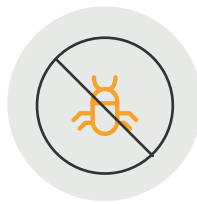
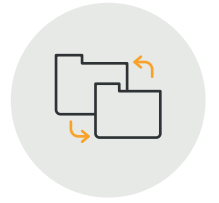




Zombie ZERO

APT · 랜섬웨어 OUT! 신변종 악성코드 대응 솔루션



랜섬웨어 / APT OUT !

신변종 악성코드 대응 솔루션

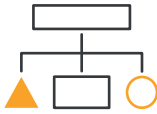
ZombieZERO

랜섬웨어, 지능적 지속위협(APT) 등
신변종 악성코드를 탐지/차단하는
AI기반의 행위 분석 보안솔루션



특장점

AI기반 신변종 악성코드 대응 솔루션 ZombieZERO

다차원 분석  AV/정적/동적/평판 등 다차원 분석 기능	가상머신 우회 방지  리얼머신과 동일한 동적 행위 분석 제공	MITRE ATT&CK 분류  MITRE ATT&CK 분류 및 카테고리화 적용
악성 행위 흐름도 제공  공격 형태 상세 정보 및 모니터링 기능 제공	ECSC 공식 연동  교육부 사이버안전센터 Yara Rule 연동	AI기반 악성코드 탐지  AI기반의 빠르고 정확한 악성코드 탐지 기술

ZombieZERO APT

좀비제로 APT 대응 솔루션

다양한 구간을 통해 유입되는 악성코드를 탐지/차단

- 어플라이언스 형태의 일체형 보안솔루션(HW+SW)
- 네트워크 / 이메일 / 망연계 구간에 구축



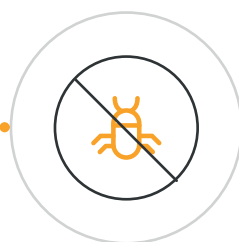
주요기능



Sandbox 기반의
악성 행위 분석

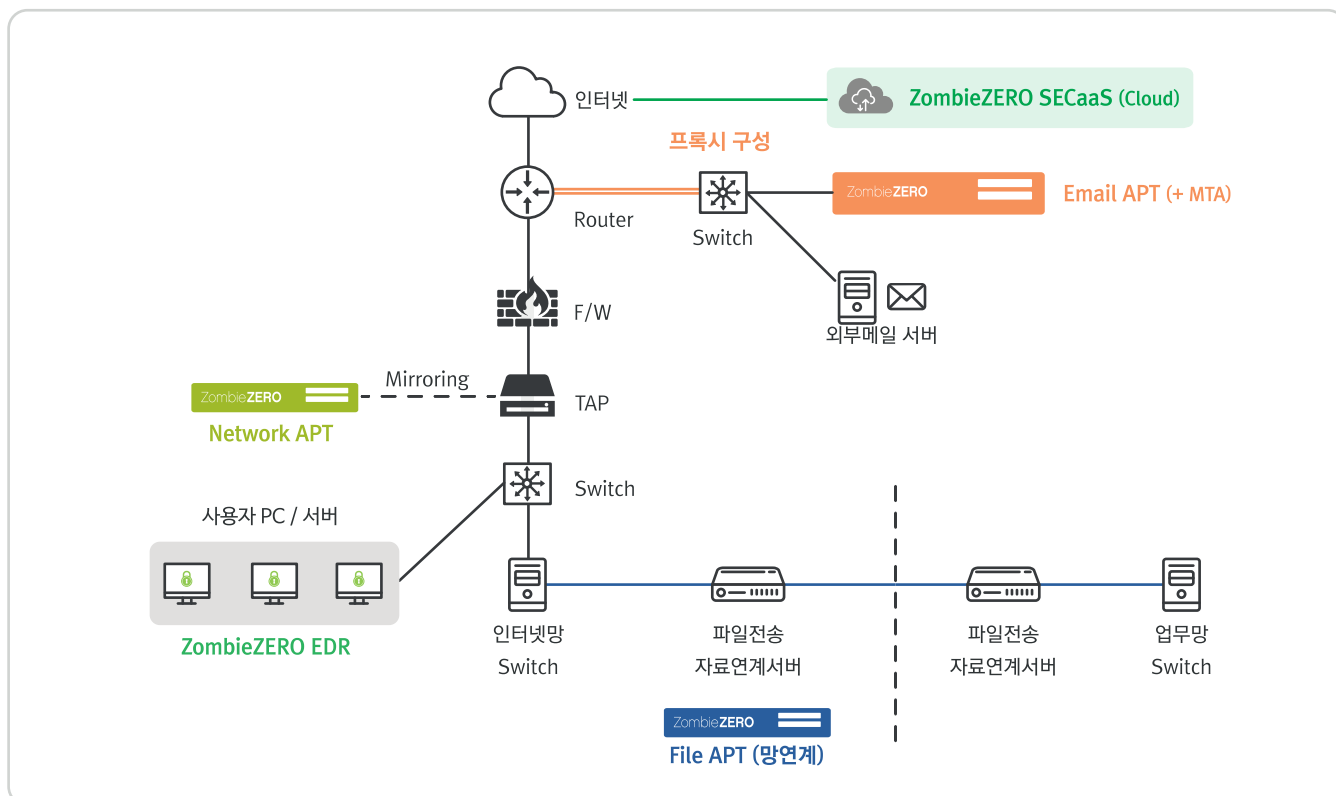


MITRE ATT&CK
분석 정보 제공



다차원 분석을 통한
신변종 악성코드 탐지

ZombieZERO 구성도



ZombieZERO EDR

좀비제로 EDR (Endpoint Detection and Response)

PC, 서버 등 사용자 구간을 통하여 유입되는 악성코드를 탐지/차단

- 에이전트 형태의 소프트웨어 보안솔루션
- 온프레미스 / 클라우드 2가지 방식으로 구축



주요기능



실시간 랜섬웨어 행위 탐지/차단

랜섬웨어의 파일 암호화 및 위변조 대응
글로벌 백신 Bitdefender의 AV 기능 지원



NPCore ZeroTrust 보안

신규 파일의 유입 또는 위협 파일 실행 시
파일의 실행을 보류하여 분석 서버로 전송



IOC기반의 실시간 위협 탐지

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



ZombieZERO SEaaS

ZombieZERO EDR의 클라우드 서비스

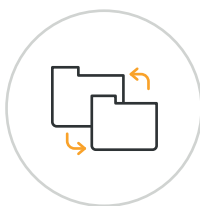
- 전용 웹페이지를 통하여 에이전트 형태로 설치
- 웹에서 구매 / 설치 / 중앙관리 등 전체 기능 제공
- 사용자 관리 및 편의성이 높고, H/W 도입 비용 없음
- 중소기업과 원격/재택 근무 환경에 적합한 서비스

실시간 순간 백업

- 파일 변조 직전의 순간, 일반 프로세스가 접근 할 수 없는 보안 폴더에 파일을 백업
- 커널 드라이버단에서의 백업 실행으로 어플리케이션간 충돌 이슈와 성능 저하 없음



파일
모니터링



파일 열기 및
프로그램 변경



Driver의 보안 폴더로
순간 백업 실행



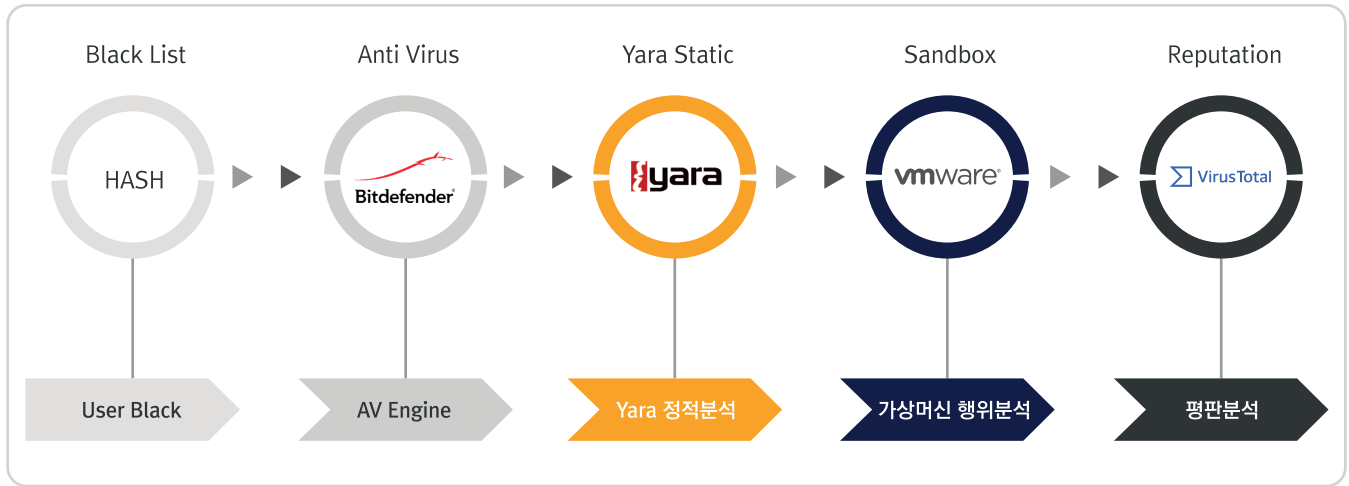
저장된 백업 파일 복원
(손상 없는 원본 파일)



완벽한 이중 보호

다차원 분석

- 시그니처/정적/동적 분석 등의 알려지지 않은 악성코드 다차원 분석



가상머신 우회 방지

- 01 가상머신 우회 방지 기술 실행 : CPU ID 정보 변경, 가상머신 고유정보 숨기기 등
- 02 악성코드는 가상머신을 리얼머신으로 인식하여 악성 행위를 실행
- 03 악성 행위에 대한 동적 분석을 진행하여 악성코드를 차단

MITRE ATT&CK / 악성 행위 흐름도

- 표준화된 MITRE ATT&CK 분류에 맞는 악성코드의 카테고리화 적용
- 악성 행위 흐름도 제공을 통한 공격 방법에 대한 상세 정보 및 모니터링 기능 제공



제품 라인업

APT Security



Network APT



Email APT



File APT



통합관리 솔루션

EDR Security



EDR



SECaaS

교육부 ECSC 공식 연동

- 2018년 MTM(APT) 부문 **적합** 판정을 받은 유일한 APT 솔루션
- 전남 / 경북 / 대구 교육청 등 다수의 **ECSC 연동 실적 보유**



인증 및 특허

국제 CC인증 / 국내 CC인증 / GS인증 보유
미국 특허 2건을 포함한 12건 이상의 특허 등록



인증내역

- “ZombieZERO Inspector V3.0” 국내CC (EAL2 인증)
- “ZombieZERO Inspector V3.0” GS 인증
- “ZombieZERO Inspector V4.0” 국제CC (EAL2 인증)

국내외 특허 등록 - 12건

- APPARATUS AND METHOD FOR BLOCKING ZOMBIE BEHAVIOR PROCESS
- MALICIOUS CODE DEACTIVATING APPARATUS AND METHOD OF OPERATING THE SAME
- 악성 코드 차단 장치 및 이의 동작 방법

기대 효과



Security

다차원 탐지/분석
가상머신 우회 방지



Profit

경쟁사 대비
합리적 비용



Flexibility

교육부 사이버안전센터
ECSC 공식 연동



Safety

수집 전용 가속보드
IOC 침해지표 탐지



Innovation

MITRE ATT&CK 분류
실시간 순간 백업