어서오세요.
어떤 보안 솔루션을 찾으시나요?

EDR?

XDR?

APT?

RansomZERO?

NPCore
(주)엔피코어

AI기반 랜섬웨어, 신·변종 악성코드 탐지 및 대응 보안 솔루션

ZombieZERO APT
Network | Email | File

APT 대응 · 어플라이언스

ZombieZERO EDR
엔드포인트 보안 솔루션

구축형 · APT 연동 O

ZombieZERO XDR
통합 위협 분석 및 대응 플랫폼

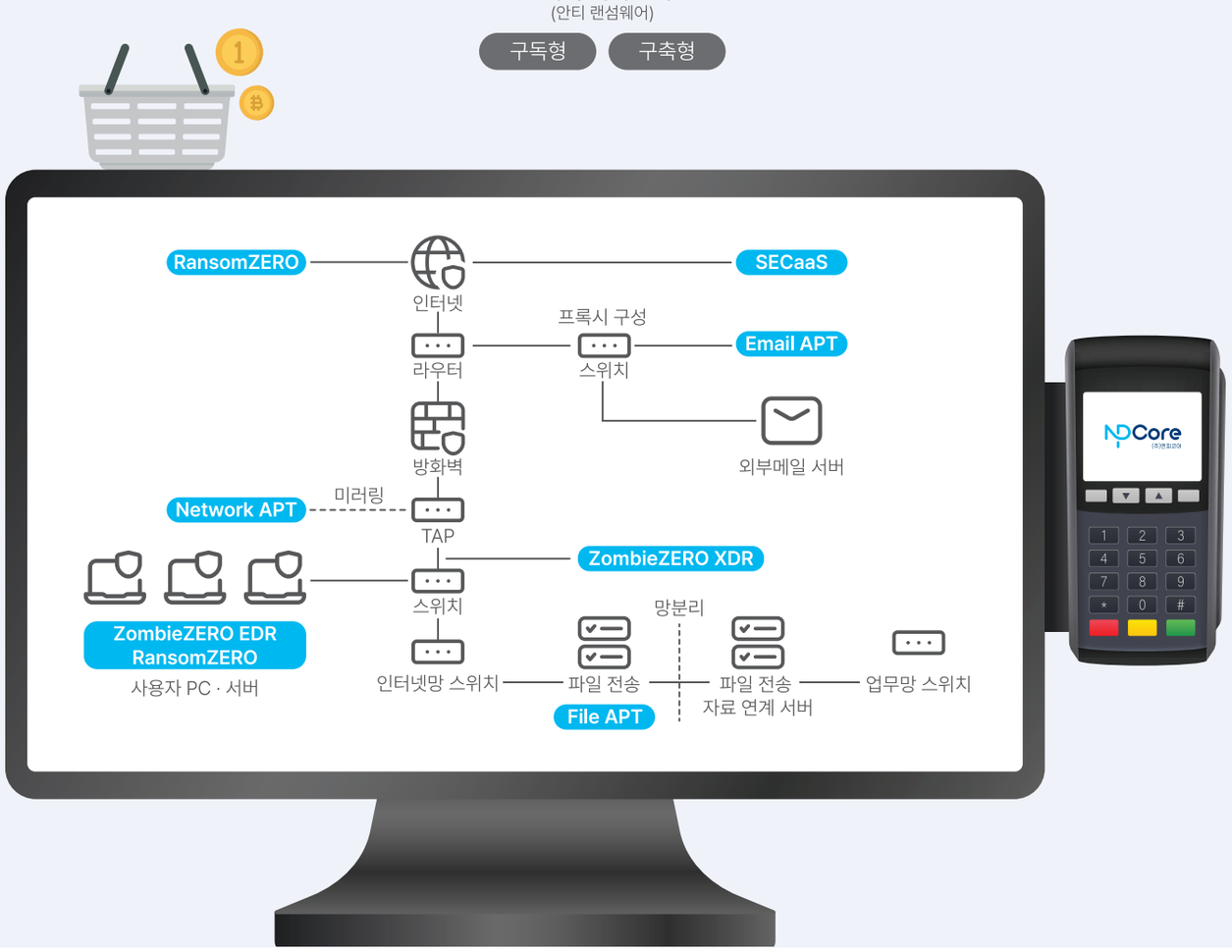
플랫폼

ZombieZERO SECaaS
소기업 환경에 적합한 보안 솔루션

구독형 · 에이전트

RansomZERO
랜섬웨어 특화 솔루션
(안티 랜섬웨어)

구독형 · 구축형



RANSOMZERO
랜섬제로

국내 최초 국정원 가이드 라인 적용한 **'랜섬웨어 대응' 유형**
보안기능확인서 인증받은 **딥러닝 (AI분석)솔루션**

랜섬웨어도 이제는 ZERO 시대

당신의 데이터를 지키는 완벽한 방패!

실행보류 및 사전탐지
실행보류 (제로트러스트)
ML백신 (AI 딥러닝 분석)
목록기반 블랙리스트

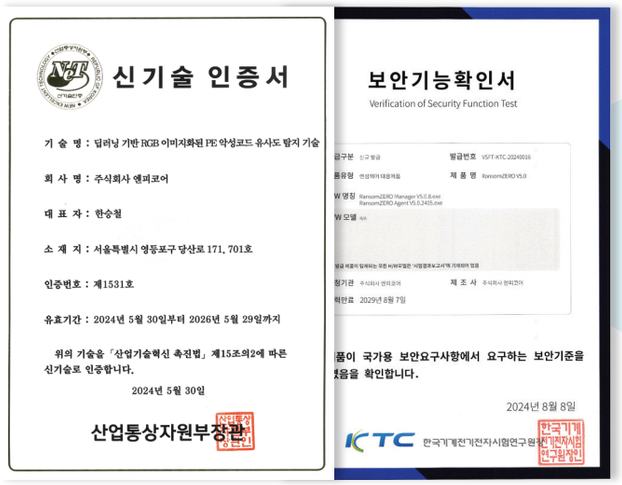
실시간 복원
실시간 순간백업 (복원)
스케줄 백업 (복원)

실시간 행위기반 탐지
임계치 기반 탐지
더미 파일 암호화 탐지
MBR 부트영역 접근 탐지
랜섬웨어 차단 · 격리 · 제거

딥러닝 (AI분석)
신규 파일 유입 시(네트워크) 및
엔드포인트에서 수집된 정보를
RGB 이미지로 변환
딥러닝 분석하여 신변종 악성코드 탐지

'RGB 이미지화된 PE 악성코드 유사도 탐지 기술'
NET(신기술)인증 기술 적용

- 유사도 기반 탐지율 98.8%, 0~2^{24} 범위 내 데이터 손실 없는 파일 변환
- 이미지화된 데이터로 알려지지 않은 악성코드 탐지
- 0.06초 내 고속 분석 및 가상 머신 우회 탐지 가능



신 기 술 인 증 서

기 술 명 : 딥러닝 기반 RGB 이미지화된 PE 악성코드 유사도 탐지 기술

회 사 명 : 주식회사 엠피코어

대 표 자 : 한승철

소 재 지 : 서울특별시 영등포구 당산로 171, 701호

인증번호 : 제1531호

유효기간 : 2024년 5월 30일부터 2026년 5월 29일까지

위의 기술을 「산업기술혁신 촉진법」 제15조의2에 따른 신기술로 인증합니다.

2024년 5월 30일

산업통상자원부장관

보안기능확인서
Verification of Security Function Test

품이 국가용 보안요구사항에서 요구하는 보안기준을 음을 확인합니다.

2024년 8월 8일

KTC 한국기계전기전자시험연구원

인공지능 기반 확장 탐지 및 위협 자동 판단 및 대응 솔루션

ZombieZERO XDR

비 전문가라도 신속·정확한 위협 대응 가능

데이터 소스의 상호 연관을 통해
평균 탐지시간 단축

분류를 가속화, 조사 및 범위 지정 시간을
줄여서 평균 조사시간 단축

간단하고 빠르게 관련성이 높은 자동화 구현,
평균 대응시간 단축

위협의 가시성 확보를 통해 사이버킬체인 전략수립 가능

단말 및 네트워크에서 발생되는
모든 이벤트 수집

각각의 솔루션이 아닌 전체 보안에
대한 가시성 향상

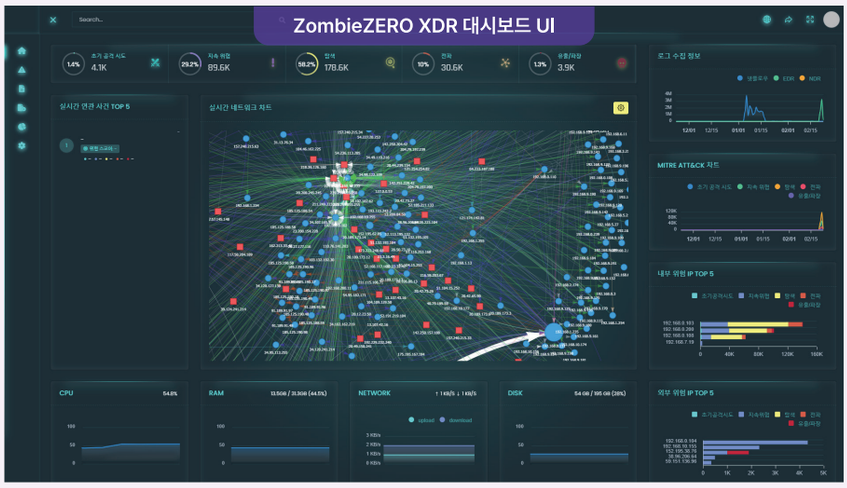
사이버 공격 발생 시, 연동 분석을 통한
공격현황 파악 및 대응판단

통합 및 확장하여 자동화 분석

여러 보안요소를 통합 및 확장하여 분석

분석가의 개입없이 최종판정

자동화 기반으로 가장 효과적인
대응이 가능한 기술



What's ZombieZERO XDR?

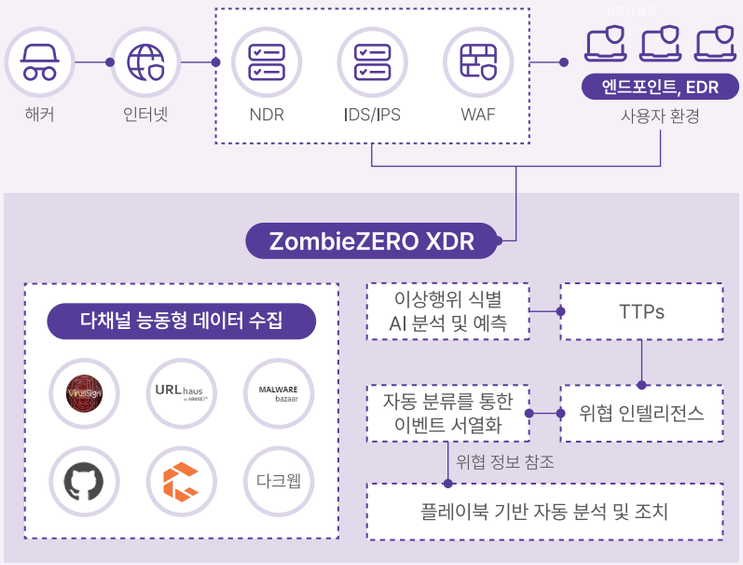
보안 요소별 탐지 체계에서 엔드포인트를 포함한
모든 보안 요소를 통합&확장하여, 위협의 실체를
탐지하고, 보안 **위협을 자동으로 판단**하고
대응 가능한 차세대 플랫폼

SOC
효율성 증대로
시간, 인력,
비용 절감

비즈니스
리스크 감소로
보안위협으로부터
기업 보호

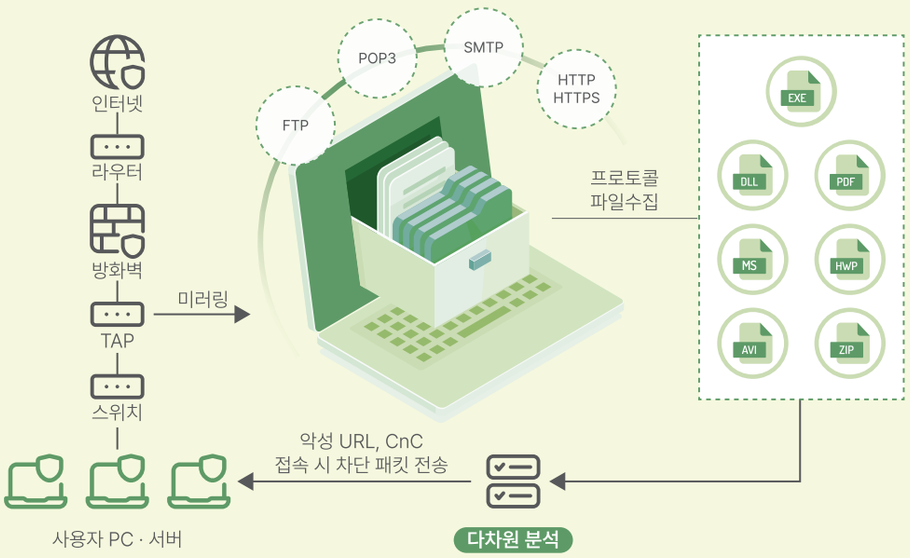
위협에 대한 예방,
차단, 탐지, 조사
그리고 대응 가능

기능 구분	구현 방식
위협판정, 위협케이스 관리	AUTO
대응 조치	
침해위협조사	AUTO Analysis
공격자 식별	
공격유형 분류	
정보 수집	엔드포인트·네트워크·보안장비
위협 인텔리전스 생성	위협 헌팅기반 (사고정보, 악성코드 유사도, 위협사이트 예측, 공격기법, 공격그룹) 제공



네트워크 트래픽을 통하여 유입되는 악성코드를 탐지/차단하는 APT 대응 솔루션

ZombieZERO Network APT



*ZombieZERO Inspector V4.0
(Network, Email, File, 통합) 인증
보안기능 확인서

위협 탐지/분석
네트워크 트래픽에서 실시간
다운로드 파일·URL 정보 추출

SSL 트래픽 분석
SSL 복호화 장비와 연계하여 암호화
트래픽을 분석하여 탐지·차단

행위기반 분석
시그니처 기반의 보안 시스템이 탐지하지
못하는 ZERO-DAY 취약성 보완

What's ZombieZERO Network APT?

네트워크 트래픽을 가속보드를 이용하여 수집하고
신변종 악성코드를 **행위기반 다차원 분석**을
이용하여 **가상 분석머신**으로 탐지 및 사전 대응

C&C 서버 접속 및 악성코드 배포 사이트 URL 접속 실시간 차단

위협에 대한 증거 기반의 위협 인텔리전스를 활용한 대응

공격 활동 기록 생성, 저장하여 포렌식 분석& 사고조사 지원

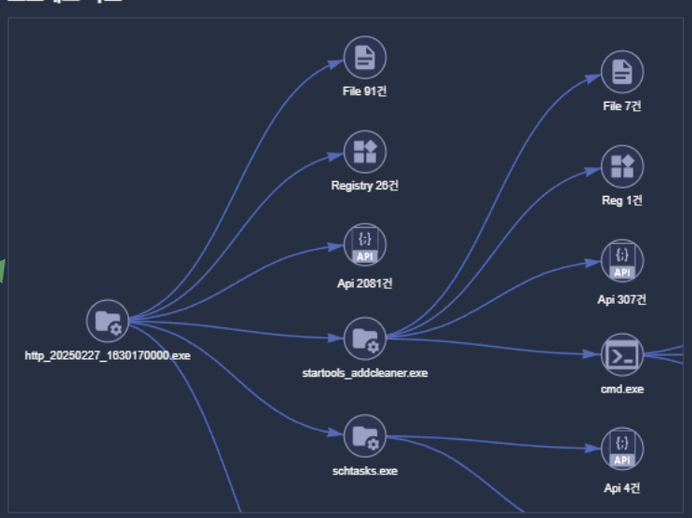
분석 요약

사전 탐지	정상
안티 바이러스	Gen:Variant.Nemesis.33109
정적 분석	●●●○○
동적 분석	●●●●●
분석 결과	악성

정적 YARA를 탐지내역

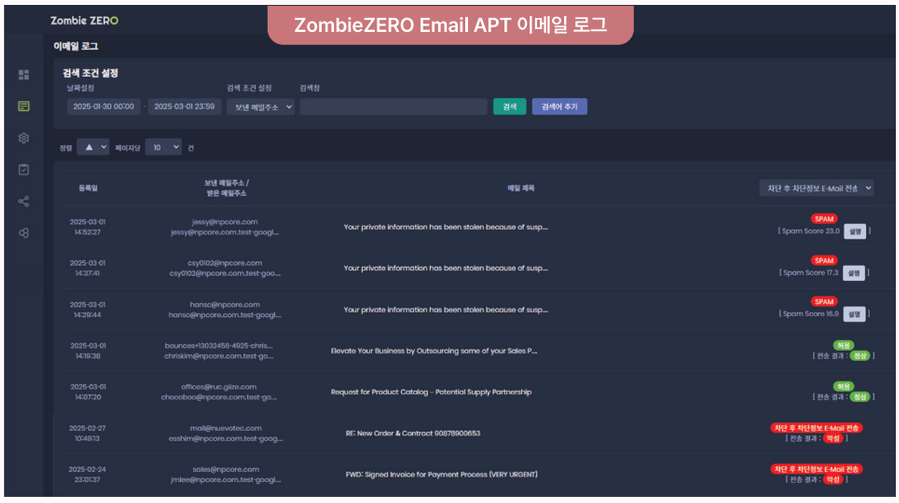
YARA	MITRE	설명	위험도
SocialEngineering	T1106 T1073 T1527	Execution through API, DLL Side-Loading, Application Access Token	●●●○○
ExecutableFile	T1204	User Execution	●●○○○

프로세스 차트

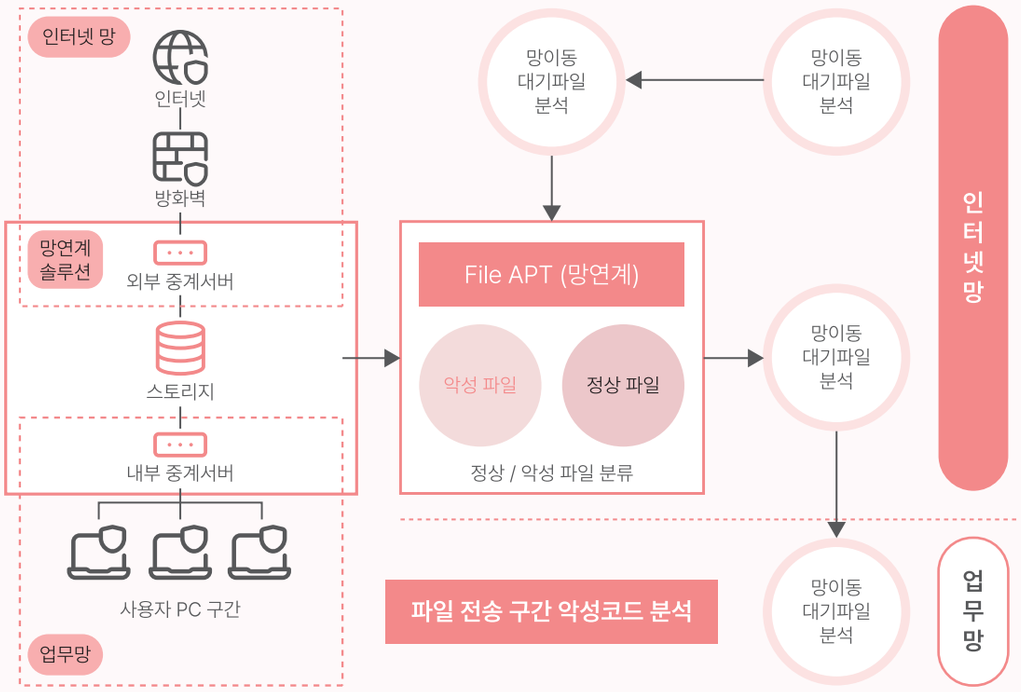


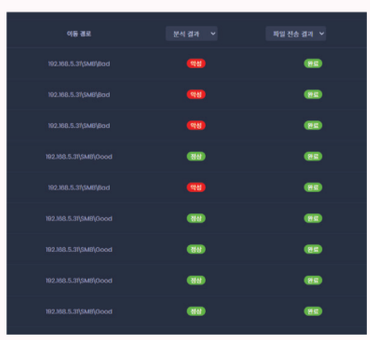
이메일·망연계 파일전송 구간을 통하여 유입되는 악성코드를 탐지/차단하는 APT 대응 솔루션

ZombieZERO Email·File APT



- 필터 규칙 / DB 연계 스팸메일 차단
- SandBOX 행위분석 (동적분석)
  악성 첨부 파일 제거 후 송신
  격리 메일 보관 및 재전송 기능
- 가용성 확보를 위한 ByPASS
  (용량 및 개수 기준 차단 / 패스 설정)





PC, 서버 등 사용자 구간을 통하여 유입되는 악성코드를 탐지/차단하는 APT 대응 솔루션

ZombieZERO EDR·SECaaS

실시간 랜섬웨어 행위 탐지·차단

랜섬웨어의 파일 암호화 및 위·변조 대응

글로벌 백신 Bitdefender의 AV 기능 지원

ZERO-TRUST보안 (실행보류 기능)

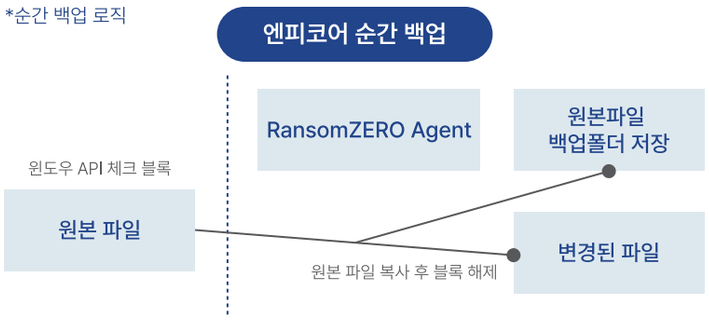
신규파일의 유입 또는 위협 파일 실행 시 파일의 실행을 보류하여 분석 서버로 정보 업로드

IOC기반의 실시간 위협 탐지

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

*순간 백업 로직

엔피코어 순간 백업



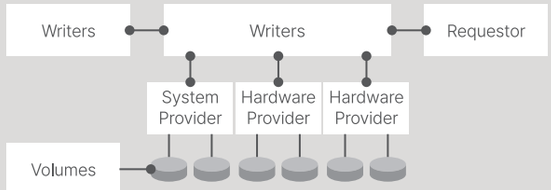
순식간에 진행됨 — 파일 저장/변경될 시 > RansomZERO Agent가 커널단에서 윈도우 Write API 체크 > 변경되는 시점에 잠시 파일 변경 블록 > 원본 파일을 Rans 백업 폴더에 저장 > 블록된 Write API를 해제시켜 변경된 파일로 저장

시스템 파괴 / 변조 바로 직전까지의 파일을 완벽히 복구

최근 작업 되었던 최신 파일까지 복원

적은 리소스 / 용량만으로도 효과적으로 데이터 백업

타사 백업 (VSS 복원)

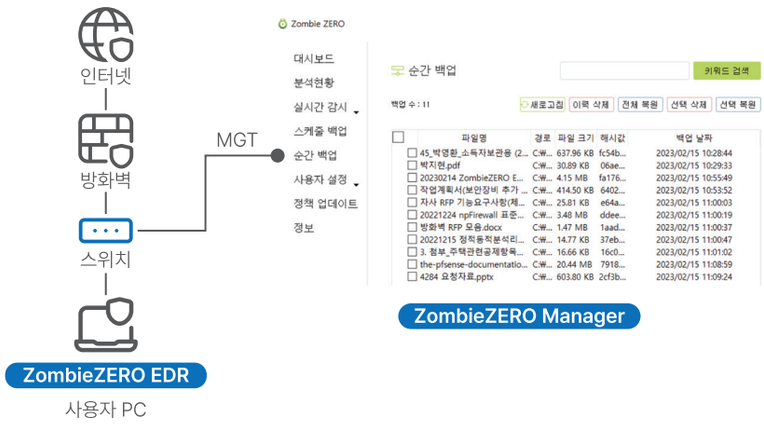


VSS (Volume Shadow Copy Service)
과거 특정 시점으로 복원 시켜주는 스냅샷 기술

특정 시점으로 시스템 전체를 복원, But 백업 이후의 파괴된 파일은 복구 불가능

백업 이미지 (스냅샷)에 대한 많은 용량 필요

백업 이미지에 대한 직접적인 공격으로 손상 발생시 복구 불가능



What's ZombieZERO SECaaS?

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

ZombieZERO EDR의 클라우드 서비스

트래픽 암호화 기반 사설가상망 (SSL VPN) 기능 통합

랜섬웨어 및 신/변종 악성코드 탐지 /차단 기능

(재택근무자 접속 가능)

주요 공통 기능 TOP 3

다차원 분석

MITRE ATT&CK 분류

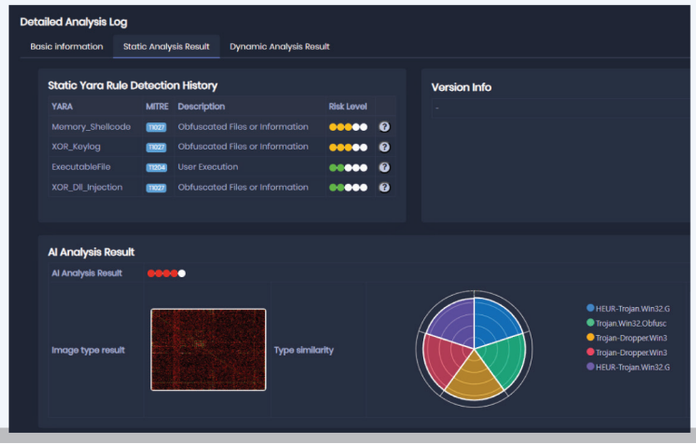
AI기반 악성코드 탐지

다차원 분석 + AI 분석

1	2	3	4	5
Hash	Bitdefender	yara	vmware	VIRUSTOTAL
Black List	Anti Virus	Yara룰 AI 분석	가상머신 분석	평판 분석

(라이선스 키 별도 구매 필요)

MITRE ATT&CK 분류 및 AI 분석 결과



주요 레퍼런스 & 파트너

경찰청 KOREAN NATIONAL POLICE AGENCY
검찰 PROSECUTION SERVICE
대한민국 국방부 Ministry of National Defense
우정사업본부 KOREA POST
Your Best Credit Partner SGI서울보증
서민금융진흥원
관세청
병무청
책임운영기관 국가정보자원관리원
경상남도 GYEONGNAM
경상북도 GYEONGSANGBUK-DO
서울특별시교육청 SEOUL METROPOLITAN OFFICE OF EDUCATION
경기도교육청 GYEONGGIDO OFFICE OF EDUCATION
부산광역시교육청 BUSAN METROPOLITAN CITY OFFICE OF EDUCATION
인천광역시교육청 INCHEON METROPOLITAN CITY OFFICE OF EDUCATION
경상북도교육청
전라남도교육청
대구광역시교육청 DAEGU METROPOLITAN OFFICE OF EDUCATION
재단법인 한국장학재단
동덕여자대학교
한국전통문화대학교
OSB저축은행
BNK경남은행
금융위원회
해양수산부
posco
jtbc
LS엠트론
보훈공단 중앙보훈병원
보훈공단 부산보훈병원
서울특별시 서울의료원
제주대학교병원 JEJU NATIONAL UNIVERSITY HOSPITAL
창원한마음병원 CHANGWON HANMAEUM HOSPITAL
indosat ooredoo
Kamisu City Hall, Japan
Vietnam Posts and Telecom Group VNPT
Vietnam Cryptography University
Royal Malaysia Police

총판영업

iTWIN 대신정보통신(주) PIOLINK

아이티윈, 파이오링크, 대신정보통신 등 우수한
총판과 협업을 통하여 공공, 기업, 금융권 등에 판매

해외영업

CYROBE beyond Spry TECHLAB SECURITY
SANfinity BlueZebra Asteria Cyberindo Pratama

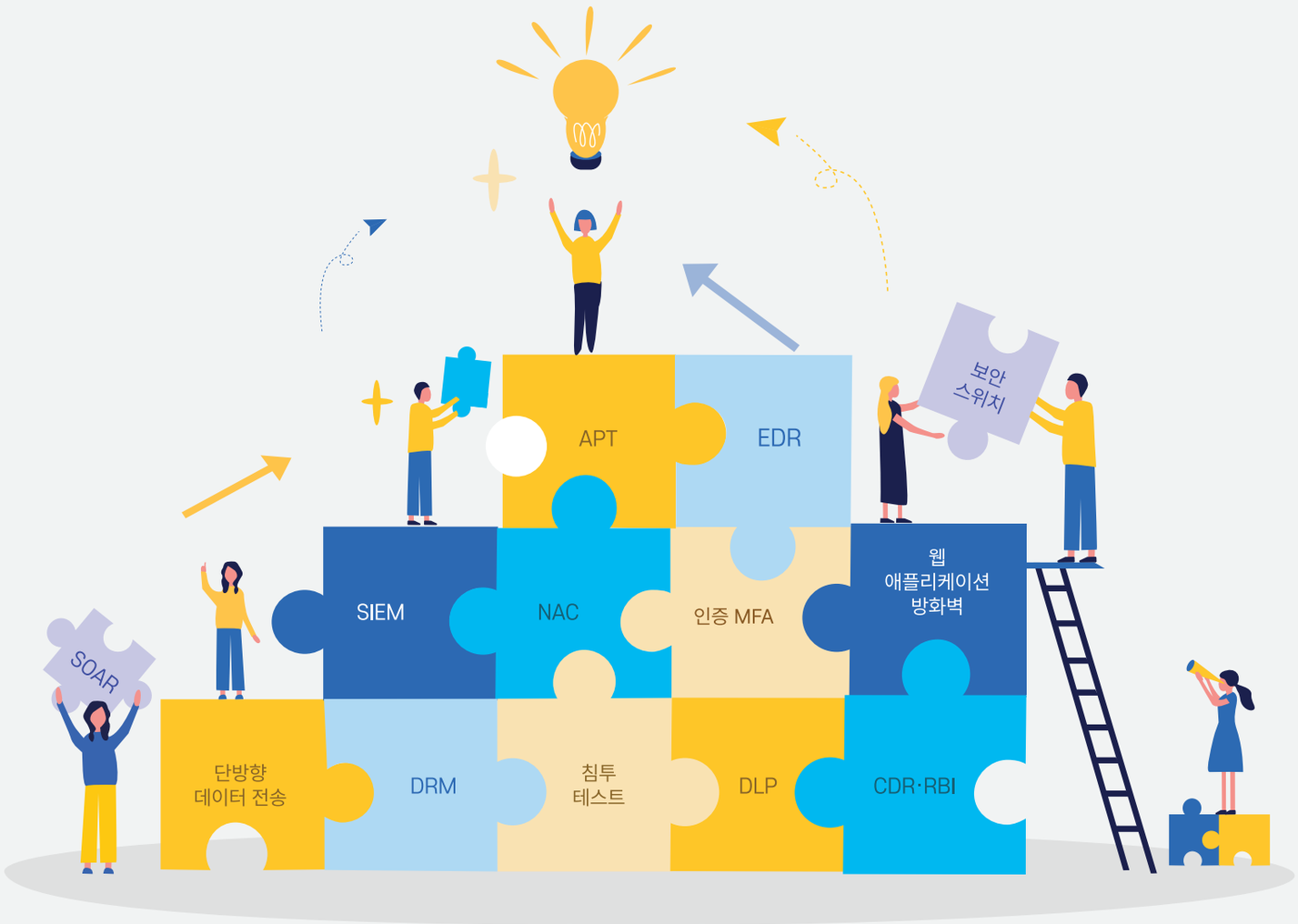
우수한 파트너와의 계약을 통하여 미국 및 동남아 지역
네트워크를 구축하여 해외 판매를 위한 요구사항 충족
및 영업기회 발굴

해외진출 국가

미국, 베트남 합작법인 및 싱가포르 거점 설립을 통해
싱가포르, 베트남, 태국, 인도네시아, 말레이시아 등의
동남아시아 뿐만 아니라 일본으로 확대 중

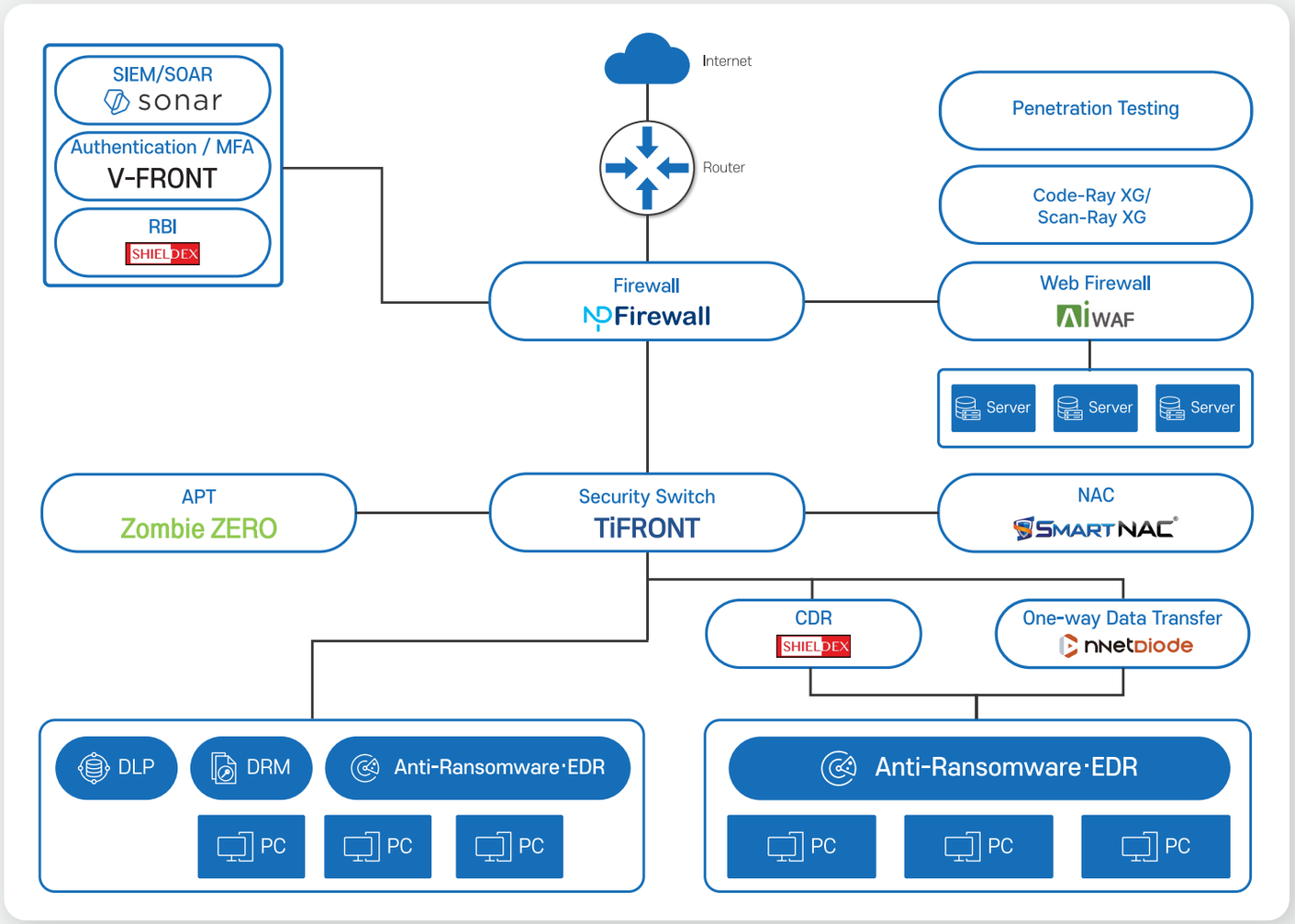
2025 K-Cyber Security Solutions Suite

K-Cyber Security Suite



NDCore
New Paradigm Core

K-Cyber Security Suite



솔루션 분류	제품/서비스 명	기업명	웹사이트
APT·Anti-Ransomware·EDR·Firewall	ZombieZERO Series, npFirewall	엔피코어	www.npcore.com
Security Swich	TiFront Series	파이오링크	www.piolink.com
Web Application Firewall	AIWAF Series	모니터랩	www.monitorapp.com
Authentication·MFA	V-FRONT	에어큐브	www.aircuve.com
NAC (Network Access Control)	Smart NAC	NetNam	www.netman.co.kr
SIEM·SOAR	SONAR	로그프레소	www.logpresso.com
CDR·RBI (Remote Browser Isolation)	SHIELDEX	소프트캠프	www.softcamp.co.kr
DLP (Data Loss Prevention)	Waterwall DLP	워터월시스템즈	www.wwsystems.co.kr
Penetration Testing		랩 시큐리티	www.rapsec.io
DRM (Digital Rights Management)	DocuRay	블루문소프트	www.bluemoonsoft.com
One-way Data Transfer	nNet Series	앤앤에스피	www.nnsp.co.kr
Secure Coding Assessment	Code Ray XG / Scan-Ray XG	트리니티 소프트	www.trinitysoft.co.kr

여러분의 사이버 보안 안전은
엔피코어가 항상 **환하게** 밝혀줄게요.

NPCore
(주)엔피코어