# AhnLab EDR

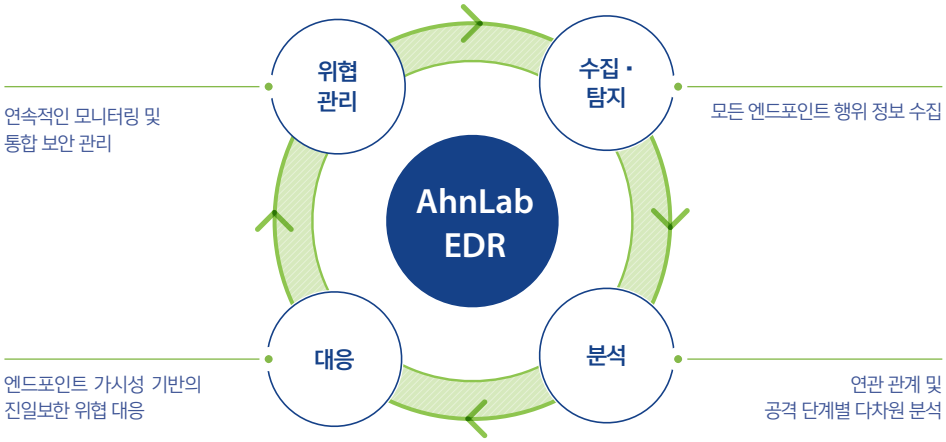
## 더 쉬운 적용, 더 강력한 위협 대응

AhnLab EDR은 엔드포인트 보안의 최강자 안랩이 만든
엔드포인트 위협 탐지 · 대응 솔루션입니다.

가시성 탐지 대응 편의성

### 제품 개요

**AhnLab EDR**은 엔드포인트 영역에 대한 지속적인 모니터링을 통해 진일보한 위협 관리를 제공하는 차세대 **엔드포인트 위협 탐지 및 대응**(Endpoint Detection & Response) 솔루션입니다. 최고의 엔드포인트 보안 기업의 30년 악성코드 분석 기술이 응축된 AhnLab EDR은 엔드포인트 위협 가시성 기반의 더욱 강력한 위협 대응력 확보에 기여합니다.




### 왜 EDR인가

위협 정보 수집 · 분석 및 대응 관점의 변화가 반영된 진일보한 보안 기술인 EDR(Endpoint Detection & Response)은 엔드포인트 영역 전반에 대한 지속적인 모니터링을 통해 위협 가시성을 제공하며 다양한 보안 솔루션과의 연계를 기반으로 더욱 강력한 위협 대응을 실현합니다.

## AhnLab EDR, 무엇이 다른가

안랩의 독자적인 분석 기술과 마이터 어택(MITRE ATT&CK) 프레임워크가 적용된 AhnLab EDR은 차세대 엔드포인트 보안 플랫폼 AhnLab EPP를 기반으로 다양한 보안 기능 연계를 통해 확장된 엔드포인트 위협 가시성과 함께 실질적인 위협 대응을 제공합니다.

### 위협 탐지 고도화 및 정밀한 위협 가시성을 통한 보안 사각지대 해소

- 독자적인 MDP 행위 분석 엔진(V3 연동)을 통해 모든 엔드포인트 행위 정보 수집
- MITRE ATT&CK 프레임워크 기반의 탐지 기법으로 알려지지 않은 행위 탐지
- 위협 이벤트 타임라인 분석으로 공격 흐름 전반에 대한 이해 제공
- 위협 유형, 유입 경로, 행위, 연관 관계, 위험도, MITRE ATT&CK 정보, 인증서 정보, 위협 정보 링크, 머신러닝 기반의 신뢰도 등 상세한 위협 정보 및 대응 조치 제공

### 차세대 엔드포인트 보안 플랫폼 기반의 강력한 위협 대응

- AhnLab EPP를 기반으로 다양한 엔드포인트 보안 솔루션의 연계 정책 설정 · 조치 가능
- 제3자 솔루션과의 유연한 연동을 통한 위협 인텔리전스 강화
- 실시간 엔드포인트 파일 수집 및 검색, AhnReport/Artifact 수집
- 온디맨드(on-demand) 검사를 통한 의심 프로세스 검사

### 도입 및 운영 부담 최소화로 업무 효율성 극대화

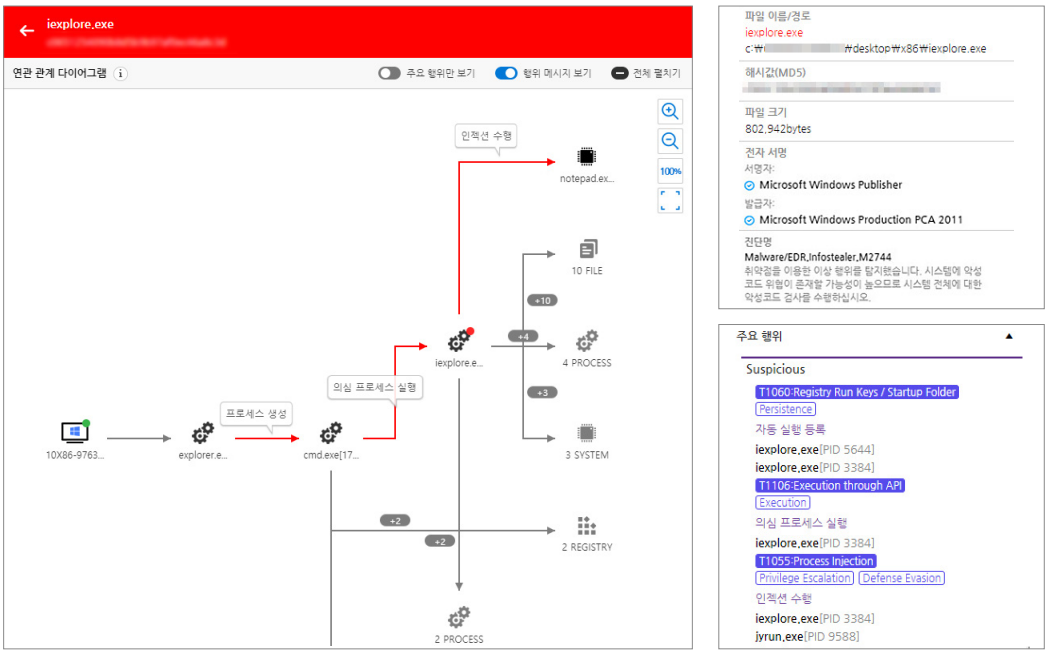
- 라이선스 적용만으로 솔루션 구축 완료 (*AhnLab EPP Management 및 V3 이용 시)
- 사용자 시스템 리소스 부담 최소화 – 단일 에이전트, 단일 커널 드라이브 사용
- AhnLab EPP 기반의 효율적인 보안 운영으로 보안 담당자의 업무 생산성 향상

### 최고의 엔드포인트 보안 기업의 검증된 위협 대응 역량

- 다수의 글로벌 인증 기관을 통해 인정받은 악성코드 탐지 성능
- 30년간 축적된 악성코드 분석 기술력
- 다양한 엔드포인트 보안 솔루션 구축 및 서비스 운영을 통한 위협 대응 노하우

## 엔드포인트 위협 가시성

AhnLab EDR은 독자적인 행위 분석 엔진인 MDP 엔진을 통해 엔드포인트의 실제 OS 상에서 모든 행위 정보를 수집 및 분석합니다. 이벤트 타임라인 분석과 함께 마이터 어택(MITRE ATT&CK) 프레임워크 기반의 고도화된 탐지 기법을 통해 위협의 종류, 유입 경로, 공격 대상(target), 위험도, 주요 행위, 신뢰도 등에 대한 상세한 정보를 제공합니다. 타임라인 기반 에이전트 이벤트 정보와 직관적인 연관 관계 다이어그램을 통해 위협에 대한 인사이트를 제공하며 공격 단계별 최적화된 대응을 제공합니다.



## 더 강력한 위협 대응

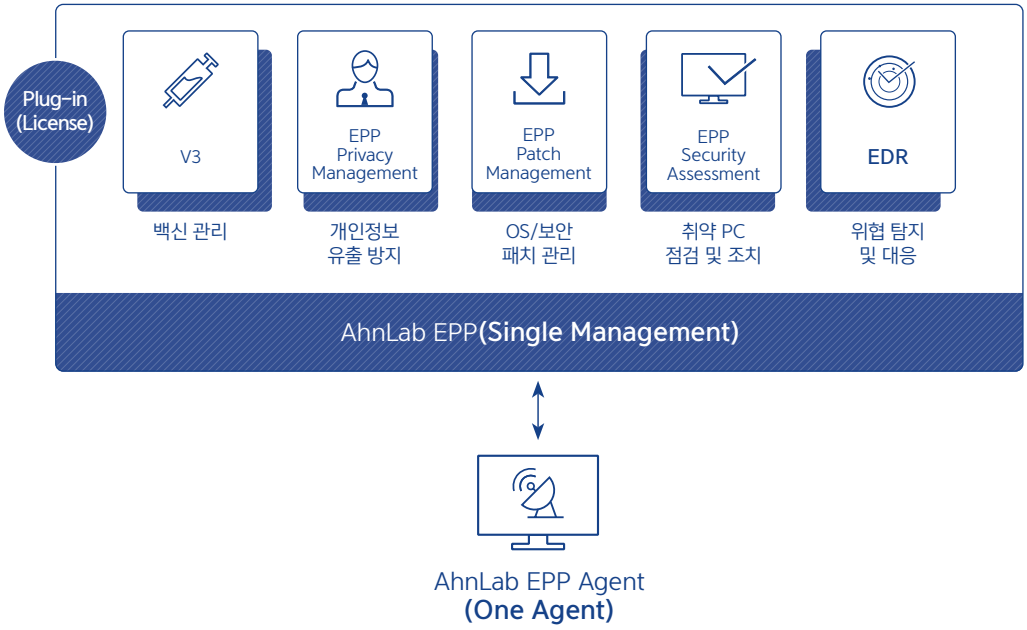
AhnLab EDR의 다양한 관리 기능을 통해 기업 및 기관의 환경에 따라 주도적이며 능동적인 위협 대응이 가능합니다. 또한 차세대 엔드포인트 보안 플랫폼인 AhnLab EPP를 기반으로 다수의 엔드포인트 보안 솔루션과의 유기적인 연계를 통해 더욱 강력하고 효율적인 보안 운영 및 위협 대응을 제공합니다.

### 고객 주도적 · 능동적 위협 대응

- 프로세스, 파일, 레지스트리, 네트워크, 시스템 등에 대한 행위 정보 수집
- 에이전트, 파일, 행위 등 정보 단위로 상세한 조건별 검색 및 조회 가능
- IOC(Indicator of Compromise, 보안 침해 지표) 및 Yara를 통한 탐지 지원
- 위협 탐지 시 즉각적인 대응 가능(네트워크 차단, 프로세스 종료, 파일 수집/검색/격리/복원 등)
- 사용자(보안 관리자) 정의 보고서 생성 – CSV, XLS, PDF 등 다양한 포맷 제공
- 온디맨드(on-demand) 검사를 통한 의심 프로세스 검사
- 랜섬웨어, 인젝션, 네트워크 연결, C&C 접속, 시스템 설정 변경, 권한 상승, 파일리스, 정보 탈취 등 주요 악성 유사 행위별 감시 파일 정보 제공
- 알려진 파일 및 알려지지 않은 파일의 워크플로우(workflow) 관리: 미확인, 보류, 확인 완료, 예외 처리 설정 가능

### 플랫폼 기반의 통합 보안 운영 및 관리

- 차세대 엔드포인트 보안 플랫폼 AhnLab EPP 기반의 강력한 위협 대응 체계
  – 단일 매니지먼트, 단일 에이전트 기반의 효율적인 보안 운영 및 관리
- 유연한 연계 정책 설정을 통해 유기적인 위협 대응 및 조치 가능
- 확장된 엔드포인트 가시성을 기반으로 위협 탐지 및 대응 시간 최소화
- AhnLab EPP Management의 웹 기반 관리 콘솔을 통한 편리한 모니터링 및 관리 가능




▲ AhnLab EPP 기반의 강력한 엔드포인트 위협 대응 체계

### 풍부한 위협 인텔리전스를 통한 대응력 향상

- 제3자 솔루션과의 유연한 연동을 통해 풍부한 위협 인텔리전스(Threat Intelligence) 확보
- SIEM, ESM, 통합 로그 등과 Syslog 연동 가능
  – 콘솔을 통한 손쉬운 연동 설정
  – 다양한 프로토콜 제공(UDP/TCP/TCP over SSL 등)

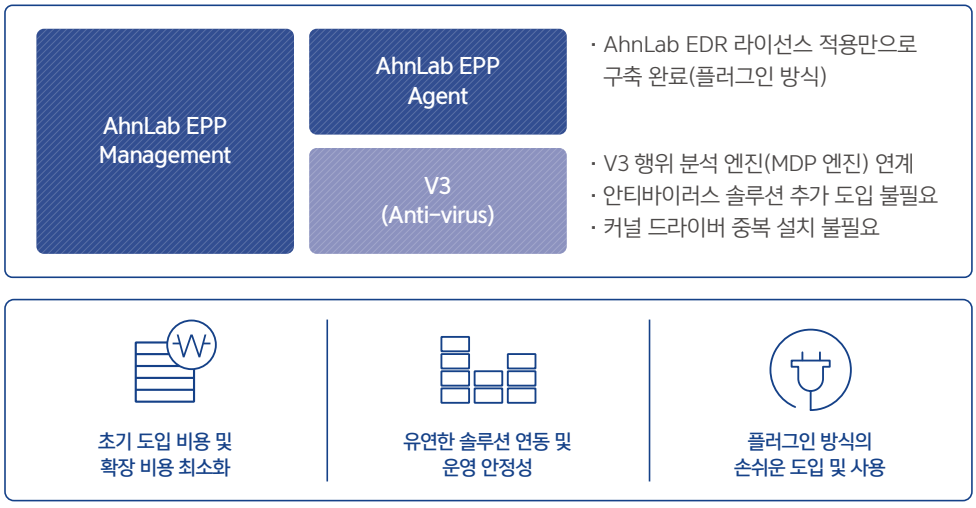
### 전문 서비스 연계를 통한 사후 대응

- 모든 행위 정보 수집 및 저장 – 이벤트와 관련된 전반적인 위협 정보 상시 확인 가능
- 안랩의 전문가 서비스(AhnLab Professional Service) 연계를 통한 사후 위협 분석 및 침해사고 대응

## 손쉬운 도입 · 운영

AhnLab EDR은 차세대 엔드포인트 보안 플랫폼 AhnLab EPP의 매니지먼트 콘솔과 에이전트를 기반으로 라이선스만 추가하여 손쉽게 구축, 즉각적인 운영이 가능합니다. (*AhnLab EPP Management 및 V3 이용 시)

또한 V3의 행위 분석 엔진 연계를 통해 엔드포인트의 행위 정보 모니터링을 수행하기 때문에 커널 드라이버 추가 설치가 필요하지 않아 시스템의 성능 부담이 적습니다.




## 사용 환경

AhnLab EDR은 엔드포인트 보안 플랫폼 AhnLab EPP Management를 기반으로 효율적인 통합 관리를 제공합니다.

### AhnLab EDR 에이전트 설치 환경

| 구분 | 상세 버전 |
|---|---|
| 운영체제 | Windows XP SP3 / Vista / 7 / 8(8.1) / 10<br>Windows Server 2003 SP1(R2 포함)<br>Windows Server 2008(R2 포함) / 2012(R2 포함)<br>Windows Server 2016 / 2019<br>* 상기 OS의 64비트 호환 모드 지원 |

### 관리 콘솔(AhnLab EPP Management) 운영 환경

| 구분 | 상세 버전 |
|---|---|
| 웹 브라우저 | Internet Explorer 11 이상<br>Chrome 최신 버전 |

AhnLab
경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901