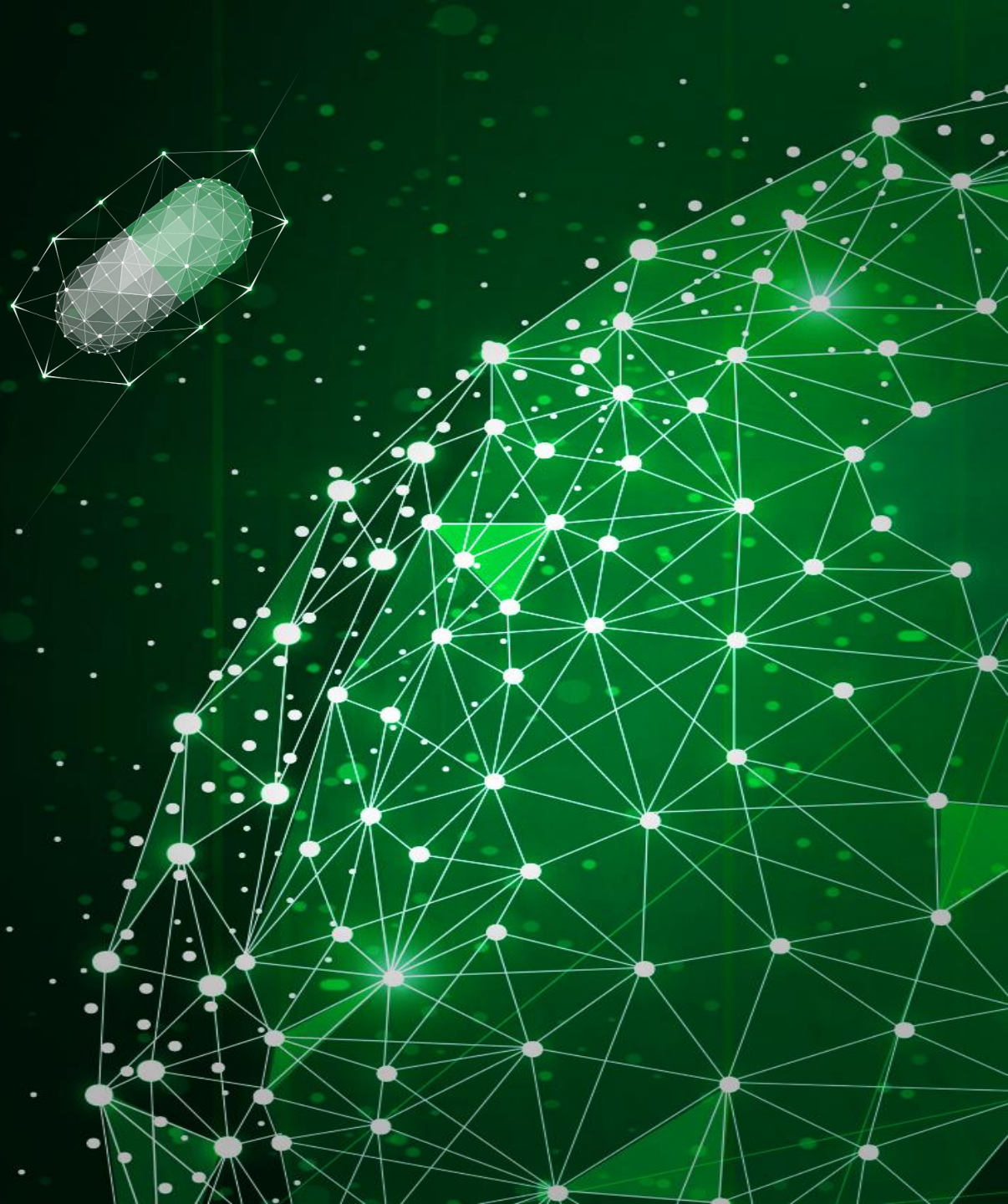
ESTsecurity

Make World More Secure with A.I.

알약 EDR

엔드포인트 위협 탐지-대응 솔루션



Contents.

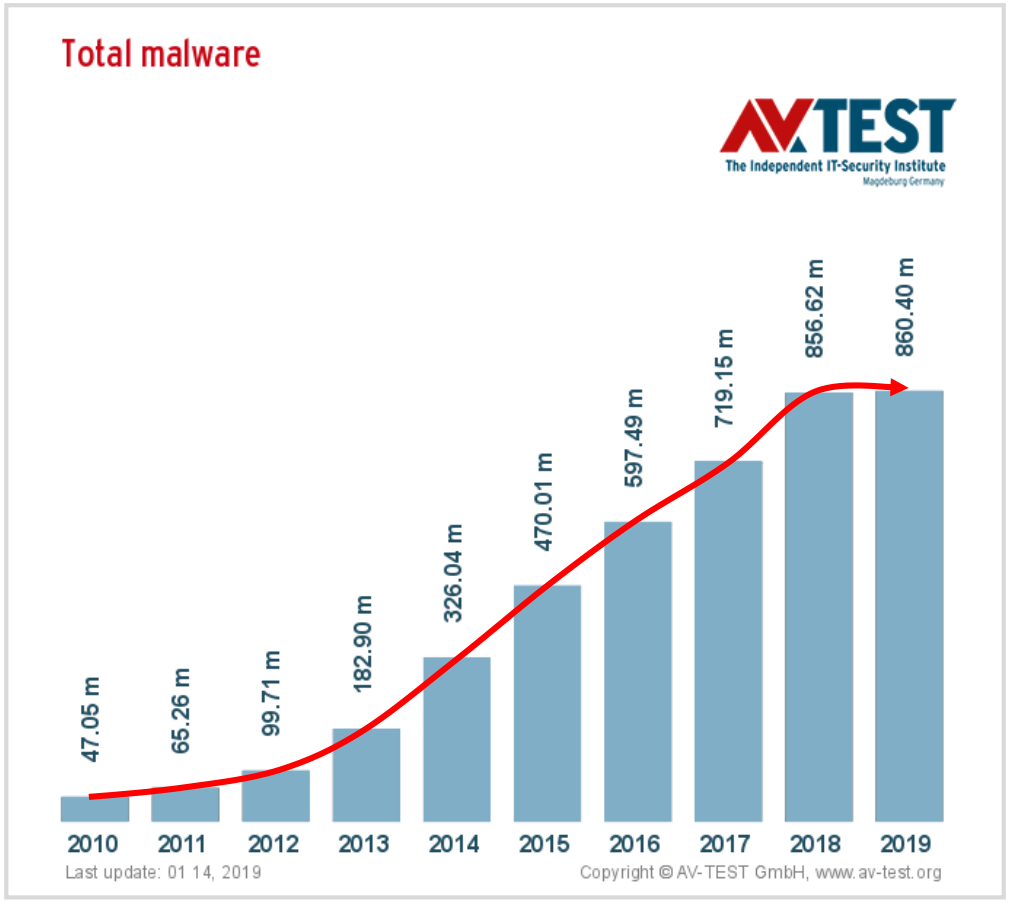
PART 01

알약 EDR

개발 및 제안 배경

지속적으로 증가하는 사이버 위협과 지능/조직화된 APT 공격

IT 기술이 발전하고 플랫폼이 늘어나면서 공격의 대상, 종류, 방법 등 사이버 위협 요소 또한 증가하고 있습니다.
해가 거듭될수록 사이버 공격은 더욱 지능화되며, 제로데이 위협은 갈수록 커지고 있습니다.



출처 : AV-TEST Statistics (www.av-test.org)

제로데이 공격 증가

- 제로데이 취약점 공격 사상 최대 기록
- 시스템 및 애플리케이션의 취약점 악용

지능/조직화된 APT 공격

- 새로운 공격 기법 접목시켜 응용화
- 다양한 유입 경로를 통한 공격

엔드포인트 보안 관점의 전환

엔드포인트 보안 솔루션은 기존 시그니처 기반 백신의 한계를 극복하고자 EDR(Endpoint Detection & Response), EPP(Endpoint Protection Platform) 등 최신 보안 기술이 결합된 실질적인 위협 대응 솔루션 형태로 진화하고 있습니다.

보안의 대상에 대한 인식 변화

"진짜 보안을 해야 할 부분은 서버 단이 아닌, 엔드포인트 단이다"

시그니처 DB 기반 안티바이러스(AV), 보안패치

신.변종 악성코드 & 지능형 지속위협(APT)의 범람

전통적 개념의 엔드포인트 보안 솔루션, 고도화되는 위협 대응에 한계

EDR | EPP | 인텔리전스

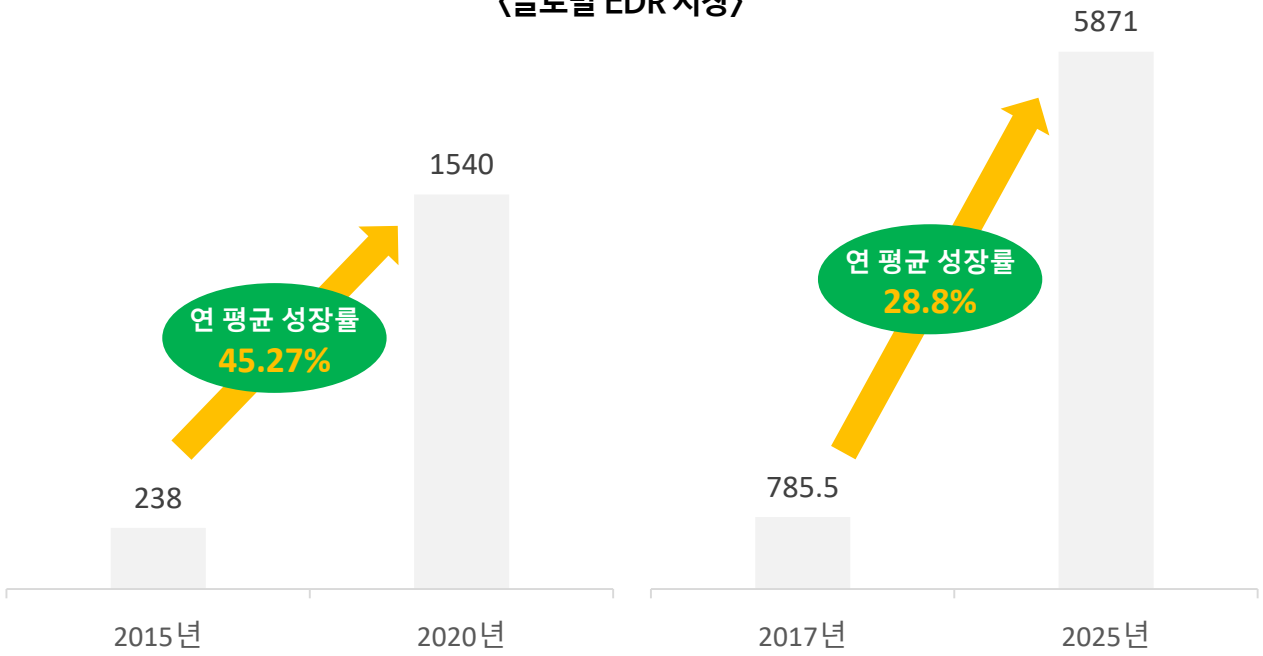
알려지지 않은 위협까지 탐지

위협에 대한 상관관계 분석과 인텔리전스 기반의 즉각적인 대응

EDR: 위협 대응의 새로운 대안

그 중 엔드포인트 탐지 및 대응 솔루션인 EDR은 최근 글로벌 보안 시장에서 가장 큰 폭으로 성장하고 있습니다.
해외에서는 이미 약 70%의 기업이 EDR 제품을 사용하고 있으며, 국내에서도 공공기관을 중심으로 도입이 빠르게 확산되고 있습니다.

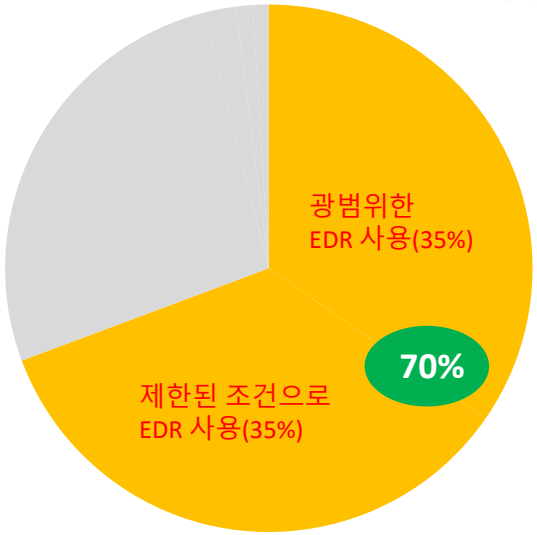
〈글로벌 EDR 시장〉



출처: 글로벌 시장조사기관 **'Gartner'**(2017)

출처: 글로벌 시장조사기관 **'리서치앤마켓'**(2018)

〈EDR 제품 사용률 조사〉

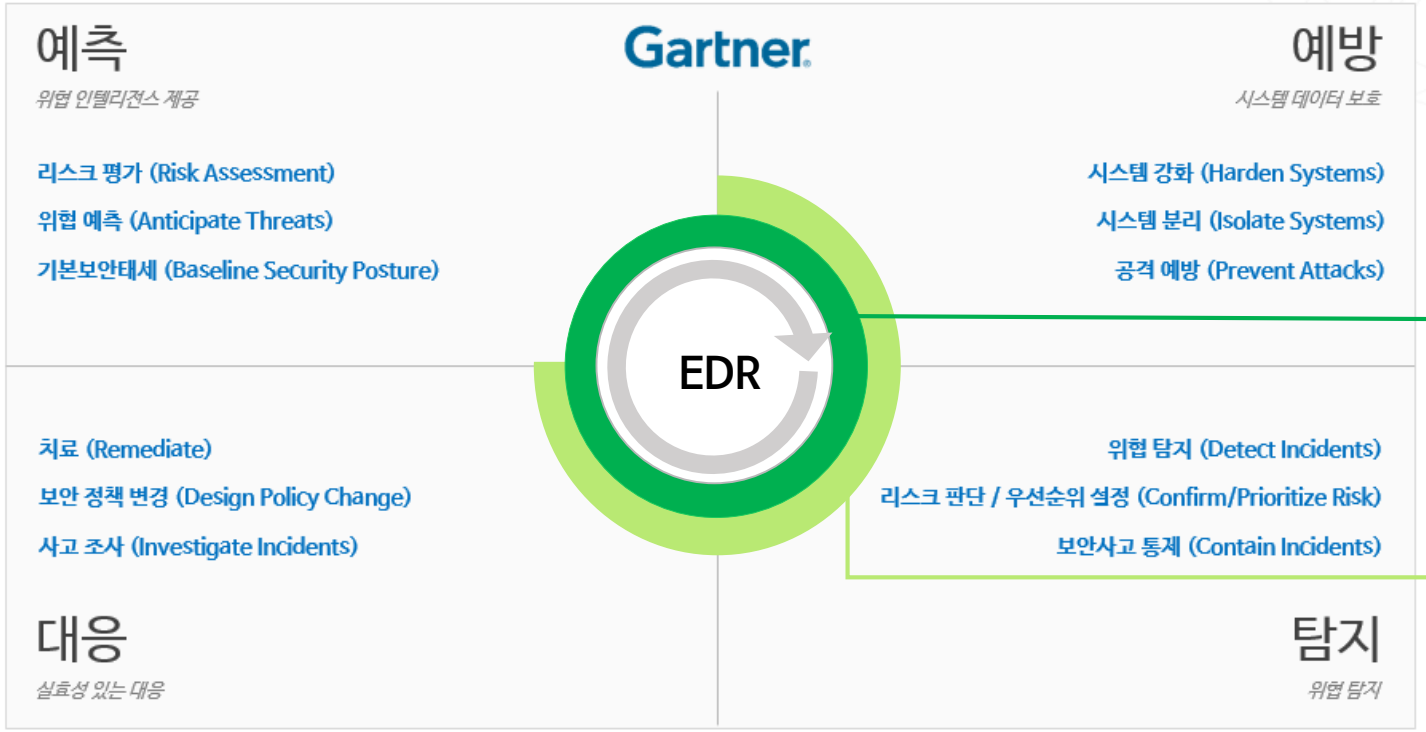


출처: 글로벌 시장조사기관 **'ESG'**(2017)

ESTsecurity

EDR: 위협 대응의 새로운 대안

EDR은 엔드포인트 영역에서 지속적인 모니터링과 대응을 제공하는 보안솔루션입니다.
이벤트 수집과 분석을 통해 위협에 대한 가시성을 확보할 수 있으며, 보안관리자는 신속한 대응을 취하여 추가적인 피해를 예방할 수 있습니다.



가트너 EDR 기술 정의

가시성 확보

- 이벤트 수집
- 위협 분석
- 위협 흐름도 제공

차단 및 치료

- 행위 기반 차단
- 프로세스 종료
- 네트워크 차단

EDR 제공 기능

변하지 않는 현실, 풀리지 않는 문제

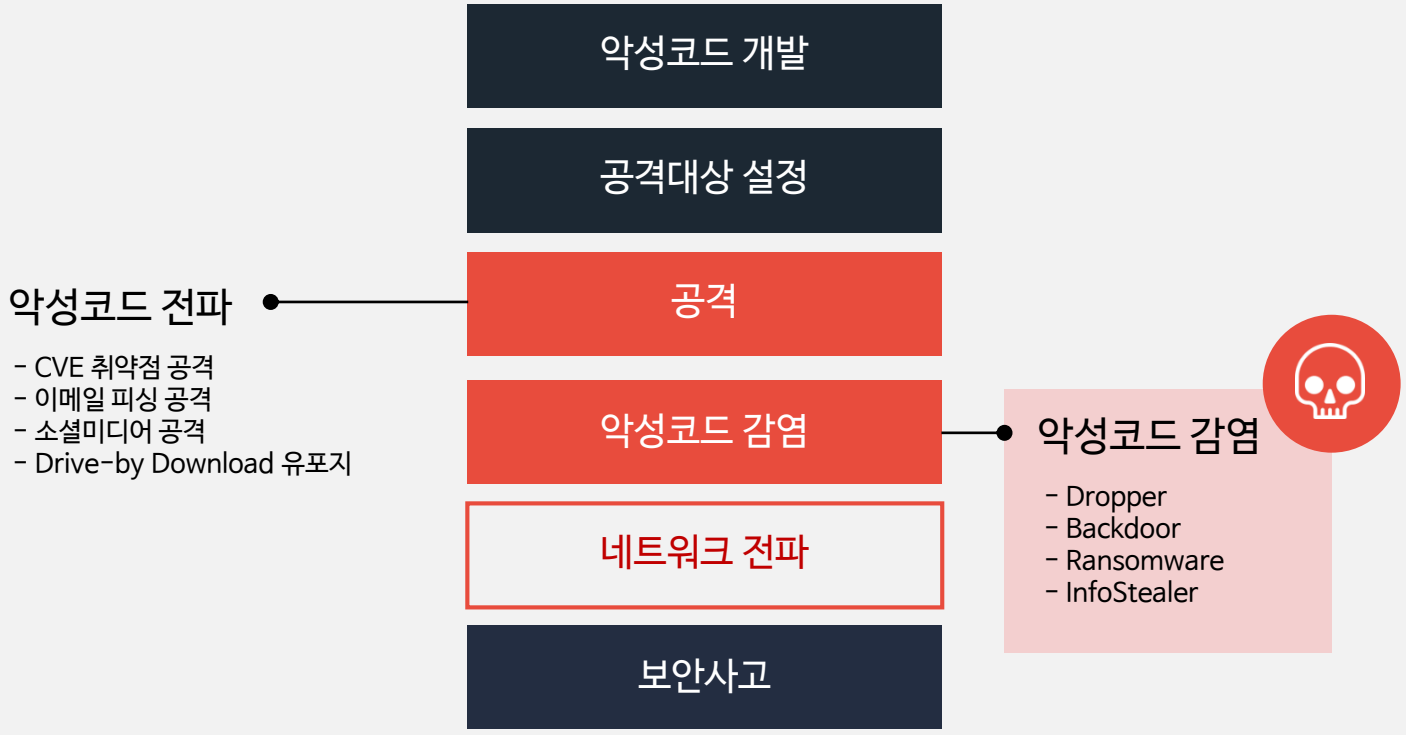
그러나 EDR 제품을 포함한 새로운 솔루션을 도입한다 해도 모든 문제가 해결되지는 않습니다.
단편적으로 제공되는 정보로는 위협에 대한 실질적인 대응이 어렵고, 보안 관리자들의 업무는 줄어들지 않는 현실입니다.

알약 EDR의 탄생

알약 EDR은 이스트시큐리티가 다년간 수집해온 악성코드 데이터와 최고의 악성코드 분석 기술 및 인공지능 기술을 바탕으로,
보안 관리자의 고질적인 고민을 해결할 수 있는 실질적이면서도 빈틈없는 엔드포인트 위협 대응 방안을 제공합니다.

알약 EDR의 탄생

이스트시큐리티는 모든 보안 사고의 시작은 악성코드부터라는 기조 아래 악성코드 식별 기능에 집중합니다.
위협의 유형을 정확히 파악하고 향후 이어질 공격을 예측함으로써, 지속 가능한 보호 방안을 제시하기 위해서입니다.



알약 EDR의 탄생

알약 EDR은 악성코드를 포함한 위협에 대한 자동 치료/차단 기능을 제공함으로써 보안 관리자의 관리 부담을 최소화하며,
인텔리전스 솔루션과의 연동을 통해 악성코드 상세 분석 정보가 포함된 차별화된 대응 가이드를 제공합니다.

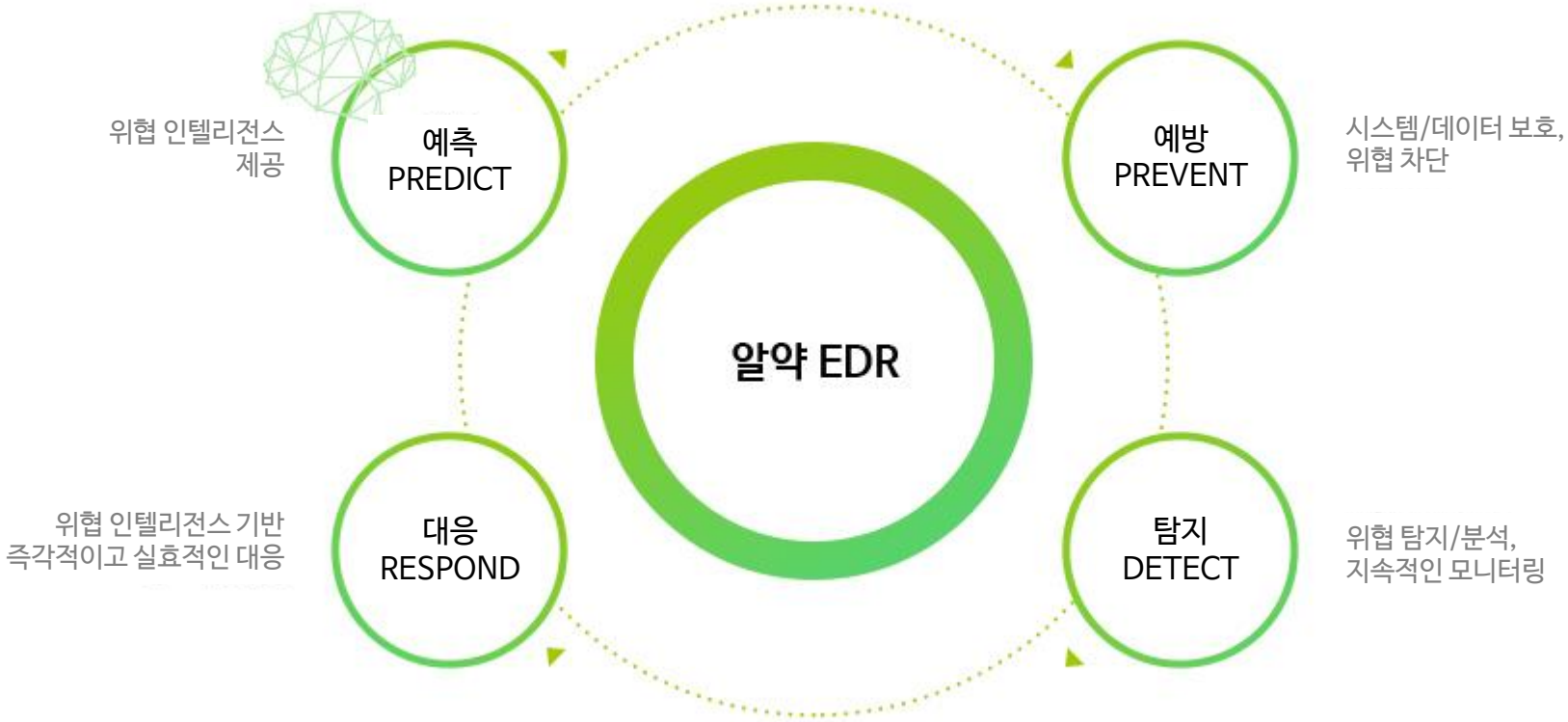
PART 02

알약 EDR

제품 소개 및 특장점

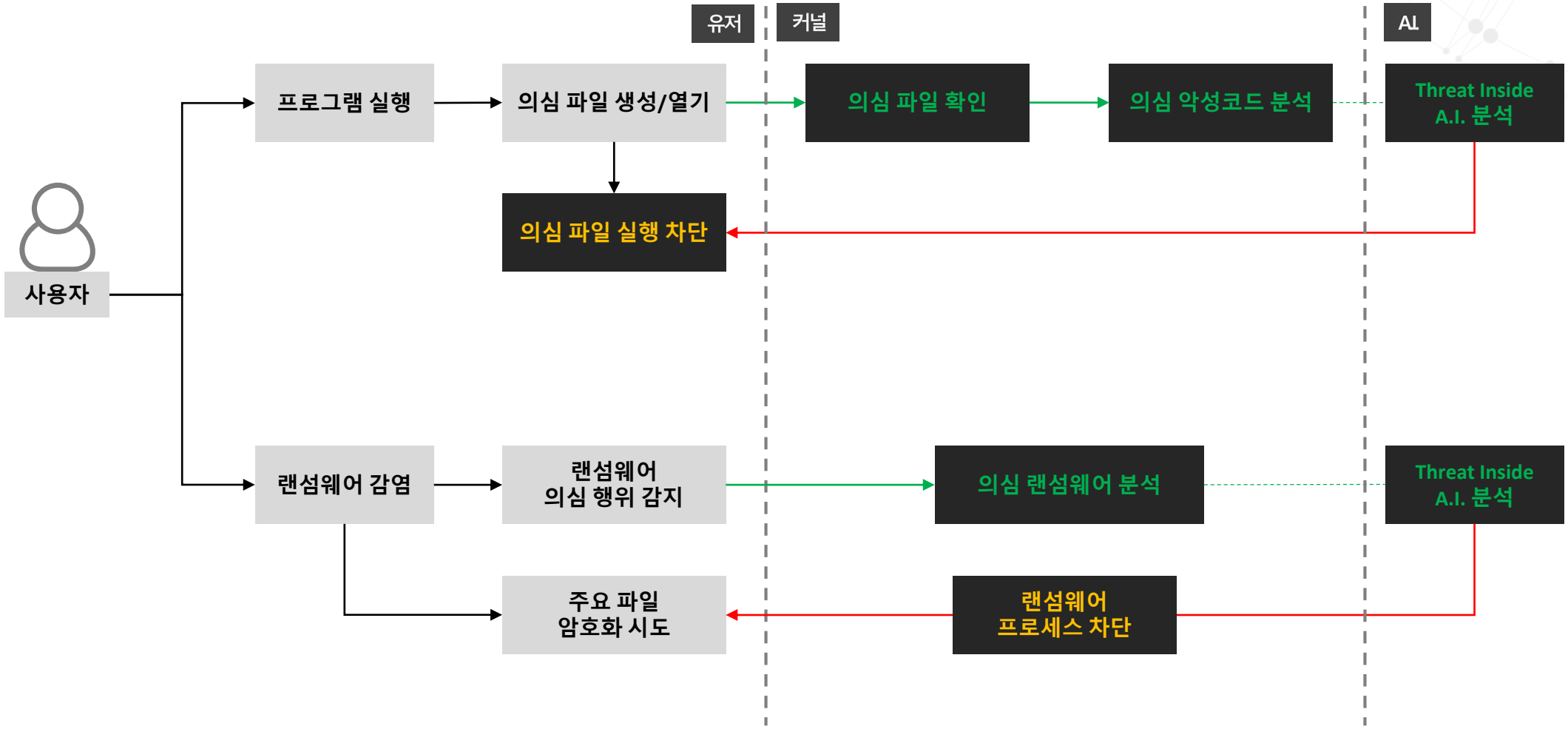
알약 EDR: 엔드포인트 위협 탐지-대응 솔루션

기업과 기관의 엔드포인트를 대상으로 각종 위협을 지속적으로 탐지 및 모니터링하고 실효적으로 대응할 수 있는 엔드포인트 위협 탐지 대응 솔루션으로 [예측 - 예방 - 탐지 - 대응] 전반을 구현합니다.



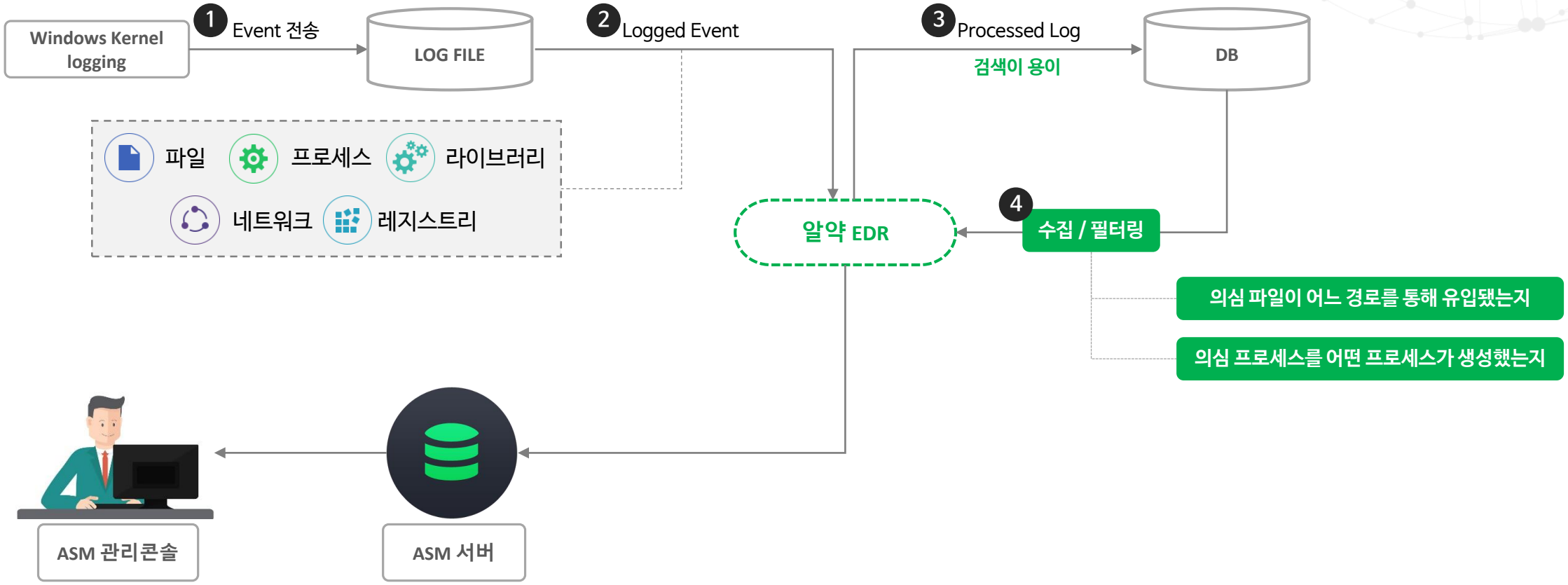
알약 EDR의 고도화된 행위 기반 차단 기술

행위 기반 감시, 랜섬웨어 차단 기능은 커널 모드 기술을 활용해서 구현되어
유저 모드, 훅 등을 이용한 타사 기능보다 더욱 강력하고 효율적으로 차단할 수 있습니다.



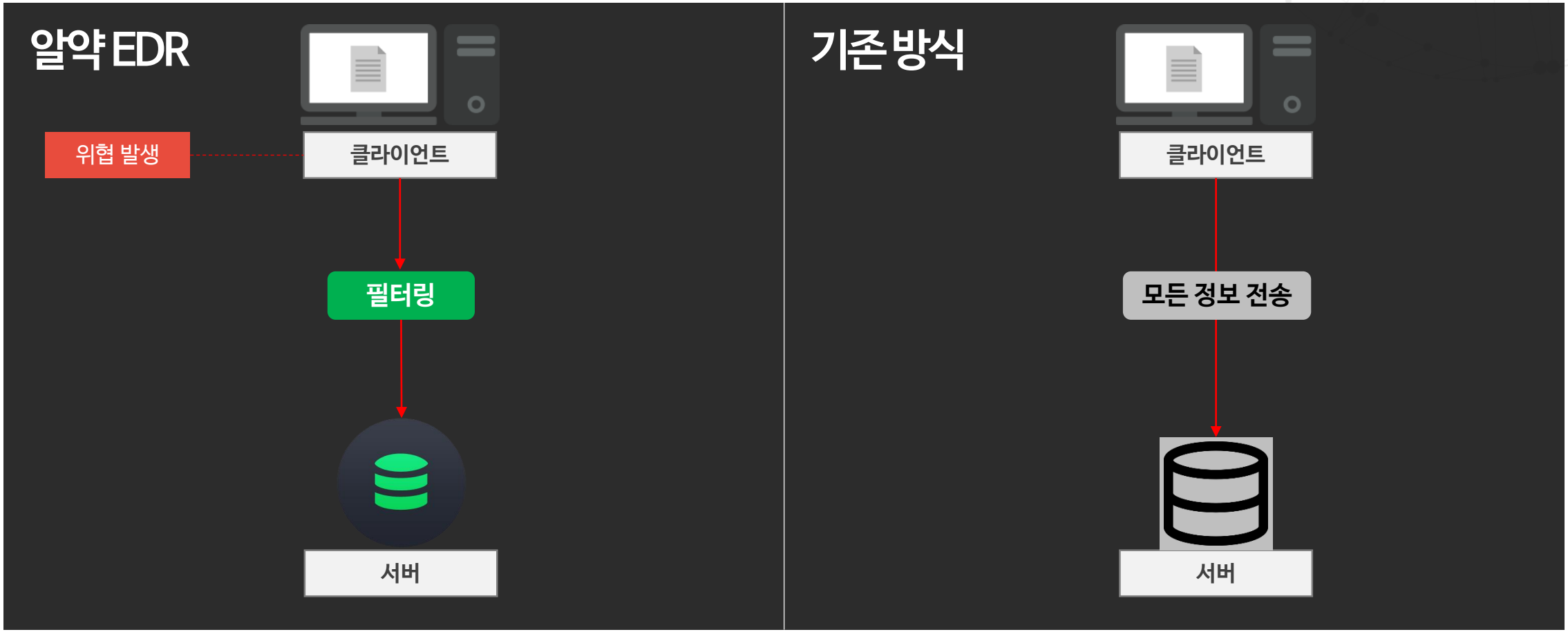
ESTsecurity 자체 행위 정보 수집 기술을 바탕으로 엔드포인트 가시성 확보

윈도우 커널 로깅 기능을 사용하여 파일, 프로세스, 레지스트리, 네트워크 등의 정보를 안정적으로 수집합니다.
알약 에이전트가 비정상 종료되거나, 업데이트가 발생하는 상황에서도 로그의 유실 걱정이 없습니다.



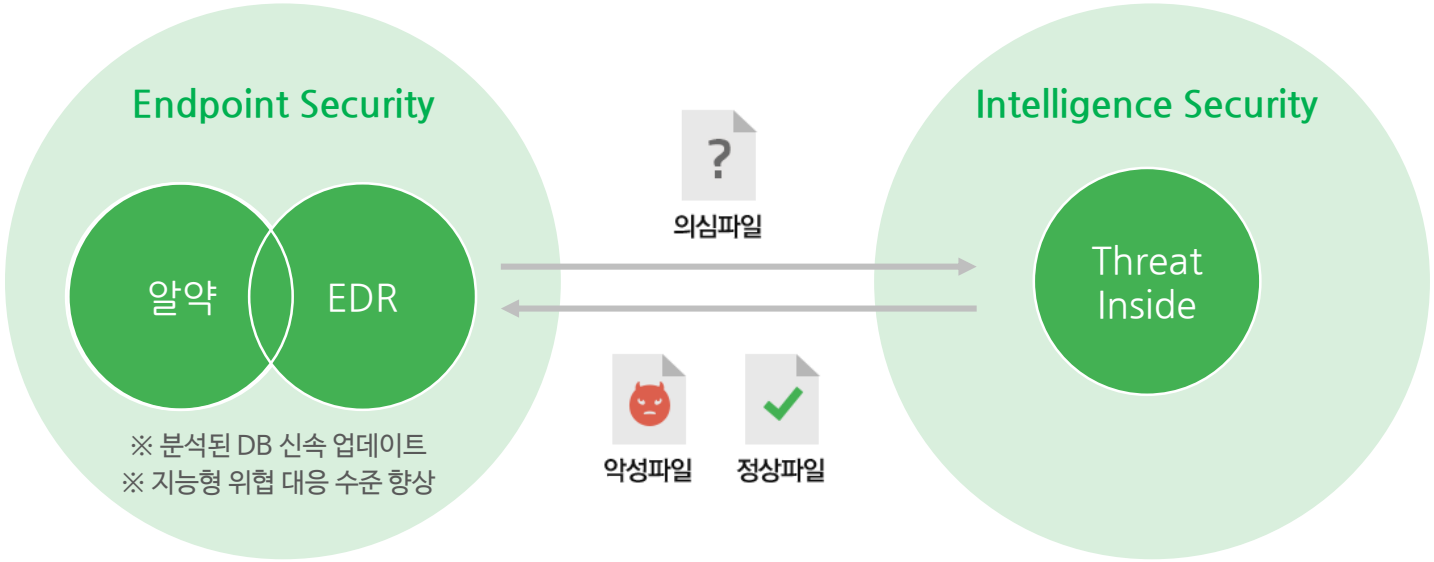
ESTsecurity 자체 행위 정보 수집 기술을 바탕으로 엔드포인트 가시성 확보

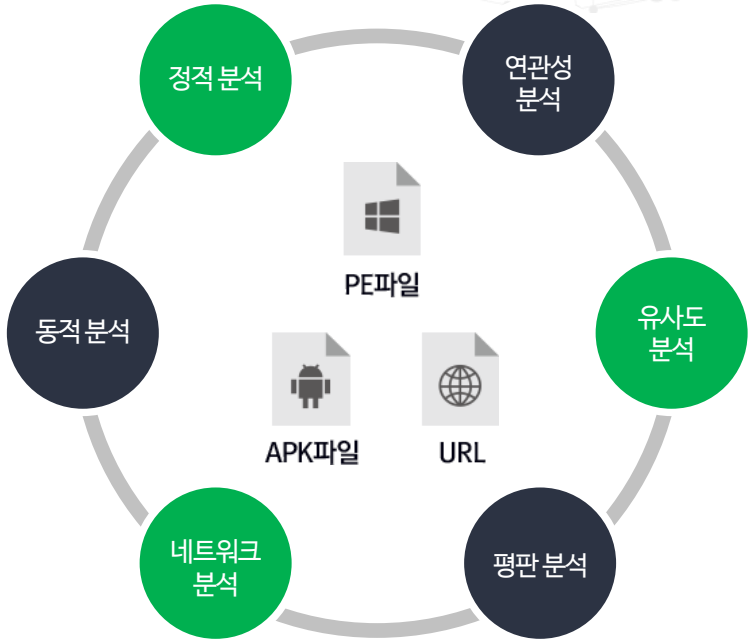
엔드포인트에서 위협이 발생한 시점부터, 차단된 위협에 대한 유입 경로를 역으로 추적합니다.
모든 정보를 보내는 것이 아니라, 필터링 된 정보가 전송되기 때문에 관리 서버의 부하가 거의 없습니다.



알약 EDR과 위협 인텔리전스 솔루션 Threat Inside 연동

모든 엔드포인트의 실질적인 보안 위협은 엔드포인트의 악성코드로부터 발생하기 때문에
각종 악성코드를 식별하고 분류하는 것이 차세대 엔드포인트 보안의 핵심입니다.
알약 EDR에 Threat Inside의 A.I. 기술을 접목한 이유입니다.

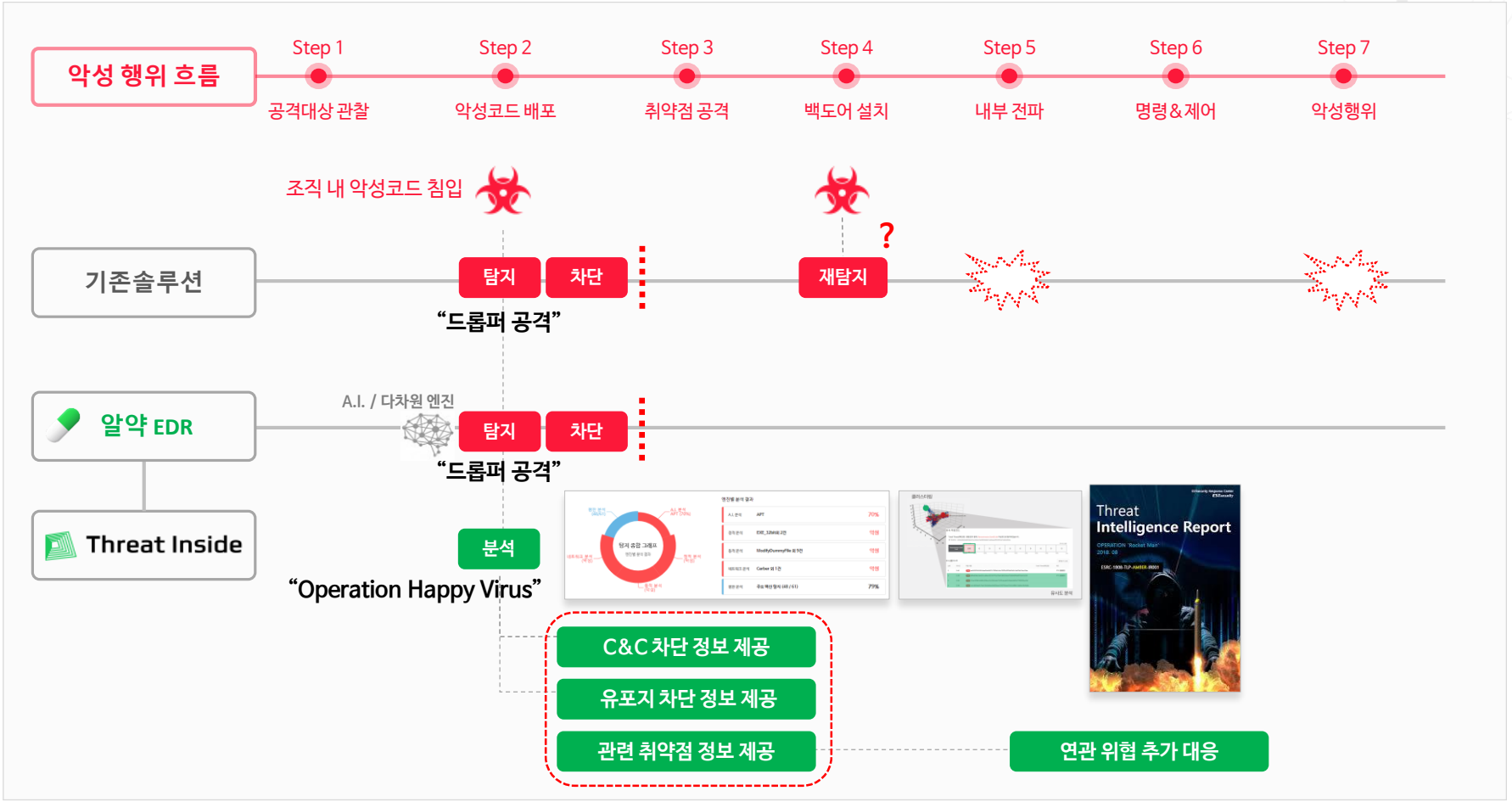




※ 인공지능 분석부터 리얼 머신 분석까지
전방위적인 분석 진행

대응(Response)의 확장

위협 인텔리전스 솔루션인 Threat Inside를 통해 위협의 식별이 가능하여 한층 더 강화된 위협 대응을 제공합니다.



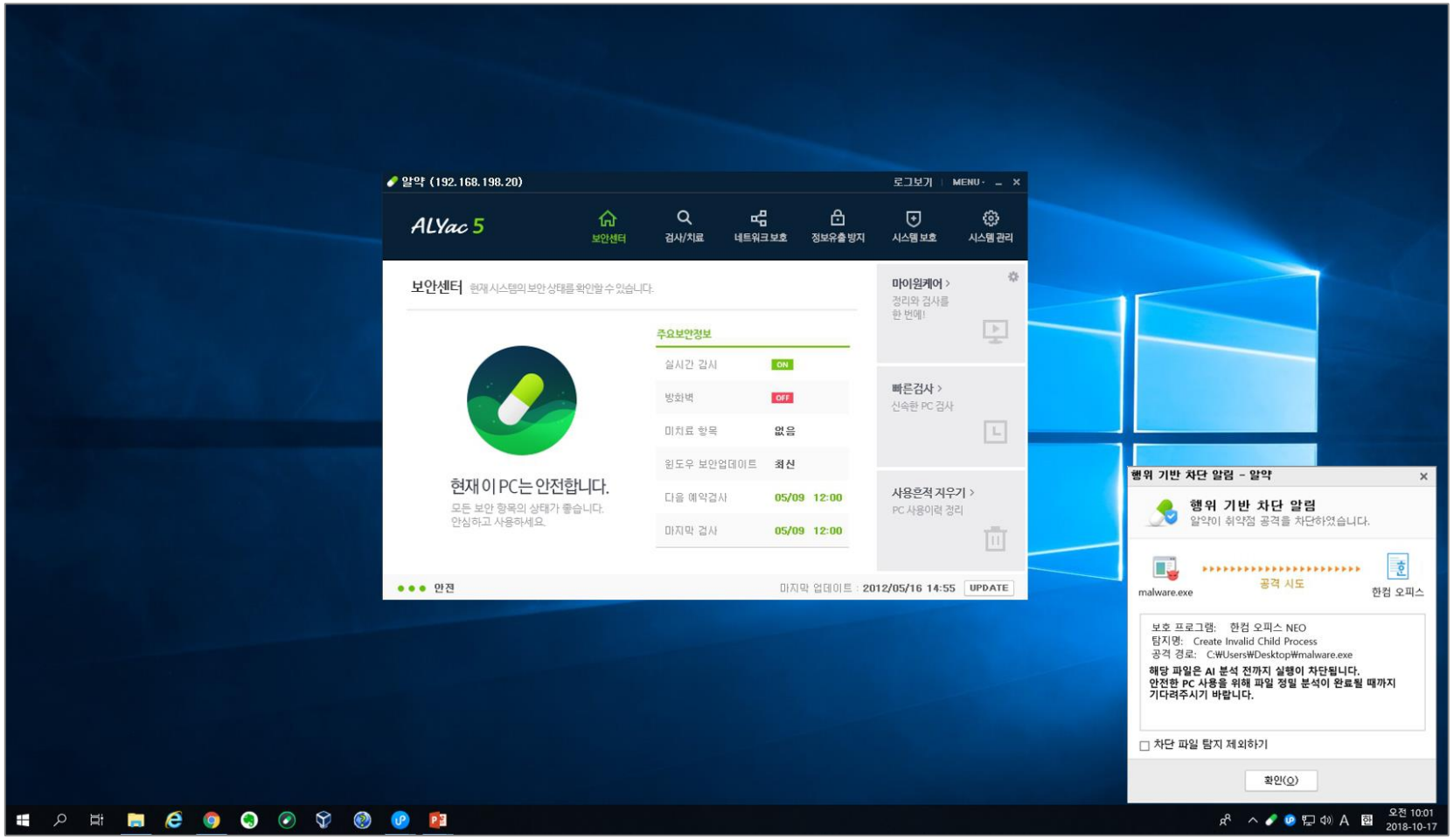
PART 03

알약 EDR

위협 대응 시나리오

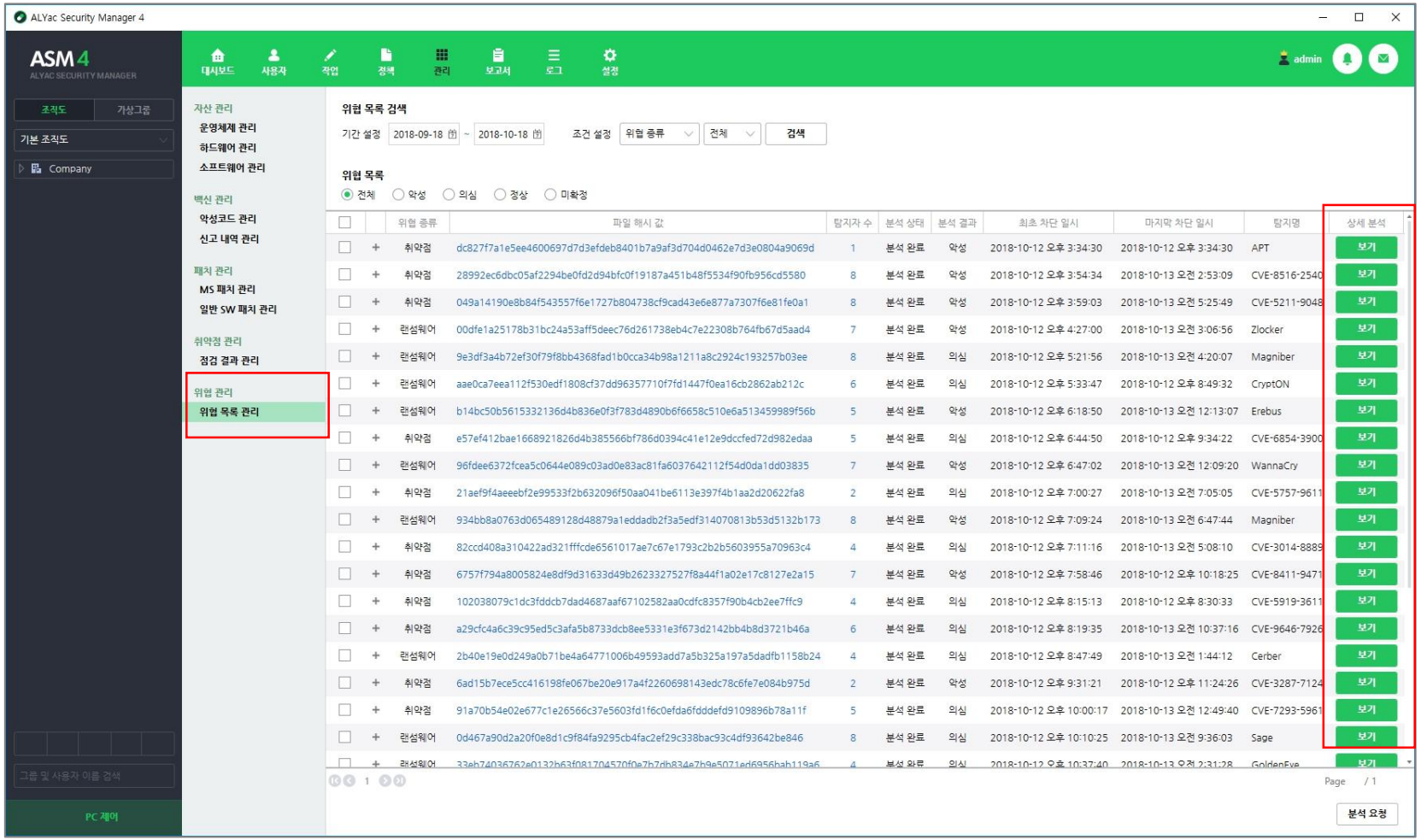
알약 EDR 위협 대응 시나리오 - ①

알약 EDR 에이전트는 알려지지 않은 위협이 발생 시, 행위 기반 탐지 기술을 통해 의심 파일의 실행을 사전 차단합니다.



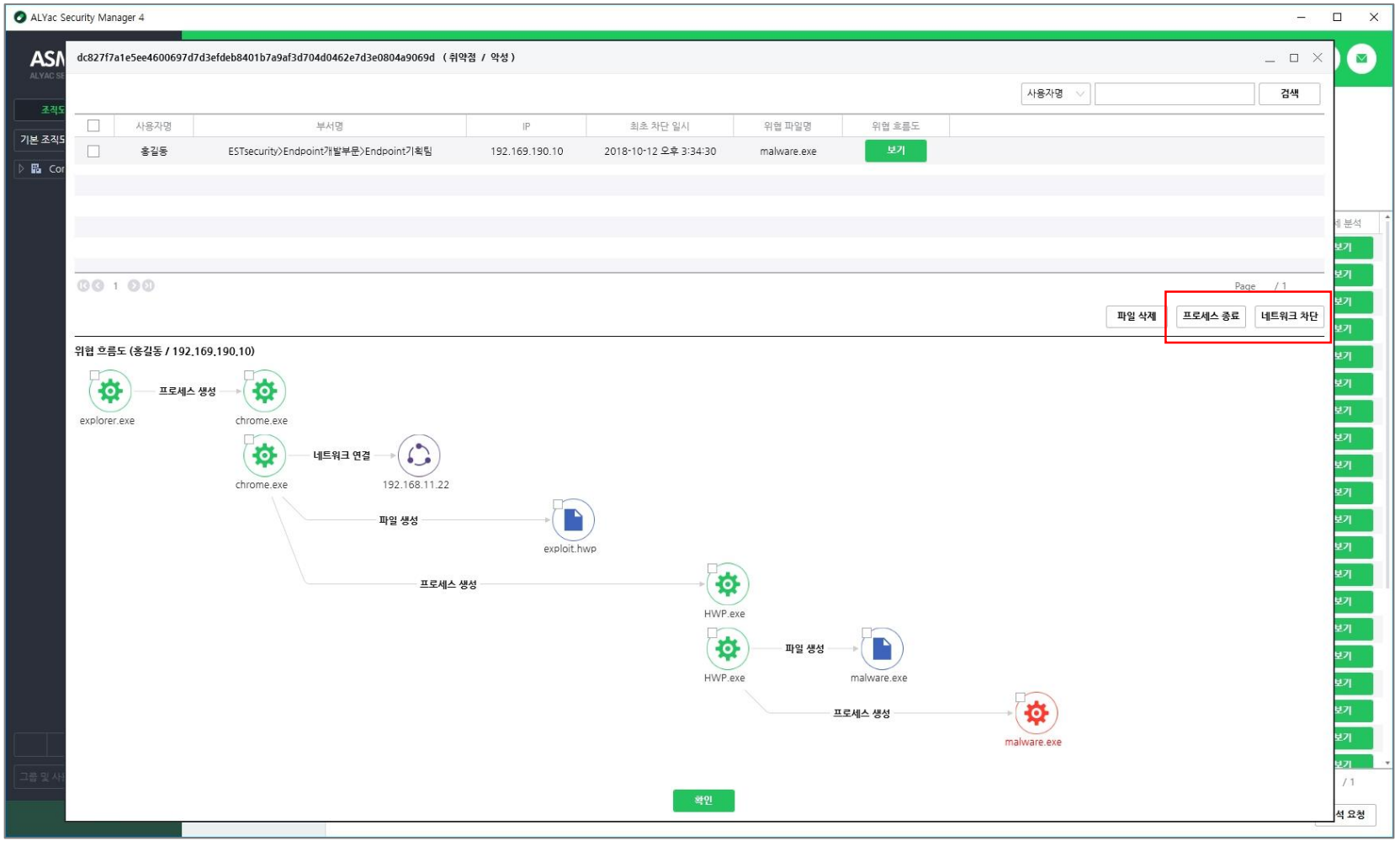
알약 EDR 위협 대응 시나리오 - ②

관리자는 ASM4의 위협 관리 메뉴를 통해 에이전트에서 차단된 위협 목록을 확인할 수 있습니다.
수집된 의심 파일은 Threat Inside를 통해 분석되며, 분석 완료 후 위협의 상세 분석 결과를 제공합니다.



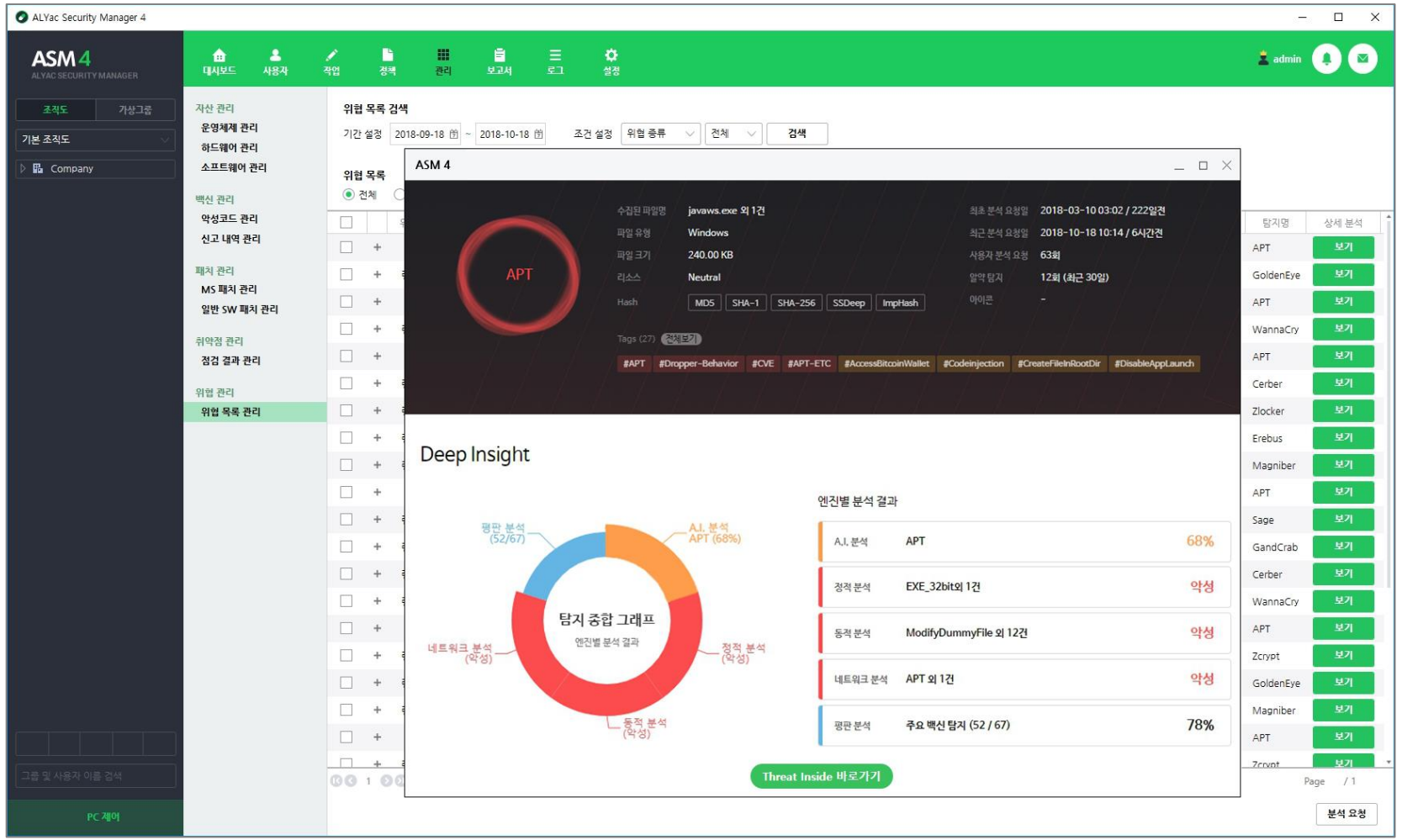
알약 EDR 위협 대응 시나리오 – ③

관리자는 동일한 위협으로 차단된 기업 내 사용자 목록을 확인할 수 있고, 선택한 사용자의 위협 흐름도를 확인할 수 있습니다.
수집된 엔드포인트 행위 정보를 바탕으로 프로세스 종료, 네트워크 차단 등 추가적인 조치를 취할 수 있습니다.



알약 EDR 위협 대응 시나리오 - ④

관리자는 Threat Inside에서 제공되는 요약 정보를 받아 볼 수 있고, 실제 Threat Inside 페이지로 넘어가 상세 분석 정보와 체계적으로 이어지는 대응정보까지 확인할 수 있습니다.



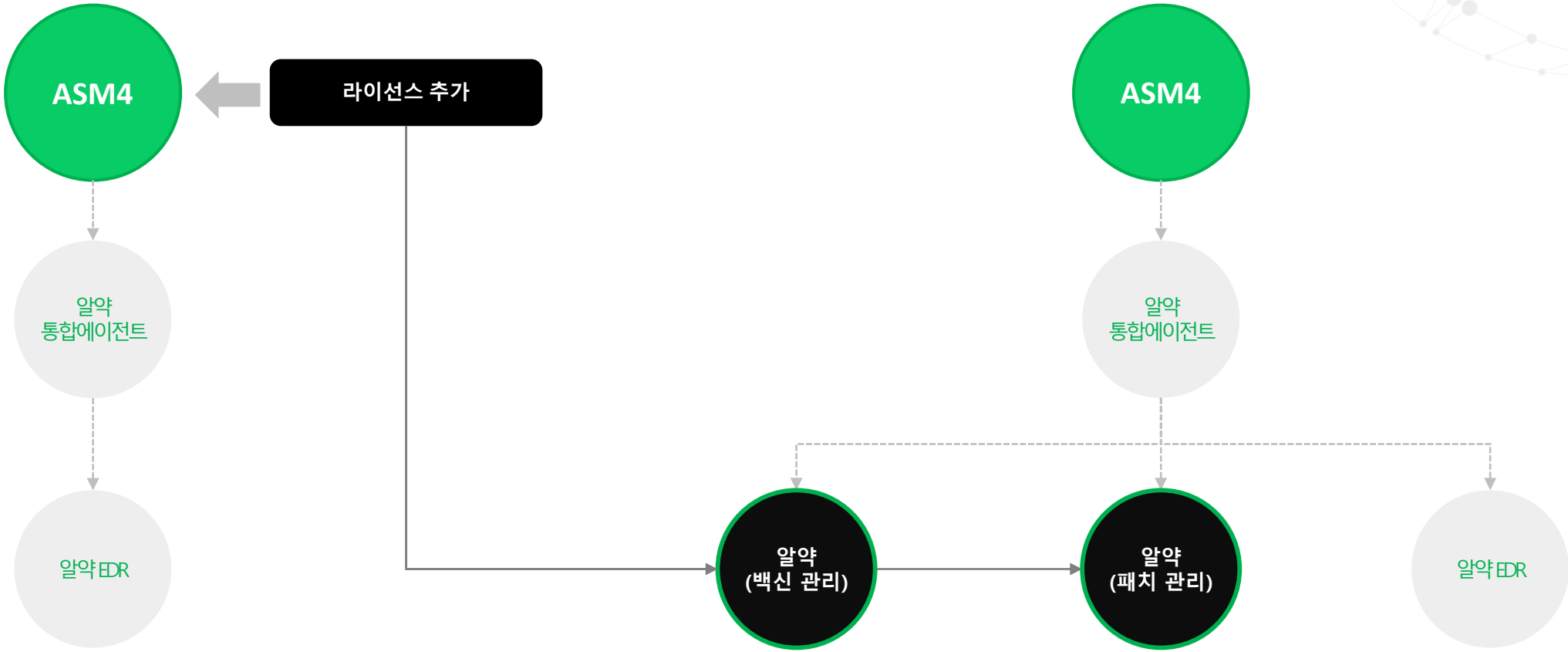
PART 04

ESTsecurity

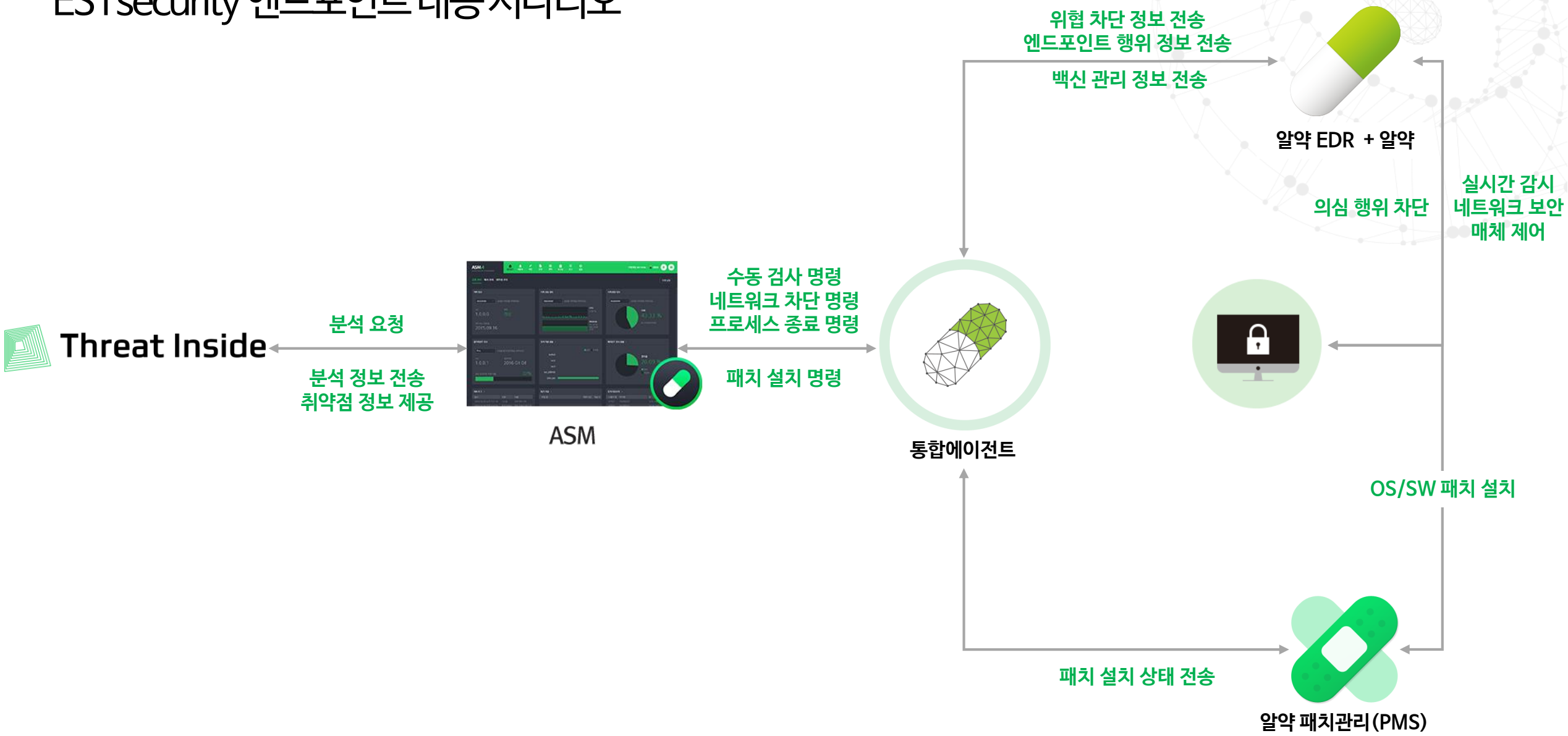
엔드포인트 보안 전략

ESTsecurity 엔드포인트 라인업 추가 구축

별도의 서버 구축 없이 라이선스 구매만으로 ESTsecurity의 엔드포인트 제품을 활성화할 수 있습니다.
단일 에이전트를 통해 복수의 보안 서비스를 일괄 관리하며 사내 보안 수준을 강화할 수 있습니다.



ESTsecurity 엔드포인트 대응 시나리오



알약 도입효과

알약은 뛰어난 탐지율을 보장하는 3개의 멀티 엔진을 탑재하여 글로벌 위험 요소로부터 시스템을 빈틈없이 보호하고
실시간 감시, 네트워크 보안, 매체 제어 기능을 통해 원천적으로 위험 요소의 유입을 차단합니다.

01 강력한 악성코드 탐지

- 국제 인증을 통해 검증받은 트리플 엔진을 통해 강력한 악성코드 탐지
- 전 세계에서 광범위하게 수집되는 해외 위협요소 DB와 국내 최대의 사용자를 기반으로 구축된 국내 위협요소 DB를 통한 포괄적 탐지

02 오탐 검증 시스템

- 오진 위험 최소화를 위해 업데이트 전 OS 및 주요 보안 프로그램, 범용 프로그램의 오진 여부 확인 프로세스 도입

03 자료 유출 사전 차단

- 매체 제어 기능을 통해 USB 및 다양한 이동식 저장 장치를 이용한 자료 유출 사전 차단

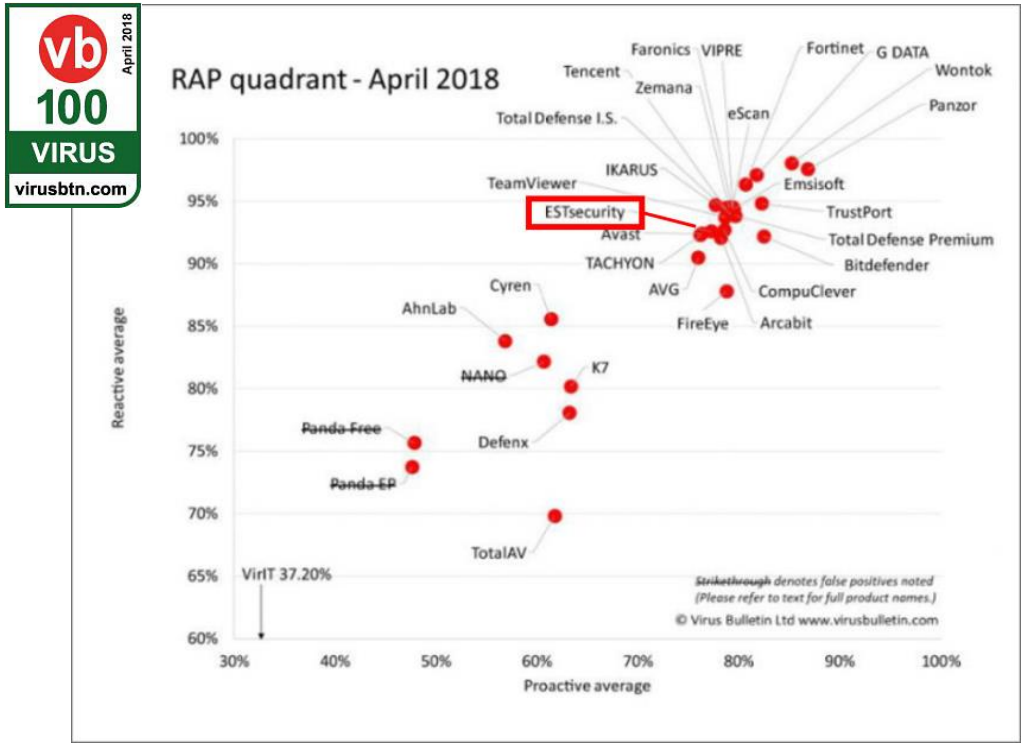
04 빠른 검사 속도

- Smart Scan 기술을 통해 실시간 감시 또는 정밀 검사 시 실제 검사가 필요한 파일 분류
- 안전함이 검증된 파일은 검사에서 제외하여 검사 속도 향상, 실시간 감시 부하 제거

알약의 기술 강점

알약은 5년 연속 ICSA 인증 획득 및 VB100 인증 & 높은 RAP 결과로 제품 경쟁력을 인정받았습니다.

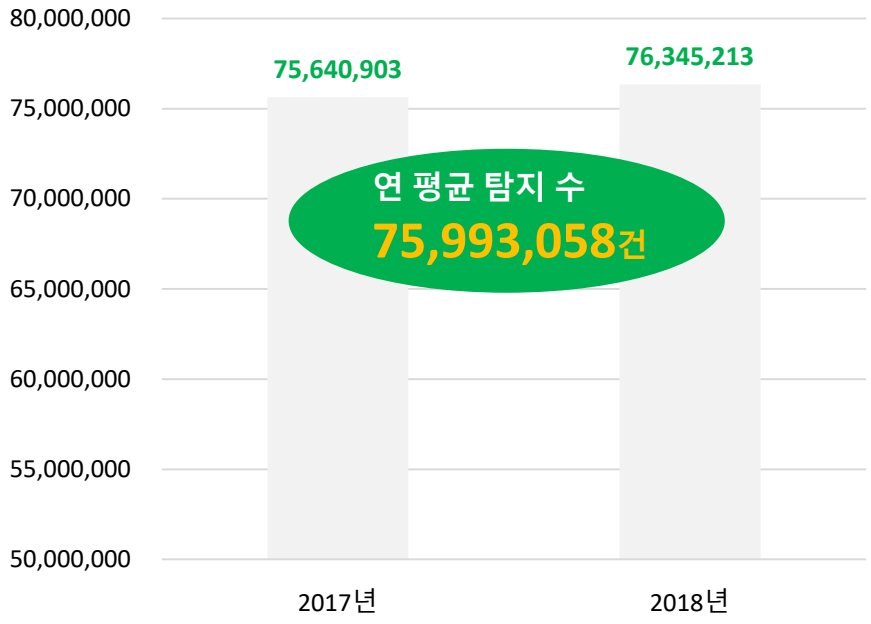
* RAP(Reactive Detection and Proactive Detection) 테스트
Reactive Detection: 업데이트 시점을 기준으로 그 이전에 수집된 악성코드 진단율 측정
Proactive Detection: 업데이트 중단한 시점 이후에 수집된 샘플로 진단율 측정



* EIST 어워드
ICSA의 인증 테스트에서 5년 이상 빠짐없이 우수한 성적을 낸 기업에 수여하는 상

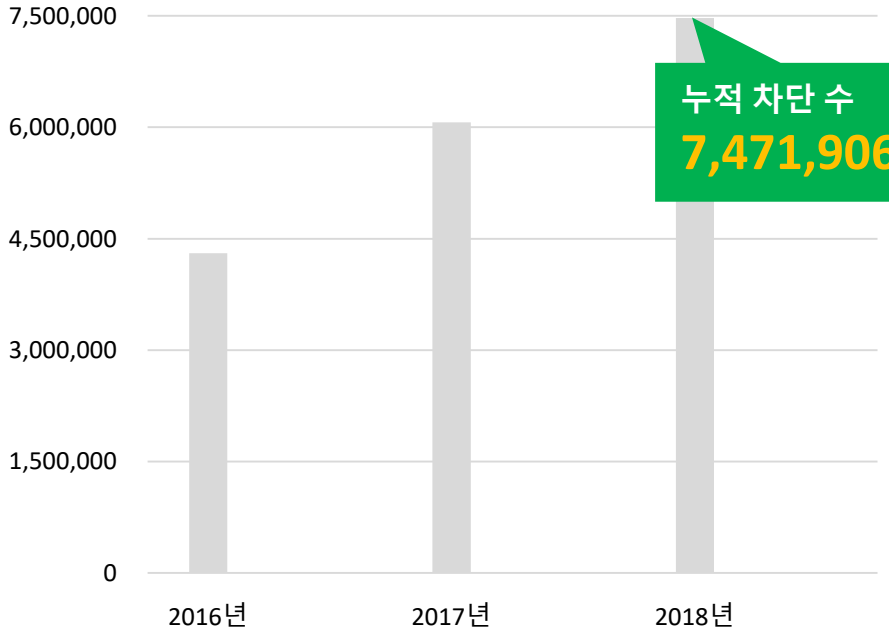
알약의 탐지/차단 통계

2017~2018 악성코드 탐지 통계



* 감염 통계를 월별로 합산하여 산출한 TOP15 기준 수치입니다.

2016~2018 알약 랜섬웨어 누적 차단 통계



연간 평균 차단 건수
2,490,635건

월간 평균 차단 건수
207,553건

일간 평균 차단 건수
6,824건

* 알약의 패턴 탐지 건수는 제외한 수치입니다.

알약 패치관리(PMS) 도입효과

관리자가 기업 내 PC의 윈도우 업데이트 및 주요 S/W 패치 설치 현황을 실시간으로 확인하고
신속하고 간편하게 패치 파일을 배포할 수 있는 전문 패치 솔루션입니다.

01 차별화된 사용성

- 직관적 패치 현황 파악을 위한 대시보드 및 통계 보고서 제공
- 용도와 목적에 따라 대시보드 커스터마이징 가능
- 조직도 연계된 직관적인 작업 및 정책 명령

02 높은 효율성

- 사내 인사 DB와 연동되어 관리 연속성 유지
- ASM4 연동을 통해 보안 제품 통합 관리

03 효율적인 패치 관리

- MS 패치에 대해 백그라운드 설치 제공하여 최신 패치 적용 가능
- 사용자 및 부서별 일괄 사내 보안 정책 유지

04 안전한 패치 배포

- 자체 검증 및 테스트를 거친 안전한 패치 파일 배포
- PC 환경 및 상태별 패치 자동 설치
- 배포 트래픽 자동 분산 처리를 통한 배포 안정성 확보

위협 인텔리전스 솔루션 Threat Inside 도입 효과

Threat Inside 구축을 통해 좀 더 심층적인 분석과 다차원 정보를 받아볼 수 있습니다.
24시간 언제든지 의심되는 파일이나 정보들을 분석하고 악성 여부나 종류를 자동으로 판별하여,
기하급수적으로 늘어나고 있는 신/변종 악성코드를 탐지하고 대응하는 최상의 방법을 제공합니다.

01 Deep Core _ A.I. 엔진

- 실시간 탐지 악성코드의 자가학습을 통한 A.I. 성능 고도화
- 수년간 백신을 운영한 노하우를 바탕으로 오탐 검증 시스템의 더블 체크를 통해 오탐지 가능성 최소화
- 정/동적 분석 대비 월등히 빠른 분석 속도로 실시간 대응
- 국내외 주요 기관 및 기업들과의 긴밀한 네트워크를 통해 국내 보안 환경에 최적화된 서비스 제공

02 Deep Analysis _ 다차원 분석

- 리얼 머신 분석부터 인공지능까지 위협에 대한 전방위적 분석 수행
- 악성코드의 특징과 행위 정보뿐만 아니라 해당 악성코드와 연관된 위협 정보 함께 제공
- 기업 IT 관리자부터 악성코드 분석 전문가까지, 수준별 분석 정보 제공

03 Deep Insight _ 위협 인텔리전스 리포트

- Deep Core의 인공지능 분석을 통한 악성코드 유형의 자동 분류
- 악성코드의 유형별 특징부터 수동 분석 결과, 구체적 대응 방안까지, Deep Insight (인텔리전스 리포트)를 통한 보안 전문 지식 제공
- 탐지된 랜섬웨어 등 APT 공격에 대한 근거 기반의 정보 및 상세 인사이트 제공

위협 인텔리전스 솔루션 Threat Inside의 기술 강점: Deep Core _ A.I. 엔진

■ **Top Tag 기반의 Precision 값을 기준으로 99.5% 확률로 위협을 정확하게 분류**

-〉 해당 결과는 한 데이터 셋 내에서 학습셋과 검증 셋을 나누지 않고 학습 이후 새롭게 수집되는 샘플 셋을 기준으로 나온 검증 결과

〉〉 **Timeline 기반의 Evaluation 기법을** 사용함 (기존에 많이 사용되는 X(교차) Evaluation 기법은 공격자들의 우회 기법에 대해 검증하는데 제한적)

〉〉 2018년 6월 테스트 결과 : 3월~4월 샘플로 학습한 엔진으로 학습되지 않은 5월 수집 샘플을 검사한 결과 : **92.8%**

〉〉 2018년 8월 테스트 결과 : 3월~6월 샘플로 학습한 엔진으로 학습되지 않은 7월 수집 샘플을 검사한 결과 : **99.0%**

〉〉 2018년 10월 테스트 결과 : 3월~9월 샘플로 학습한 엔진으로 학습되지 않은 9월 수집 샘플을 검사한 결과 : **99.5%** (지속적인 정확도 증가)

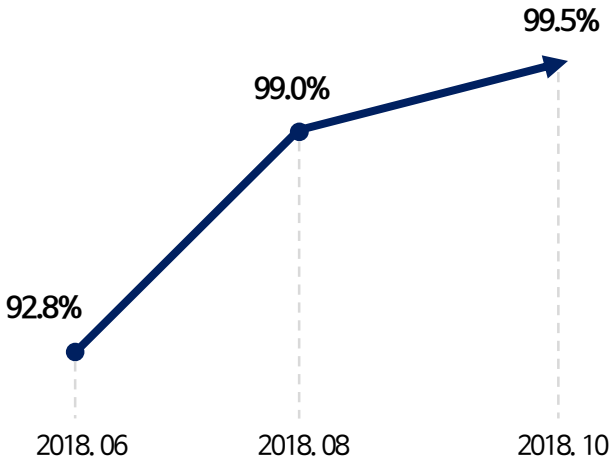
■ **12개의 대분류와 100개의 소분류로 악성코드를 정확히 판별**

-〉 Threat Inside에서 분류 가능한 전체 분류는 총 484개이며, Deep Core에서는 이 중 100개의 소분류 확진

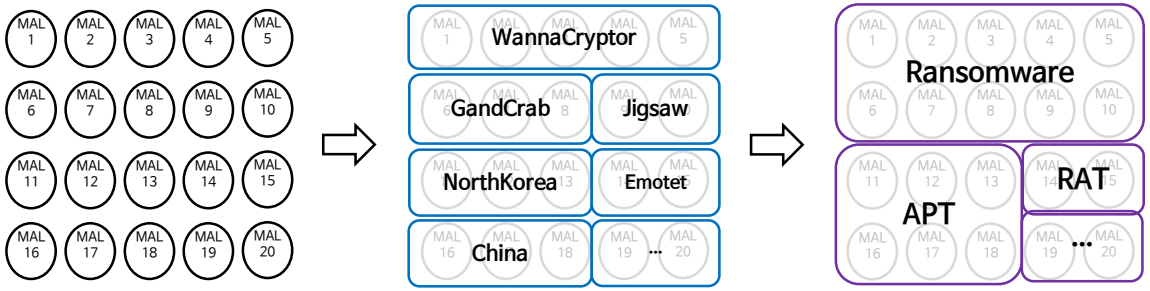
-〉 확진 가능한 분류 체계는 학습이 거듭될수록 지속 증가 중

-〉 분류되는 유형에는 Ransomware, Banker, Spyware 등의 악성코드 분류와 APT NorthKorea, China 등 APT 그룹에 대한 분류가 모두 포함

(1) 탐지/분류 결과



(2) 위협 분류 체계



빅데이터 기반의 샘플 | 소분류 : 100개 | 대분류 : 12개

위협 인텔리전스 솔루션 Threat Inside 기술 강점: Deep Analysis _ 다차원 분석

■ **Windows, Android 기반의 샘플 파일 및 URL을 분석하여 확진된 분류명과 함께 악성 여부 판별**

-〉 다차원 분석 : A.I. / 정적 / 동적 / 네트워크 / 평판 분석으로 구성된 **5개의 엔진**

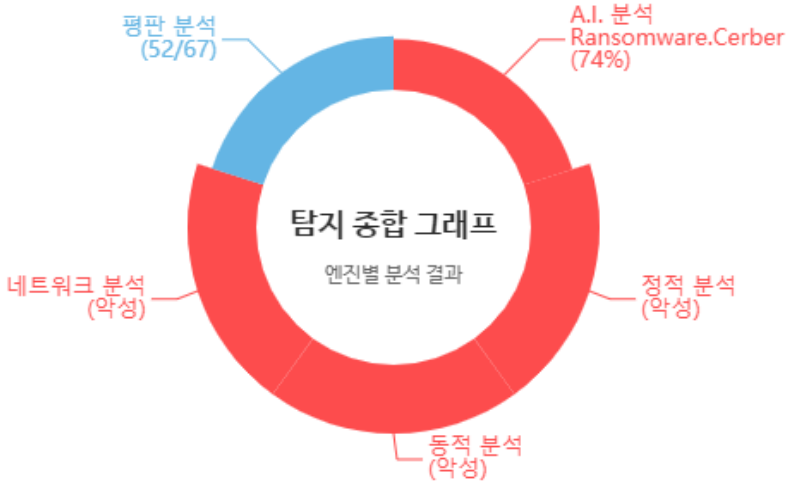
-〉 다차원 분석 시스템에서 나오는 결과들을 종합적으로 판단하여 **확진명**과 **위험도** 제공

-〉 정제되고 해석된 요약 결과뿐만 아니라, 각 엔진 별로 상세한 탐지 결과, 판단 근거, 데이터 제공

■ **자체 개발 엔진과 탐지 패턴**

-〉 12년 동안의 알약(Anti-Virus) 운영 노하우와 데이터, 분석 기술, 시스템 집약

-〉 이스트시큐리티가 자체 개발한 분석 엔진과 탐지패턴으로 위협 탐지 (평판 엔진 제외 : Virustotal)



엔진별 분석 결과

A.I. 분석	Ransomware.Cerber	74%
정적 분석	EXE_32bit외 1건	악성
동적 분석	ModifyDummyFile외 12건	악성
네트워크 분석	Cerber외 1건	악성
평판 분석	주요 백신 탐지 (52 / 67)	78%

위협 인텔리전스 솔루션 Threat Inside Reference

Threat Inside

웹서비스
ThreatInside.com

API 서비스

On-premise
(구축형)

2015
1개

경찰청

사이버 수사 업무와 관련된 파일의 악성 여부를 판단하고 연관된 분석 정보를 제공하는 시스템

2016
2개

금융보안원

대한민국 주요 금융기관과 관련된 다양한 샘플을 수집하여 악성 여부를 검증하는 솔루션

2017
4개

KISA

국내 도메인을 통해 유포되는 악성코드를 탐지하고 대응하기 위한 정적/동적 분석 솔루션

KT

'지능형 보안 플랫폼' 악성코드를 분석하고 위협 인텔리전스를 추출, 제공하는 솔루션

2018
9개

Malaysia CSM

말레이시아 공공 CERT에서 악성코드 유포지와 위협을 관제/탐지하고 대응하기 위한 솔루션으로 도입

ThreatInside.com 정식 서비스 출시

공식 미디어데이 행사를 통해 정식 웹서비스 출시 (2018. 10. 23)

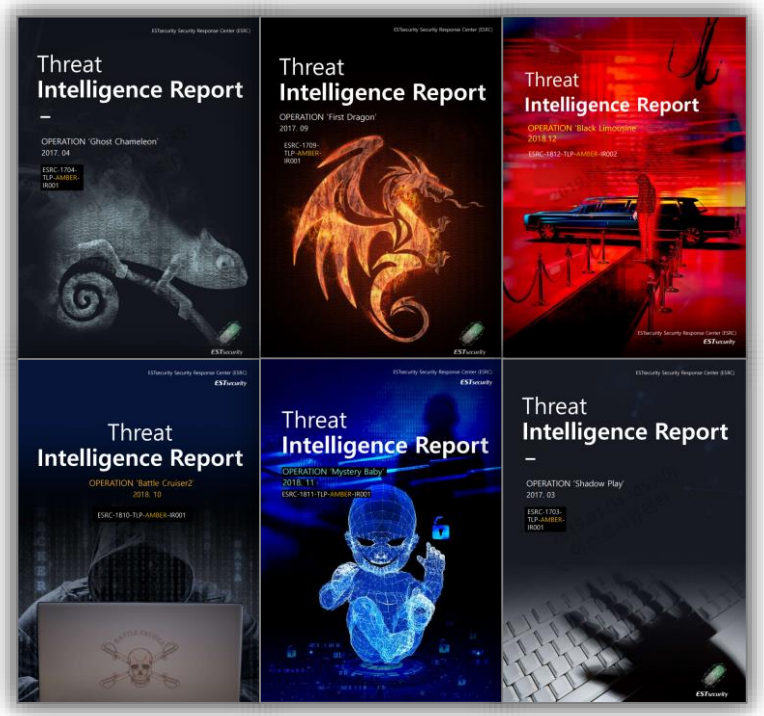
ETRI 외 4개 기관

정식 서비스 출시 이후 공공, 교육, 연구소, 금융권, IT 관련업체 등에서 도입 및 컨설팅 진행 중

이스트시큐리티 대응센터(ESRC: ESTsecurity Security Response Center)

ESRC는 실시간 모니터링 시스템을 구축하여 정부 주요 기관들과 연계한 상시 대응 체계를 유지하고 있습니다. DDos, 해킹, 랜섬웨어 등 긴급상황 발생 시 고객사를 포함한 민간의 피해를 최소화하고자 하며, 전용 백신 개발 및 배포를 통해 위기 상황에 신속하게 대응하고 있습니다. 또한 국가기반 위협 그룹에 대한 체계적인 인텔리전스 연구와 추적을 통해 '위협 인텔리전스 리포트'를 발행하고 있습니다.

* 위협 인텔리전스 리포트
APT 관련 사건을 심층적으로 분석하고 추적하여 최상위 레벨의 종합 인텔리전스 제공
공격자의 전략, 기술 절차(TTPs)에 따른 체계적인 코드 분석 내용과 원본 샘플, 침해 지표(IOC) 포함



위협 인텔리전스 리포트 2018.12.19
안보·외교·통일 관련 분야를 겨냥한 APT 공격, '작전명 블랙 리무진' 주의
증전선언 | 개인정보활용동의서 | 미국_정상회담_전망_및_대비 | padosori.co.kr/_controller/admin/upload_sec/down.php
artndesign2.cafe24.com/skin_board/s_build_cafeblog/exp_include/img.png | rentcartoday.com/home/skin_member/mem_standard/lib/upload/down.php
FF9EFF561FD793DDB9011CF7006D5F6C | 8332BE776617364C16868C1AD6B4EFE7
TLP:AMBER

위협 인텔리전스 리포트
국제 정세 문서 파일을 미끼로 정보를 노리는 '오퍼레이션 디코이 플레인(Operation Decoy Plane)'
Konni | phpschboy.prohosts.org | jams481.site.bz | minvostokarzvitia.webatu.com | dowhelsitjs.netau.net | patchfilepacks.net23.net
member-daumchk.netai.net | donkeydancehome.freeiz.com | 59D39C774D48137D2A91E286F47626F0 | BC95C7A5713760EB7D39CA0976F2FFD5

해외 인용 사례 (ESRC – Threat Intelligence Report)

- N. Korean hackers suspected of continuing attacks amid friendly inter-Korean relations
- North Korean hacker group infiltrates popular South Korean
- Alien Vault : Operation Mystery Baby
- Alien Vault : Operation Ghost Puppet
- Geumseong121が政府を騙って北朝鮮関連団体に調査依頼のデコイで仕掛けている模様。
- 韓国で新たな規制法案も：度重なる大手取引所ハッキング被害
- 借南北韓離散家庭團聚　黑客發釣魚攻擊
- Вредонос KevDroid способен тайно записывать телефонные звонки жертв
- کشف بدافزاری که تماس‌ها را پنهانی ضبط می‌کند

(이하 생략)

이스트시큐리티 "통일부 기자들 겨냥 해킹 메일 발견"

이스트시큐리티, 입사지원 사칭 메일로 '갠드크랩 랜섬웨어' 국내 확산 중

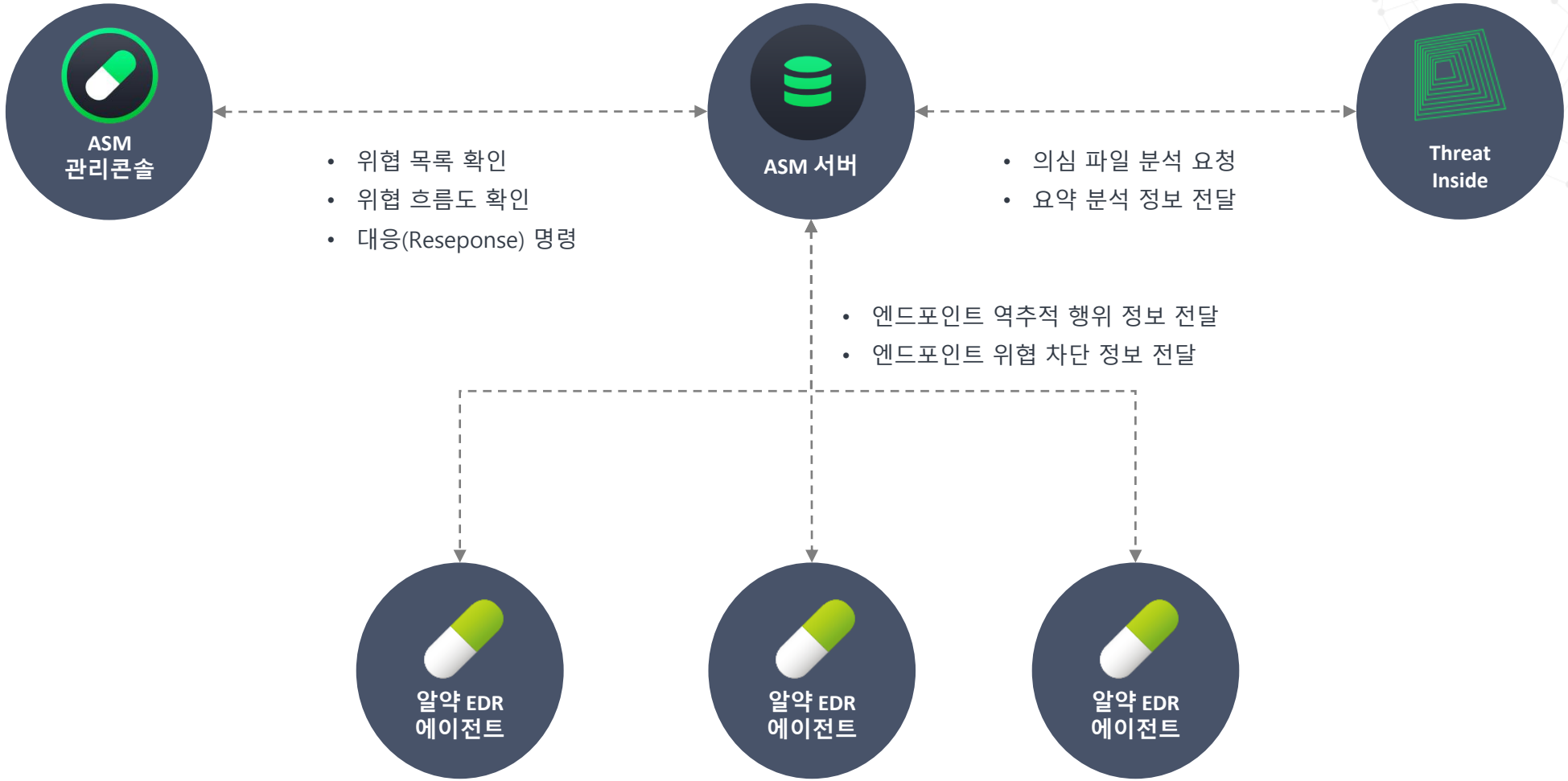
"홈택스 사칭 악성메일로 갠드크랩 랜섬웨어 유포"
이스트시큐리티 "연말정산 관련 위장 메일로 랜섬웨어 유포중…출처 불분명한 이메일 주의해야"

이스트시큐리티, '2019년 북한 신년사 평가 내용' 담은 APT 악성코드 발견

PART 05

제품 구성 및 사양

제품 구성도


ASM
관리콘솔
• 위협 목록 확인
• 위협 흐름도 확인
• 대응(Reseponse) 명령
ASM 서버
• 의심 파일 분석 요청
• 요약 분석 정보 전달
Threat
Inside
• 엔드포인트 역추적 행위 정보 전달
• 엔드포인트 위협 차단 정보 전달
알약 EDR
에이전트
알약 EDR
에이전트
알약 EDR
에이전트

제품사양

HW 설치 환경

		CPU	RAM	HDD
서버	최소	알약 EDR 운영을 위한 서버의 HW 권장 사양은 고객사 환경에 따라 차이가 있습니다. 별도의 상담을 통해 내용 확인이 가능합니다.		
	권장			
관리콘솔	최소	Intel Dual Core 1Ghz	1GB	1GB 이상 여유공간
	권장	Intel Dual Core 2Ghz	2GB	2GB 이상 여유공간
에이전트	최소	Intel Dual Core 1Ghz	512MB	500MB 이상 여유공간
	권장	Intel Dual Core 2Ghz	1GB	1GB 이상 여유공간

SW 설치 환경

	OS	DB
서버	Windows Server 2003 SP2 이상/ 2008 / 2012 / 2016 (R2 포함) Microsoft Windows 7 / 8 / 8.1 / 10 (모든 OS 64bit 지원) CentOS 6.x 이상	MariaDB(내장) Windows XP SP3 이상 기존 DB 설치 시 MSSQL 만 지원
관리콘솔	Windows Server 2008 SP2 / 2012 / 2016 (R2 포함) Microsoft Windows Vista SP2 / 7 / 8 / 8.1 / 10 (모든 OS 64bit 지원)	
에이전트	Windows Server 2003 SP2 이상 / 2008 / 2012 / 2016 (R2 포함) Microsoft Windows XP SP2 / Vista / 7 / 8 / 8.1 / 10 (모든 OS 64bit 지원)	

감사합니다

ESTsecurity
이스트시큐리티 서울시 서초구 반포대로 3 이스트빌딩 (우) 06711