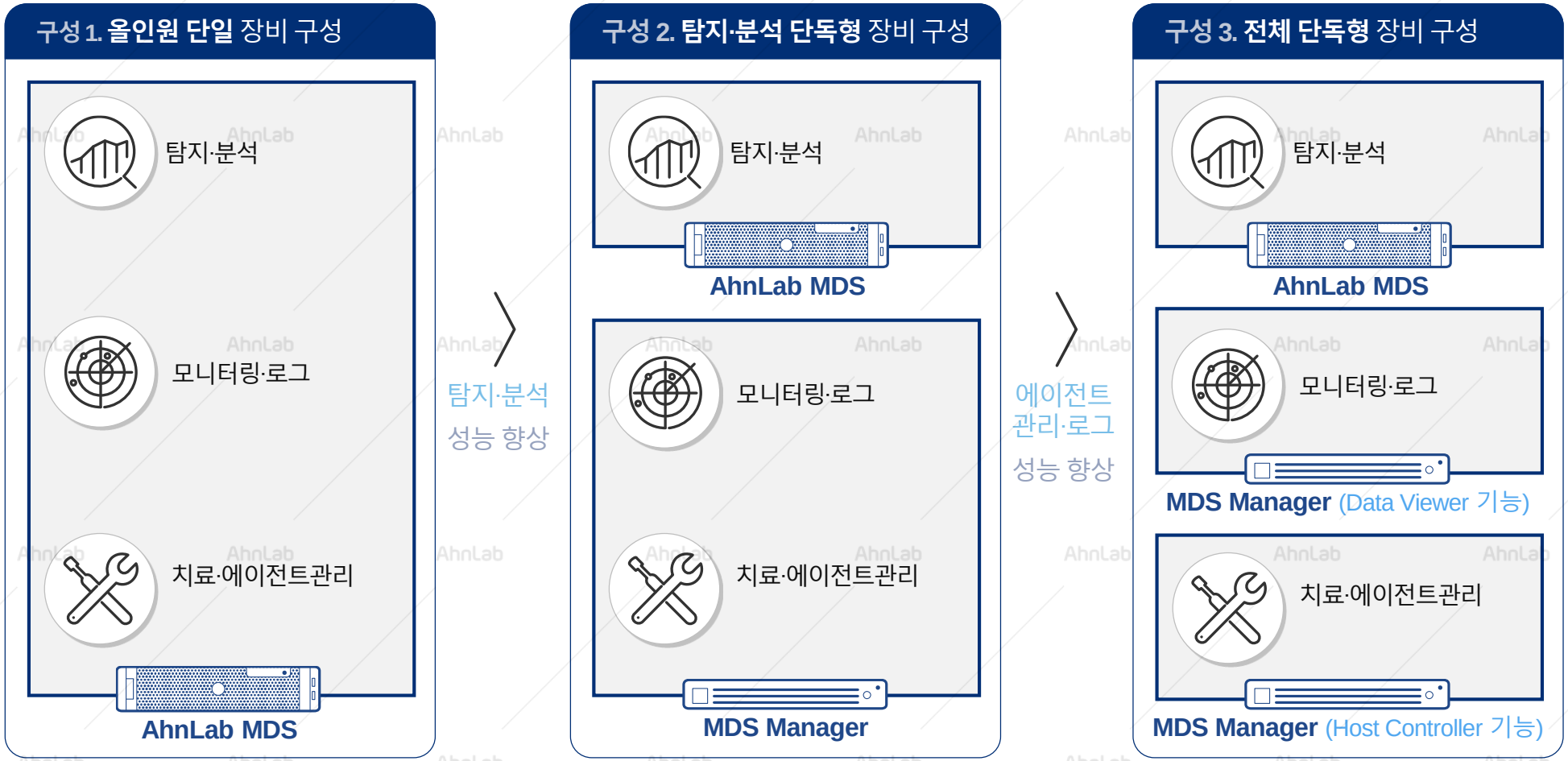
## 다양한 샌드박스(VM) 우회 기법 탐지



# 특장점4 – 비용 효율성

AhnLab MDS는 1) 탐지·분석, 2) 모니터링·로그 및 3) 치료·에이전트 관리의 세가지 모듈을 유연하게 구성할 수 있는 옵션을 제공해 최적화된 **초기 구축 비용과 확장 편의성**을 제공합니다.

## 구성 방식



# 특장점5 – V3 통합 에이전트 제공

고객사 환경에 따라 AhnLab MDS 에이전트(Agent)는 V3 제품과 하나의 설치본 형태로 제공 가능하며,
이를 통해 랜섬웨어를 비롯한 신•변종 악성코드까지 능동적으로 방어하는 통합 대응 체계를 구축할 수 있습니다.


## 통합 설치본 제공(설치 프로세스 효율화)

- AhnLab MDS Agent + V3
  → AhnLab V3-MDS 통합 에이전트로 동작
- 고객사 환경에 따른 통합 설치본 구축 가능

## 통합 아이콘 및 메뉴 제공(직관적인 인터페이스)

- 통합 형태의 시스템 트레이 아이콘 및 메뉴 제공
- 기존 V3 사용 고객에게 익숙한 V3 아이콘을 그대로 통합 설치본 사용 가능
  - V3 아이콘 및 메뉴를 기본으로 MDS 관련 메뉴가 추가된 형태
- 에이전트 추가 설치 과정에서 발생되는 임직원의 거부감 및 관련 헬프데스크 문의 이슈 최소화

## 관련 프로세스 성능 최적화

- 시스템 트레이 아이콘 통합으로 인한 관련 시스템 부하 최소화
- 통합 에이전트를 통한 향후 지속적인 성능 최적화 토대 마련

## 악성코드 통합 대응 체계 구축

- 알려진(Known) 악성코드 및 악성 행위는 V3 제품을 통해 실시간 탐지 및 대응
- 알려지지 않은(Unknown) 신·변종 악성코드는 MDS를 통한 사전 차단 및 대응

# 특장점6 – 다양한 보안 솔루션 연동

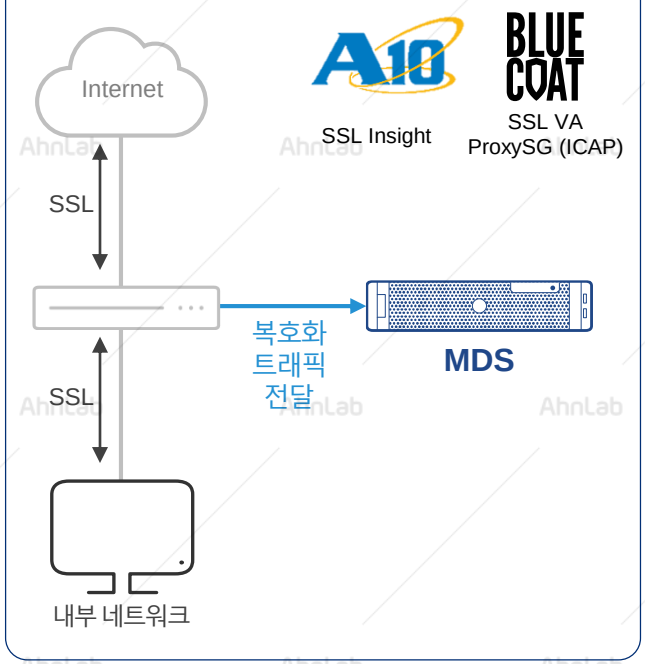
AhnLab MDS는 나날이 진화하는 보안 위협에 대한 보다 적극적인 대응 체계 구현을 위해
다양한 제3자(3rd- Party) 보안 솔루션(암호화 트래픽 복호화 솔루션, 스팸 차단 솔루션, 망연계 솔루션)과의 유연한 상호 연동을 제공합니다.

다양한 보안 솔루션과의 상호 연동을 통한 탐지 및 대응 고도화

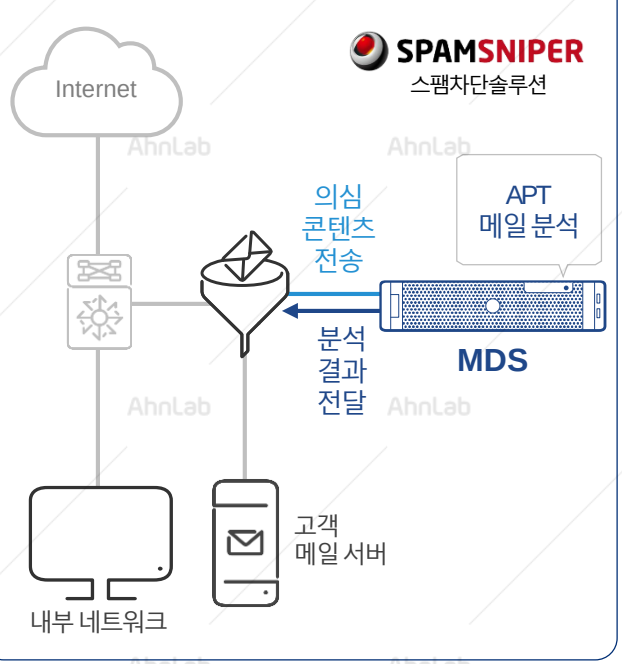
분야별 선도 업체와의 유연한 상호 연동을 통해

## 지능형 보안 위협에 대한 탐지 및 대응력 강화

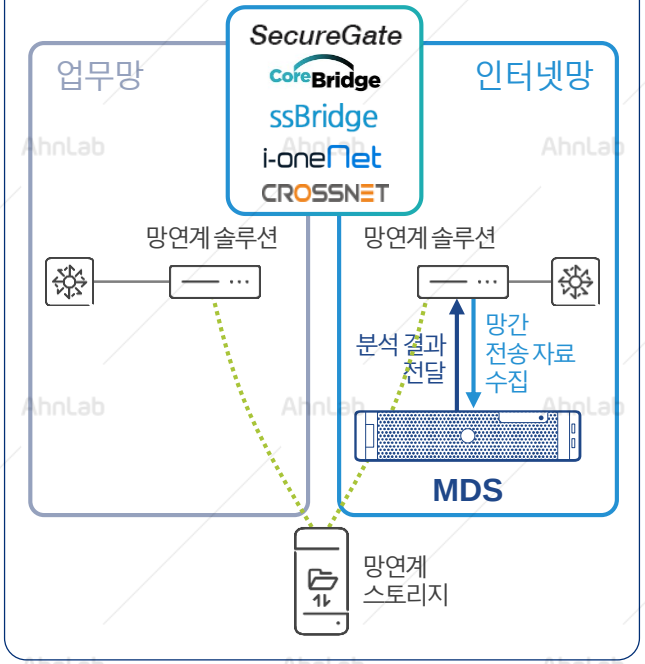
### 트래픽 복호화 솔루션 연동을 통해 암호화된 트래픽 분석/ 대응




### 스팸 차단 솔루션 연동을 통한 이메일 보안 강화



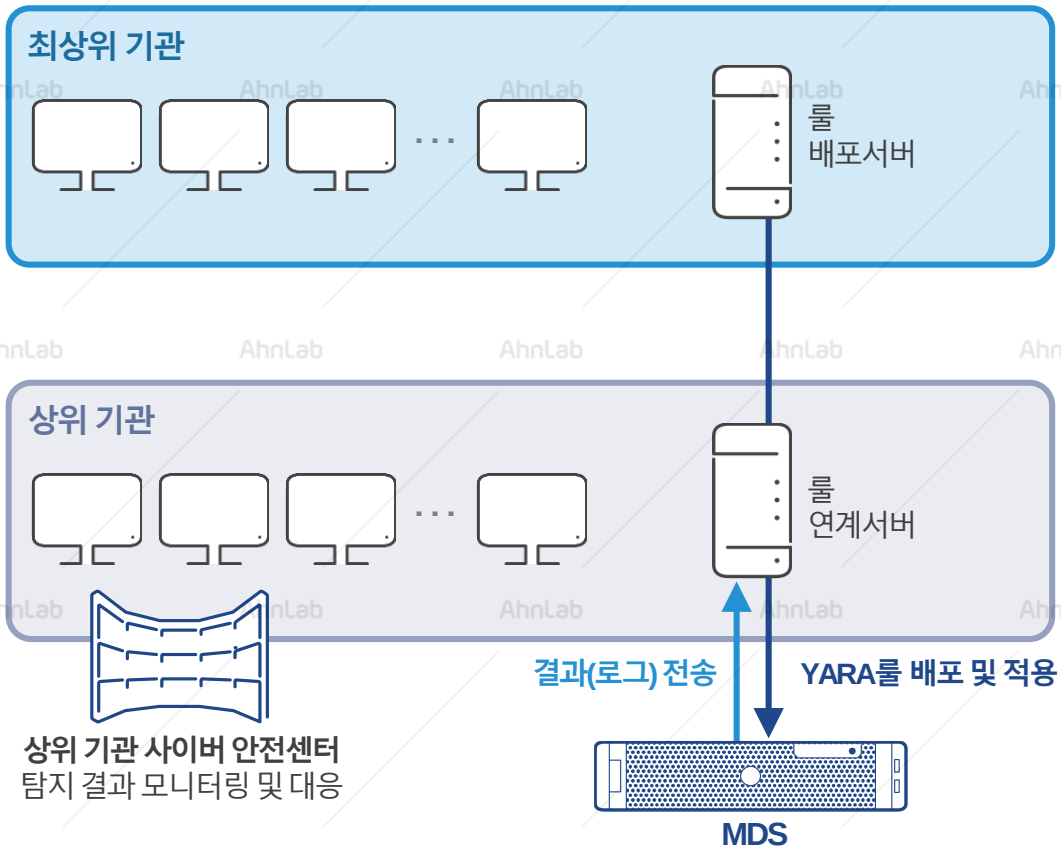

### 망연계 솔루션 연동을 통해 외부에서 유입되는 악성코드 대응 강화



# 특장점7 – 상위 기관 배포 룰 연계 (공공기관 대상)

AhnLab MDS는 상위 기관에서 배포하는 위협 정보(YARA 룰)을 별도의 릴레이(Relay) 서버 없이 직접 적용함으로써 위협의 확산을 차단하며, 탐지된 위협 정보를 수집하여 상위 기관에 제공합니다.

## 상위 기관 배포 룰 연계




yara

```
rule my_rule
{
strings:
        $a = "aaaa" nocase
        $b = "bbbb" nocase
        $c = "www.fghie87134.com" nocase
        $d = "www.foijv18073.com" nocase
        $e = "www.ieuiu01143.com" nocase
condition:
        any of them
}
```

# 도입 효과

AhnLab MDS는 차별적인 위협 가시성을 기반으로 고도화된 최신 공격에 대해 능동적이며 효과적인 대응 방안을 제시합니다.

## AhnLab MDS 도입 전

**위협 대응의 한계**

- 악성코드 감염 시 해당 PC 포맷 > **근본적인 악성코드 위협 제거 불가능**
- 각종 보안 솔루션을 우회하여 유입되는 **고도화된 악성코드에 대한 모니터링 및 대응 불가능**

## AhnLab MDS 도입 후

지능형 보안 위협 대응 솔루션
**AhnLab MDS**

### ✓ 뛰어난 가시성 기반의 효율적인 위협 관리 및 대응 체계 구축

- 다양한 경로를 통해 유입되는 위협에 대한 전반적인 모니터링 및 감염 현황에 대한 가시성 제공
- 이상 트래픽(C&C 접속, 악성코드 경유/배포지) 접속 차단으로 선제적인 대응 가능
- 비정상 프로세스 실행 차단 및 '실행 보류' 기능을 통해 탐지된 랜섬웨어 및 악성코드의 동작을 원천 차단

### ✓ 최적화된 대응 프로세스 적용으로 비즈니스 연속성 확보

- 안랩과 고객의 상호 공조 체계 구축을 통한 고도화된 신·변종 악성코드 대응
- 신·변종 악성코드 공격에 대한 효율적이며 최적화된 방어로 비즈니스 중단 방지

### ✓ 도입 비용 절감 및 보안 운영 부담 최소화

- 가상머신(VM)에 사용되는 분석용 OS 및 애플리케이션 라이선스 추가 구매 불필요
- 도입 환경에 따라 다양한 구성(올인원/단독형) 가능 - 초기 구축 비용 절감 및 확장 편의성
- 에이전트를 통한 자동 대응(실행보류/악성코드 삭제/의심 호스트 격리)으로 보안 운영 부담 최소화

# 04
# 제품 구성 및 사양

제품 구성 및 주요 기능

구축 방안

구성도

제품 사양

# AhnLab MDS 구성 및 주요 기능

## AhnLab MDS

| 기능 요약 | 상세 내용 |
|---|---|
| 위협 분석 및 탐지 | • 주요 인터넷 서비스 프로토콜 수집 및 분석 (HTTP, SMTP, SMB/CIFS, FTP 등)<br>• 파일 유입 및 유출에 대한 양방향 트래픽 모니터링 (IPv4/IPv6)<br>• 이메일 본문 및 첨부파일에 대한 위협 탐지 및 격리 (MTA License 적용)<br>• 시그니처, 머신러닝 기반의 정적 진단 및 샌드박스 기반 동적 분석을 통한 신종 위협 탐지<br>• MS오피스, 한컴오피스(한글) 등 비실행형(non-PE) 파일의 악성코드 탐지를 위한 전용 엔진 탑재<br>• VM 분석 과정 및 C&C 탐지 내역에 대한 PCAP 기반 패킷 캡쳐 및 PCAP 파일 다운로드<br>• 악성코드 감염 PC의 유해 사이트 접근 및 C&C 통신 탐지/차단<br>• MDS Manager를 통한 행위 분석 결과 및 클라우드 기반 행위 분석 정보 공유 |

## AhnLab MDS Manager

| 기능 요약 | 상세 내용 |
|---|---|
| 통합 모니터링 및 로그 관리 (Data Viewer) | • 주요 현황 및 이벤트 정보를 한눈에 파악할 수 있는 대시보드<br>• 이벤트 종류, IP 주소, 행위 내역(파일/프로세스/레지스트리/네트워크) 등에 대한 상세 로그<br>• 네트워크 구간, 이메일 구간, 공유폴더 등 다중 경로에 설치된 MDS 장비들의 탐지 이벤트 및 로그 통합 관리<br>• MDS 장비의 행위 분석 결과 공유 기능 (다수의 MDS 장비 구성 시, 중복 분석 및 탐지 최소화)<br>• YARA 룰 관리 및 연동 기능<br>• 인사 DB, AD(Active Directory) 연동을 통한 탐지 및 대응 호스트 정보 제공<br>• Syslog 전송 기능 (CEF, LEEF 포맷)<br>• 로그 및 설정 정보 백업 기능 (자동/수동)<br>• 다양한 유형의 보고서 제공 |
| MDS Agent 통합 관리 (Host Controller) | • MDS Agent 그룹 및 정책 관리<br>• MDS Agent 설치 및 패치 관리<br>• MDS Agent 대응 명령 및 공지사항 전송 기능 |

## AhnLab MDS Agent

| 기능 요약 | 상세 내용 |
|---|---|
| 엔드포인트 내 의심 파일 수집 및 대응 | • 독자적인 머신러닝 기술이 적용된 엔드포인트 의심 파일 수집 기능<br>• 악성코드 감염이 의심되는 호스트에 대한 네트워크 격리 등의 대응 조치<br>• 비정상적인 프로세스 실행 탐지 및 의심스러운 파일에 대한 실행 보류 기능<br>• 유사 시, 삭제된 파일에 대한 복원 기능<br>• V3 통합 설치 형태의 에이전트를 통한 엔드포인트 영역의 악성코드 치료 및 방어 체계 강화 |

# 구축 방안

기본적으로 탐지/분석 · 모니터링 · 에이전트 관리 기능이 포함된 일체형 장비 형태로 제공되며
고객사 환경과 보안 수준 요구에 따라 MDS 및 MDS Manager로 유연하게 구성 및 확장할 수 있습니다.

## 소규모·지사(SOHO)

**AhnLab MDS**
Analyzer(탐지·분석)
Data Viewer(모니터링)
Host Controller(에이전트관리)

**AhnLab MDS Agent**

- AhnLab MDS 4000A

- AhnLab MDS Agent

## 중견 기업(SMB)

**AhnLab MDS**
Analyzer(탐지·분석)

**AhnLab MDS Manager**
Data Viewer(모니터링)
Host Controller(에이전트관리)

**AhnLab MDS Agent**

- AhnLab MDS 4000A
- AhnLab MDS 8000A

- AhnLab MDS Manager 5000AR
- AhnLab MDS Manager 10000AR

- AhnLab MDS Agent

## 대기업(Enterprise)

**AhnLab MDS**
Analyzer(탐지·분석)

**AhnLab MDS Manager**
Data Viewer(모니터링)

**AhnLab MDS Manager**
Host Controller(에이전트관리)

**AhnLab MDS Agent**

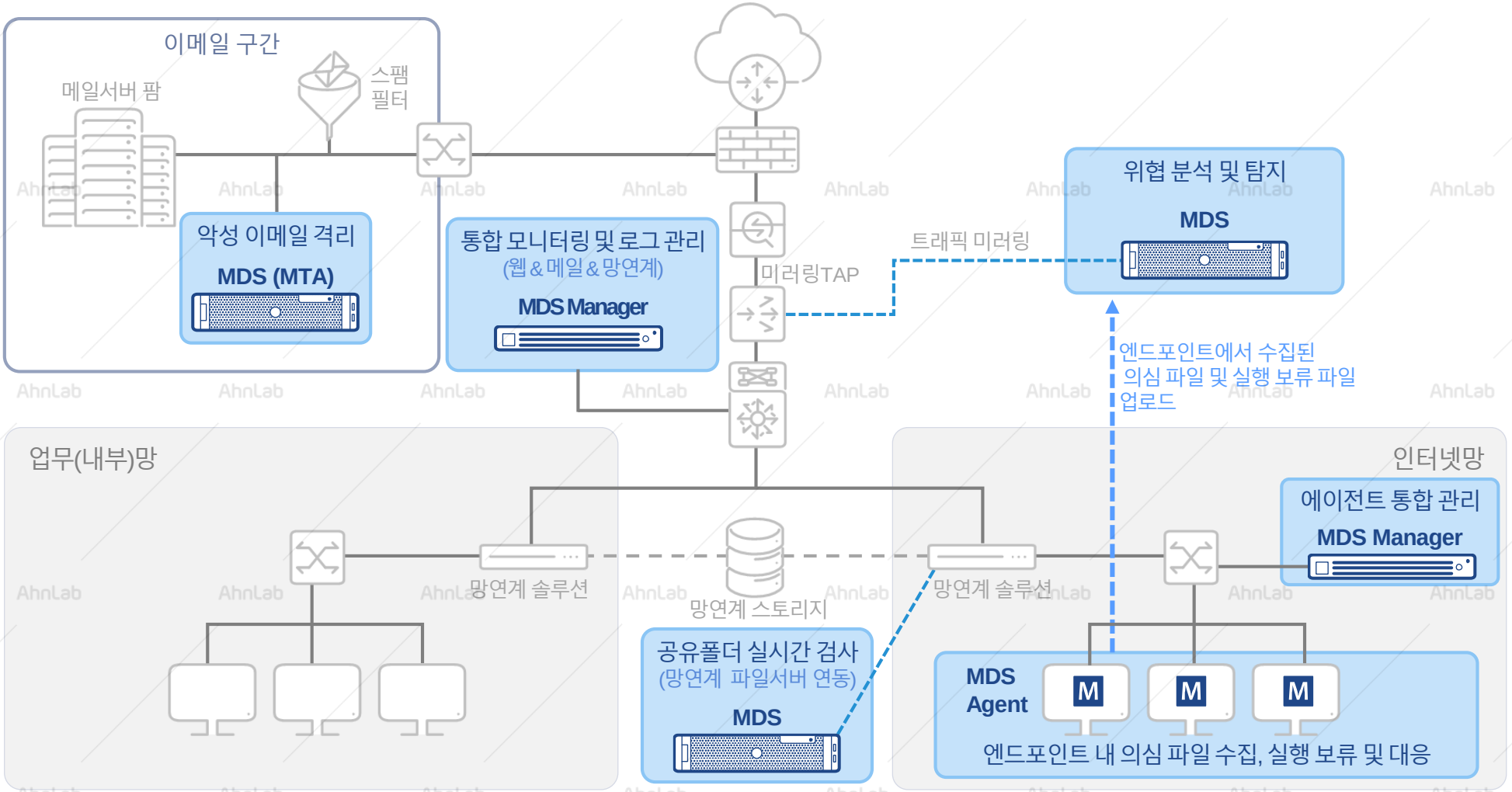
- AhnLab MDS 8000A
- AhnLab MDS 10000A

- AhnLab MDS Manager 5000AR
- AhnLab MDS Manager 10000AR

- AhnLab MDS Agent

# 통합 구축 방안 및 구성도

네트워크, 이메일, 엔드포인트, 망연계연동 구간 등 다양한 경로를 통해 유입되는 위협에 대한 효과적인 대응 체계를 구축할 수 있습니다.



# 제품 사양(1/2)

## AhnLab MDS

| 구분 | | AhnLab MDS 4000A | AhnLab MDS 8000A | AhnLab MDS 10000A | |
|---|---|---|---|---|---|
| 제안 성능 | 동적 분석 건수 | 35,000 건/1일 | 90,000 건/1일 | 200,000 건/1일 | |
| | 관리 에이전트 | 700개 | 2,000개 | 5,000개 | |
| | 트래픽 처리 (Throughput) | 800Mbps | 1.5Gbps | 4Gbps | |
| HDD | | 1TB x 2ea. | 1TB x 4ea. | 1TB x 8ea. | |
| RAID | | RAID 1 | RAID 10 | RAID 10 | |
| 네트워크 인터페이스 | | 1GbE 4 Ports (Copper)<br>1/10G SFP+ 4 Ports (Optical) | 1GbE 4 Ports (Copper)<br>1/10G SFP+ 4 Ports (Optical) | 기본 | 옵션 |
| | | | | 1GbE 2 Ports (Copper)<br>1/10G Base-T 2 Ports (Copper)<br>1/10G SFP+ 4 Ports (Optical) | 1GbE 2 Ports (Copper)<br>1/10G Base-T 4 Ports (Copper)<br>1/10G SFP+ 6 Ports (Optical) |
| 전원 | | 750W Redundant Power | 750W Redundant Power | 750W Redundant Power | |
| 랙 마운트 | | 1U, 19 inch | 1U, 19 inch | 2U, 19 inch | |
| 사이즈 (WxDxH, mm) | | 482 x 721.91 x 42.8 | 482 x 721.91 x 42.8 | 482.4 x 715.5 x 86.8 | |
| 구성 방식 | | Out-of-band / BCC<br>MTA (이메일 격리) | Out-of-band / BCC<br>MTA (이메일 격리) | Out-of-band / BCC<br>MTA (이메일 격리) | |
| 구축 가능 조합 | | • Analyzer + Host Controller + Data Viewer<br>• Analyzer + Data Viewer<br>• Analyzer | | | |

# 제품 사양(2/2)

## AhnLab MDS Manager

| 구분 | | AhnLab MDS Manager 5000AR | AhnLab MDS Manager 10000AR |
|---|---|---|---|
| 관리 에이전트 | 통합형<br>(DV + HC) | 2,000개 | 5,000개 |
| | 단독형<br>(Host Controller 전용 ) | 5,000개 | 10,000개 |
| HDD | | 1TB x 2ea., 2TB x 2ea. | 2TB x 2ea., 4TB x 2ea. |
| RAID | | RAID 1 | RAID 1 |
| 네트워크 인터페이스 | | 2 x 1GbE Ports (Copper) | 2 x 1GbE Ports (Copper) |
| 전원 | | 500W Redundant Power | 740W Redundant Power |
| 랙 마운트 | | 1U, 19 inch | 2U, 19 inch |
| 사이즈 (WxDxH,mm) | | 437 x 650 x 43 | 440 x 650 x 89 |
| 구축 가능 조합 | | • Host Controller + Data Viewer<br>• Data Viewer<br>• Host Controller | |

* DV(Data Viewer) : 통합 모니터링 및 로그 관리 기능
* HC(Host Controller) : 에이전트 관리 기능

## AhnLab MDS Agent

| 구분 | Client PC | Server |
|---|---|---|
| 운영체제 (OS) | Windows XP SP3 이상 / 7 / 8(8.1) / 10 | Windows Server 2003 SP2 이상<br>Windows Server 2008 / 2012 / 2016 |

* 상기 OS의 32/64 bit 지원

# 05
# 대응 사례

랜섬웨어 대응

스피어 피싱 대응

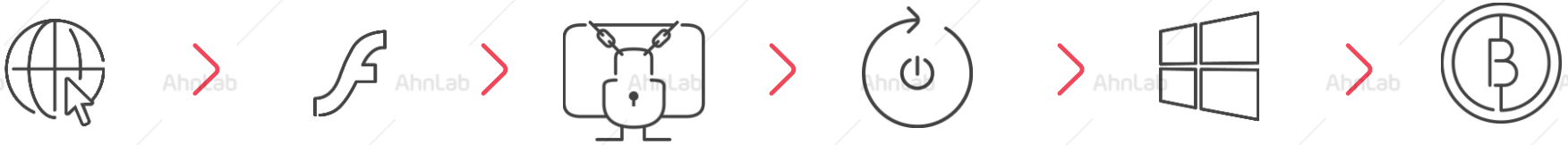
뱅커 및 파밍 공격 대응

# 대응 사례1 – 랜섬웨어(Ransomware)

웹 익스플로잇(Web Exploit), 포털/SNS를 통한 드라이브-바이-다운로드(Drive-by-download)

## 지능형 위협 공격 프로세스

최초 유입 악성코드에 대한 감염 차단 불가



1. 포털 및 SNS 접속
2. 플래시플레이어 익스플로잇 발생 (랜섬웨어 다운로드)
3. 랜섬웨어 동작
4. 강제 재부팅
5. Windows 부팅 차단
6. 결제 요청

## MDS 구축 후 대응 프로세스

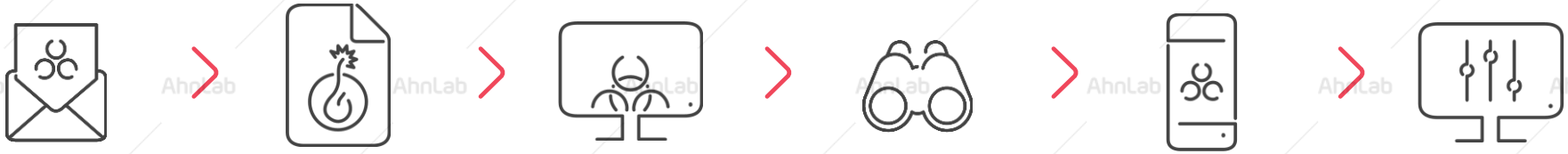
1. 포털 및 SNS 접속
2. 플래시플레이어 익스플로잇 동작 (동적 분석 시작 - MDS)
3. MDS 에이전트 (다운로드된 랜섬웨어 실행 보류 )
4. 악성 여부 분석 완료 (MDS)
5. 경고 알림 및 실행 보류된 랜섬웨어 삭제
6. 대응 결과 모니터링

# 대응 사례2 –스피어 피싱(Spear Phishing)

(암호화)압축파일/Non-PE 익스플로잇, 암호화 구간(TLS)

## 지능형 위협 공격 프로세스

메일 암호화 구간(TLS) 및 정교하게 제작된 문서형 악성코드 대응 불가



1. 이메일 수신, 악성코드 다운로드
2. 비실행형 첨부 문서 기반의 익스플로잇 발생
3. 클라이언트 PC 잠복
4. 프로세스 감시 및 키로깅
5. 로깅 정보 C2 서버 전송
6. 클라이언트 PC 제어

## MDS MTA 구축 후 대응 프로세스

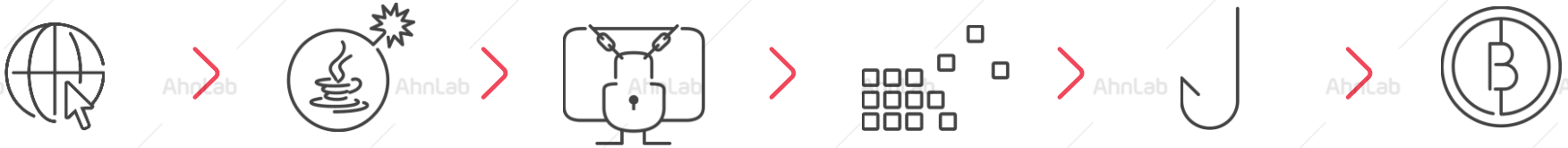
1. 이메일 수신
2. 비실행형 파일 동적 콘텐트 분석 시작 (MDS)
3. 악성 여부 분석 완료 (MDS)
4. 악성 이메일 격리
5. 경보 메일 발송 (메일 수신자, 보안 관리자)
6. 대응 결과 모니터링

# 대응 사례3 – 뱅커(Banker) 및 파밍(Pharming)

웹 익스플로잇(Web Exploit), SSL 암호화 통신

## 지능형 위협 공격 프로세스

암호화 통신에 대한 대응 불가



1. 워터링 홀
웹 페이지 접속
2. JAVA 익스플로잇 발생
3. 암호화 트래픽(SSL) 통한
악성코드 Down & Drop
4. 시작 프로그램/
서비스 등록
5. 피싱 사이트
접속 유도
6. 금융정보 탈취 및
예금 절도

## MDS 구축 후 대응 프로세스

1. 워터링 홀
웹 페이지 접속
2. JAVA 익스플로잇 동작
(동적 분석 시작 - MDS)
3. MDS 에이전트
(실행 보류 동작)
4. 악성 여부 분석 완료
(MDS)
5. 경고 알림 및
파일 삭제
6. 대응 결과 모니터링

# ※ 별첨

글로벌 평가 기관 APT 인증 획득

왜 APT 대응 솔루션이 필요한가?

왜 APT 대응 솔루션도 '안랩'인가?

주요 UI (AhnLab MDS v2.1.10 기준)

V3 통합 에이전트 구축 방안

# 글로벌 평가 기관 APT 인증 획득

※ 별첨

AhnLab MDS는 글로벌 보안 평가 기관인 ICSA Labs가 실시한 지능형 위협 대응(Advanced Threat Defense, ATD) 테스트에서 알려지지 않은 위협 99.1% 탐지, 정상 파일에 대한 오탐율 제로 등 모든 평가 항목에서 기준치보다 높은 성적으로 통과하며 인증을 획득했습니다.

AhnLab MDS 탐지율

탐지 **99.1%**

AhnLab MDS 오탐율

638개 정상 앱에 대한 오탐 없음

오탐 **0.0%**

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

***"안랩 MDS는 오탐 없이 알려지지 않은 위협에 대한 탁월한 탐지 성능을 보였다"***

AhnLab MDS 테스트 요약

| 테스트 기간 | 테스트 횟수 | 평균 탐지율 | 1시간 이내 탐지 | 정상 파일 오탐 |
|---|---|---|---|---|
| 32일 | 1,517회 | 99.1% | 99.1% | 0.0% |

*자료 출처: ICSA Labs 'ATD Certification Testing Report', Q3 2019

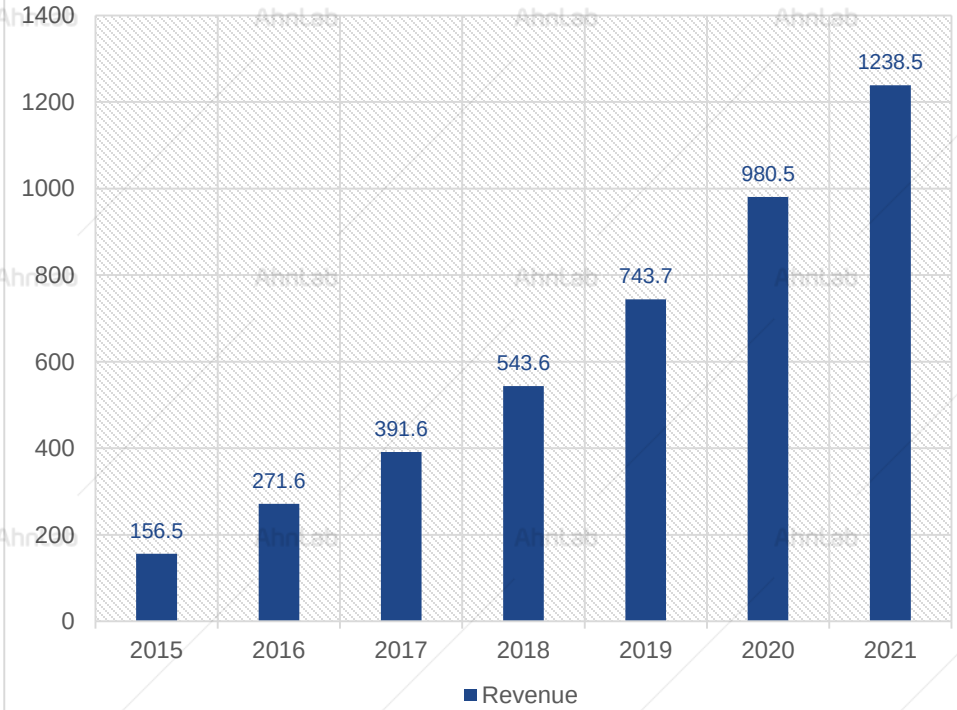
# 왜 APT 대응 솔루션이 필요한가?

※ 별첨

글로벌 시장조사 기관 Frost & Sullivan은 지능화된 악성코드 공격에 대한 우려가 증가함에 따라 아시아태평양 지역(APAC)의 지능형 위협 대응 솔루션 2021년까지 연평균 35.5%의 높은 성장률을 보일 것으로 전망하고 있습니다.

## APAC 지능형 위협 대응 솔루션 시장 전망 (2016-2021)

**Total NAMA Solution Market** :
Revenue Forecast, Asia-Pacific, 2015-2021 CAGR(2016-2021)=35.5%




### APAC 지능형 위협 대응 솔루션 시장 특징

- 지속적인 타깃 공격, APT 공격으로 인한 고도화된 악성코드 분석 위협 가시성 니즈 증가
- 통합적인 대응 체계 구축을 위한 사전 대응 니즈 증가
- 공공기관, 사회기반시설, 서비스 산업 등의 주요 시설 보안 요구 증가
- 보안 침해 사고에 따른 비용 손실 및 브랜드 손실 우려

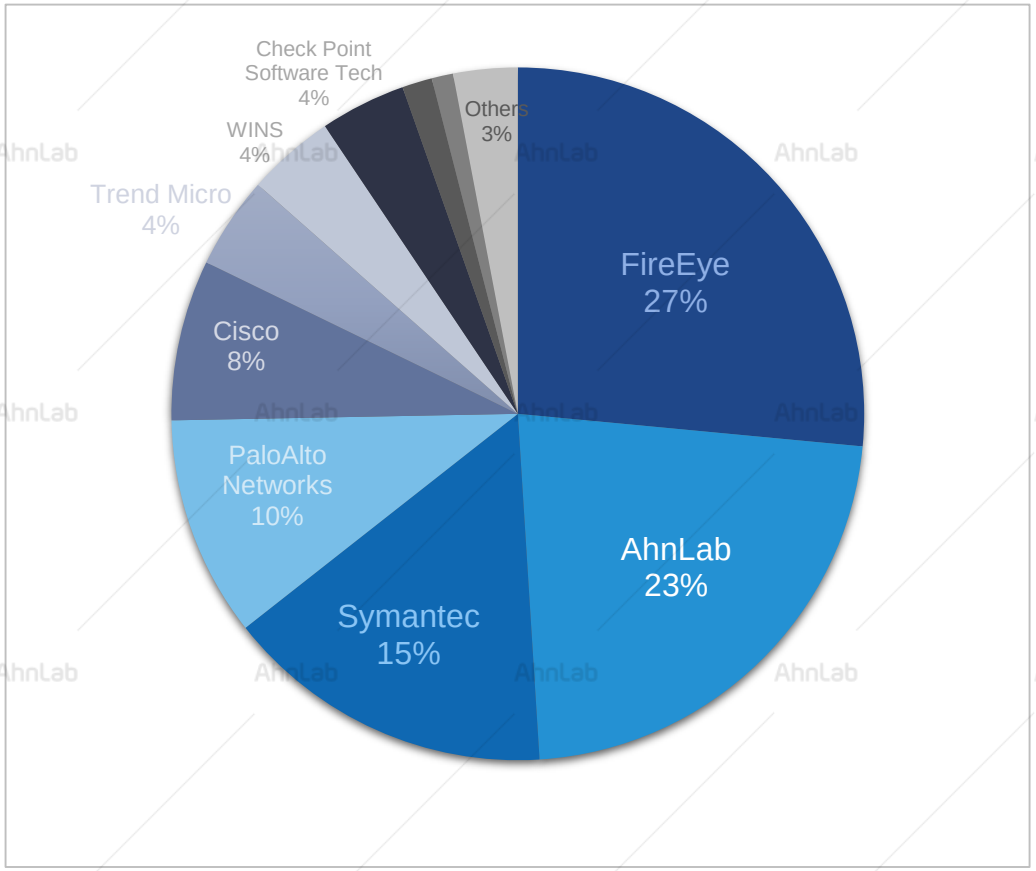
*자료 출처: Frost & Sullivan 'Asia-Pacific Network-based Advanced Malware Analysis(NAMA) Solution Market', 2017

# 왜 APT 대응 솔루션도 '안랩'인가?

※ 별첨

Frost & Sullivan의 조사에 따르면, AhnLab MDS는 네트워크부터 엔드포인트 연계를 통해 악성코드 침입에 대응 가능하다는 것이 강점으로, 이를 기반으로 한국 지능형 위협 대응 솔루션 시장에서 높은 점유율을 차지하고 있습니다.

## 지능형 위협 대응 솔루션 한국 시장 점유율 (*2017년 기준)




### 한국 지능형 위협 대응 솔루션 시장 특징

- 설치형 (On-premise) 제품 선호
  - 제품 소유 및 관리 측면
  - 정보보안 컴플라이언스 준수 관련

> *"안랩(AhnLab MDS)은 한국의 지능형 위협 대응 솔루션 분야에서 근소한 차이로 2위를 차지하고 있으며, 악성코드가 유입되는 주요 경로인 네트워크 및 엔드포인트 대응이 가능하다"*

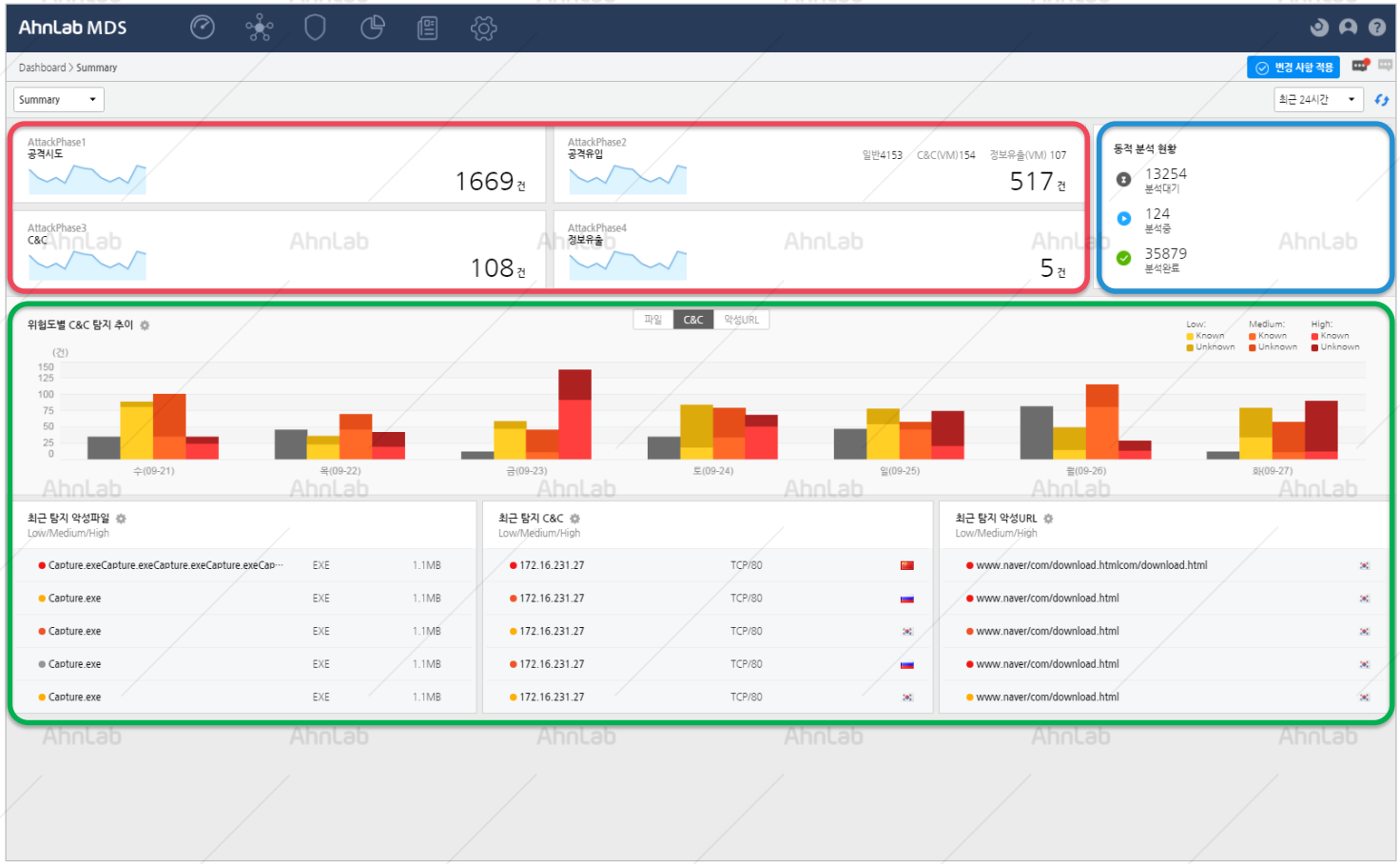
*자료 출처: Frost & Sullivan 'Asia-Pacific Network-based Advanced Malware Analysis(NAMA) Solution Market', 2019

# UI – 대시보드

※ 별첨

메인 대시보드(Dashboard)를 통해 각 공격 단계별 위협 탐지 추이 및 상세 내역, 가상머신(VM) 내 동적 분석 현황에 대한 정보 제공

공격 단계별
실시간 이벤트




가상머신(VM) 기반
동적 분석 현황
실시간 모니터링

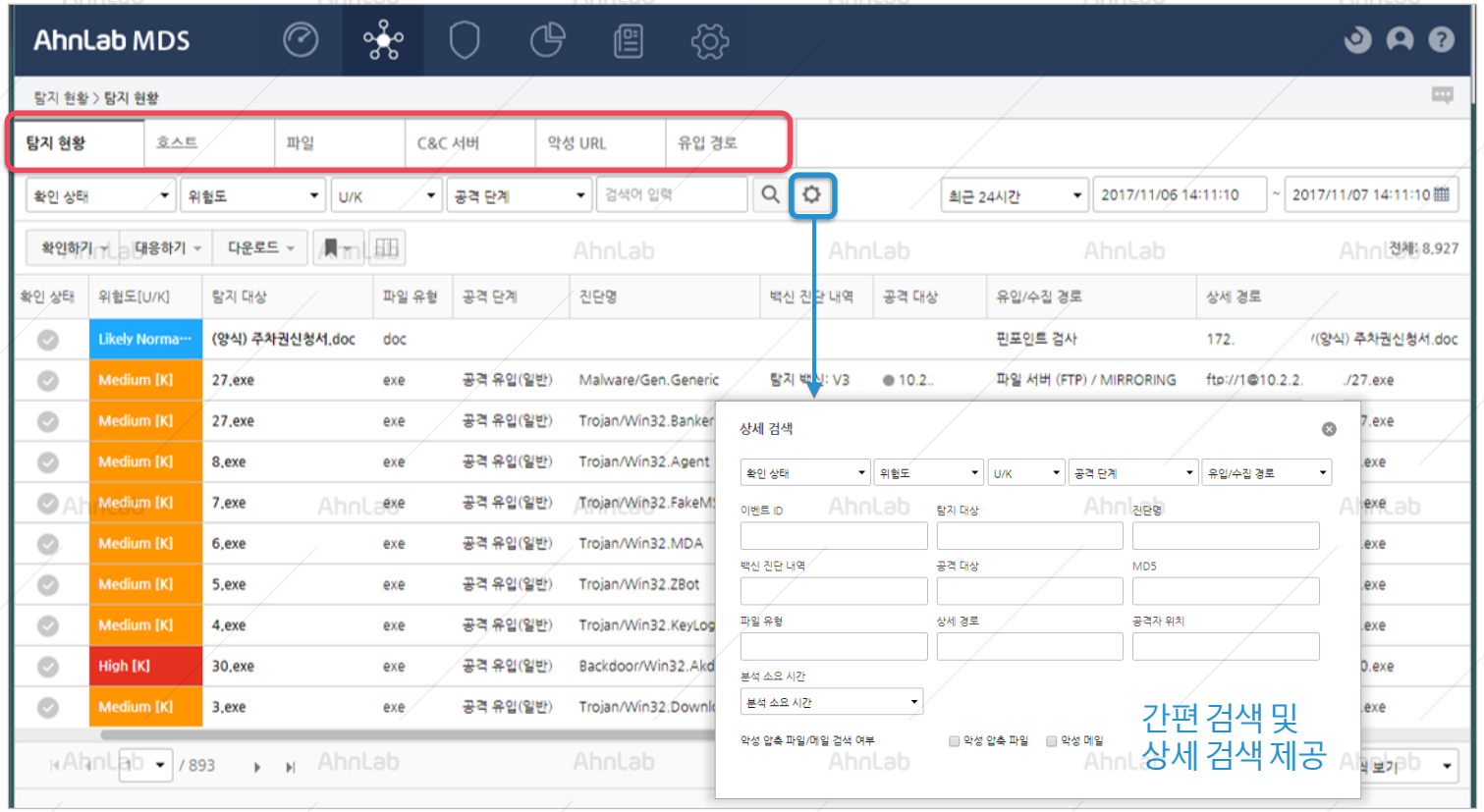
위협 탐지 추이 및
탐지 내역 모니터링
(파일/C&C/악성URL)

# UI – 로그 및 이벤트 정보

※ 별첨

탐지 현황에 대한 상세 현황 및 다양한 기준의 로그•이벤트 정보 제공

다양한 기준의
탐지 현황 제공

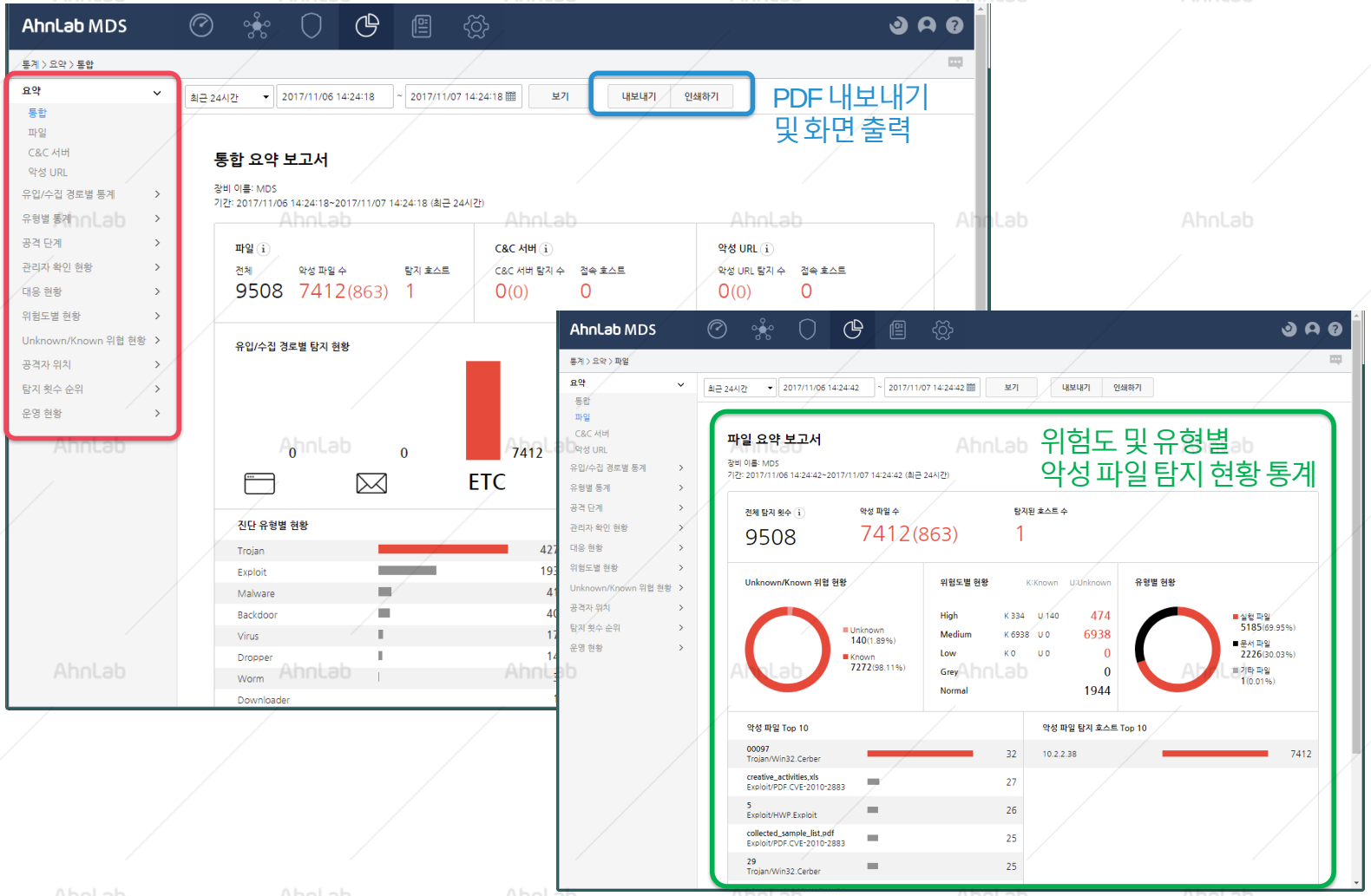


# UI – 별도 통계 정보 페이지 제공

※ 별첨

통계 메뉴를 통해 특정 시간 및 유형별 다양한 형태의 통계 정보 제공

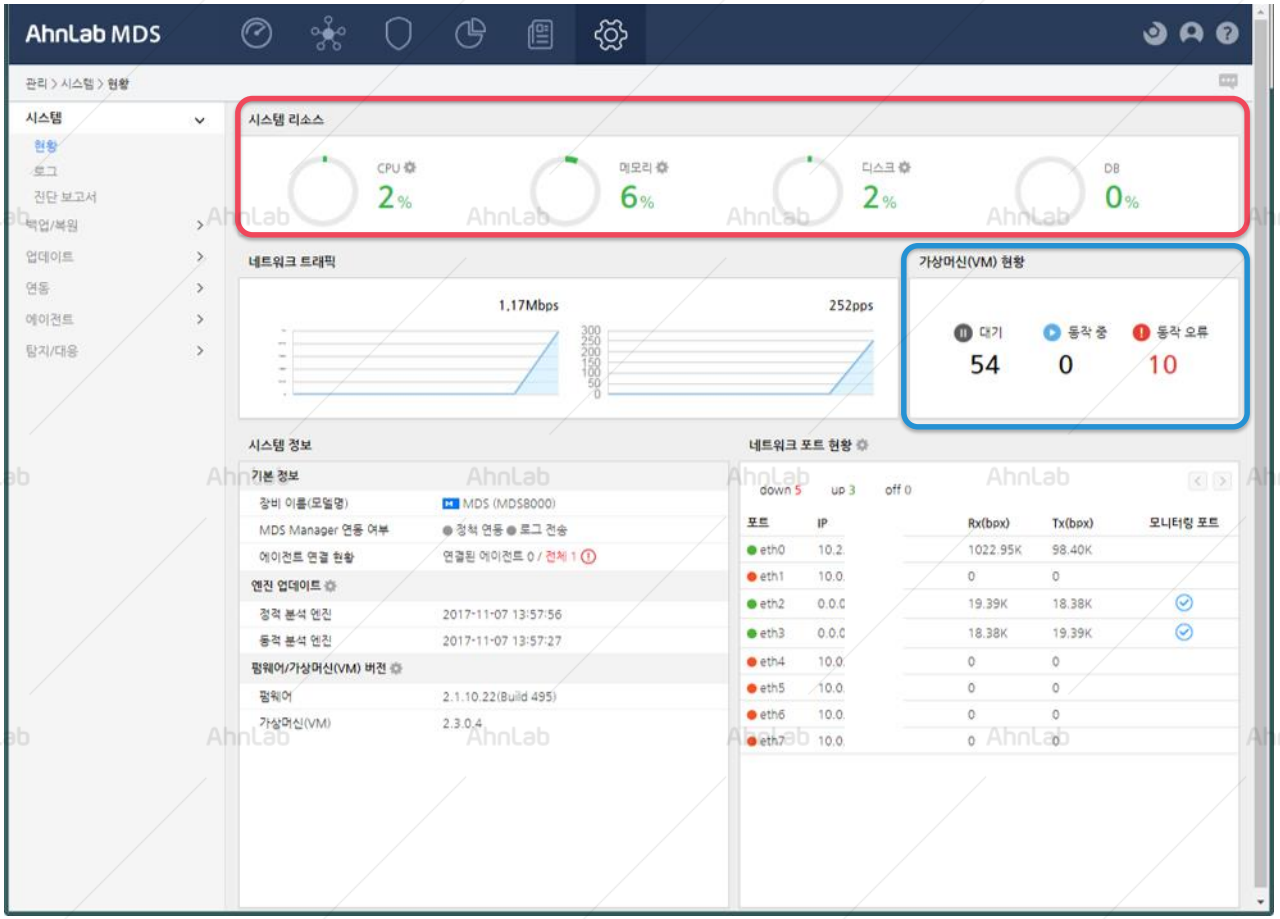
다양한 형태의 통계 보고서 제공



# UI – 실시간 모니터링

※ 별첨

실시간 시스템 리소스, 네트워크 트래픽 정보, 가상머신(VM)의 동작 현황에 대한 실시간 모니터링




시스템 리소스
및 트래픽 정보
실시간 모니터링

가상머신(VM) 현황
실시간 모니터링
(대기/동작/오류)

# UI – 상세 분석 정보(1/2)

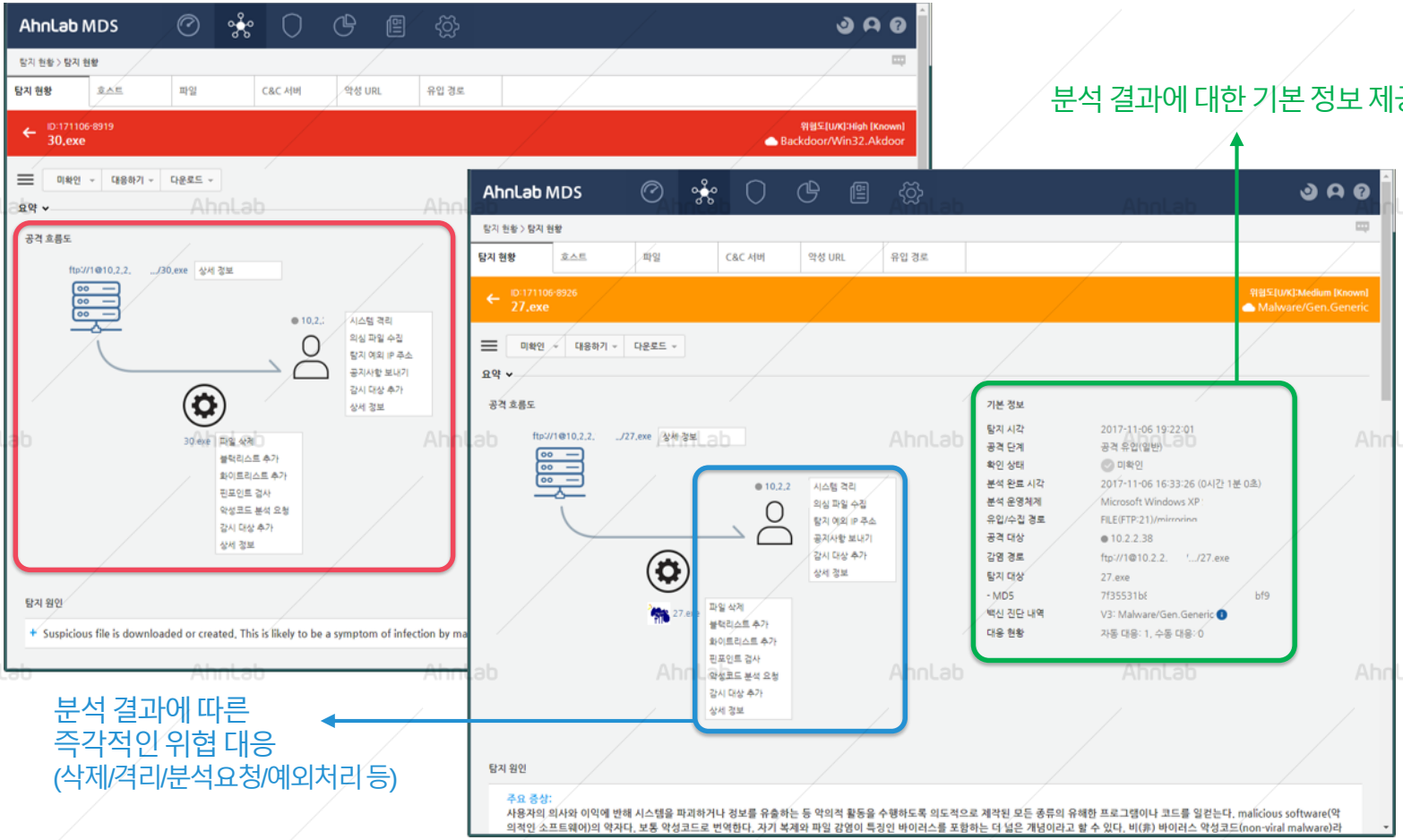
※ 별첨

상세 탐지 현황을 통해 직관적인 '공격 흐름도' 제공 및 분석 결과에 따른 즉각적인 위협 대응 가능

가상머신(VM)
분석 결과에 따른
공격 흐름도 제공

분석 결과에 대한 기본 정보 제공

분석 결과에 따른
즉각적인 위협 대응
(삭제/격리/분석요청/예외처리 등)

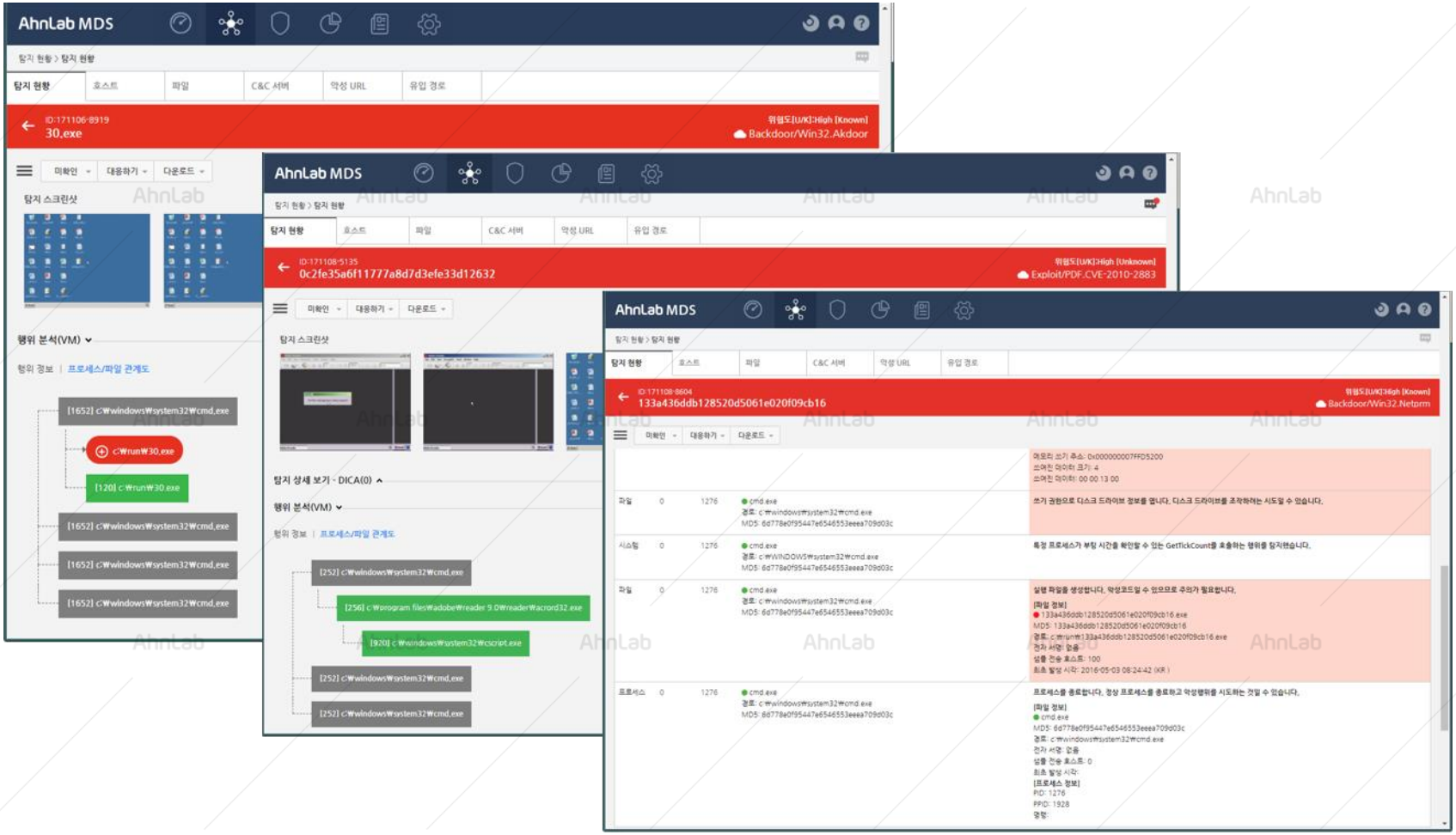


# UI – 상세 분석 정보(2/2)

※ 별첨

상세 탐지 및 분석 결과 제공

(탐지 스크린샷, 프로세스 및 파일 관계도, 비실행형 파일의 메모리 기반 정적 분석 결과, 행위분석 리포트 다국어 지원)

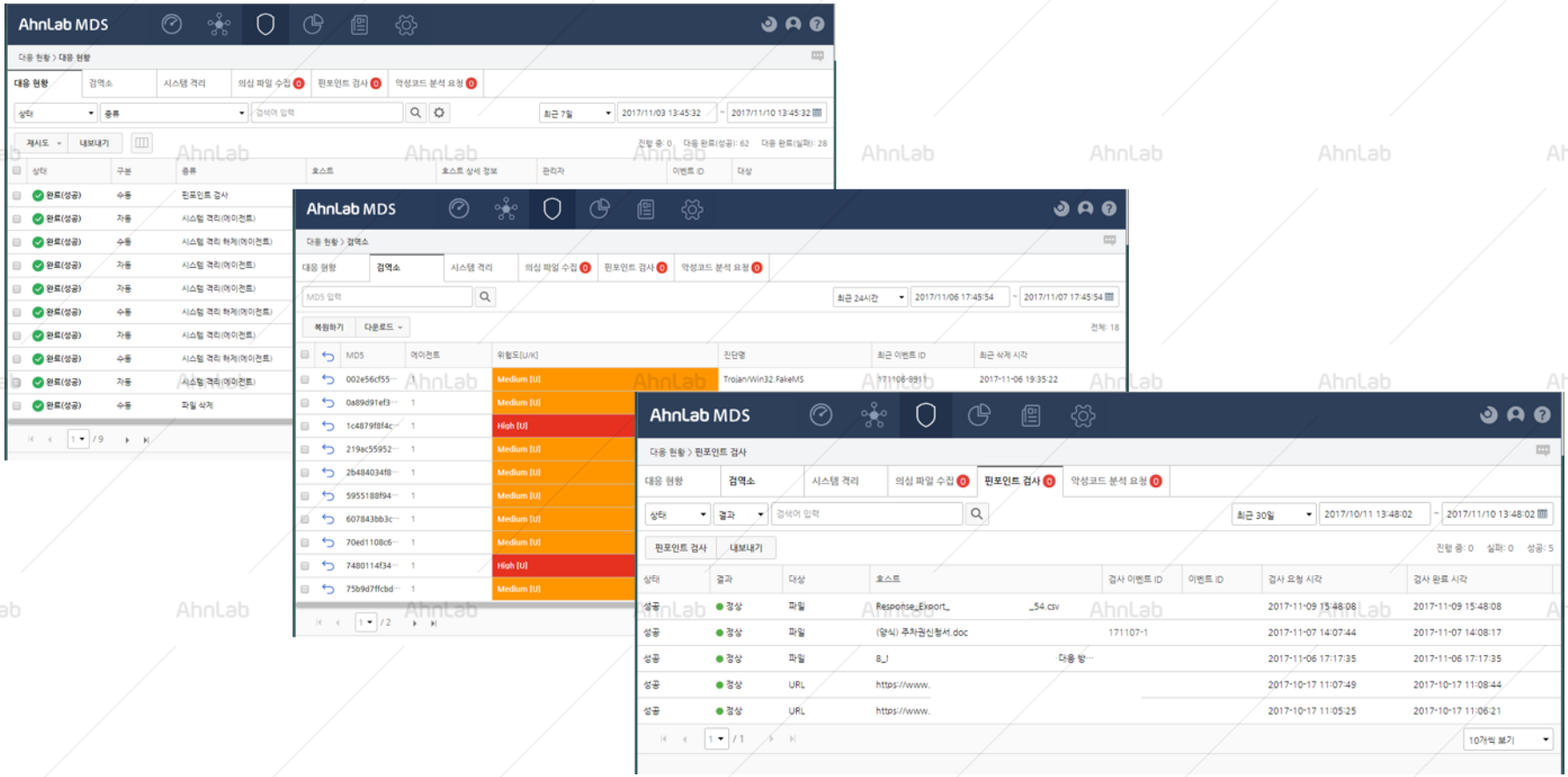


# UI – 대응 현황 정보 관리

※ 별첨

다양한 형태의 대응 현황 정보 로그 관리 및 모니터링

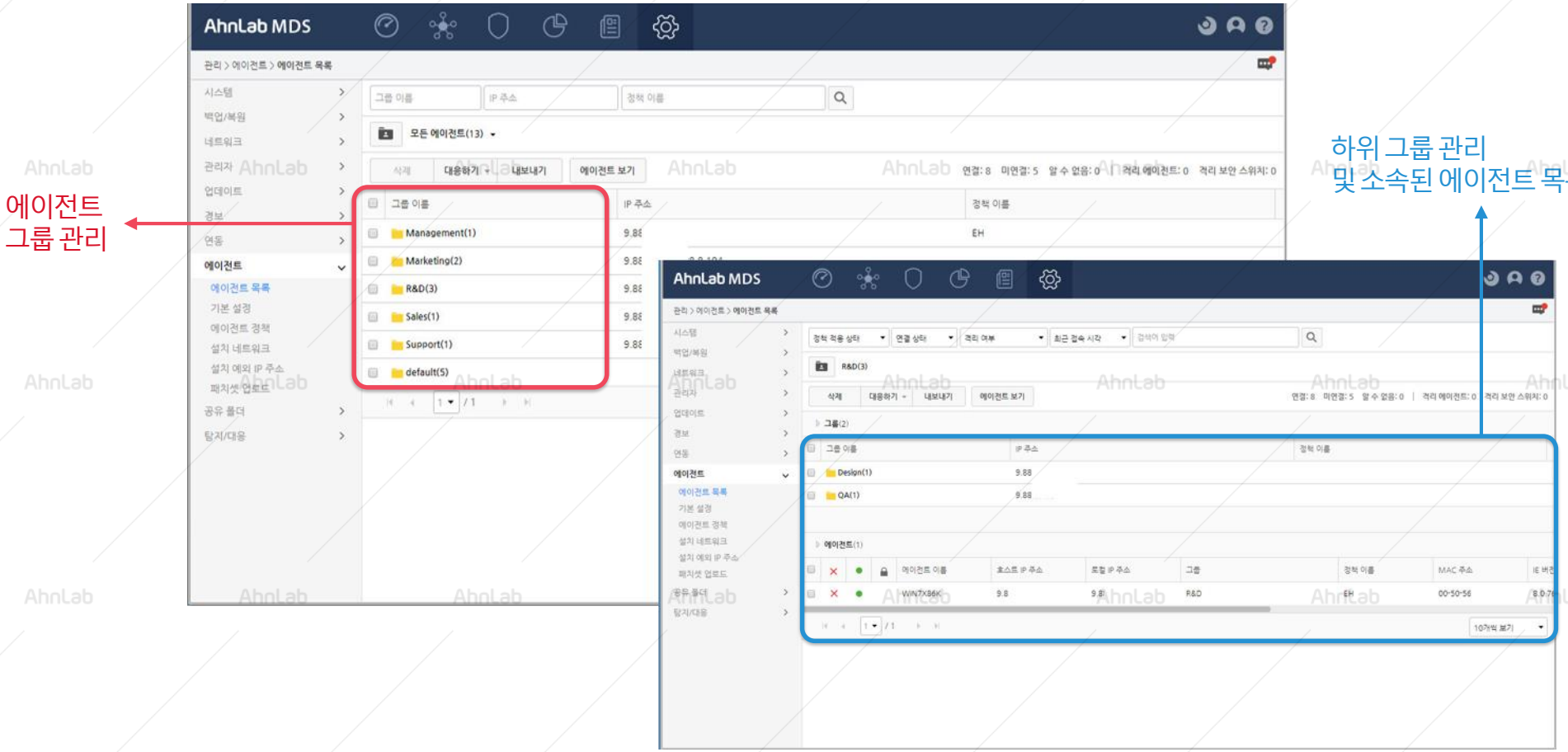
- 대응 현황 요약(Summary), 삭제된 악성 파일 내역(검역소), 시스템 격리 현황, 호스트(에이전트) 기준 머신러닝 기반의 의심파일 수집/대응 현황, 핀포인트 분석 현황/결과, 악성코드 분석 서비스 요청 진행 사항 및 보고서 열람 등



# UI – 에이전트 그룹 및 정책 관리

※ 별첨

에이전트에 대한 그룹 관리 및 그룹별 정책 설정•관리 가능 (상/하위 그룹 관리, 그룹 내 에이전트 관리)



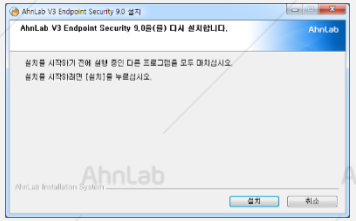
# V3 통합 에이전트 구축 방안

※ 별첨

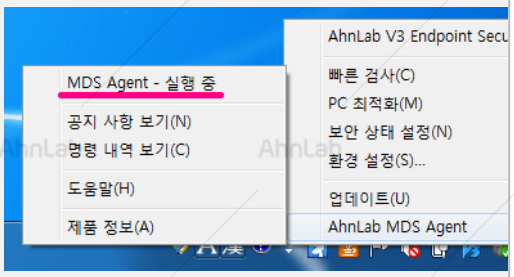
간단한 프로세스를 통해 안랩 MDS에이전트 - V3 통합 설치본 구축이 가능합니다.

MDS 에이전트 추출
→ V3 통합 설치본 준비

V3 통합 설치본 배포
(예: APC를 통한 배포)

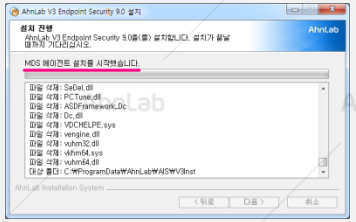


V3 통합 설치본 실행




V3 트레이 아이콘 내
MDS 에이전트 메뉴 확인

V3-MDS 통합 에이전트
설치 완료



V3 설치 완료 후
MDS 에이전트 모듈 설치 진행

AhnLab MDS

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우)13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com



FOLLOW US ON

www.ahnlab.com
www.facebook.com/AhnLabEP
www.youtube.com/user/OfficialAhnLab

AhnLab