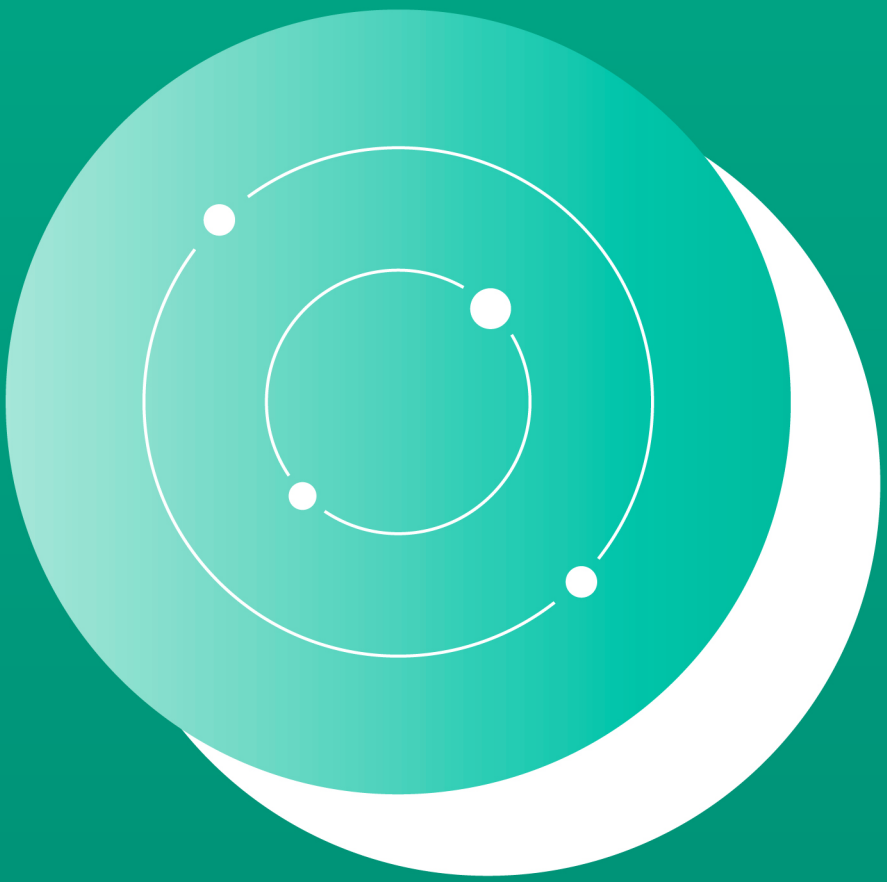
Endpoint Security

알약 EDR

엔드포인트 위협 대응 솔루션



ESTsecurity

국내 EDR 시장 본격화!

EDR 솔루션이 기업/기관의 새로운 보안 전략으로 떠오른 이유는 무엇일까요?

시그니처 기반의 기존 엔드포인트 보안 솔루션을 보완하기 위해 엔드포인트 내 의심 위협을 탐지하는 EDR 솔루션이 해결책으로 부상했습니다. 하지만 오히려 수많은 노이즈로 인해 관리 업무가 증가하고, 위협의 식별이 되지않아 제대로 된 대응이 어렵다는 결정적인 문제 때문에, 많은 기업/기관이 도입에 어려움을 겪어왔습니다.

이 같은 한계는 이제 위협 인텔리전스를 통해 해결될 수 있습니다. 위협 인텔리전스는 탐지된 위협의 숙주 제거와, 새롭게 발견된 위협의 정체 파악 및 이를 통한 자동화된 대응을 가능케 합니다.

이에 위협 인텔리전스와 결합한 형태의 EDR(Endpoint Detection and Response)이 차세대 엔드포인트 보안 위협 대응 솔루션으로 주목받고 있습니다.

차세대 엔드포인트 보안을 위한 3단계

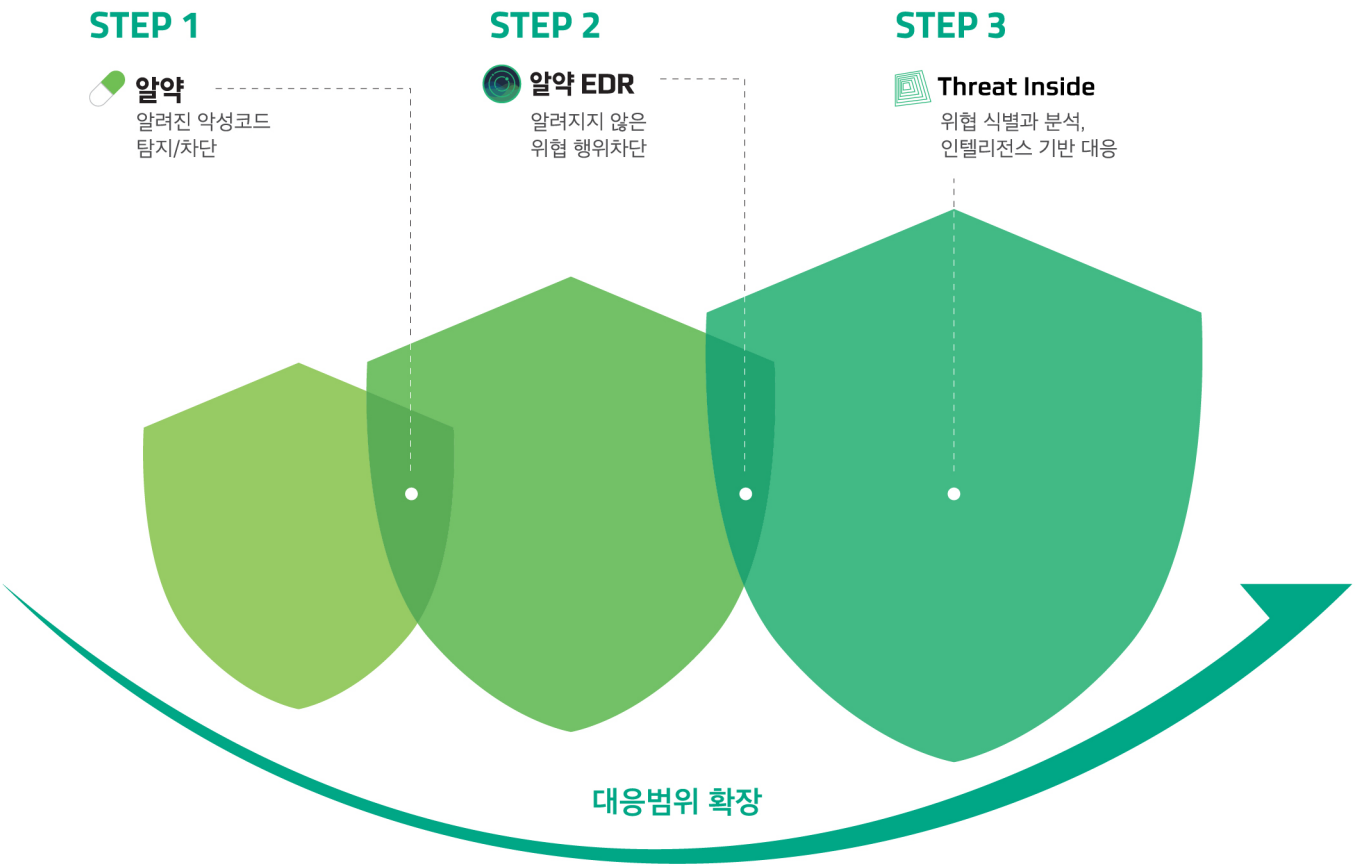
알약 EDR은 백신 제품인 알약과 악성코드 위협 인텔리전스 솔루션인 Threat Inside와 결합하여
이상적인 차세대 엔드포인트 보안 체계를 완성합니다.

알약 EDR은 알려진 공격의 실시간 감시/탐지부터, 알려지지 않은 의심 행위의 선제적인 차단이 가능합니다.
또한 이스트시큐리티 1,600만 실사용자 데이터와 10년 이상의 엔드포인트 보안 노하우를 집약한
위협 인텔리전스 솔루션과 완벽히 연동되어 정확한 위협 식별 정보와 상세한 분석 리포트까지 제공하며,
대응 범위의 확장과 즉각적인 조치가 가능합니다.

1단계 알약을 통한 알려진 악성코드 위협 탐지/차단

2단계 알약 EDR을 통한 알려지지 않은 위협 행위차단

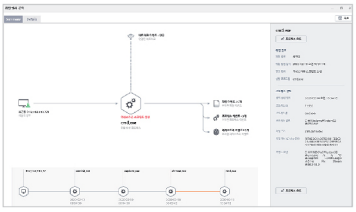
3단계 Threat Inside를 통한 위협 식별과 분석, 인텔리전스 기반의 대응 정책 설정



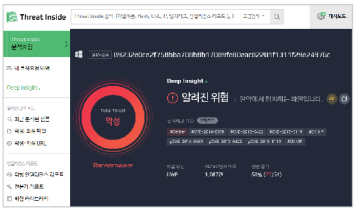
기업 엔드포인트 보안의 해답, 알약 EDR이 제시합니다.

알약 EDR의 주요 기능

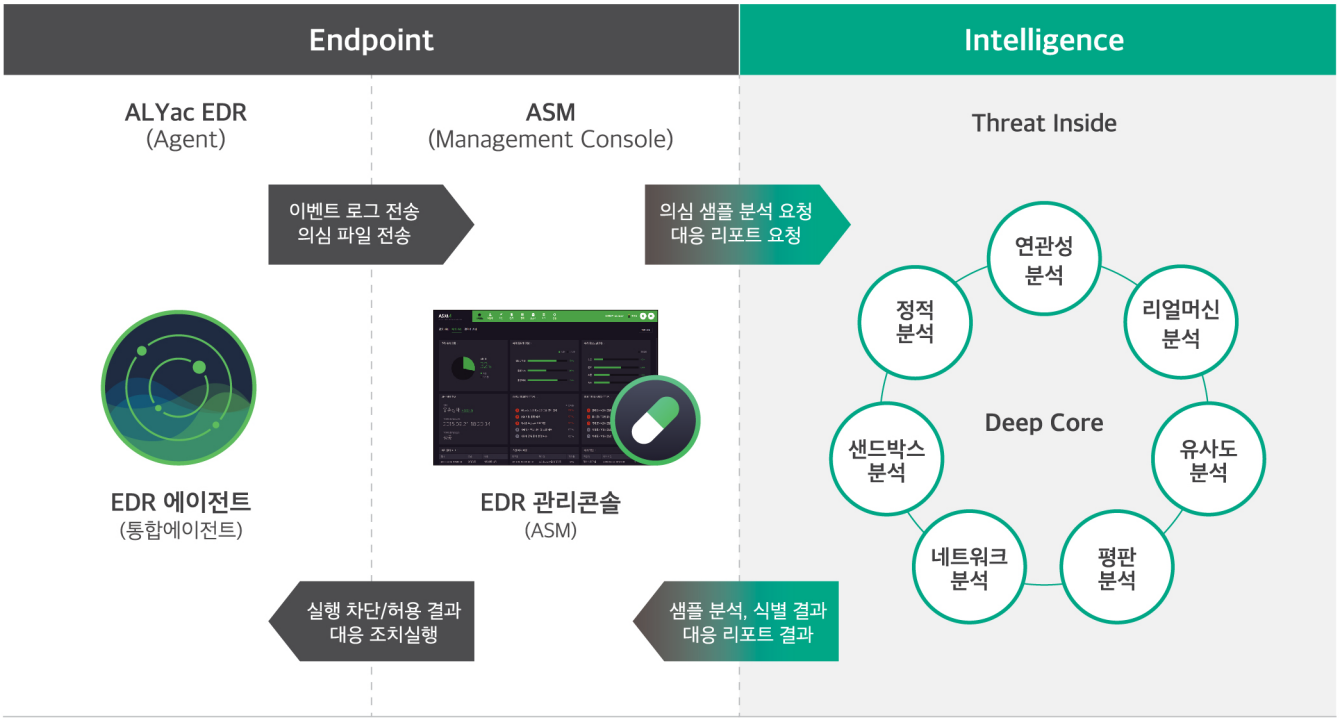
엔드포인트 내의 위협 정보를 선별/모니터링하며, 알려진 위협 및 의심되는 위협 프로세스를 탐지/차단합니다.



직관적인 위협 흐름도를 제공하여, 위협의 종류, 행위, 공격 단계에 대한 신속한 파악과 즉각적인 보안 정책 적용을 도와 시스템을 보호합니다.



자사 위협 인텔리전스 솔루션 Threat Inside와 완벽히 연동되어, 신/변종 위협의 식별 정보와 상세 인텔리전스 분석 정보를 제공합니다.



고도화된 알약 EDR의 특장점

가시성을 극대화한 위협 흐름도

- 악성/의심 프로세스와 연관된 요약 흐름도, 상세 흐름도 제공
- 진단 행위에 대한 상세한 표기 제공
- 데이터 수집 서버 구축 시 대시보드에서 데이터 양과 추적 범위 확대 가능

'행위 기반 의심'으로 탐지력 강화

- 위협 종류를 세분화하여 알려진 악성코드의 실시간 감시/탐지 부터, 확실한 악성 행위의 차단뿐만 아니라, 의심 행위 모두를 감시함
- 코드 인젝션, 취약점(Exploit) 공격, 랜섬웨어, 자동 실행 등록 등 의심 행위 감시로 보안 대응 범위 확장

차세대 EDR의 필수요소, 위협 인텔리전스 서비스 통합

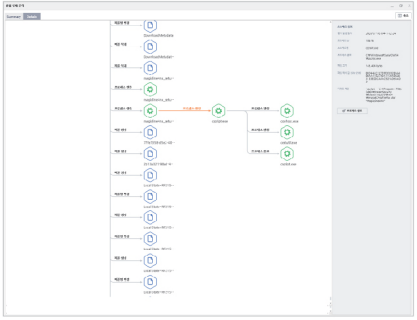
- Threat Inside의 A.I. 분석 및 다차원 분석 결과를 통한 정확한 악성코드 식별/분류와 상세 위협 인텔리전스 정보 제공
- YARA, IoC 등 Threat Hunting 정보화 체계 지원 가능
- 탐지 및 위협 카테고리 표준 MITRE ATT&CK 프레임워크, STIX 2.0이 반영된 위협 인텔리전스로 구체적이고 실효적인 대응 방안 제시

커널 로깅 기능으로 안정적인 운용 가능

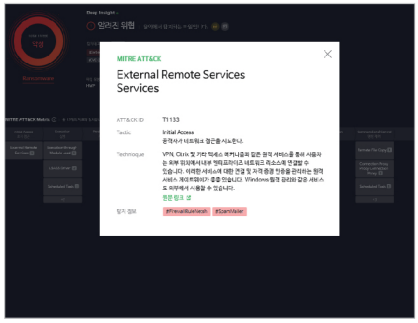
- 강력한 커널 로깅 기능으로 위협 관련 데이터를 모니터링하며 알약과 알약 EDR의 단일 커널 레벨 드라이버 지원으로 충돌 이슈 제거

1개의 통합 에이전트로 엔드포인트 보안 솔루션 통합관리

- 알약, 알약 패치관리(PMS), 알약 내PC지키미 등 엔드포인트 보안 솔루션과 연계
- 엔드포인트에서 발생하는 위협 행위에 대한 안정적이고 효율적인 정보 수집 및 분석 가능



상세 위협 흐름도



MITRE ATT&CK 위협 정보

수집된 데이터의 다양한 대시보드

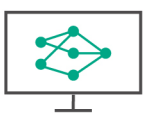
백신과의 차이점

기존 백신 솔루션과 가장 큰 차이점은 대응 기능의 범위와 가시성입니다.
알약 EDR은 백신에서 파악하지 못한 알려지지 않은 위협을 효과적으로 파악하고 실질적으로 대응하는 것을 목표로 합니다.

백신과 함께 사용함으로써 위협 대응 범위를 확장하고, 침해대응 관리를 효율화시킬 수 있습니다.

	백신	EDR
위협 탐지 / 차단 방식	시그니처 DB	행위 기반 (의심 행위, 악성 행위)
알려진 위협 탐지	○	△
알려지지 않은 위협 탐지	×	○
악성 파일 치료 여부	○	○
엔드포인트 가시성 확보	× (가시성 확보 한계, 감염 경로 확인 불가)	○
추가 대응	×	프로세스 종료, 네트워크 차단

이스트시큐리티라서 가능한 고도화된 위협 대응



1,600만+국내 최다 사용자

1,600만 이상의 실사용자를 통한
악성코드 빅데이터 보유

30+ESRC 분석 전문가

국내 특화 위협에 빠르게 대응하는
악성코드 전문 인력

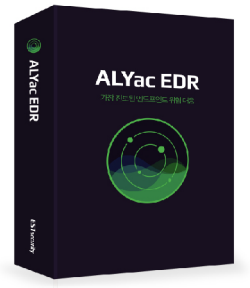
10+년 백신 운영 노하우

최근 2년간 탐지한 악성코드 3억 7천만 건
최근 4년간 랜섬웨어 행위 차단 850만 건

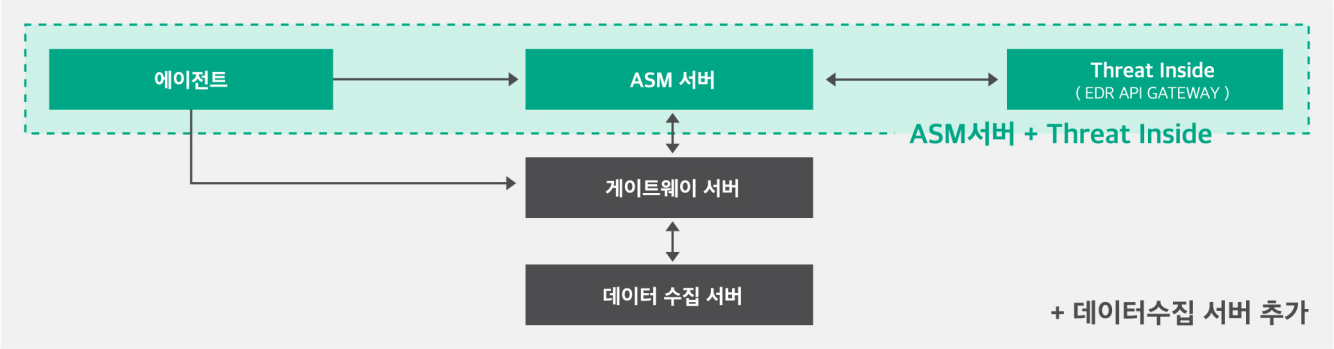
알약 EDR 패키지 타입

보안 관리자는 라이선스, 제품 정책, 업데이트 경로에 따라 이를 분리하고
관리콘솔(ASM)을 통해 제품 모드를 선택하여 조직 내에서 유동적으로 사용 가능합니다.

알약 EDR Lite	알약 EDR Premium
알약 EDR 단독 라이선스 구매 ※ 타백신 연동 사용 가능	알약 5.1 + 알약 EDR 라이선스 패키지 구매 ※ 사내 그룹별 패키지 타입 유동적인 사용 가능 (알약 / 알약 + 알약 EDR / 알약 EDR)



알약 EDR 구성 타입



※ 알약 EDR은 PC용, 서버용 2가지 형태로 제공 가능합니다.
※ 조직 규모 및 망 환경에 따라 서버 구성 환경은 달라질 수 있습니다. 상세 컨설팅을 통해 확인 가능합니다.

알약 EDR 설치 환경

HW 설치 환경

		CPU	RAM	HDD / SSD
서버	최소	2.xGHz 8core 16Thread	16GB	1TB * 2EA
	권장	2.xGHz 8core 16Thread	32GB	SSD 960GB * 2EA
관리콘솔	최소	Intel Dual Core 1Ghz	2GB	5GB 이상 여유공간
	권장	Intel Dual Core 2Ghz	4GB	6GB 이상 여유공간
에이전트	최소	Intel Dual Core 1Ghz	4GB	2GB 이상 여유공간
	권장	Intel Dual Core 2Ghz	8GB	4GB 이상 여유공간

SW 설치 환경

	OS	DB
서버 OS	Windows Server 2008 R2 SP1 (KB4490628 및 KB4474419 설치) / 2012 (R2 포함) / 2016 / 2019 / 2022 CentOS 6.x 이상 / Oracle Linux 7.x 이상 / Rocky Linux 7.x 이상 (모든 OS 64bit 지원)	MariaDB 기본 지원 (내장)
관리콘솔	Windows Server 2008 SP2 (KB4493730 및 KB4474419 설치) / 2008 R2 SP1 (KB4490628 및 KB4474419 설치) / 2012 (R2 포함) / 2016 / 2019 / 2022 Windows 7 SP1 (KB4490628 및 KB4474419 설치) / 8.1 / 10 / 11 (모든 OS 64bit 지원)	
에이전트	Windows Server 2008 SP2 (KB4493730 및 KB4474419 설치) / 2008 R2 SP1 (KB4490628 및 KB4474419 설치) / 2012 (R2 포함) / 2016 Windows 7 SP1 (KB4490628 및 KB4474419 설치) / 8 / 8.1 / 10 (모든 OS 64bit 지원)	

주요고객사

알약 EDR은
대한민국 10,000+ 엔드포인트를
보호하고 있습니다.

(주)신세계조선호텔, 알약 EDR 전사 도입

SHINSEGAE CHOSUN HOTEL

THE CHALLENGE
글로벌 업체 EDR 솔루션 사용 중 위협 근본 원인 파악 어려움과 잦은 보안 알림으로 업무부담 가중

OUR SOLUTION
알약 EDR은 알려지지 않은 위협의 의심 행위를 선차단해 보안 알림 부담을 최소화하고,
위협 인텔리전스 솔루션 Threat Inside와 연동되어 위협 식별 및 분석 정보를 제공하여 즉각적인 보안 정책 적용 지원

THE RESULTS
알약 EDR을 통해 신종 악성코드의 선차단과 숙주의 완전 제거 및 보안 관리자의 리소스 최소화로 실효적인 대응 가능

ESTsecurity

이스트시큐리티(주)

서울시 서초구 반포대로 3 이스트빌딩 (우)06711 www.estsecurity.com

T : 02-583-4616 F : 070-4850-9024 E : bizcenter@estsecurity.com

알약 EDR