

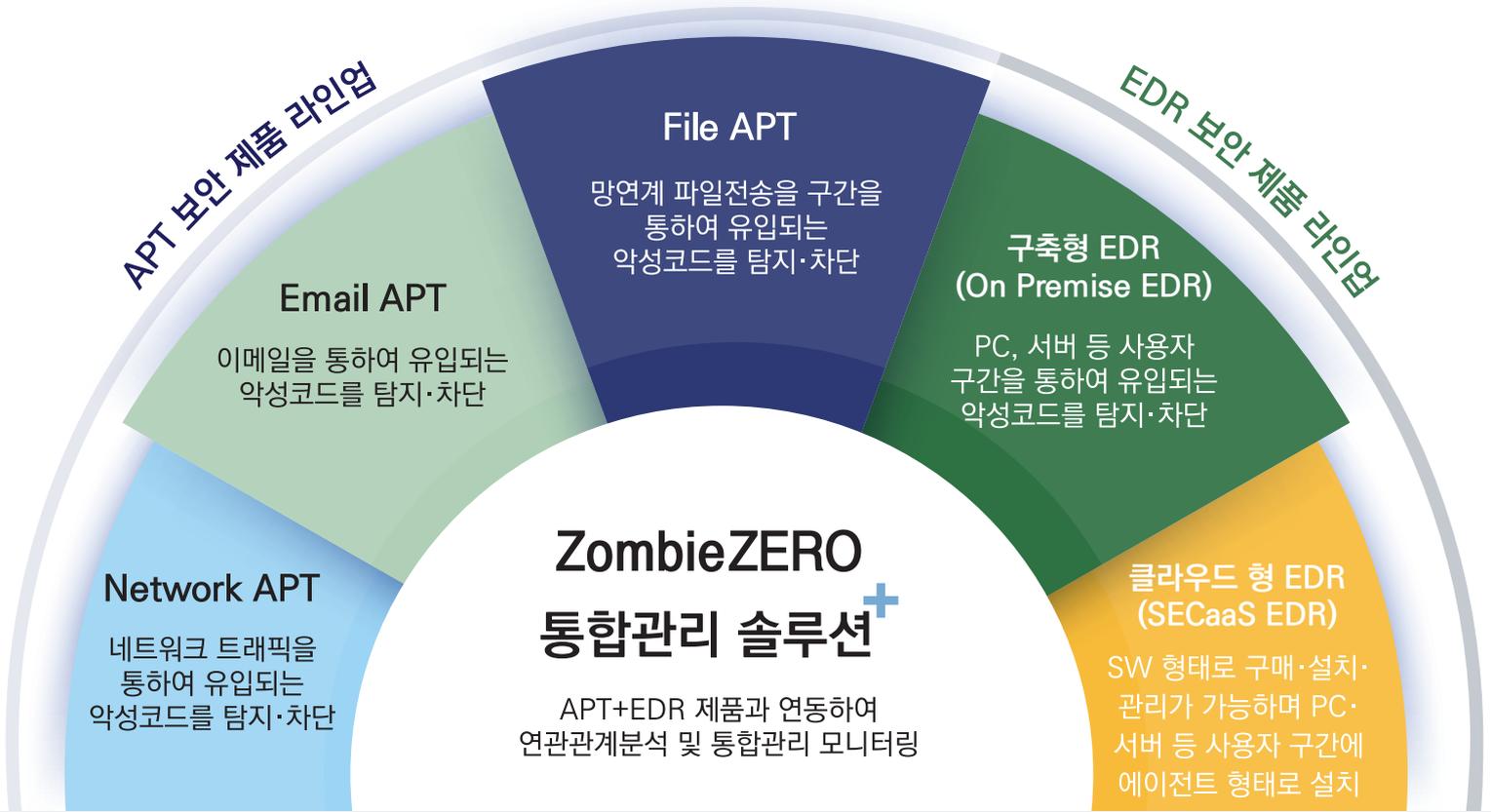
Zombie ZERO

AI기반 신·변종 악성코드 및 랜섬웨어 대응 솔루션



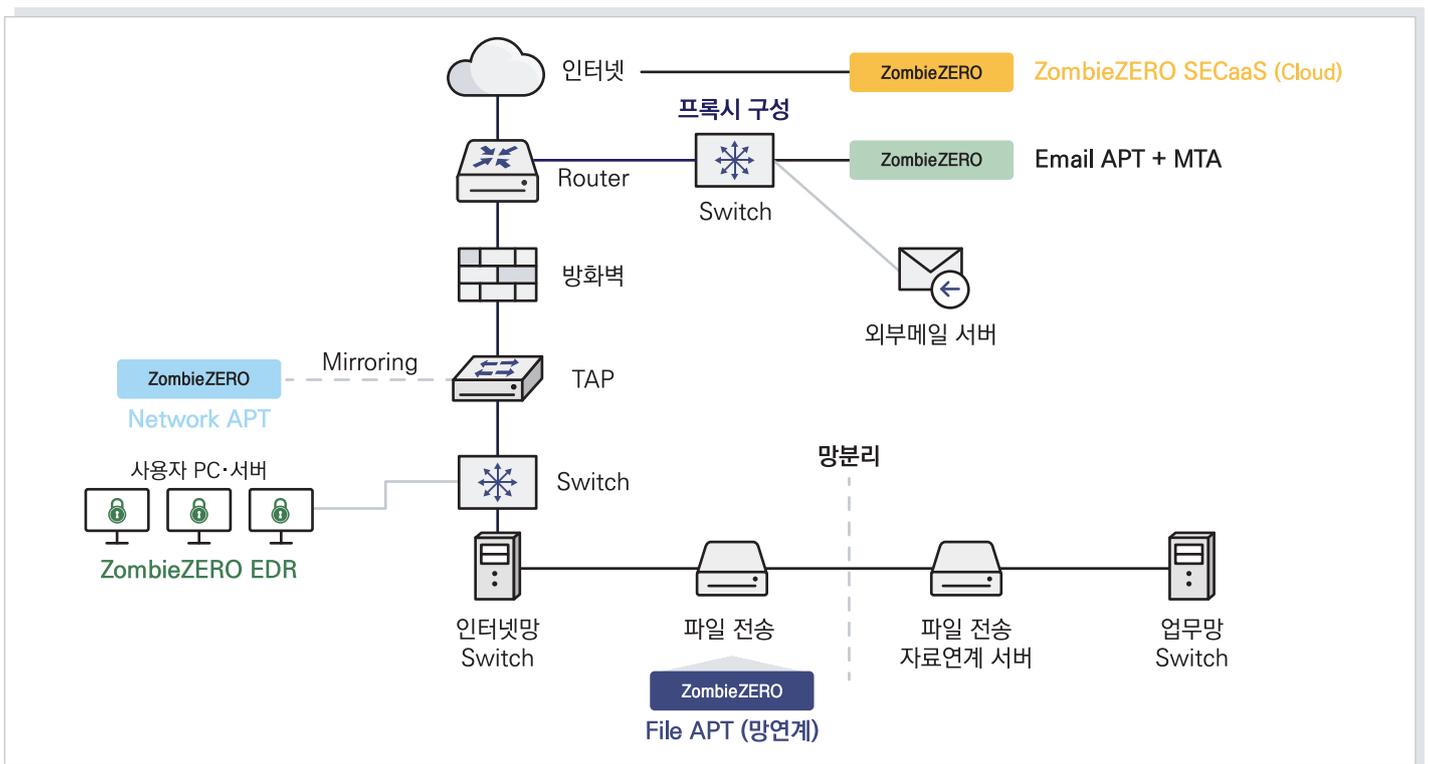
● ● ● ● ● ● ● ●
사이버 위협으로부터 안전한 보안 환경을 구축해드립니다.

랜섬웨어, 지능형 지속위협(APT) 등 신·변종 악성코드를 탐지·차단하는 SI기반 행위 분석 보안 솔루션



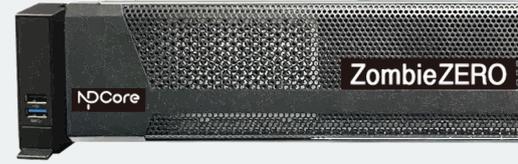
ZombieZERO 시스템 구성도

· 악성코드가 유입될 수 있는 다양한 경로에 솔루션 구축 가능



| ZombieZERO APT

어플라이언스 형태의 일체형 보안솔루션 (HW+SW)
네트워크·이메일·파일 (망연계 구간)에 구축



Network APT

행위기반 분석을 통해 기존 시그니처 기반의 보안 시스템이 탐지하지 못하는 **Zero-day 취약성 보완**

- 파일 유입 및 유출에 대한 양방향 네트워크 트래픽 모니터링
- 주요 인터넷 서비스 프로토콜 수집 및 분석
- 유해사이트 접근 및 C&C 통신 시 탐지·차단

Email APT

악성코드에 취약한 기존의 시그니처 기반 **스팸메일 솔루션의 한계 보완**

- APT와 MTA (메시지 전송 에이전트) 통합
- 스팸·스피어피싱·악성코드가 포함된 메일에서 악성 정보만 차단
- 이메일 첨부파일 및 URL 분석 후 정상 메일만 메일서버로 전송

File APT

외부망과 내부망 사이에서 파일 전송이 이루어지는 망연계 구간에서 **서버 보호**

- 망연계 솔루션과 연동하여 이동 대기 중인 파일에 대한 분석·차단
- 분석된 파일을 분류하여 **정상**으로 판단된 파일만 **업무**망으로 전송
- 공유 폴더(SMB·NFS·Web API 등)를 이용한 분석 결과 전달

도입효과

· APT 제품 및 EDR 제품 동시 구축 시 적용

<p>악성코드, 랜섬웨어 대응</p> <p>백신이 탐지할 수 없는 알려지지 않은 신·변종 악성코드 탐지·차단하여 사전에 대응 가능</p>	<p>엔드포인트 가시성 확보</p> <p>엔드포인트에서 발생하는 사이버 공격의 구체적인 진행 상황 확인으로 가시성 확보</p>	<p>악성코드 침입 가능성 예방</p> <p>악성코드 침입 경로와 시스템 간의 연결을 확인하여 내부에서 취약한 부분을 보완하여 보안 강화</p>	<p>보안제품 도입비용 절감</p> <p>랜섬웨어 대응, 백업 그리고 일부 백신 기능이 내장되어 있어 별도의 제품 구매 불필요</p>
---	--	---	--

| ZombieZERO EDR

PC, 서버 등 사용자 구간을 통하여 유입되는 악성코드를 탐지·차단
온프레미스 / 클라우드 2가지 방식으로 구축



주요기능



실시간 랜섬웨어 행위 탐지·차단

- 랜섬웨어의 파일 암호화 및 위·변조 대응
- 글로벌 백신 Bitdefender의 AV 기능 지원



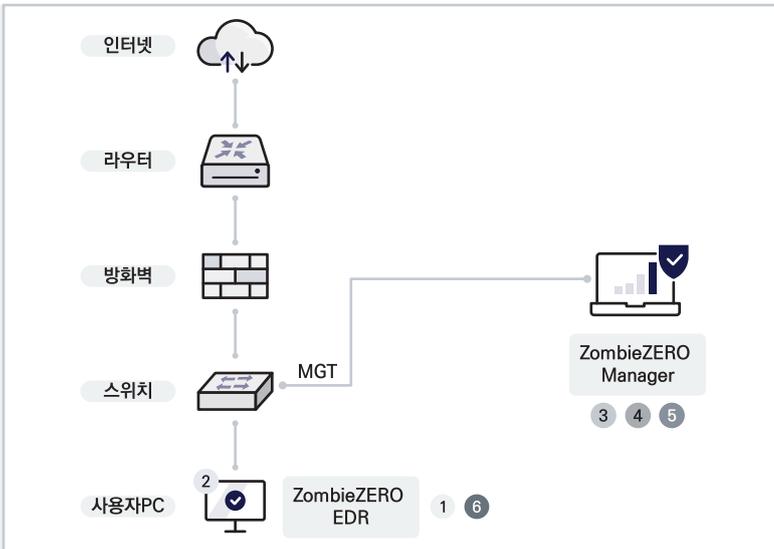
Zero Trust 보안 (실행보류 기능)

- 신규 파일의 유입 또는 위협 파일 실행 시 파일의 실행을 보류하여 분석 서버로 정보 업로드



IOC 기반의 실시간 위협 탐지

- 사용자 단말의 행위에 대한 침해지표 (IOC) 탐지 (네트워크, 파일, 프로세스, 레지스트리 등)

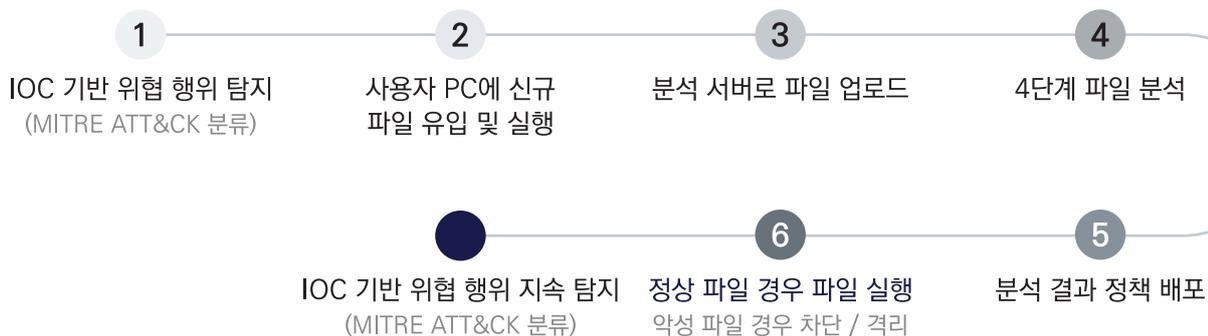


ZombieZERO SECaaS

ZombieZERO EDR의 클라우드 서비스

- 전용 웹페이지를 통하여 에이전트 형태로 설치
- 웹에서 구매·설치·중앙관리 등 전체 기능 제공
- 사용자 관리 및 편의성이 높고, H/W 도입 비용 X
- 중소기업과 원격·재택 근무 환경에 적합한 서비스

EDR 탐지 및 분석 기능 흐름도



ZombieZERO UI

- 관리자가 빠르고 정확한 상황 파악을 할 수 있도록 시각적 디자인 적용
- 권한을 가진 사용자만 접근 가능한 인증 및 권한 제어 기능으로 보안 강화



주요 공통 기능

다차원 분석



AV·정적분석·동적분석·평판분석 등 다차원 탐지·분석

가상머신 우회 방지



리얼머신과 동일한 동적 행위 분석 제공

MITRE ATT&CK 분류



악성행위 MITRE ATT&CK 기준 탐지

악성행위 흐름도 제공



침해지표 (IOC)에 따라 공격 형태 상세정보 및 모니터링 기능 제공

ECSC 공식 연동



교육부 사이버안전센터 Yara Rule 연동

시 기반 악성코드 탐지



시 기반의 빠르고 정확한 악성코드 탐지 기술

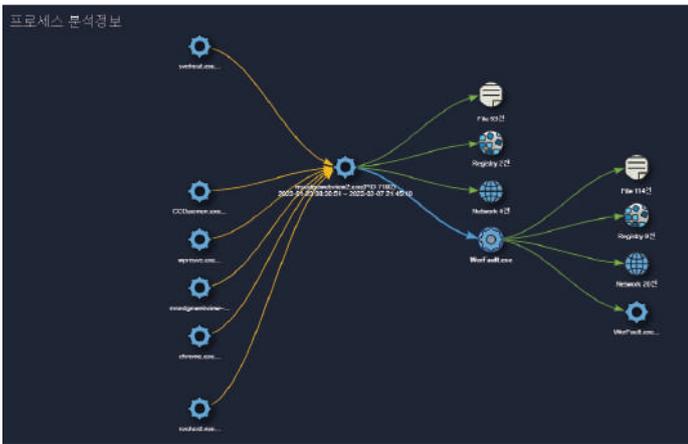
다차원 분석

- 외부에서 내부로 네트워크를 통하여 유입된 트래픽을 다차원 분석으로 악성코드 탐지·차단

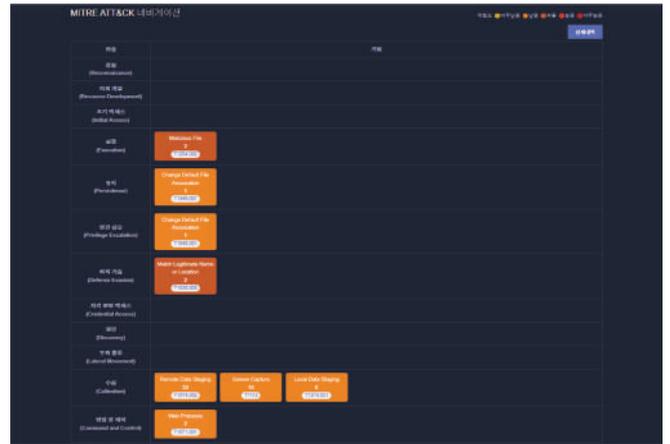


MITRE ATT&CK · 악성행위 흐름도

- 공격의 결과가 아닌 진행 중인 공격에 대한 기술 및 방법의 형태 모니터링



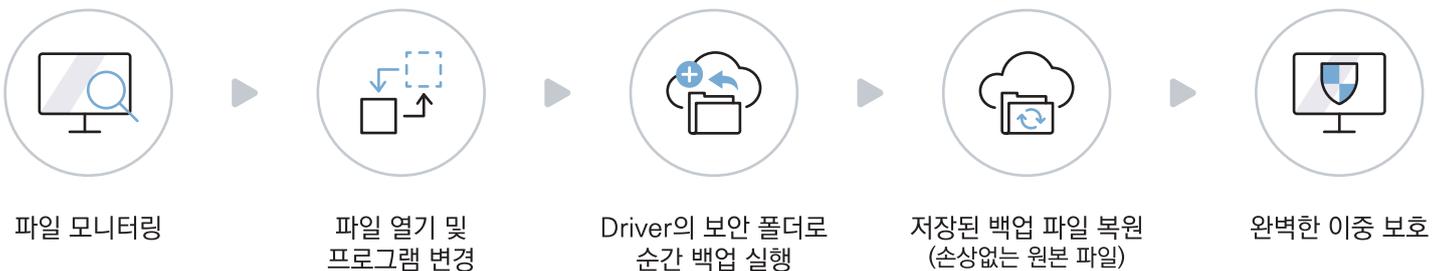
프로세스 분석 정보 (악성행위 흐름도)



MITRE ATT&CK 네비게이션

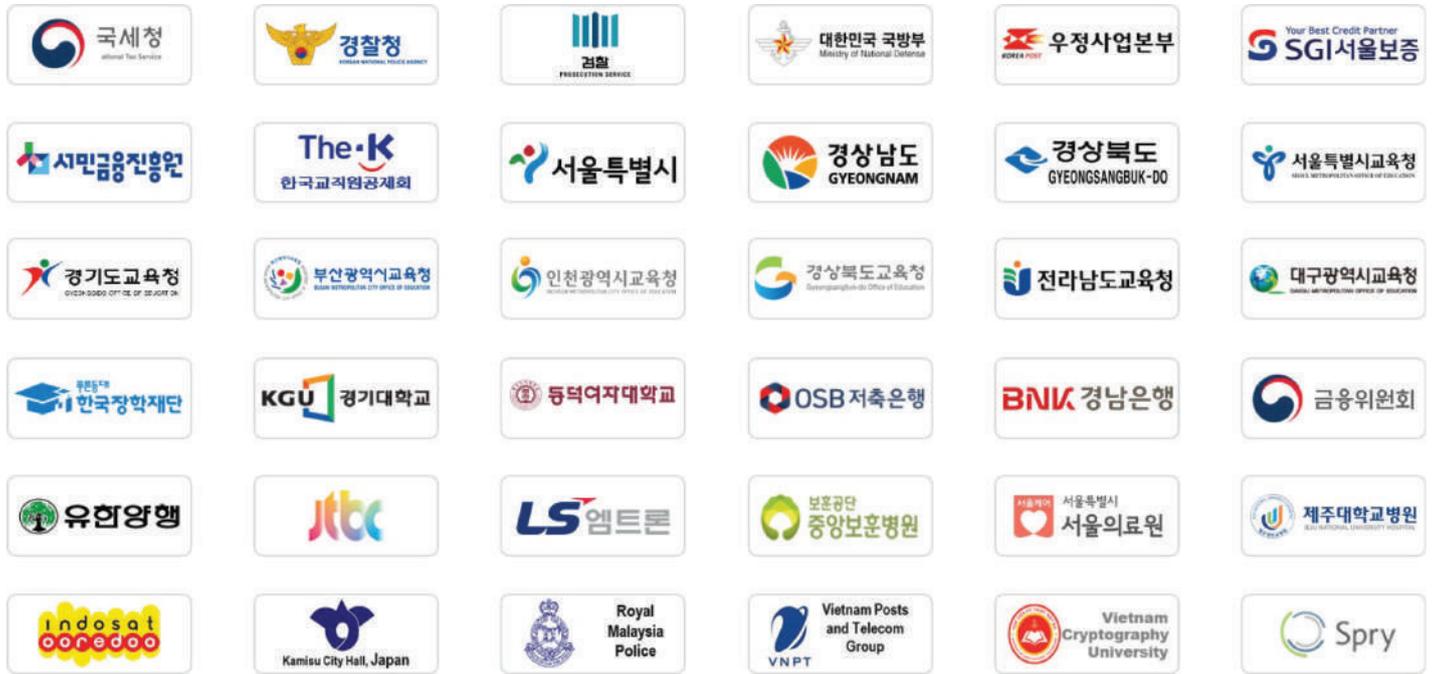
실시간 순간 백업

- 파일 변조 직전의 순간, **일반 프로세스가 접근할 수 없는 보안 폴더**에 파일을 백업
- 커널 드라이버단에서의 백업 실행으로 **어플리케이션간 충돌 이슈와 성능 저하 없음**



레퍼런스

국내 APT 판매 1위 엔피코어는 150개 이상의 국내·외 레퍼런스를 보유하고 있습니다.



인증 및 특허

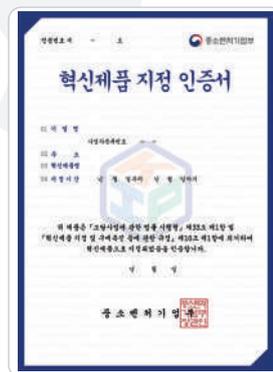
국제 CC인증·GS인증·혁신제품 인증·보안기능확인서를 보유하고 있으며, 미국 2건, 일본 1건을 포함하여 14건의 특허를 등록하였습니다.



국제 CC 인증



GS 인증 1등급



혁신제품 인증



보안기능확인서

