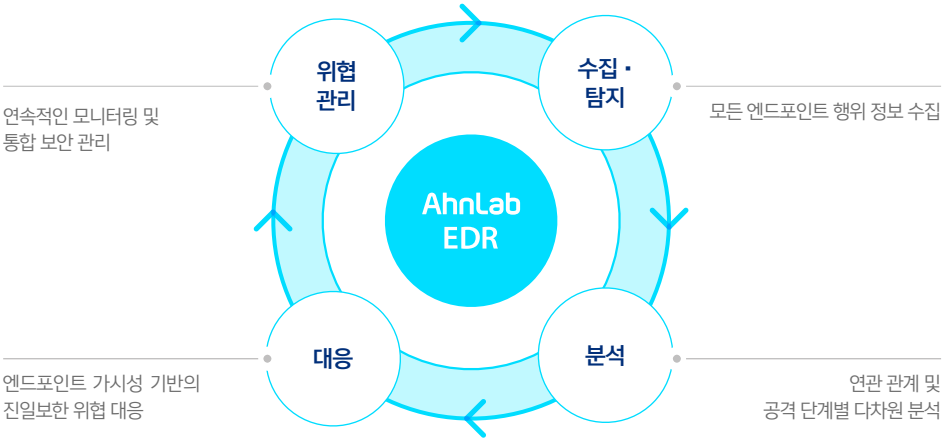
AhnLab EDR

정교한 탐지, 전문적인 분석 & 대응, 능동적인 사냥

AhnLab EDR은 MITRE ATT&CK 평가를 통해 검증된 탐지, 분석, 대응 역량을 기반으로
위협을 능동적으로 추적하여 기업의 강력한 보안 체계 수립에 기여합니다.

제품 개요

AhnLab EDR은 국내 유일의 행위 기반 분석 엔진을 기반으로 엔드포인트 영역에 대해 강력한 위협 모니터링과 분석, 대응 역량을 제공하는 차세대 엔드포인트 위협 탐지 및 대응 솔루션입니다. MITRE ATT&CK 평가에서 우수한 성적을 거둔 AhnLab EDR은 MDR(Managed Detection & Response) 서비스와 결합해 위협 탐지 및 대응 프로세스 전반에 전문성을 강화합니다.



AhnLab EDR의 필요성

엔드포인트를 노린 공격은 점점 고도화되고 있습니다. 날마다 수많은 신·변종 악성코드가 출현하고 있어 모든 위협을 사전 차단하는 것은 거의 불가능합니다. 따라서 상시 감시와 신속한 침해사고 인지를 통해 위협을 최소화하는 보안 체계를 수립해야 합니다. AhnLab EDR은 행위 정보를 탐지·분석해 폭넓은 엔드포인트 가시성을 제공하고, 간편한 구축과 운영으로 진일보한 위협 탐지 & 대응을 구현합니다. 또한, 위협을 능동적으로 추적하기 때문에 기업이 사전 예방 및 재발 방지 체계를 구축하는 데 유용합니다.

행위 정보 탐지·분석을 통한 엔드포인트 가시성 확보 및 대응	AhnLab EDR	간편한 구축, 손쉬운 운영 더 강력한 위협 대응
언제 조직 내부로 침입한 파일인가?		파일이 유입된 이후 실행된 적이 있는가?
어떻게 악성코드에 감염됐는가?		동일한 파일이 얼마나 많은 시스템에 존재하는가?
악성코드와 유사한 파일 구조를 갖고 있는가?		어떤 모듈(들)과 관계 있는가?
		어떤 행위를 했는가?

특장점

운영 편의성

AhnLab EDR은 안랩의 전문 기술력과 전문성이 응축된 전용 콘솔 'EDR Analyzer'를 지원합니다. EDR Analyzer는 탐지 및 분석, 대응 관점에서 사용자가 위협을 정확하게 인식하고 조건을 설정하도록 구성됐습니다. AhnLab EDR은 의심스러운 행위에 관한 유형별 정보를 상시 수집해 EDR Analyzer 중앙 서버에 저장하며, 고객사의 환경에 따라 행위 수집의 레벨을 다르게 조정함으로써 관리를 최적화하고 용량 부담을 줄입니다.

▲ AhnLab EDR Analyzer 대시보드

정교한 위협 탐지와 분류

AhnLab EDR은 행위 기반 엔진을 통해 자체적으로 국내외 공격 그룹을 분석하고, 탐지 패턴과 규칙을 만들어 위협을 정교하게 탐지합니다. 또한, MITRE ATT&CK 프레임워크에 따라 위협을 16가지 행위 카테고리로 분류해 사용자가 위협을 직관적으로 식별하도록 합니다. 이 외에 머신러닝 기술을 활용해 위협별 위험도와 악성 위험 확률에 관한 정보도 제공합니다.

전문적인 분석 및 대응

AhnLab EDR은 탐지한 위협에 대해 MITRE ATT&CK 프레임워크 기반 위협 정보와 유입 경로, 주요 행위, 연관 관계, 위험도, 위협 정보 링크 등에 대해 상세한 분석 내용을 제공합니다. 분석 정보를 ▲다이어그램 ▲타임라인 ▲프로세스 트리 형태로 표시해 사용자가 전반적인 공격 흐름을 쉽게 파악하도록 합니다. 주요 행위에 대한 온디맨드(On-Demand) 검사와 AhnLab TIP 및 AhnLab MDS 연동을 통한 추가 분석도 가능합니다.

견고함을 더하는 기본 서비스

AhnLab EDR이 탐지한 이벤트 중 위험도가 높은 이벤트에 대해 1/2차 보고서와 통계 기반 보고서를 제공하여, 고객이 EDR을 보다 더 효과적으로 활용할 수 있도록 합니다. 이와 더불어, 고객과의 사전 협의 하에 위협 대응도 수행합니다.

*해당 서비스는 AhnLab EDR 도입 시 기본적으로 제공되지만, EDR 탐지 로그를 외부로 전송하지 못하는 경우 지원하지 않습니다.

MITRE ATT&CK 평가 검증

AhnLab EDR은 가장 최근에 진행된 MITRE ATT&CK Evaluation Round 4에서, 공격 그룹 '위자드 스파이더(Wizard Spider)'와 '샌드웜(Sandworm)'이 사용하는 최신 기법을 모의 수행한 90개 공격 스탭(Step)에서 83개를 탐지해 92%의 탐지율을 기록하며, 고도화된 위협에 대한 탁월한 탐지 역량을 입증했습니다.

주요기능

AhnLab EDR은 탐지 유형별로 위협을 분류해 위협 인지부터 분석, 대응까지 신속한 워크플로우를 지원합니다. 또한, 다양한 솔루션과 연동해 대응 역량을 극대화하며, AhnLab EPP 제품 간 연계 규칙 설정을 통해 기업 환경에 최적화된 엔드포인트 보안 운영이 가능합니다.

고도화된 위협 탐지 · 분류 · 분석 · 대응

- 모든 행위 정보 수집 및 저장 – 이벤트와 관련된 전반적인 위협 정보 상시 확인 가능
  – 프로세스, 파일, 레지스트리, 네트워크, 시스템 등에 대한 행위 정보 수집
- 에이전트, 파일, 행위 등 정보 단위로 상세한 조건별 검색 및 조회 가능
- 사용자 정의 규칙(IoC, Yara, 정적/동적 행위규칙) 설정을 통한 탐지 및 자동대응 지원
- 위협 탐지 시 즉각적인 대응 가능(네트워크 차단, 프로세스 종료, 롤백, 파일 수집/검색/삭제/복원 등)
- 사용자 설정을 통한 자동 대응 (사용자 정의 규칙, 연계 규칙, Blacklist Hash 기반 프로세스 사전 차단)
- 사용자(보안 관리자) 정의 보고서 생성 – CSV, XLS, PDF 등 다양한 포맷 제공
- 온디맨드(on-demand) 검사를 통한 주요 행위 및 V3 진단 악성코드 행위 분석
- MITRE ATT&CK Tactics 기반 16개 위협 카테고리 분류
- 랜섬웨어, 인젝션, 네트워크 연결, C&C 접속, 시스템 설정 변경, 권한 상승, 파일리스, 정보 탈취 등 주요 악성 유사 행위별 감시 파일 정보 제공
- 침해대응 분석을 위한 추가 자료(AhnReport/Artifacts/윈도우 이벤트 로그) 수집 가능

플랫폼 기반 통합 보안 운영 및 관리

- 차세대 엔드포인트 보안 플랫폼 AhnLab EPP 기반 강력한 위협 대응 체계 구성
  – 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

유연한 연동을 통한 위협 인텔리전스 확보 및 대응력 향상

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

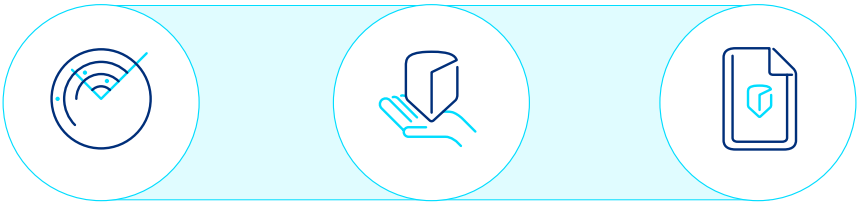
EDR Premium

EDR Premium은 AhnLab EDR과 함께 전문적인 위협 탐지 & 대응 역량을 제공하는 'MDR(Managed Detection & Response)' 서비스가 결합된 상품입니다. EDR Premium을 사용할 경우, 안랩 전문가가 알려진 위협이나 의심 행위를 모니터링, 분석 및 판단하여 능동적으로 대응합니다.

EDR Premium의 배경에는 오랜 기간 축적해온 안랩의 독보적인 위협 대응 역량이 자리하고 있습니다. EDR Premium은 고객 엔드포인트 환경에서 발생하는 위협에 대한 티켓(Ticket)을 발생시키고, 평판 정보, 악성코드 행위 정보 등을 활용해 안랩 위협 대응 프로세스에 기반하여 체계적으로 처리합니다.

이 밖에도, 안랩은 침해사고 분석 서비스, 악성코드 전문가 분석 서비스, 의심 시스템 진단 서비스 등 다양한 프로페셔널 서비스를 EDR Premium과 연계해 보안 위협 분석 및 대응 능력 제고를 위한 다양한 옵션을 제공합니다.

*EDR Premium은 유상 서비스이며, 서비스 비용 및 구체적인 내용은 별도로 문의 부탁드립니다.



위협 탐지
폭 넓은 위협에 대한
실시간 탐지

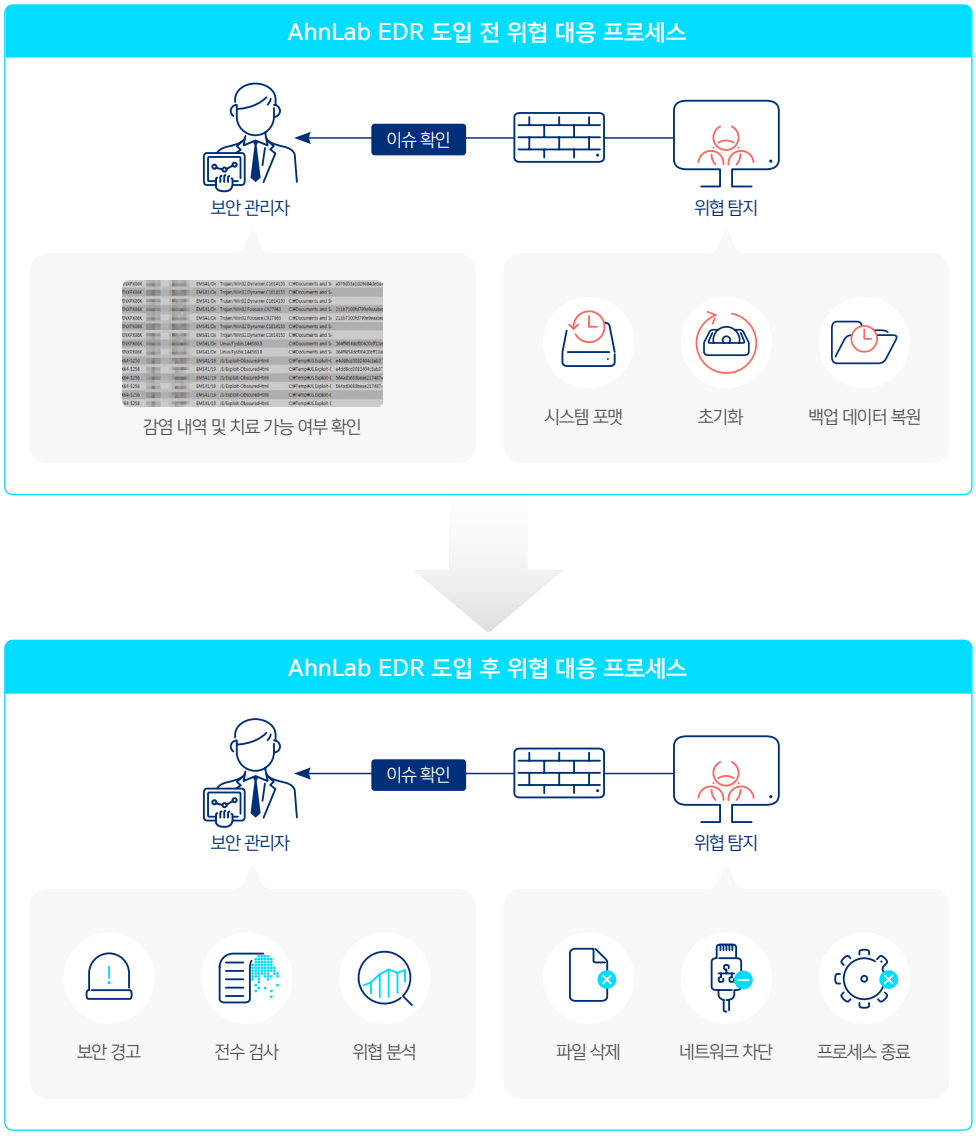
전문가 분석 & 대응
능동적인 분석 & 대응을 통한
위협 완화 및 복구

보고서
위협 탐지 & 대응 프로세스
강화를 위한 보고서 제공

도입효과

AhnLab EDR을 사용하지 않는 경우, 악성코드 감염 이력이 확인되면 시스템을 포맷하거나 초기화하고, 백업된 데이터를 복원해 업무를 재개합니다. 백신 관리 서버에 사용자 PC의 악성코드 감염 이력이 존재하지만 정확한 경로는 확인할 수 없습니다. 이로 인해 위협 대응이 일회성에 그치고, 재발 방지 대책을 수립하는 데 한계가 있습니다.

하지만 AhnLab EDR을 도입하면 종합적인 분석을 통해 원인 파악과 적절한 대응, 재발 방지 프로세스를 수립할 수 있습니다. 침해사고가 발생하면 관리자가 경고 알림을 수신한 후, 사전 정의된 규칙을 기반으로 위협 분석, 전사적인 검사를 수행합니다. 이를 통해 악성 의심파일 수집, 프로세스 종료, 네트워크 차단 등의 올바른 조치를 취할 수 있습니다. 또한, 취약점 및 감염 이력 확인을 통해 선제적인 사전 대응뿐만 아니라 사후 관리도 가능합니다.



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

AhnLab