AhnLab EDR

더 간편한 구축, 더 강력한 위협 대응

More security,
More freedom

표준제안서

AhnLab

CONTENTS

AhnLab

01
제안 배경

기업 및 기관의 침해사고 대응력

엔드포인트로 유입되는 보안 위협

기존 보안 솔루션의 위협 대응 한계

전방위적인 위협 관리 및 대응 필요성

위협 관리 및 대응 관점의 보안: EDR

기업 및 기관의 침해사고 대응력

IT 환경이 급변함에 따라 보안 위협 또한 빠르게 고도화·다변화하며 지속적으로 피해를 야기하고 있지만
여전히 대다수 기업 및 기관은 침해사고에 무방비한 상태입니다.

침해사고 유형

중복 응답

- 75.5% 악성코드(웜, 트로잔 등)
- 25.5% 랜섬웨어
- 13.0% 애드웨어/스파이웨어
- 9.1% 해킹
- 8.5% DoS 공격

2.2%
침해사고 경험률

악성코드 등 침해사고 유형은
사고경험 응답 사업체 대상에서 산출

침해사고 대응

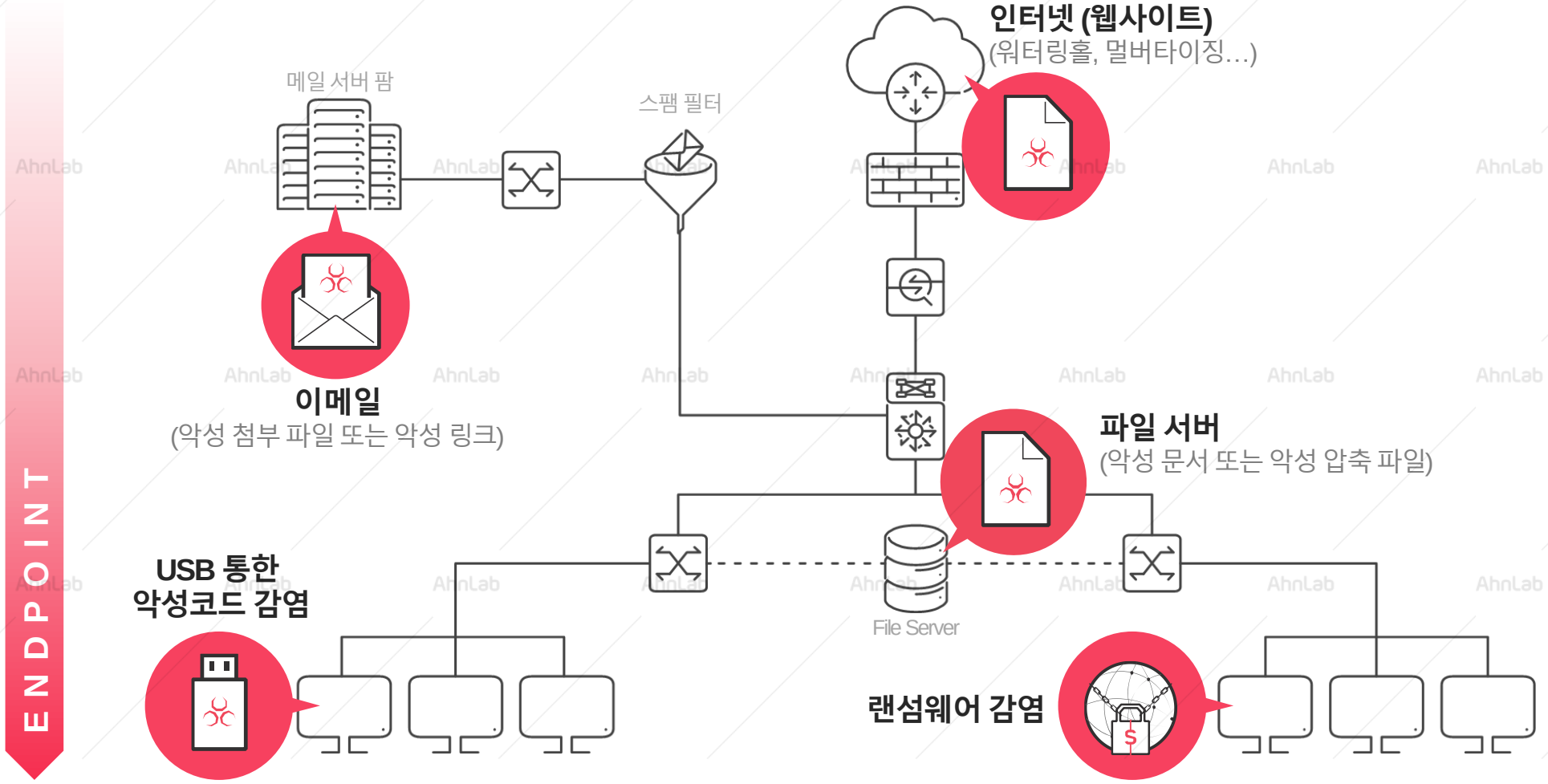
중복 응답

- 6.8% 침해사고 대응팀 구축 및 운영
- 7.1% 외부 전문 기관에 침해사고 대응 활동 위탁
- 8.0% 침해사고 대응 계획 수립
- 16.3% 침해사고 대처를 위한 긴급연락 체계 구축
- 74.1% 별다른 활동을 수행하지 않음

조사 대상 : 9,000개 기업
*출처: 한국인터넷진흥원, '2017 정보보호실태조사'

엔드포인트로 유입되는 보안 위협

다양한 OS, 애플리케이션, 디바이스 등으로 인해 기업 및 기관의 엔드포인트 환경이 다변화되면서
랜섬웨어를 비롯한 신·변종 악성코드가 다양한 경로를 통해 유입되어 직·간접적으로 엔드포인트를 위협하고 있습니다.



기존 보안 솔루션의 위협 대응 한계(1/2)

고도화된 위협이 엔드포인트에서 실행 또는 은닉, 확산됨에도 불구하고 대부분의 기업 및 기관에서는
단순 백신과 네트워크 중심으로 대응하기 때문에 실제 감염된 엔드포인트에 대한 정보(로그)를 확보하지 못하고 있습니다.

보안솔루션	한계점
차세대 방화벽 (NG-Firewall)	• 인가된 사용자에 대한 로그(감사) 수집 -과도한 로그량으로 분석 제한적
IPS (Intrusion Prevention System)	• 네트워크 시그니처 패턴 기반 대응 • 너무 많은 이벤트 관리 및 이기종 운영 관리 한계 • 오탐•미탐 발생 가능성 존재 (기업 환경에 따라 별도의 최적화 작업 필요)
네트워크 샌드박스 (Sandbox)	• SSL 통신으로 인한 트래픽 분석 한계 • 타깃 공격 기법의 고도화 - 샌드박스 우회(Anti-VM) 기법을 이용한 위협 대응 한계
DLP (Data Loss Prevention)	• 전체 데이터에 대한 모니터링 불가능 - 특정 키워드 기반의 데이터만 분석 가능 • SSL 암호화 트래픽 분석 한계
안티바이러스 (Anti-Virus)	• 엔드포인트 로그 수집 제한적 -악성코드 탐지 시 차단 또는 격리 등의 정보만 제공 -악성코드 감염 경로 추적 불가 (로그가 존재하지 않음) →엔드포인트 위협에 대한 가시성 확보 한계
UEBA (User and Entity Behavior Analytics)	• SIEM과 같은 별도의 데이터 수집 서버 필요
SIEM (Security Information and Event Management)	• 연동된 단위 보안 제품에서 로그가 생성 또는 전송되지 않을 경우 분석 제한적

기존 보안 솔루션의 위협 대응 한계(2/2)

네트워크 이벤트 분석 중심의 일반적인 네트워크 기반 보안 환경에서는
엔드포인트 로그 수집 및 분석의 한계 등으로 인해 최신 위협에 효과적으로 대응하기 어렵습니다.

대용량 데이터 처리 및 분석, 위협 인텔리전스(TI) 연계를 통한
통합적인 위협 관리·대응 필요

네트워크 기반 보안의 한계점

안티바이러스 제품 연동 시
악성코드 감염 시스템에 대한 제한적 모니터링만 가능
- 감염 경로 파악 불가능(엔드포인트 위협 가시성 부족)

동일한 악성코드(의심 파일)에 감염(또는 은닉) 된
단말 현황 파악 불가
- 잠재적 위협 파악 불가

방화벽, IPS 등 네트워크 보안 장비 기반 분석의 한계
- 엔드포인트 위협 현황 파악 불가

보완점

치료 정보 외에 '감염 경로'에 대한 정보 확보
→ 엔드포인트 위협 가시성 확보 필요

의심 시스템에 대한 엔드포인트 전수 검사 필요

엔드포인트 로그 분석 필요

전방위적인 위협 관리 및 대응 필요성

급변하는 위협 동향에 따라 네트워크와 엔드포인트 등 내부 인프라 전반에 대한 체계적인 위협 관리 및 대응의 필요성이 강조되고 있습니다.

인프라 전반에 대한 **체계적인 위협 관리·대응 필요**

다수의 보안 솔루션의 수많은 정보를
신속하게 탐지 및 대응

정확한 정보 전달을 통한
보안 관리자 반응·대응 시간 최소화

보안 솔루션 및 기능의 유기적인 연계를 통한
엔드포인트 위협 가시성 확보

- ✓ 최신 악성코드 **제어 및 대응의 한계**
- ✓ 다양한 위협 경로 **모니터링의 한계**
- ✓ 위협 고도화에 따른 **분석·대응 속도 지연**

다양한 유입 경로를 통한
의심·악성 파일 유입

사회공학기법, 표적/지능형 공격

OS/SW 제로데이 취약점 이용한
신·변종 악성코드 증가

위협 관리 및 대응 관점의 보안: EDR

기존 보안 솔루션의 한계를 보완함으로써 신·변종 위협에 대한 대응력을 강화하고 잠재 위협을 최소화하기 위해
'엔드포인트단에서의 위협 정보 수집·분석·대응 관점의 보안'이 주목받고 있습니다.

※ EDR(Endpoint Detection & Response)**이란?**

엔드포인트단에서 지속적인 모니터링 및 대응을 제공하는 보안 솔루션으로, 엔드포인트단에서의 위협의 탐지, 통제, 분석, 치료 등의 기능을 제공한다.
엔드포인트 보안을 위한 보조적인 툴(tool)로서, 안티바이러스 등 기존 보안 솔루션과의 연계를 통해 더욱 효과를 발휘한다.

*출처: Gartner

02
AhnLab EDR

AhnLab EDR 개요

특장점

주요 기능

도입 효과

AhnLab

AhnLab EDR

AhnLab EDR은 엔드포인트 영역에 대한 지속적인 모니터링을 통해 위협 탐지 및 분석, 대응을 제공하는 엔드포인트 위협 탐지 및 대응(Endpoint Detection & Response) 솔루션입니다.

- 국내 최초의 행위 기반 분석 엔진을 통한 위협 행위 분석 및 모니터링
- 엔드포인트 가시성 기반의 진일보한 위협 탐지 및 대응
- 최고의 엔드포인트 보안 및 악성코드 분석 전문 기업의 기술력이 응집된 EDR

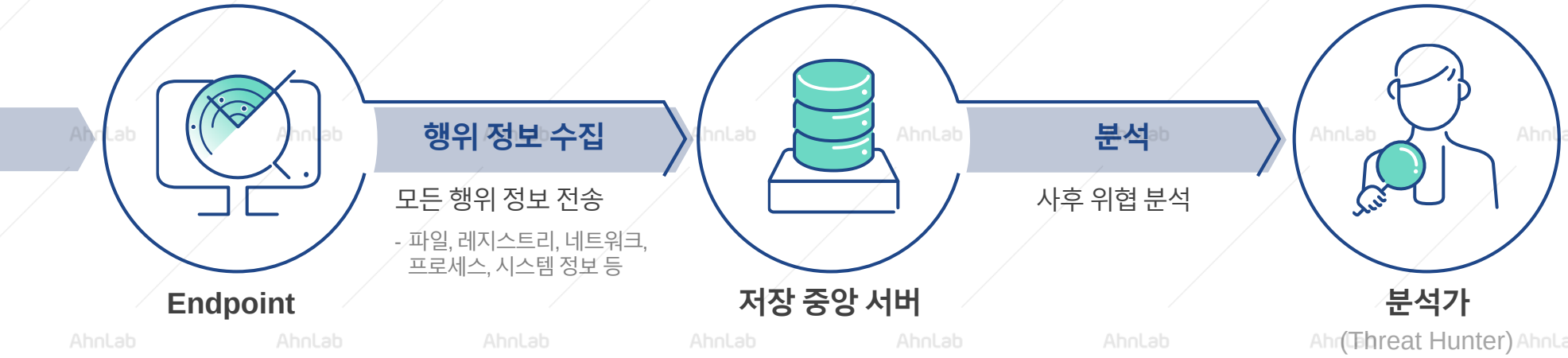
행위 정보 탐지·분석을 통한
엔드포인트 가시성 확보 및 대응

AhnLab EDR

간편한 구축, 손쉬운 운영
더 강력한 위협 대응

특장점 – 엔드포인트 행위 정보 수집을 통한 위협 가시성 강화

AhnLab EDR은 안랩의 독자적인 행위 기반 엔진인 MDP 엔진을 통해 엔드포인트의 모든 행위 정보를 수집, 저장하고 탐지된 위협에 대한 유입 경로를 추적, 분석함으로써 기업 및 기관의 위협 가시성을 강화합니다.



Threat Hunting

- 특정 이벤트 중심이 아닌 전체적, 연속적인 행위 정보 수집 및 저장
- 필요 시 언제든지 위협 및 관련 정보 확인 가능 - 사후 위협 분석 가능

Centralization

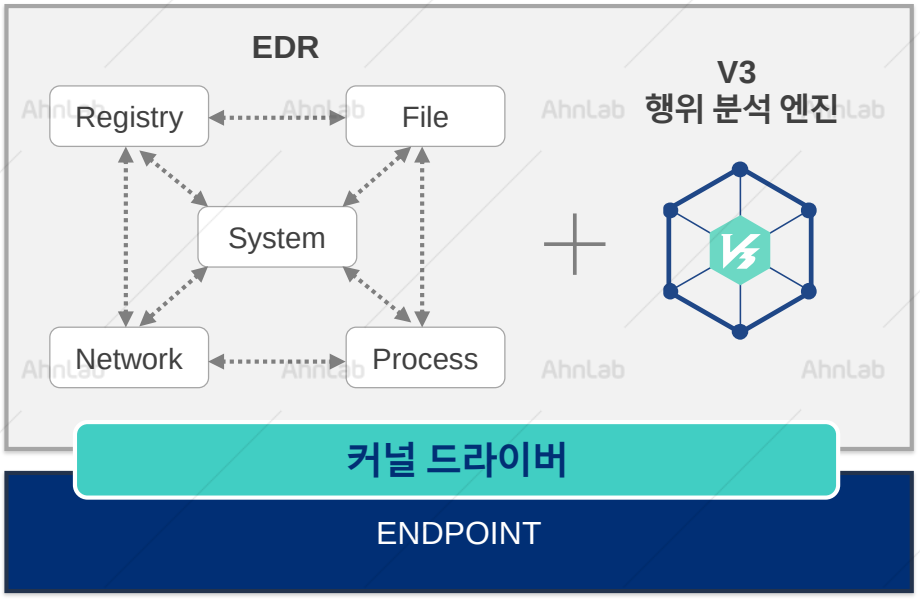
- 중앙화된 로그 저장 및 관리 - 모든 엔드포인트 로그를 중앙 서버에 저장
- 로그 관리 및 분석 편의성 향상

특장점 – V3 기반의 손쉬운 적용 및 안정적인 운영

V3를 기반으로 엔드포인트 레벨에서 운영체제의 행위 정보 모니터링을 제공하는 AhnLab EDR은
별도의 커널 드라이버 설치가 필요하지 않기 때문에 엔드포인트 성능 부담 없이 손쉽게 구축 및 운영이 가능합니다.

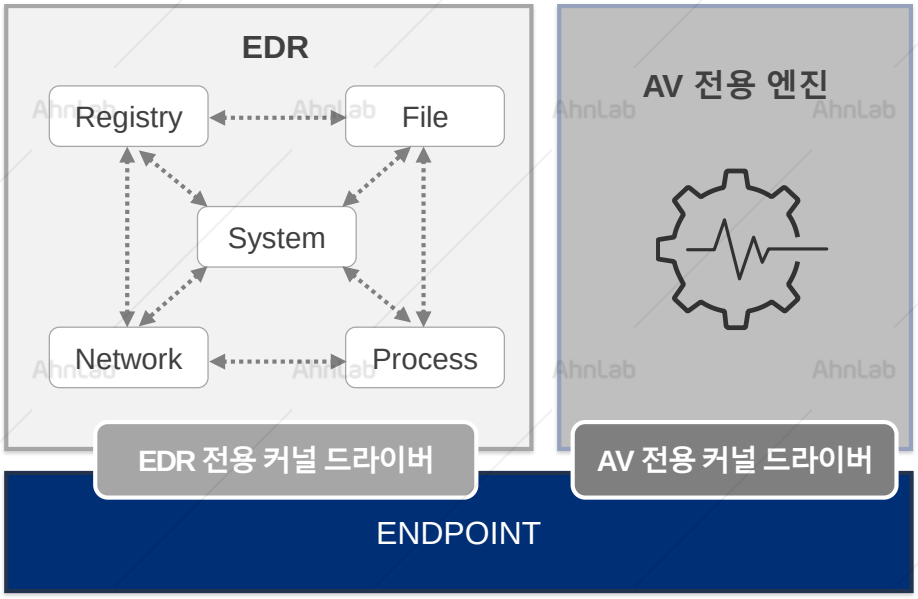
AhnLab EDR

- V3 행위 분석 엔진 연계
- 엔드포인트 행위 분석을 위한 커널 드라이버 추가 설치 불필요



타사 EDR

- 운영체제 커널 기반의 행위 정보 모니터링을 위해 AV와 EDR 운영을 위한 개별 커널 드라이버 설치 및 관리 필요
- 별도의 AV 사용으로 인한 커널드라이버 중복 설치 및 이에 따른 엔드포인트 성능 이슈 발생



특장점 – 단일 매니지먼트 기반의 효율적인 보안 운영 및 관리

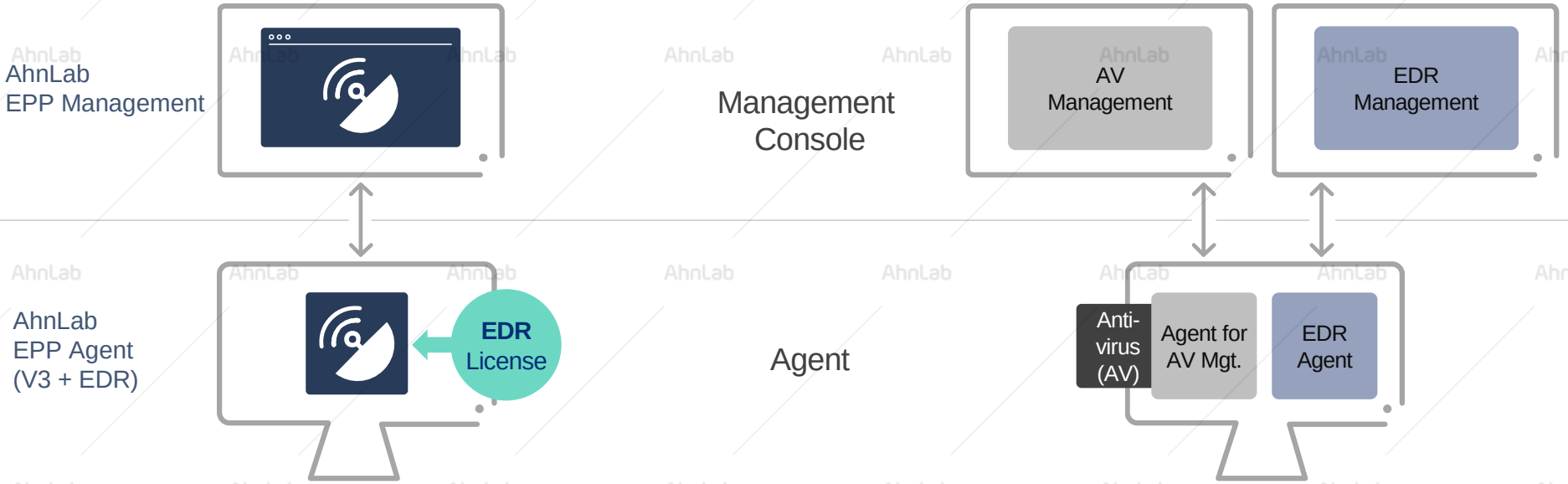
AhnLab EDR은 차세대 엔드포인트 매니지먼트 플랫폼 AhnLab EPP를 기반으로 손쉽게 구축할 수 있으며
단일 매니지먼트 콘솔을 통한 효율적인 엔드포인트 보안 통합 관리 및 대응이 가능합니다.
* V3와 AhnLab EPP Agent를 사용 중인 경우, 별도의 에이전트 설치 없이 라이선스 추가만으로 손쉽게 EDR 운용 가능

AhnLab EDR

- 단일 에이전트, 단일 매니지먼트 기반의 효율적인 보안 운용
  (One Agent, Single Management Console)
- V3 기 사용 시 EDR 라이선스 추가만으로 즉각적인 운영 가능
- EDR 운영을 위한 에이전트 추가 설치 불필요
  (로그 저장 등을 위한 DB 서버만 추가)

타사 EDR

- 백신(AV), EDR 및 그 외 엔드포인트 보안 솔루션 운영을 위한
  개별 에이전트, 개별 매니지먼트 콘솔 필요
- EDR 전용 장비 구매 및 구축 필요
- 백신 추가 사용 시 개별 설치 및 관리 필요



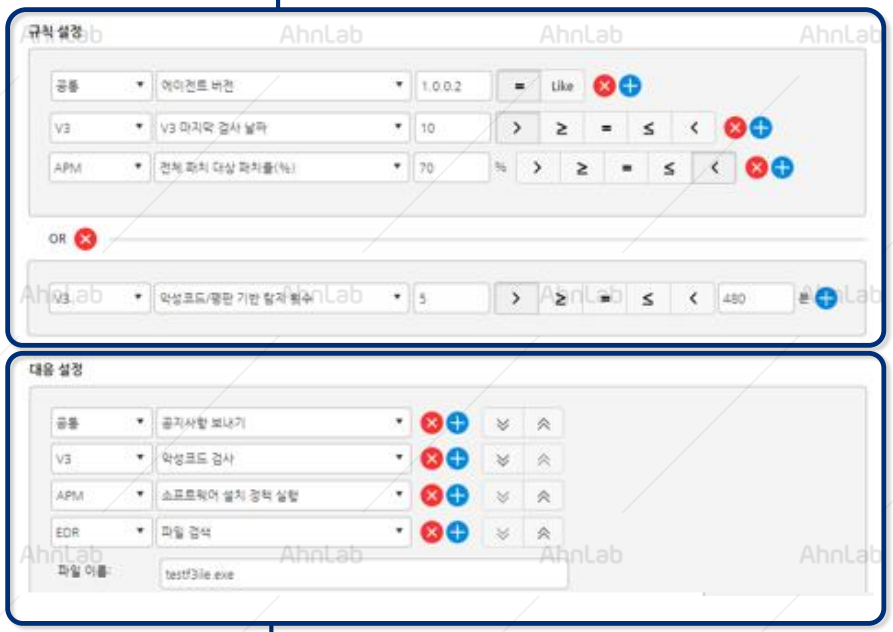
특장점 – 엔드포인트 제품간 연계 정책을 통한 위협 대응

다양한 안랩 엔드포인트 보안 제품간의 연계 정책 설정을 통해 조직의 환경에 최적화된 엔드포인트 보안 솔루션 운영이 가능합니다.

- 차세대 엔드포인트 플랫폼 AhnLab EPP에 플러그인 된 다수의 제품에 대한 정책 연계를 통해 유기적인 위협 대응 가능

연계 규칙 설정

개별 제품의 조건을 and/or 규칙으로 연계하여 정책 설정



연계 규칙 알림 설정

연계 규칙별 메일 알림, 보고서 생성

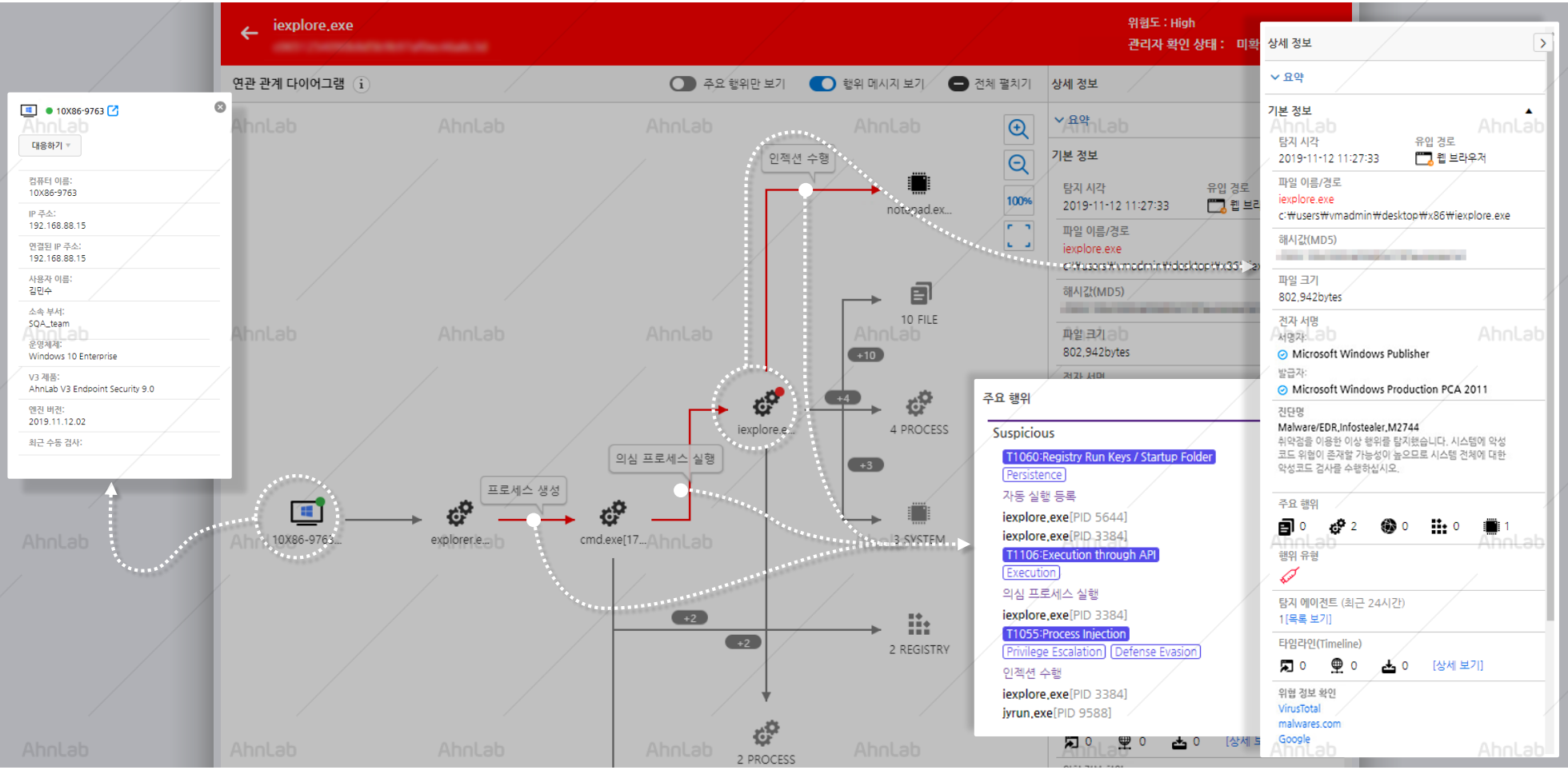
연계 대응 설정

연계 규칙을 위반한 시스템에 대한 개별 또는 공통 대응 정책 설정

특장점 – 위협 이벤트 및 공격 흐름도 제공 (1/2)

AhnLab EDR은 공격 흐름도와 함께 상세한 정보를 제공하며 위협 종류, 행위 및 공격 단계에 따라 적절한 대응 및 조치 방안을 제시합니다.

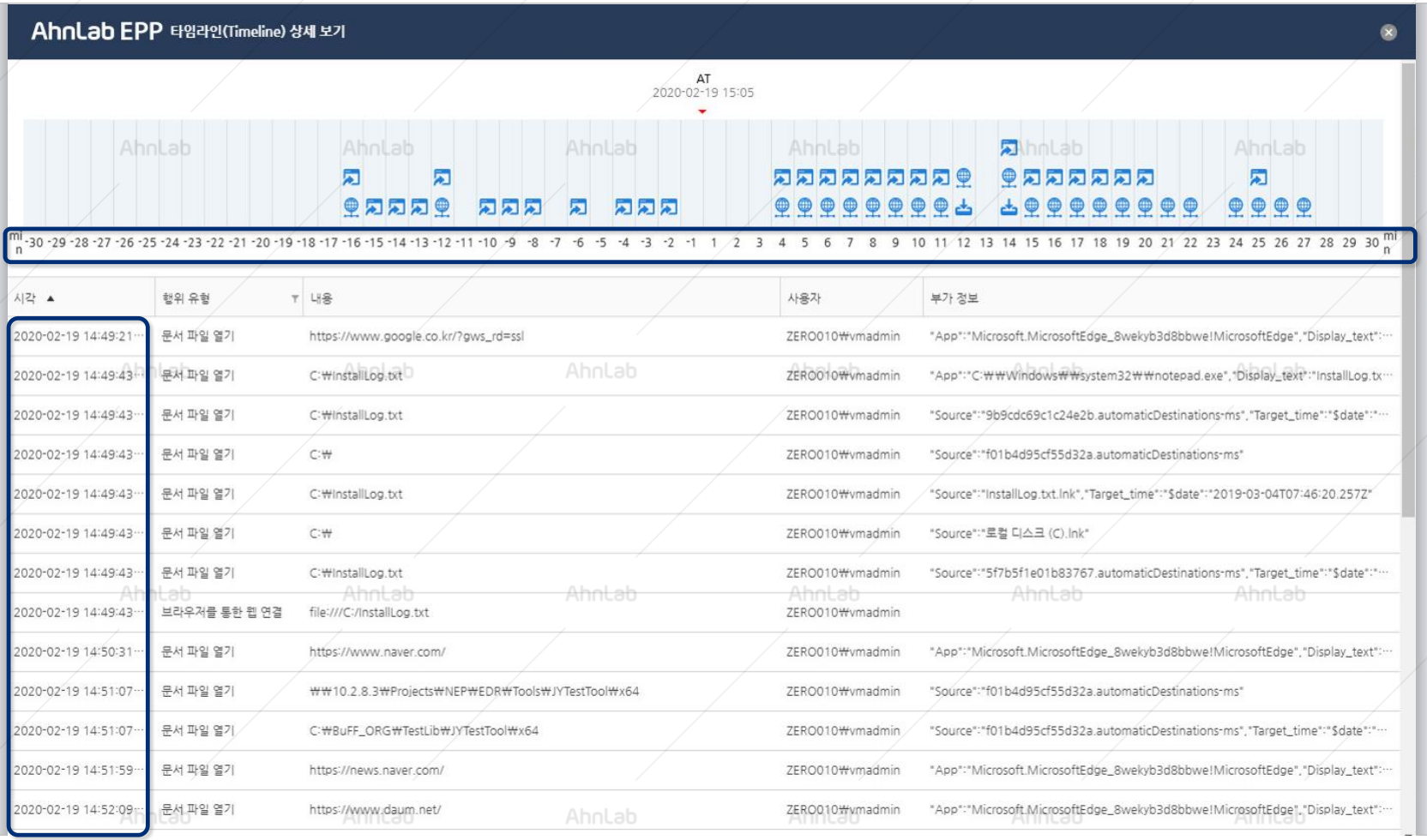
- 공격 단계별 프로세스, 에이전트, 파일 등에 대해 프로세스 종료 및 네트워크 차단, 파일 수집·검색·격리 ·복원 가능
- 위협의 종류, 유입 경로, 주요 행위, 연관 관계, 위험도, MITRE ATT&CK 정보, 인증서 정보, 위협 정보 링크 등에 대한 상세한 확인 및 대응 가능



특장점 – 위협 이벤트 및 공격 흐름도 제공 (2/2)

또한 의심스러운 행위에 대해 아티팩트 기반의 타임라인 다이어그램을 함께 제공합니다.

- Open in APP, Connect, Download 이벤트 유형에 대한 타임라인 기반의 다이어그램 확인 가능
- 각 유형에 따라 관련 상세 정보 제공: Contents, User, File Size, IP, URL 등



시각	행위 유형	내용	사용자	부가 정보
2020-02-19 14:49:21···	문서 파일 열기	https://www.google.co.kr/?gws_rd=ssl	ZERO010₩vmadmin	"App":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","Display_text":···
2020-02-19 14:49:43···	문서 파일 열기	C:₩InstallLog.txt	ZERO010₩vmadmin	"App":"C:₩₩Windows₩₩system32₩₩notepad.exe","Display_text":"InstallLog.tx···
2020-02-19 14:49:43···	문서 파일 열기	C:₩InstallLog.txt	ZERO010₩vmadmin	"Source":"9b9cdc69c1c24e2b.automaticDestinations-ms","Target_time":"$date":"···
2020-02-19 14:49:43···	문서 파일 열기	C:₩	ZERO010₩vmadmin	"Source":"f01b4d95cf55d32a.automaticDestinations-ms"
2020-02-19 14:49:43···	문서 파일 열기	C:₩InstallLog.txt	ZERO010₩vmadmin	"Source":"InstallLog.txt.lnk","Target_time":"$date":"2019-03-04T07:46:20.257Z"
2020-02-19 14:49:43···	문서 파일 열기	C:₩	ZERO010₩vmadmin	"Source":"로컬 디스크 (C).lnk"
2020-02-19 14:49:43···	문서 파일 열기	C:₩InstallLog.txt	ZERO010₩vmadmin	"Source":"5f7b5f1e01b83767.automaticDestinations-ms","Target_time":"$date":"···
2020-02-19 14:49:43···	브라우저를 통한 웹 연결	file:///C:/InstallLog.txt	ZERO010₩vmadmin	
2020-02-19 14:50:31···	문서 파일 열기	https://www.naver.com/	ZERO010₩vmadmin	"App":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","Display_text":···
2020-02-19 14:51:07···	문서 파일 열기	₩₩10.2.8.3₩Projects₩NEP₩EDR₩Tools₩JYTestTool₩x64	ZERO010₩vmadmin	"Source":"f01b4d95cf55d32a.automaticDestinations-ms"
2020-02-19 14:51:07···	문서 파일 열기	C:₩8uFF_ORG₩TestLib₩JYTestTool₩x64	ZERO010₩vmadmin	"Source":"f01b4d95cf55d32a.automaticDestinations-ms","Target_time":"$date":"···
2020-02-19 14:51:59···	문서 파일 열기	https://news.naver.com/	ZERO010₩vmadmin	"App":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","Display_text":···
2020-02-19 14:52:09···	문서 파일 열기	https://www.daum.net/	ZERO010₩vmadmin	"App":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","Display_text":···

특장점 – 알려지지 않은 위협 사전 대응

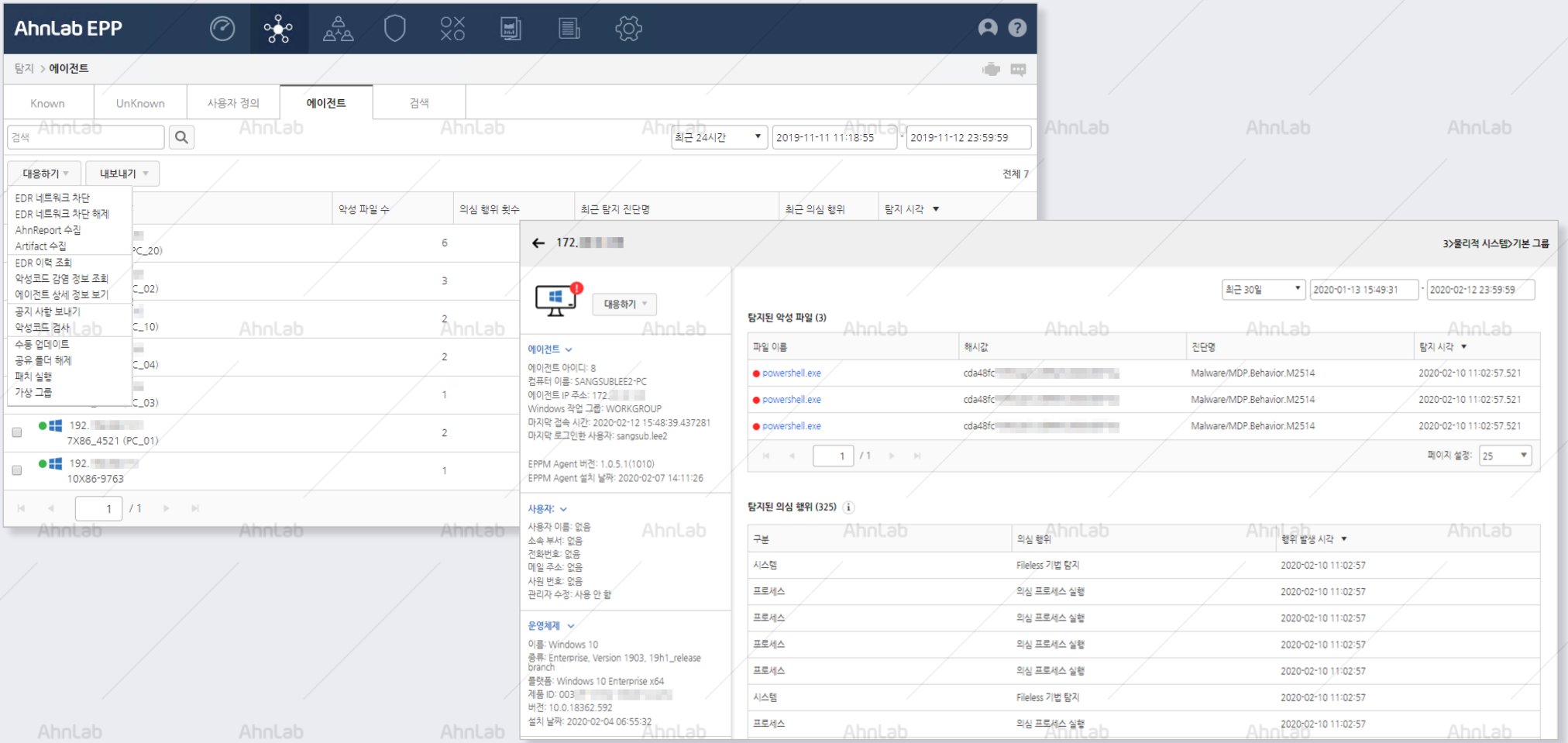
AhnLab EDR은 의심스러운 파일의 행위 정보를 위험도와 행위 유형에 따라 분류하여 상세한 정보를 제공합니다. 이를 토대로 보안 관리자는 해당 파일에 대한 추가 분석 등 능동적인 대응을 할 수 있습니다.

- 대상 파일의 의심 행위 항목 : 랜섬웨어 유사 행위, 인젝션, 네트워크 접속, 시스템 설정 변경, 권한 상승, 파일리스(Fileless)
- 대상 파일 워크플로우 관리: 미확인, 보류, 확인 완료, 예외 처리
- 대상에 대해 시간 및 파일별 그룹핑, 감시행위별 그룹핑 목록, 위험도 제공
- 의심 행위에 대한 머신러닝 기반의 신뢰도 정보 제공

특장점 – 고객 주도의 능동적인 위협 대응 지원 (1/2)

AhnLab EDR의 다양한 관리 기능을 통해 보안 관리자가 필요로 하는 엔드포인트의 정보를 수집 및 검색하고,
그 결과를 토대로 정책을 수립함으로써 보다 능동적으로 위협에 대응할 수 있습니다.

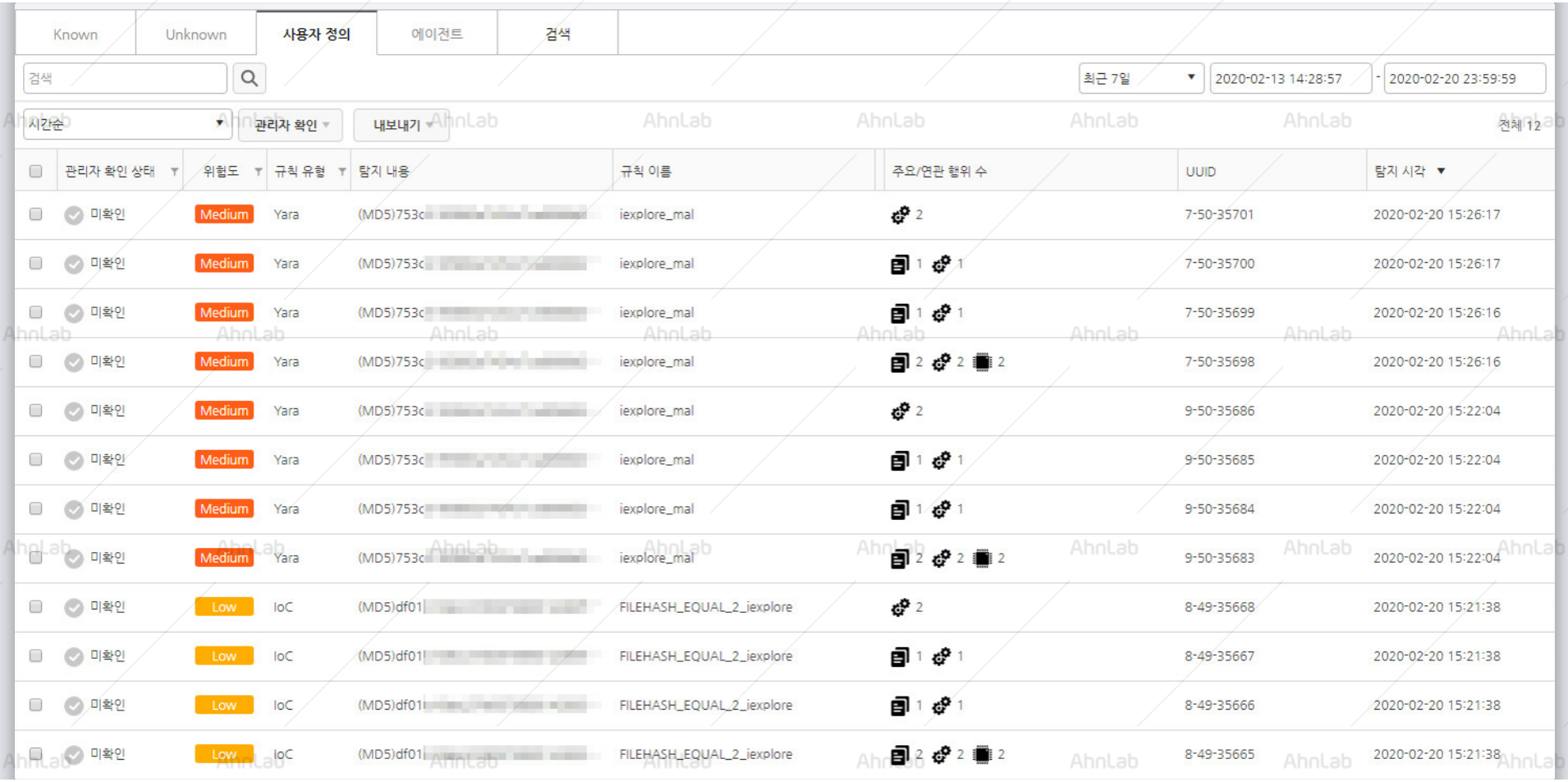
- 에이전트, 파일, 행위 등 정보 단위로 검색 및 조회 가능



특장점 – 고객 주도의 능동적인 위협 대응 지원 (2/2)

AhnLab EDR은 더욱 능동적인 보안 침해 대응을 위해 IOC(Indicator of Compromise, 침해 지표) 및 Yara 기반의 탐지 기능을 제공합니다.

- IOC(Indicator of Compromise, 침해 지표) 및 Yara 기반 탐지 가능

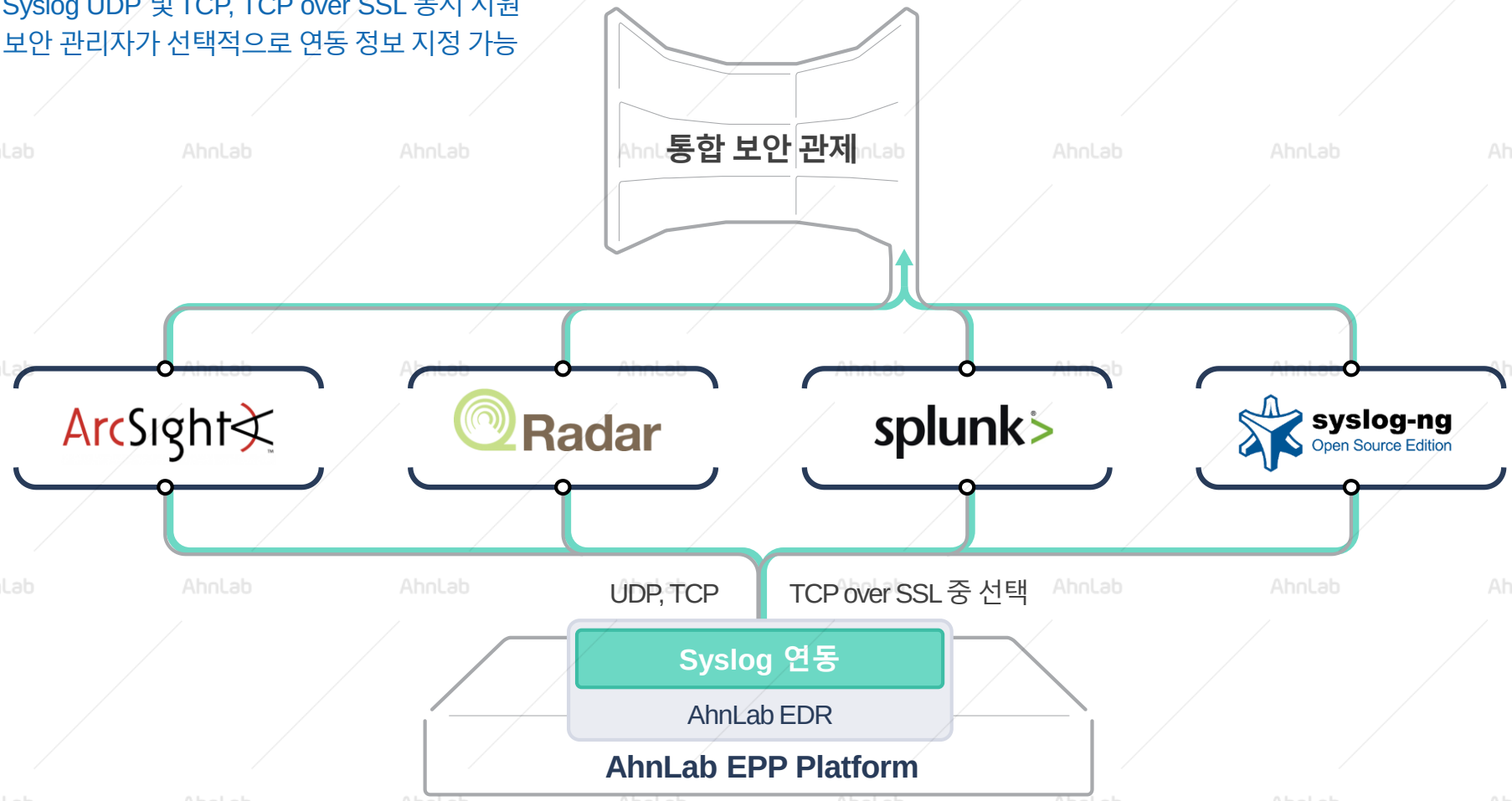


관리자 확인 상태	위험도	규칙 유형	탐지 내용	규칙 이름	주요/연관 행위 수	UUID	탐지 시각
미확인	Medium	Yara	(MD5)753c	iexplore_mal	2	7-50-35701	2020-02-20 15:26:17
미확인	Medium	Yara	(MD5)753c	iexplore_mal	1 1	7-50-35700	2020-02-20 15:26:17
미확인	Medium	Yara	(MD5)753c	iexplore_mal	1 1	7-50-35699	2020-02-20 15:26:16
미확인	Medium	Yara	(MD5)753c	iexplore_mal	2 2 2	7-50-35698	2020-02-20 15:26:16
미확인	Medium	Yara	(MD5)753c	iexplore_mal	2	9-50-35686	2020-02-20 15:22:04
미확인	Medium	Yara	(MD5)753c	iexplore_mal	1 1	9-50-35685	2020-02-20 15:22:04
미확인	Medium	Yara	(MD5)753c	iexplore_mal	1 1	9-50-35684	2020-02-20 15:22:04
미확인	Medium	Yara	(MD5)753c	iexplore_mal	2 2 2	9-50-35683	2020-02-20 15:22:04
미확인	Low	IoC	(MD5)df01	FILEHASH_EQUAL_2_iexplore	2	8-49-35668	2020-02-20 15:21:38
미확인	Low	IoC	(MD5)df01	FILEHASH_EQUAL_2_iexplore	1 1	8-49-35667	2020-02-20 15:21:38
미확인	Low	IoC	(MD5)df01	FILEHASH_EQUAL_2_iexplore	1 1	8-49-35666	2020-02-20 15:21:38
미확인	Low	IoC	(MD5)df01	FILEHASH_EQUAL_2_iexplore	2 2 2	8-49-35665	2020-02-20 15:21:38

특장점 – 외부 시스템 연계를 통한 위협 인텔리전스 강화

AhnLab EPP의 자동화된 Syslog 연동 기능을 통해 AhnLab EDR과 SIEM, ESM 등 다양한 솔루션과 연동함으로써 풍부한 위협 인텔리전스를 확보하고 보안 관제 효과를 극대화할 수 있습니다.

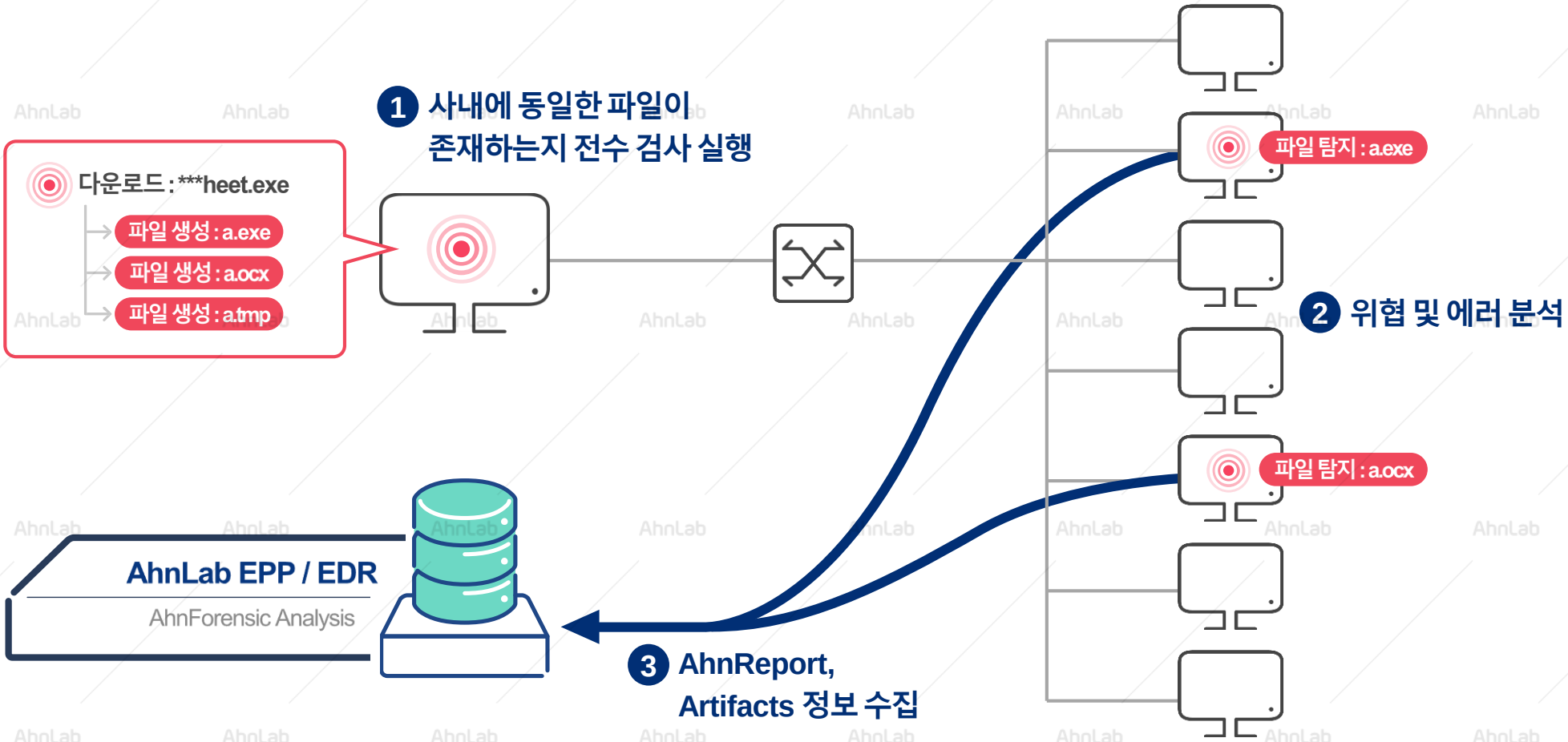
- 원활한 외부 시스템(SIEM, ESM, 통합 로그 등) 연동을 위한 다양한 Syslog 설정 옵션 제공
- Syslog UDP 및 TCP, TCP over SSL 동시 지원
- 보안 관리자가 선택적으로 연동 정보 지정 가능



특장점 – 엔드포인트 위협 정보 자동 수집

엔드포인트의 의심 단말 분석 및 위협 정보 자동 수집 기능을 이용해 악성코드 위협에 더욱 효과적으로 대응할 수 있습니다.

- AhnReport, Artifacts 자동 수집 및 뷰어 제공
- 파일 전수 검사 및 수집 가능
- 수집된 위협 정보를 안랩 프로페셔널 서비스와 연계하여 추가 분석 가능 – 상세 분석 보고서, 대응 가이드 제공



주요 기능

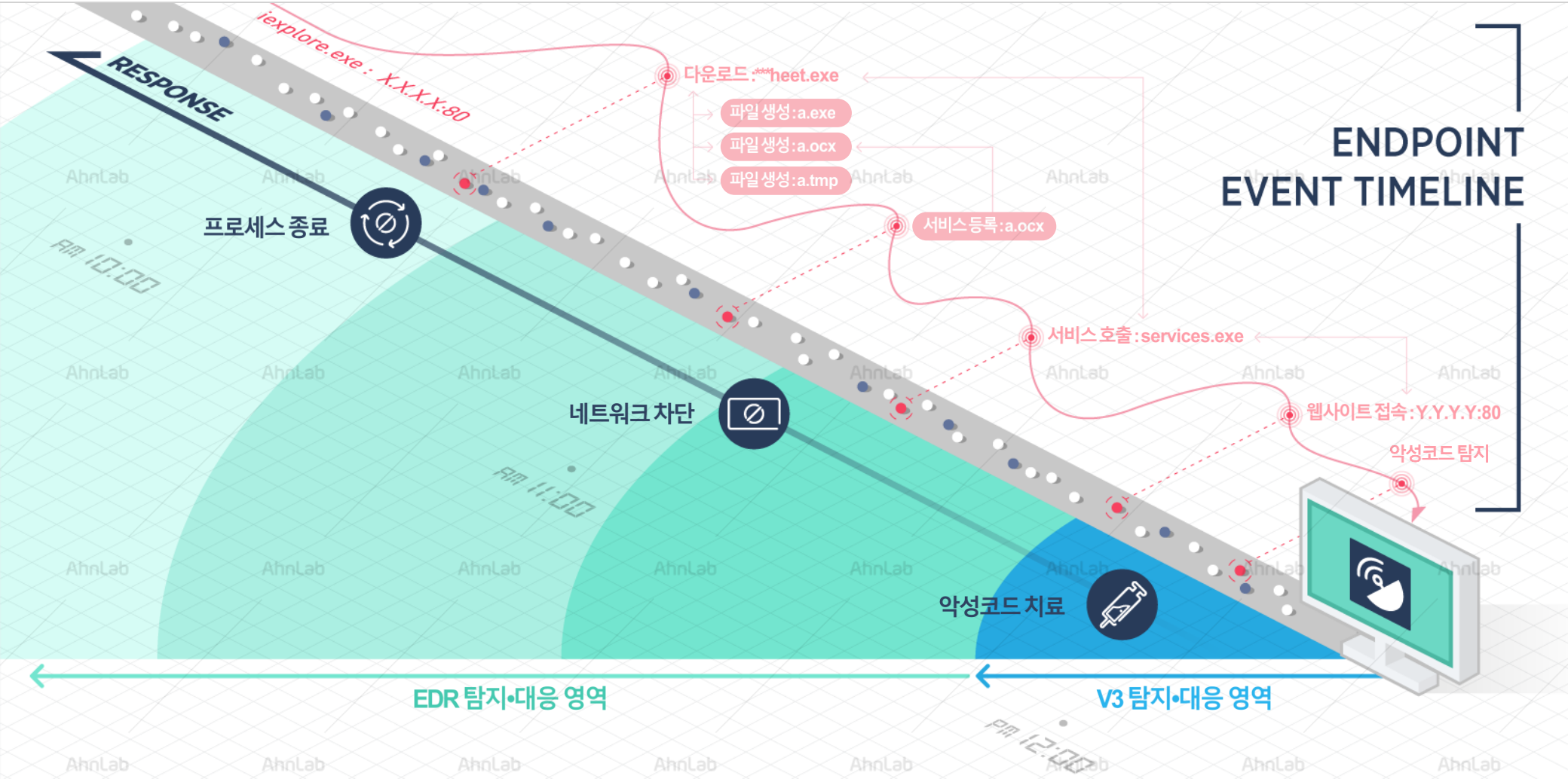
AhnLab EDR은 엔드포인트 위협 탐지 및 대응 솔루션(EDR)의 필수 요소인 탐지, 분석, 치료, 통제 관점의 다양한 기능을 제공합니다.

구분	주요 기능
수집	파일 생성/수정/삭제 정보 수집
	레지스트리 생성/삭제/수정된 정보 수집
	네트워크(IP/URL) 접속 정보 및 프로세스(PID/PPID) 정보 수집
탐지	IoC(STIX), Yara 기반 탐지
	악성코드 탐지 시 Alert 제공
분석	특정 파일에 대한 전수 검사
	다양한 파일 정보 검색 조건 - Hash, 파일 크기/이름/경로, IP/URL, 행위 로그 등
	악성/의심/감시 대상 파일에 대한 정보 제공 - 연계 및 타임라인 다이어그램 제공 - 머신러닝 기반의 신뢰도, 위협 종류, 유입 경로, 주요 행위, 연관 관계, 위험도, MITRE ATT&CK 정보, 인증서 정보, 위협 정보 링크 제공
	연계 규칙을 통해 탐지된 이벤트에 대한 관리자 알림, 메일 발송
	의심 단말 분석을 위한 덤프(Dump) 파일 정보 제공
	의심 단말에 대한 특정 아티팩트(Artifacts) 수집
	특정/의심 프로세스에 대한 온디맨드(on-demand) 검사
대응	의심 단말에 대한 네트워크 격리
	의심 파일 수집 및 검색
	특정 IP/URL에 대한 네트워크 차단
	IoC 정보를 STIX 포맷으로 Input/Output 가능
	위험 그룹을 별도 가상그룹으로 관리 가능
	네트워크 공유 폴더 정보의 수집 및 해제
	관리자 지정 악성코드 검사

구분	주요 기능
관리	관리자 로그인 시 OTP 기능
	원격에서 에이전트 패치 기능
	관리자별 권한 생성 기능
	관리자 행위에 대한 Audit 기능
	공지사항 기능
	서버별 운영 상태 모니터링 - CPU/MEM/DISK/Network 등
	에이전트별 운영 상태 모니터링 - On/Offline, IP주소, OS 정보 등
보고서	사용자 정의 보고서 생성 기능
	CSV, XLS, PDF 등 다양한 포맷으로 출력 가능
	관리자 지정 대시보드 생성 기능
기타	이중화 구성 지원
	Syslog 연동 기능 - SIEM 또는 별도 통합 로그 서버에 이벤트 전송 - UDP/TCP/TCP over SSL 방식 지원
	SNMP 연동 기능
	Open API 정보

도입 효과 1 – 엔드포인트 가시성 기반의 강력한 위협 대응력

AhnLab EDR은 엔드포인트 레벨에서 실제 OS 기반의 행위 정보 탐지 및 분석, 위협 이벤트의 타임라인 분석을 통한 엔드포인트 위협 가시성을 제공해 기업 및 기관의 더 강력한 위협 대응력 확보에 기여합니다.



도입 효과 2 – 보안 운영 편의성 및 비용 효율성

AhnLab EDR은 차세대 엔드포인트 플랫폼 AhnLab EPP를 기반으로 효율적인 엔드포인트 보안 통합 운영 및 관리를 제공합니다.

	일반적인 엔드포인트 보안 운영의 한계	AhnLab EDR 기반의 보안 통합 운영 효과
분석 및 대응	**단위 보안 솔루션의 제한적인 대응 영역** • 개별 엔드포인트 및 네트워크 보안 솔루션의 대응 영역(coverage)의 차이로 유기적인 대응 불가	**위협 유입 경로 분석 및 대응 가능** • 악성코드 유입 경로 분석을 통한 사전•사후 대응력 향상 • 악성코드 감염 시 신속한 분석 및 대응 가능 – 피해 최소화
운영	**EDR 에이전트 설치에 따른 보안 운영 부담 증가** • EDR 에이전트 설치에 따른 관리 부담 증가 • 행위 분석을 위한 별도 커널 드라이버 설치에 따른 충돌 및 대응 이슈 발생 → 보안 운영 및 관리 부담 증가 • 커널 드라이버 추가에 따른 엔드포인트 성능 저하	**기 운영 중인 V3 기반의 운영 안정성** • EDR 라이선스 적용(활성화)만으로 즉각적인 운영 가능 • 별도의 커널 드라이버 설치 없이 V3 기반의 행위 정보 수집 및 분석 (추가 드라이버 설치 불필요) **단일 매니지먼트 기반의 통합 관리** • AhnLab EPP 매니지먼트 콘솔을 통해 백신을 비롯한 EDR 등 다수의 엔드포인트 보안 솔루션에 대한 일원화된 관리 및 운영 편의성 • 연계 정책을 통해 다수의 보안 솔루션 시너지 효과
도입 및 운영 비용	**EDR 도입에 따른 비용 부담 증가** • EDR 에이전트 추가 도입에 따른 시스템(HW, SW) 관리 및 운영 비용 증가	**도입 비용 최소화** • 초기 비용 부담 최소화 - 기존 사용 중인 V3 기반으로 운영 및 구축 가능 • 유연한 서버 구조로 확장에 따른 추가 비용 부담 최소화

03
도입 방식

AhnLab EDR 구축 개념도

AhnLab EPP 기반의 구축 및 운영

유연한 서버 구성을 통한 확장

운영 환경

AhnLab EDR 구축 개념도

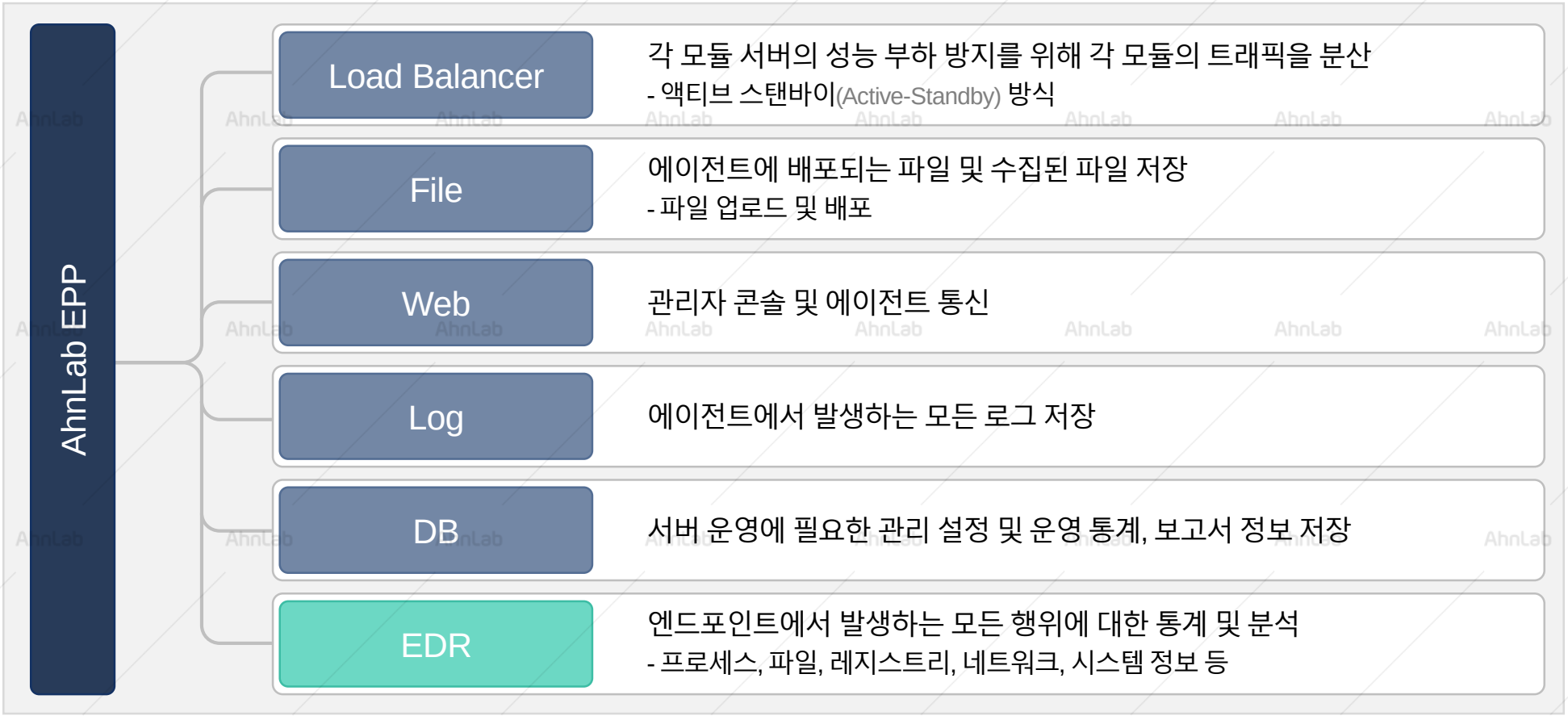
AhnLab EDR은 차세대 엔드포인트 플랫폼 AhnLab EPP를 기반으로 효율적인 엔드포인트 보안 통합 운영 및 관리를 제공합니다.

- 플러그인(plug-in) 방식 - 라이선스 적용만으로 간편하게 구축 및 다수의 보안 제품과 통합 운영 가능

AhnLab EPP 기반의 구축 및 운영

AhnLab EDR은 모듈 방식으로 구성된 차세대 엔드포인트 플랫폼 AhnLab EPP를 통해 간편하게 구축 및 운영할 수 있으며, 필요 시 유연하게 확장할 수 있습니다.

- AhnLab EPP 모듈 구성: 로드 밸런서, 파일, 로그, DB, EDR



유연한 서버 구성을 통한 확장

AhnLab EPP 기반으로 운영하는 AhnLab EDR은 고객사 환경에 따라 시스템을 유연하게 구성할 수 있는 다양한 옵션을 제공합니다.

- 최적화된 초기 구축 비용 및 확장 편의성: 사용자 수, 데이터베이스 사용량 등 고객 환경에 따른 시스템 구성
- 에이전트 확대, DB 증가에 따라 모듈별 서버 확장 가능 – 단, EDR 통계 서버는 1개 고정, 분석 서버는 확장 가능

운영 환경 (권장 하드웨어 사양)

AhnLab EDR은 차세대 엔드포인트 보안 플랫폼 AhnLab EPP를 기반으로 효율적인 통합 관리를 제공합니다.

- AhnLab EDR 운영 환경

구분	관리 콘솔(AhnLab EPP Management) 운영환경	AhnLab EDR 에이전트 운영체제
상세버전	Internet Explorer 11 이상 Google Chrome 최신 버전 - 지원 언어: 한국어, 영어, 중국어(간체), 일본어	Windows XP SP3 / Vista / 7 / 8(8.1) / 10 Windows Server 2003 / 2008 / 2012(R2 포함) / 2016 / 2019 * 64비트 호환 모드 지원 - 지원 언어: 한국어, 영어, 중국어(간체), 일본어

- AhnLab EDR 서버 사양

구분		관리 에이전트 수						
		최대 300개	최대 1,000개	최대 5,000개	최대 10,000개	최대 15,000개	최대 30,000개	최대 50,000개
CPU		4	4	8	16	16	16	16
메모리		32G	64G	64G	128G	256G	384G	512G
HDD	기본	2TB	2TB	4TB	4TB	8TB	8TB	16TB

* 의심 행위 분석(EDR) 로그 데이터 저장을 위한 Raid 구성은 검색 속도 등을 고려하여 Raid 1+0 권장

- AhnLab EPP 권장 하드웨어 사양

구분		관리 에이전트 수						
		최대 300개	최대 1,000개	최대 5,000개	최대 10,000개	최대 15,000개	최대 30,000개	최대 50,000개
CPU		4	4	8	16	16	16	16
메모리		32G	64G	64G	128G	192G	256G	384G
HDD	기본	500G	500G	1TB	1TB	1TB	1TB	2TB
	APM 사용 시	1TB	1TB	1TB	1TB	1TB	1TB	1TB

* APM 사용 시: HDD 2개 이상 물리적 분리 구성 필수, 에이전트와 서버간 네트워크 대역폭 최소 32mbps 이상 권장

※ 별첨

EDR 정의 및 목적

EDR 정의 및 목적

※ 별첨

EDR(Endpoint Detection & Response) 기술은 엔드포인트단에서 지속적이며 연속적인 모니터링 및 위협 정보 수집, 분석을 수행함으로써 위협의 잠복 기간(Dwell Time)을 최소화하여 잠재적인 피해를 방지합니다.

침해 사고 예방 또는 단순 대응이 아닌

엔드포인트 레벨의 지속적인 모니터링 및 위협 정보 수집을 통한 대응력 강화

위협 잠복 기간 최소화

기존 솔루션 연계

지속적인 모니터링

엔드포인트 가시성

EDR(Endpoint Detection & Response) 정의 및 영역

EDR이란 엔드포인트 레벨에서 지속적인 모니터링과 대응을 제공하는 보안 솔루션으로,
▲보안 침해 탐지(Detect security incident) ▲엔드포인트에서의 보안 침해 억제(Contain the incident at the endpoint)
▲보안 침해 조사(Investigate security incident) ▲치료를 통한 감염 이전 상태로의 회복(Remediate endpoint to a preinfection state) 등
4가지 기능을 제공해야 한다.

EDR은 사전 또는 실행 단계에서 위협을 자동으로 차단하는 것이 아니라 적절한 엔드포인트 위협 가시성을 제공해
지능형 위협을 발견하고 조사 및 대응하는데 기여한다.

즉, EDR은 엔드포인트 보안의 보완 도구(tool)로서, 안티바이러스 등 기존 보안 제품과 연계해야 효과적인 대응이 가능하다.

*출처: Gartner

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

AhnLab EDR

AhnLab