2023
엔피코어 소개자료

NPCore

CONTENTS

2023 엔피코어 소개자료

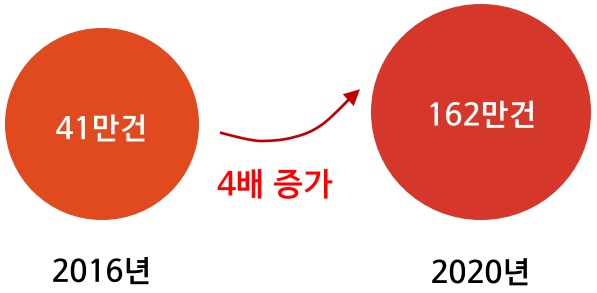
NDCore

01. 정보보안 현황

2023 엔피코어 소개자료

Contents

[국내 주요 공공기관 일평균 사이버 공격 건수]

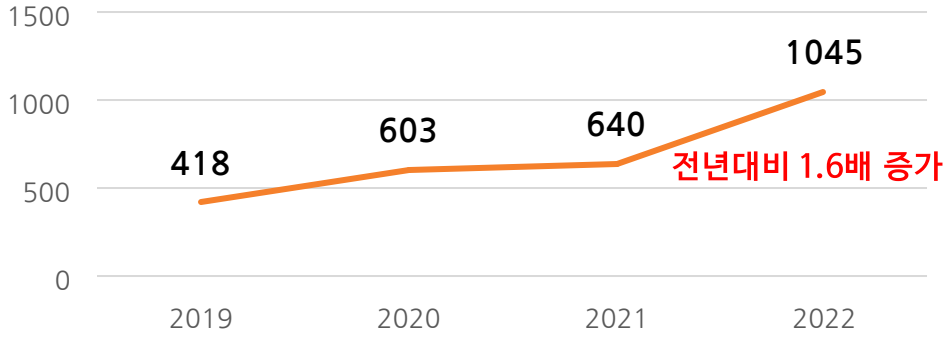


출처 : 국정원 보안발표

[전세계 랜섬웨어 피해규모 전망]

출처 : 사이버크라임매거진 2021

[연도별 전체 침해사고 건수]



출처 : 2022 사이버 보안 위협 분석 발표, 과기정통부-KISA

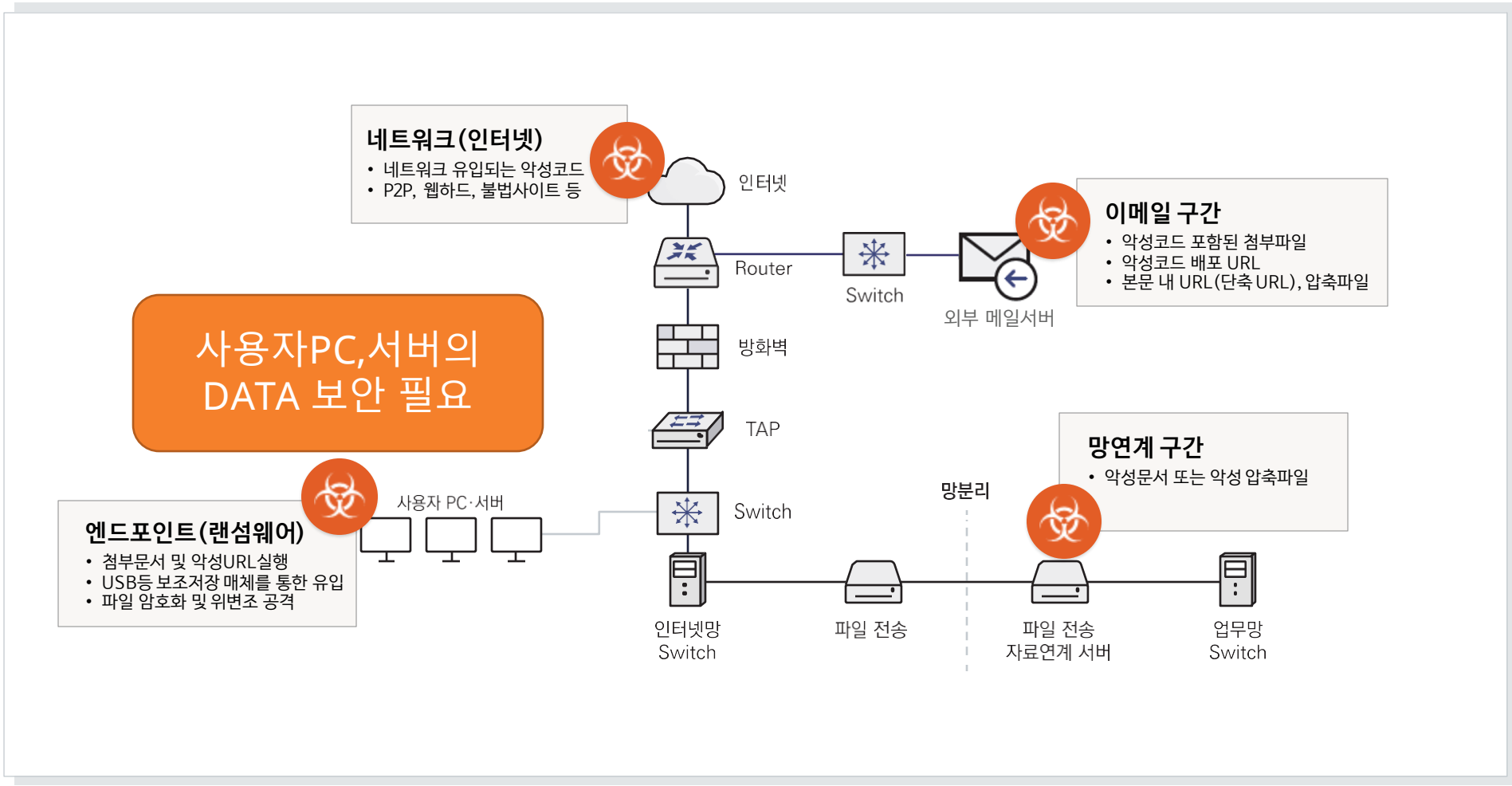
악성코드를 직접 유포하는 **악성URL 유포지 증가**
2021년 하반기 대비 38%증가

출처 : 악성코드 은닉사이트 탐지 동향 보고서, 2022 KISA

	방화벽	IPS	스팸필터	백신(안티바이러스)
목적	네트워크 및 어플리케이션 접근통제, 인가	네트워크 기반 룰을 통한 침입 방지	스팸 메일 차단	시그니처 매칭을 통한 알려진 악성코드 유입·실행 차단
특징 및 장점	- 수동적인 차단 - 내부망 보호 - 엄격한 접근통제로 인가된 트래픽만 허용	- 정책, 규칙 DB기반의 비정상적 행위 탐지 - 실시간 대응 - 세션 기반 탐지 가능	- 스팸/바이러스 메일 차단 - 스캠방지 / 발신자 인증	- 정상/악성파일 구분 및 격리(삭제) - 시그니처 기반 탐지
단점	- 내부자 공격에 취약 - 네트워크 병목 현상	- 오탐현상 발생 가능 - 고가 장비	알려지지 않은 취약점을 통해 공격하는 제로데이 공격 방어 불가능	알려지지 않은 취약점을 통해 공격하는 제로데이 공격 방어 불가능
보완점	허용된 주소, 프로토콜, 어플리케이션을 통한 **악성코드 유입차단 방안 필요**	**파일 기반 악성코드 탐지 방안 필요**	**신변종 악성 첨부파일, 압축파일 및 본문 내 악성 URL 등에 대한 행위 기반 탐지 방안 필요**	**신·변종 악성코드 탐지 랜섬웨어 행위 탐지 방안 필요**

신·변종 악성코드 지능형 위협에 대응할 방안은?

악성 코드는 네트워크, 이메일, 망연계구간, Endpoint 등의 **다양한 루트로 침입 공격**



침해사고 발생시, 유무형 자산 손실, 신뢰상실, 기업이미지 저하

보안 위협을 선제적으로 대응하고 내부 중요 자료 및 기밀 등의 자산을 보호하기 위한

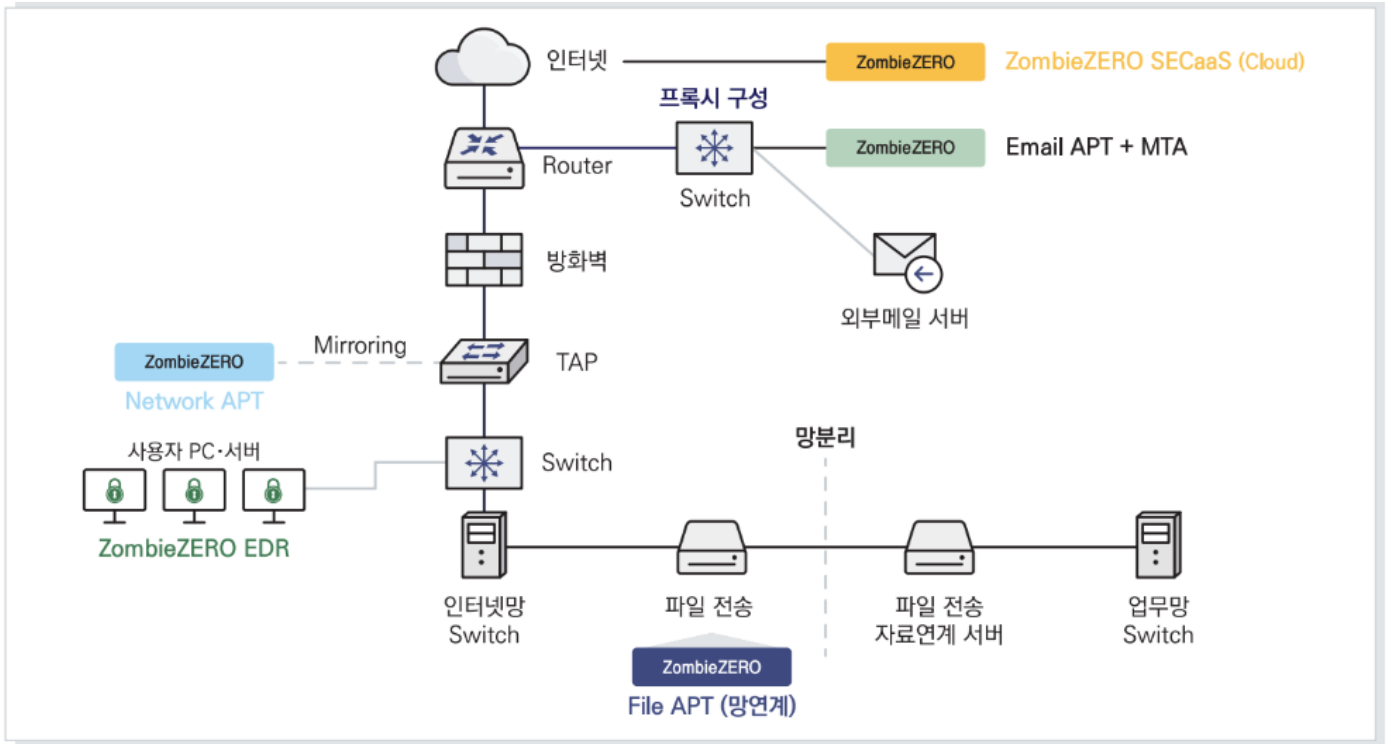
정보 보안은 선택이 아닌 필수입니다.

02. Zombie ZERO

2023 엔피코어 소개자료

Contents

Zombie ZERO 는 악성코드가 유입될 수 있는 다양한 경로에 구축하여 랜섬웨어 및 신·변종 악성코드를 탐지/분석/차단 합니다.



엔피코어는 APT와 EDR 제품군 모두 보유하고 있습니다.

Network APT

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

- 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 URL분석 후 정상 메일만 메일서버로 전송

기존 보안솔루션의
한계점을 보완한
지능형 위협 대응 솔루션

File APT

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

- 망연계 솔루션과 연동하여 이동 대기 중인 파일에 대한 분석·차단
- 분석된 파일을 분류하여 정상으로 판단된 파일만 업무망으로 전송
- 공유 폴더(SMB,NFS,Web API등)을 이용한 분석 결과 전달

EDR

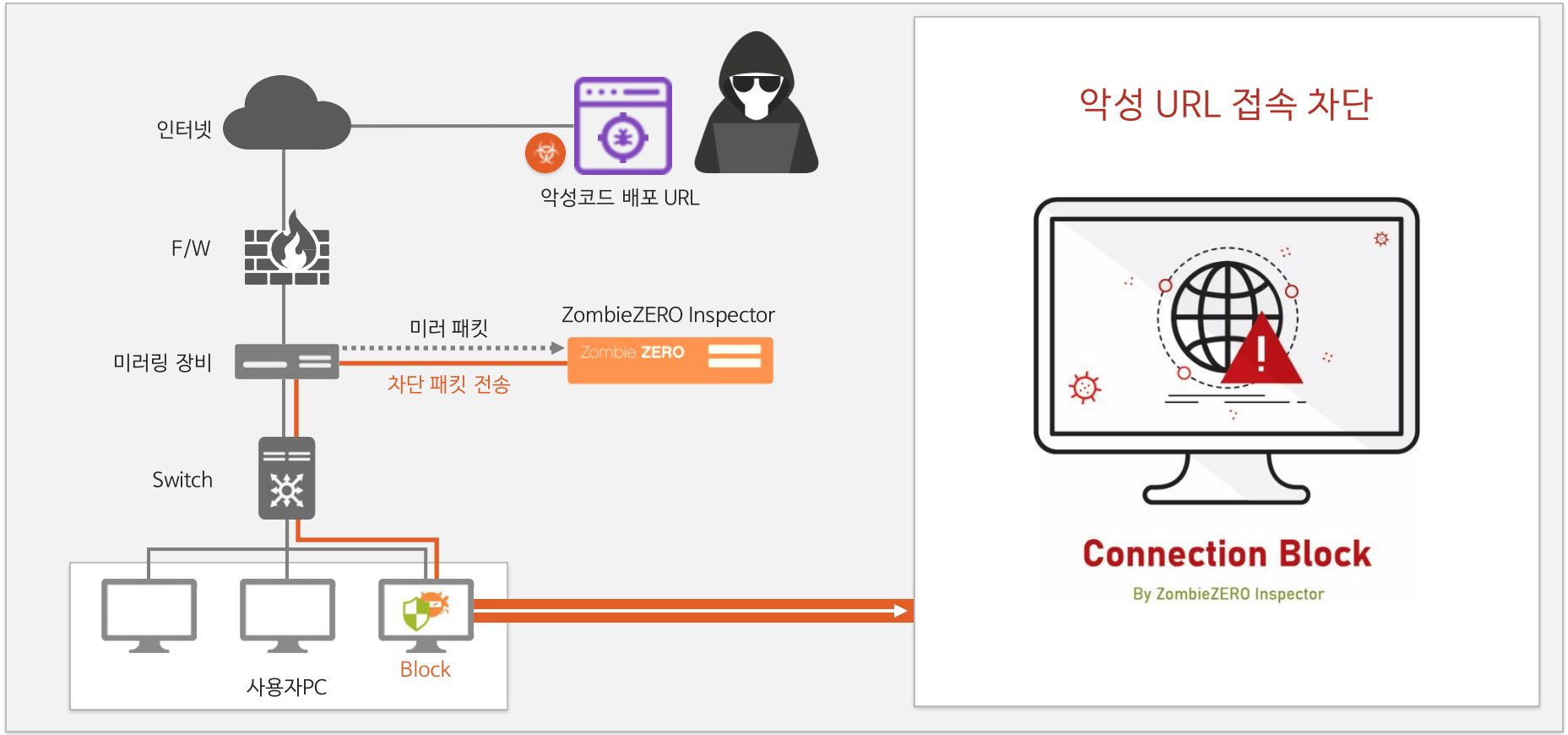
PC,서버 등 **사용자 구간을 통하여 유입되는 신·변종 악성코드** 탐지·차단

- 실시간 랜섬웨어 행위를 탐지하여 파일 암호화 및 위변조 대응
- 신규 파일 또는 위협 파일 실행시 파일의 실행을 보류하고 분석
- 순간백업을 통한 데이터의 2차 보안

Zombie ZERO

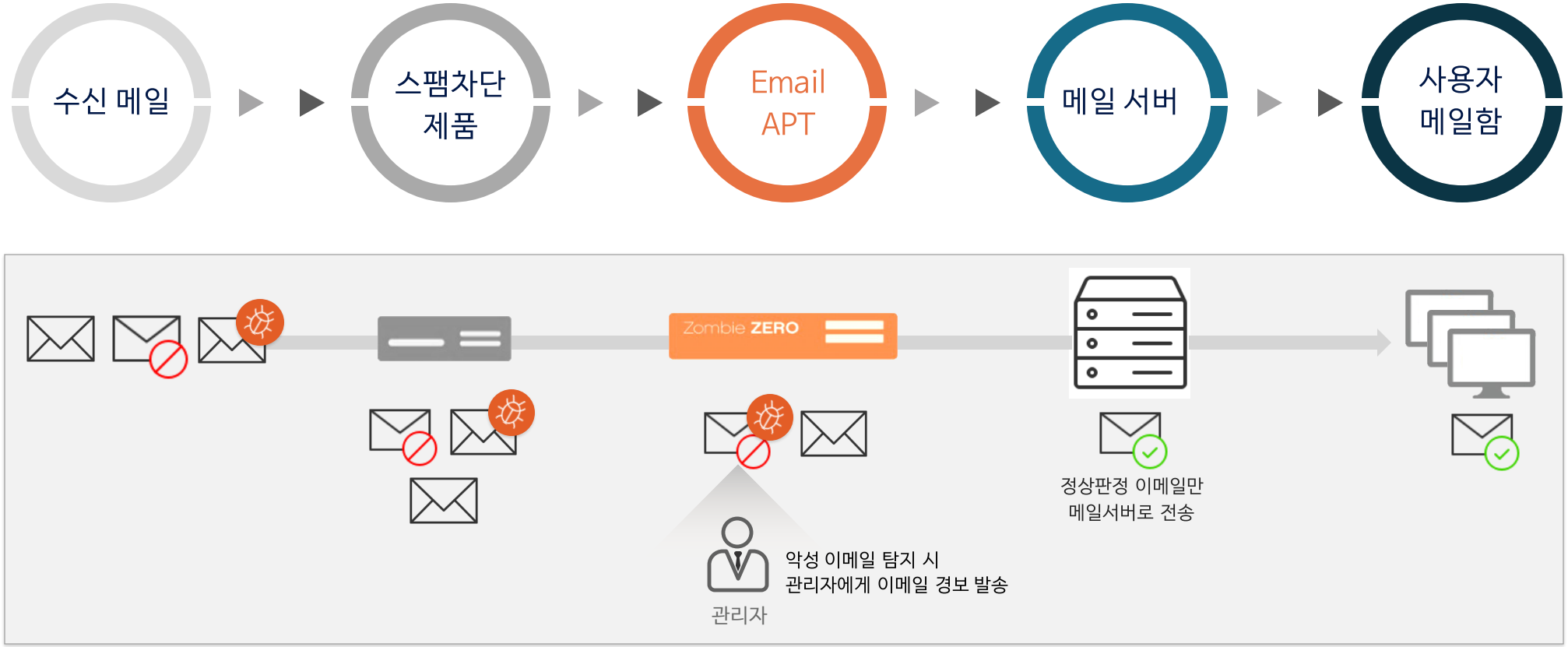
네트워크 APT

- 네트워크 트래픽을 **가속보드를 이용하여 수집**하고, 이에 대한 악성코드를 탐지/분석하여 차단
- C&C 서버 접속 및 악성코드 배포 사이트 URL 접속 차단 등 **실시간 차단**



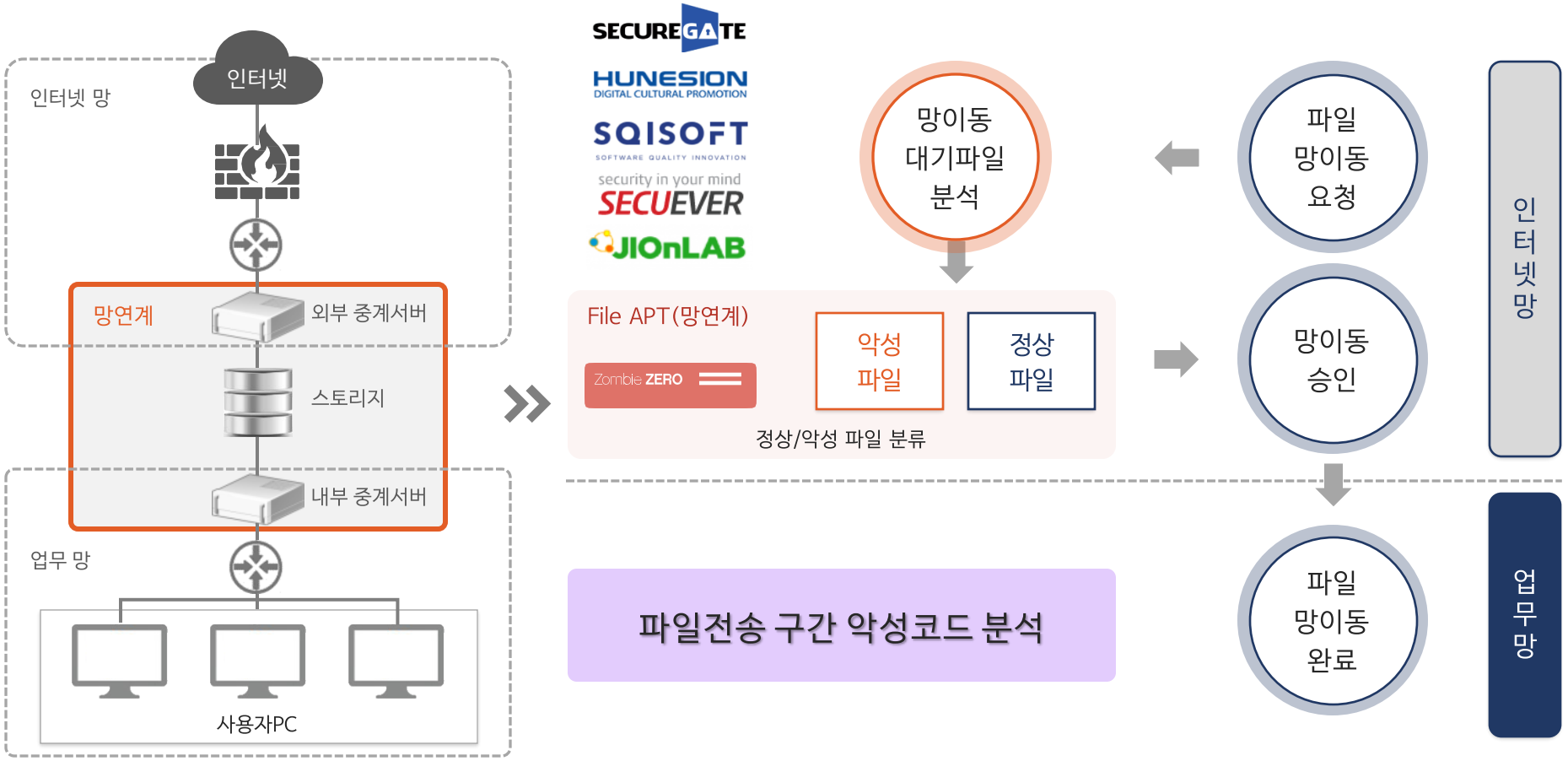
이메일 APT

- 이메일을 통해 유입되는 악성코드 탐지/차단하는 MTA와 APT 통합 솔루션
- 이메일 첨부파일 및 URL 분석 후 **정상메일만 메일서버로 전송**



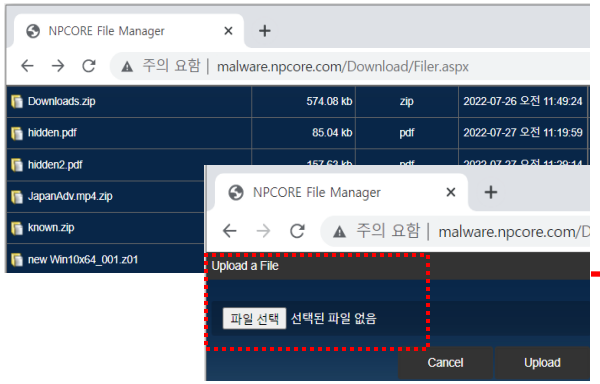
파일 APT

- 망연계 솔루션과 연동하여 **이동 대기중인 파일을 분석**
- 분석된 파일을 분류하여 **정상으로 판단된 파일만** 업무망으로 전송



파일 APT

- **게시판에 업로드 된 파일에 대한 분석** 및 결과 전달

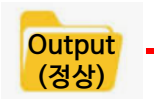


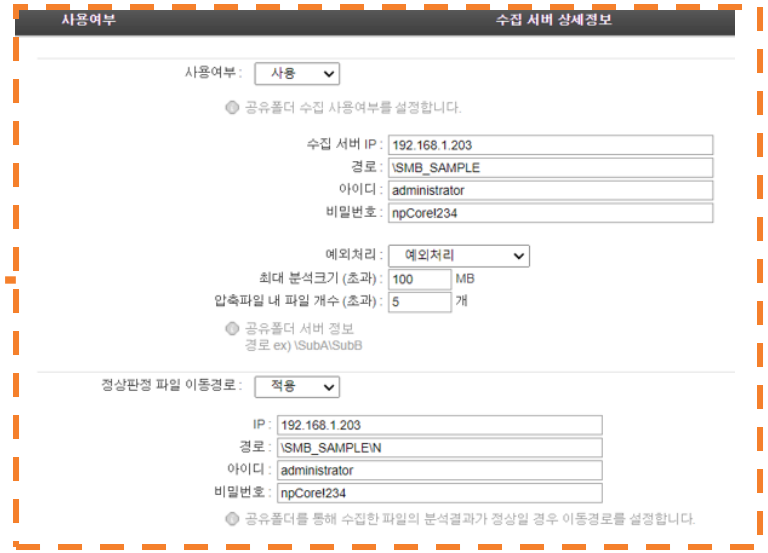
1. 사용자가 게시판에 파일 업로드 시도

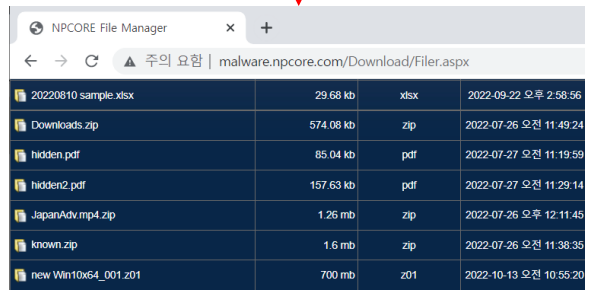
2. 업로드한 파일은
APT 검사 대상 폴더로 이동

3. 파일분석 후 정상/악성 판별

4. 정상인 파일만
게시판 업로드 폴더로 이동



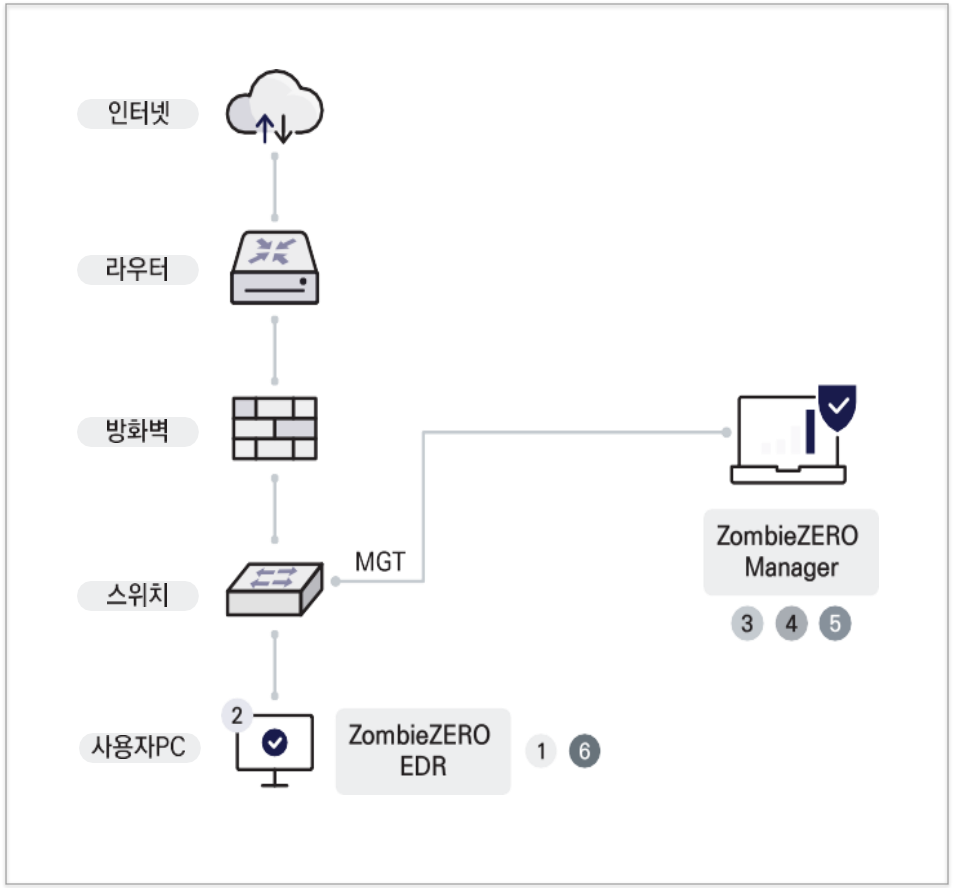




5. 게시판 파일 업로드

EDR

- Endpoint(사용자PC)단에서 APT 및 신변종 악성코드를 탐지/차단
- 랜섬웨어/백신 등 다양한 보안 솔루션으로의 확장 운영 가능

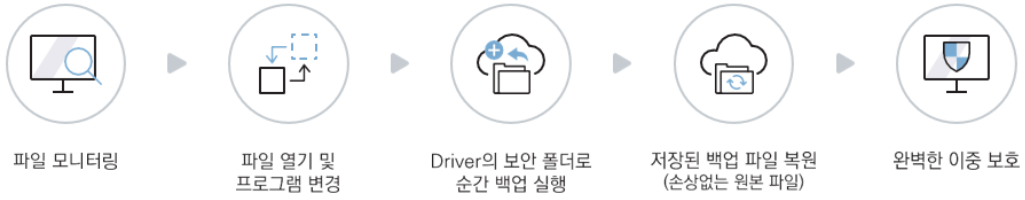


EDR 탐지 및 분석 기능 흐름도

1. IOC 기반 위협 행위 탐지 (MITRE ATT&CK 분류)
2. 사용자 PC에 신규 파일 유입 및 실행
3. 분석 서버로 파일 업로드
4. 4단계 파일 분석
5. 분석 결과 정책 배포
6. 정상 파일 경우 파일 실행 (악성 파일 경우 차단 / 격리)
7. IOC 기반 위협 행위 지속 탐지 (MITRE ATT&CK 분류)

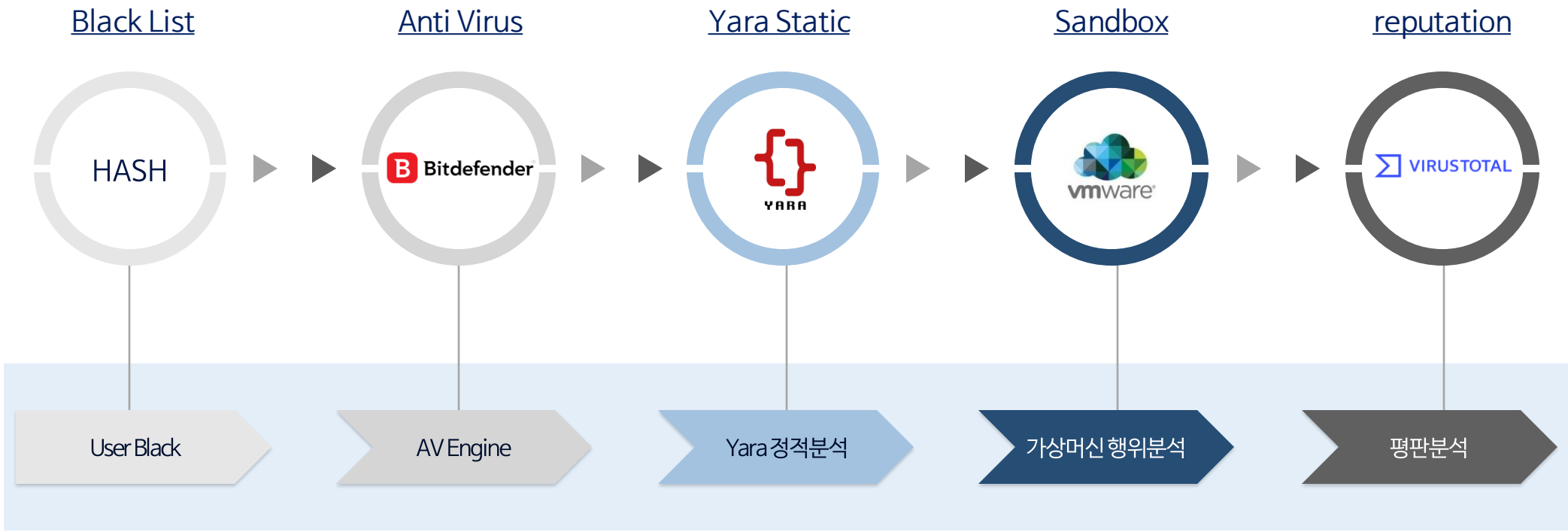
실시간 순간 백업

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



다차원분석

- 샌드박스 기반의 행위 분석으로 알려지지 않은 신·변종 악성코드 및 고도화된 위협을 분석합니다.

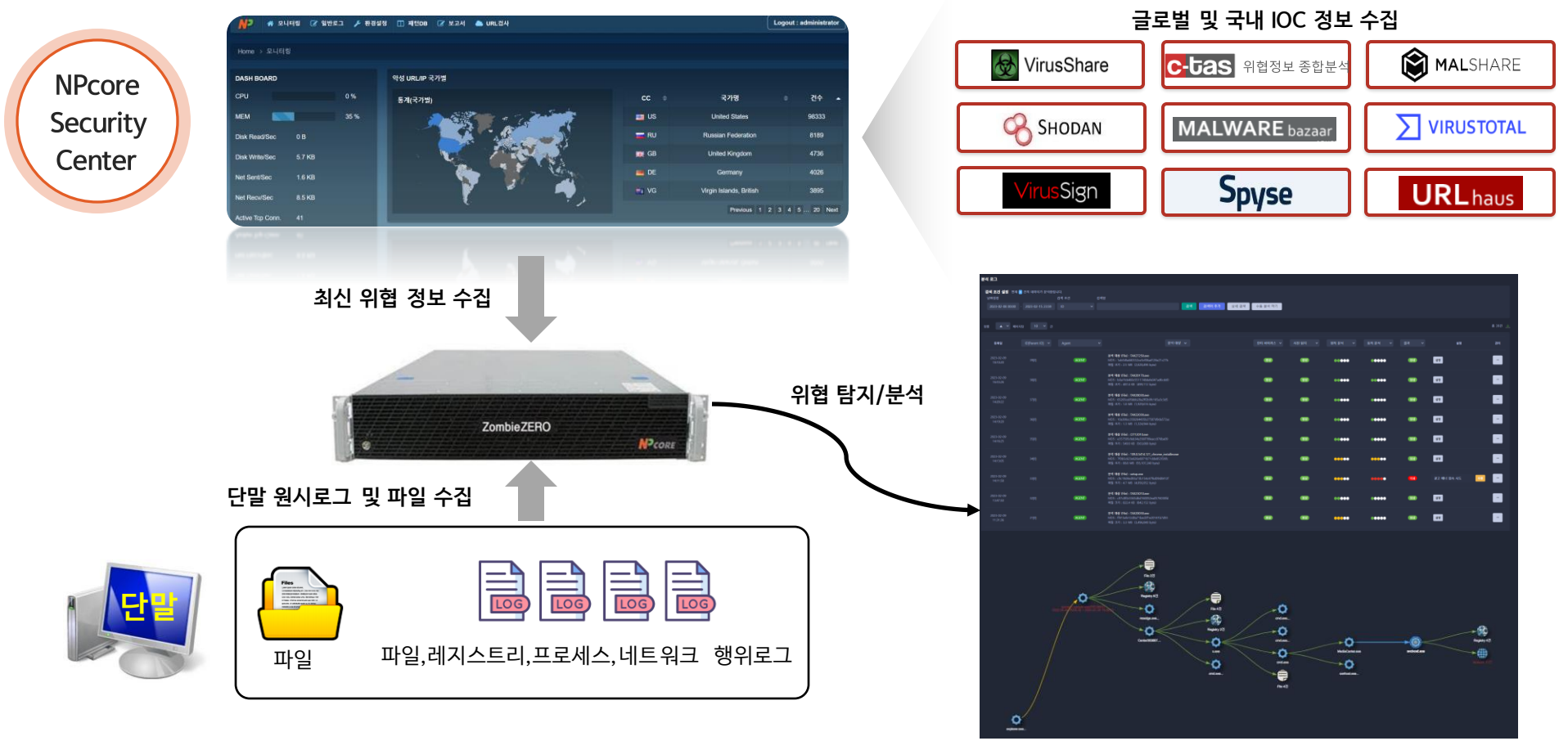


성능

- **네트워크 APT :** 단방향 최대 ~40Gbs 처리 | **이메일 APT :** 일일 처리 30만 이상 | **EDR 매니저 :** 장비당 최대 10만 Agent User 운영
- 가상머신 **최대 운영 128개 (동적분석 일일 20만)**
- **트래픽 수집 가속보드**를 사용한 패킷 유실 최소화

IOC 침해지표

- **글로벌/국내 위협 지표**에 대한 지속적 정보 수집
- 단말단에서의 **원시 로그 (네트워크, 파일, 레지스트리, 프로세스) 및 파일 수집**을 통한 침해지표 분석



MITRE ATT&CK

- 사이버 공격을 프로세스(Mitre ATT&CK 프레임)상으로 분석
- 공격의 결과가 아닌 진행 중인 공격에 대한 기술 및 방법에 대한 신속한 파악 및 대처 가능

MITRE | ATT&CK

해커 그룹 사용 기법

악성 코드 공격 기법

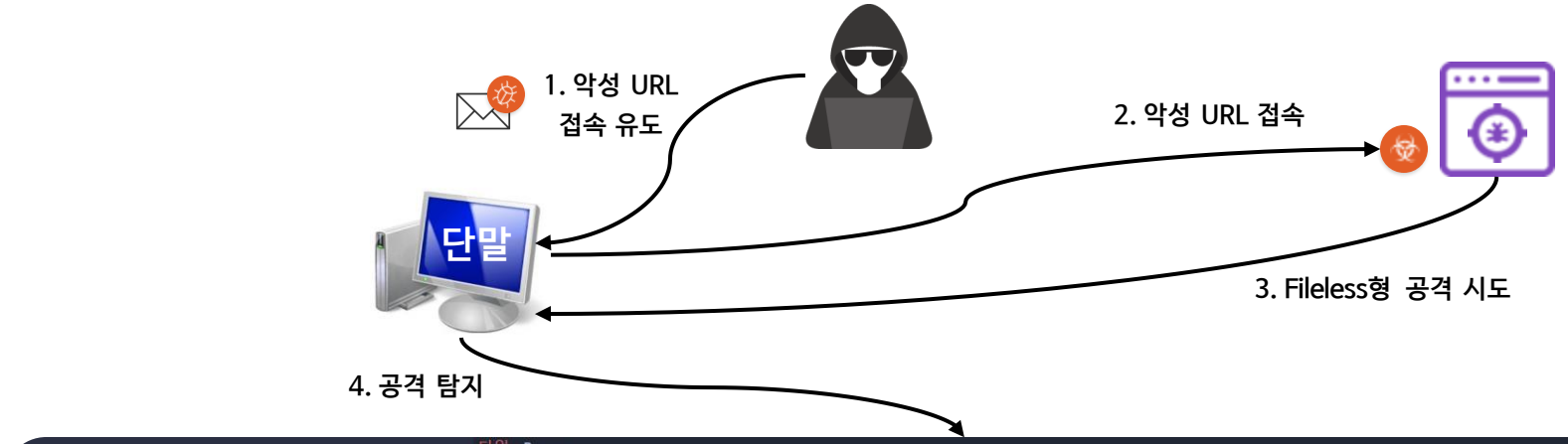
TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005
정찰	자원개발	초기 액세스	실행	지속유지	권한획득	방어회피
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion

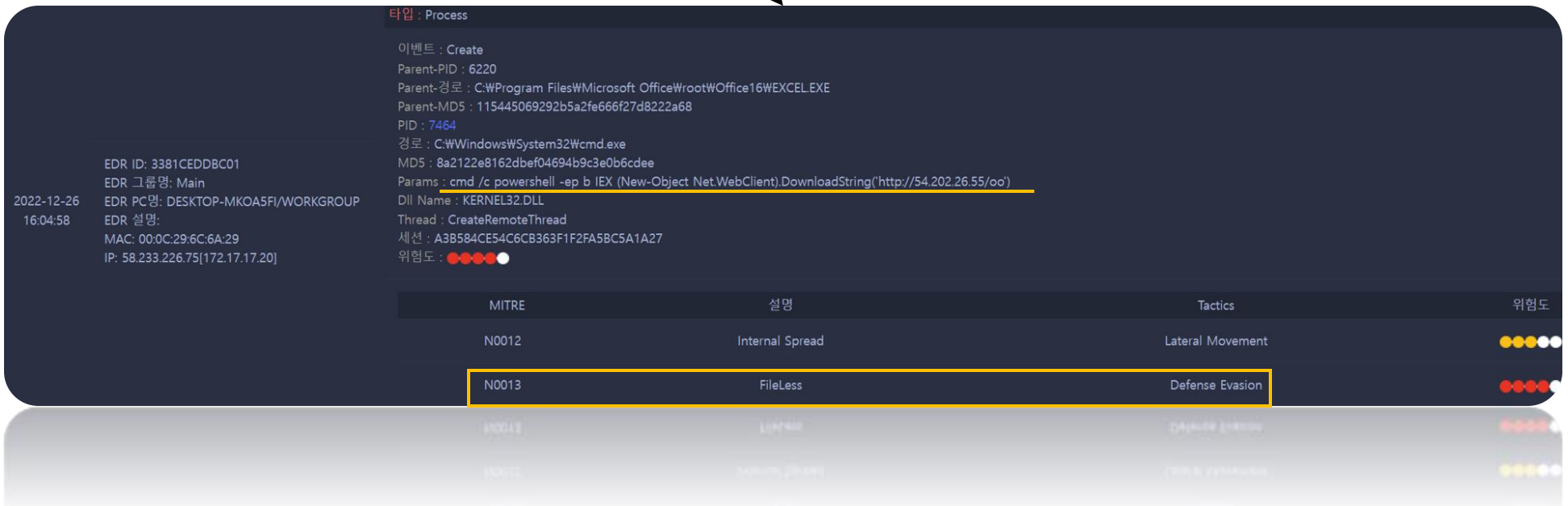
TA0040	TA0010	TA0011	TA0009	TA0008	TA0007	TA0006
타격	유출	명령제어	수집	측면이동	타겟발견	자격증명
Impact	Exfiltration	Command and Control	Collection	Lateral Movement	Discovery	Credential Access

악성행위 로그에 대한
Mitre ATT&CK
공격 단계 테이블 매칭

Fileless Attack

- 원시 로그 수집을 통한 Fileless형 공격 탐지





도입효과

악성코드, 랜섬웨어 대응

백신이 탐지할 수 없는 알려지지 않은 **신·변종 악성코드**를 탐지하고 차단하여 사전에 대응 가능

엔드포인트 가시성 확보

엔드포인트에서 발생되는 사이버 공격의 **구체적인 진행 상황 확인**으로 가시성 확보

악성코드 침입 가능성 예방

악성코드 **침입 경로**와 시스템 간의 연결을 확인하여 내부에서 취약한 부분을 보완하여 **보안 강화**

보안제품 도입비용 절감

랜섬웨어 대응, 백업 그리고 일부 백신 기능이 내장되어 있어 **별도의 제품 구매 불필요**

* APT 제품 및 EDR 제품 동시 구축 시 적용

APT 비교

		NPCore	W사	A사
인증		CC인증, GS인증	CC인증	CC인증, GS인증
수집		HTTP, SMTP, POP3, IMAP, FTP	HTTP, FTP, SMTP, POP3	HTTP, SMTP, POP3, IMAP, FTP
대응	네트워크 레벨	- C&C 차단 - 악성사이트 차단	- C&C 차단 - 악성사이트 차단 (IPS제품과 연동 필요)	- C&C 차단 - 악성사이트 차단
	엔드포인트 레벨	- 신종 악성코드 자동/수동 삭제 - 엔드포인트 의심파일 추출 EDR 기능 지원(순간백업)	- 신종 악성코드 자동/수동 삭제 - 엔드포인트 의심파일 추출 EDR기능 미지원	- 신종 악성코드 자동/수동 삭제 - 엔드포인트 의심파일 추출 EDR기능 지원
기타		샌드박스 커스터마이징 지원 트래픽 수집 가속보드 사용 (타사대비 2~3배 수집성능)	X	X
엔피코어 APT 타사대비 특장점		1. CC 인증, GS인증 보유 2. 글로벌 AV엔진을 활용하며, 정적분석 및 동적분석 등 다차원 분석을 통한 신변종 APT 공격 대응 3. 전용 트래픽 수집 가속보드를 사용하여 패킷 유실을 최소화 4. MITRE ATT&CK 분류로 공격 흐름 및 상세 분석 내용 제공 5. 탐지/분석 통합장비로 구성이 가능 6. APT제품 중 가장 많은 국내 레퍼런스 실적 보유		

EDR 비교

	NPCore	G사	A사
CC인증	O	X	O
샌드박스	O	O (타사연동)	O
IOC침해지표	O	O	O
실행보류 (제로트러스트)	O	X	O
파일 보호	O (순간백업)	X	X
랜섬웨어 대응	O	X	X
사이버 안전센터 Yara rule 연동	O	X	X
엔피코어 EDR 타사대비 특장점	1. 가상머신 및 다차원 분석을 통한 신변종 알려지지 않은 악성코드 탐지 2. 랜섬웨어 및 유사행위 프로세스 탐지 차단으로 암호화 및 위변조 대응 3. 실행보류 기능(제로트러스트 보안)을 이용한 악성코드 사전 차단/대응 4. 순간백업을 이용한 단말내 중요 파일 보호 5. IOC 침해지표연동으로 엔드포인트 가시성 제공 6. 에이전트 운영 시 기존 시스템 및 PC영향 최소화		

03. 엔피코어 소개

2023 엔피코어 소개자료

엔피코어는 신변종 악성코드(APT) 대응
AI기반 보안솔루션을 제공하는 정보보안 기업입니다.

회 사 명	㈜엔피코어
설 립 일	2008년 11월 19일
대 표 자	한 승 철
주요제품	정보보안솔루션 (APT 및 EDR)
홈페이지	www.npcore.com
소 재 지	서울특별시 영등포구 당산로 171, 701호

회사 신용도
BBB-

기술등급
TI-1

엔피코어는 2008년 설립된 APT 및 EDR 전문
APT 공공분야 1위 보안 기업입니다.

2008 - 2015

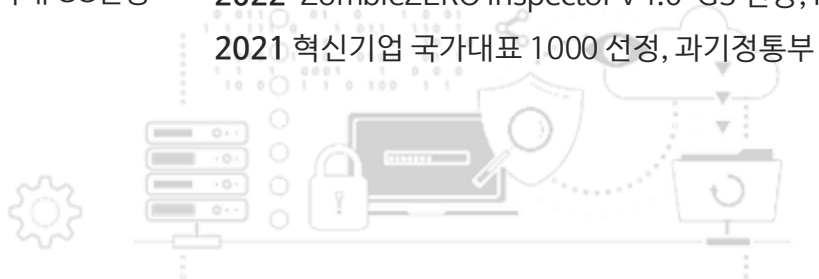
2015 '창조기술대상 우수상 수상
2015 '이동 단말기의 해킹 방지 시스템 및 그 방법' 국내 특허 등록
2014 베트남 하노이 지사 설립
2013 'ZombieZERO V2.0' GS인증 획득
2013 'ZombieZERO Inspector V2.0' 국내 CC인증 획득
2011 'ZombieZERO V2.0' 국내 CC인증 획득
2010 중소기업청 벤처기업 지정
2009 기업부설연구서 NP연구소 설립
2008 주식회사 엔피코어 설립

2014 - 2020

2020 ZombieZERO AI 출시
2020 정보통신공사업 등록
2019 MSA 솔루션 런칭 (MTA+SSL+APT 통합장비)
2019 SECaaS 솔루션 런칭 (클라우드형 APT)
2019 'ZombieZERO Inspector V4.0' 국제 CC인증
2018 '악성코드 차단 장치 및 이의 동작 방법' 국내 특허 등록
2017 'ZombieZERO Inspector V3.0' GS인증
2016 'ZombieZERO Inspector V3.0' 국내 CC인증
2016 제4회 '수출 첫걸음상' 수상

2021 - 2023

2023 기술역량 우수기업 인증(T1) -NICE평가정보㈜
2023 해외조달시장 진출 유망기업(G-PASS 기업) 지정
2023 '이미지 기반 악성코드 탐지 방법 및 장치와 이를 이용하는 인공지능 기반 엔드포인트 위협탐지 및 대응 시스템' 특허 등록
2023 '악성행위 탐지를 위한 클라우드 기반 가상화 장치, 시스템 및 운영 방법' 특허 등록
2023 비상대비 중점관리대상업체 지정, 행정안전부
2023 청년친화강소기업 선정, 고용노동부
2022 'ZombieZERO Inspector V4.0' 우수연구개발 혁신제품 지정
2022 'ZombieZERO Inspector V4.0' GS 인증, KTC
2021 혁신기업 국가대표 1000 선정, 과기정통부



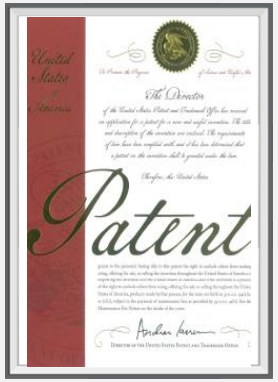
국제 CC인증 / GS인증 / 혁신제품 인증을 보유하고 있으며
미국 2건, 일본 1건을 포함하여 15건의 특허를 등록하였습니다.

인증내역

- "ZombieZERO Inspector V4.0" 국제CC EAL2 인증
- "ZombieZERO Inspector V4.0" GS 인증
- "ZombieZERO Inspector V4.0" 보안기능확인서 획득
- "ZombieZERO Inspector V4.0" 조달청 혁신제품 선정

국내외 특허등록 – 15건

- APPARATUS AND METHOD FOR BLOCKING ZOMBIE BEHAVIOR PROCESS (미국)
- MALICIOUS CODE DEACTIVATING APPARATUS AND METHOD OF OPERATING THE SAME (미국)
- HACKING PREVENTION SYSTEM FOR MOBILE TERMINAL AND METHOD THEREFOR (일본)
- 악성 코드 차단 장치 및 이의 동작 방법



수상내역

- 정보보호산업발전 유공자 (미래창조과학부장관)
- 우수연구개발 유공자 (서울시장상)
- 수출 첫걸음상 수상 (한국무역협회)
- 정보통신산업진흥원 SW신사업 아이디어 공모대회 우수상 수상
- 한국정보통신진흥협회 글로벌벤처기업 은상 표창
- 중소기업기술정보진흥원 창조기술대상 우수상 수상
- 미래창조과학부장관 K-Global 300 선정
- 지능형 지속위협대응 시스템 구축 감사장


감 사 장


표 창 장


표 창 장


優秀賞
창조기술대상

표 창 장


상 장

국내 APT 판매 1위 엔피코어는 200개 이상의 국내·외 레퍼런스를 보유하고 있습니다.

Korean National Police Agency	Prosecution Office	Ministry Of National Defense	Korea Post	Seoul Guarantee Insurance	National Fire Agency
Korea Inclusive Finance Agency	Korean Customs Service	Millitary Manpower Administration	National Information Resources Service	Gyeongsangnam-do	Gyeongsangbuk-do
Seoul Metropolitan Office Of Education	Gyeonggido Office Of Education	BUSAN Metropolitan City Office Of Education	INCHEON Metropolitan City Office Of Education	Gyeongsangbuk-do Office Of Education	JEOLLANAMDO Office Of Education
DAEGU Metropolitan Office Of Education	Korea Student Aid Foundation	Dongduk Women's University	OSB Savings Bank	BNK Kyongnam Bank	Financial Services Commission
POSCO	JTBC Broadcast Stations	Ls Mtron Industrial Machinery Company	VHS Medical Center	Seoul Medical Center	Jeju National University Hospital
Indosat Ooredoo	Kamisu City Hall, Japan	Royal Malaysia Police	Vietnam Posts And Telecom Group	Vietnam Cryptography University	Ministry of Transport

04. 향후 로드맵-XDR

2023 엔피코어 로드쇼

XDR(Extended Detection and Response이란?

엔드포인트 이상으로 탐지 범위를 확장하여, 확장된 데이터의 수집 및 분석을 통해 위협을 탐지/대응하고 전반의 공격 경로에 대한 통합뷰를 제공하여 통합 보안 체계를 구축할 수 잇는 차세대 플랫폼

EDR (Endpoint Detection Response)

- 홈 CCTV -

단말 (집안)에서 발생 되고 있는 정보 수집

- 네트워크 행위
- 파일 행위
- 프로세스 행위
- 레지스트리 행위
- 어플리케이션 / 사용자 등

⊕

NDR (Network Detection Response)

- 도로 CCTV -

네트워크·클라우드 (도로/지역)에서 발생되고 있는 정보 수집

- 패킷 네트워크 어플리케이션
- 패킷 메타 데이터 및 파일
- 패킷 데이터 정보 등
- FW 로그 / NW 트래픽 등

EDR + NDR

=

XDR

집안과 도로의 상황(정보) 수집

사건 발생 시 연관 지어 한번에 파악 / 대응

XDR의 장점 - 속도

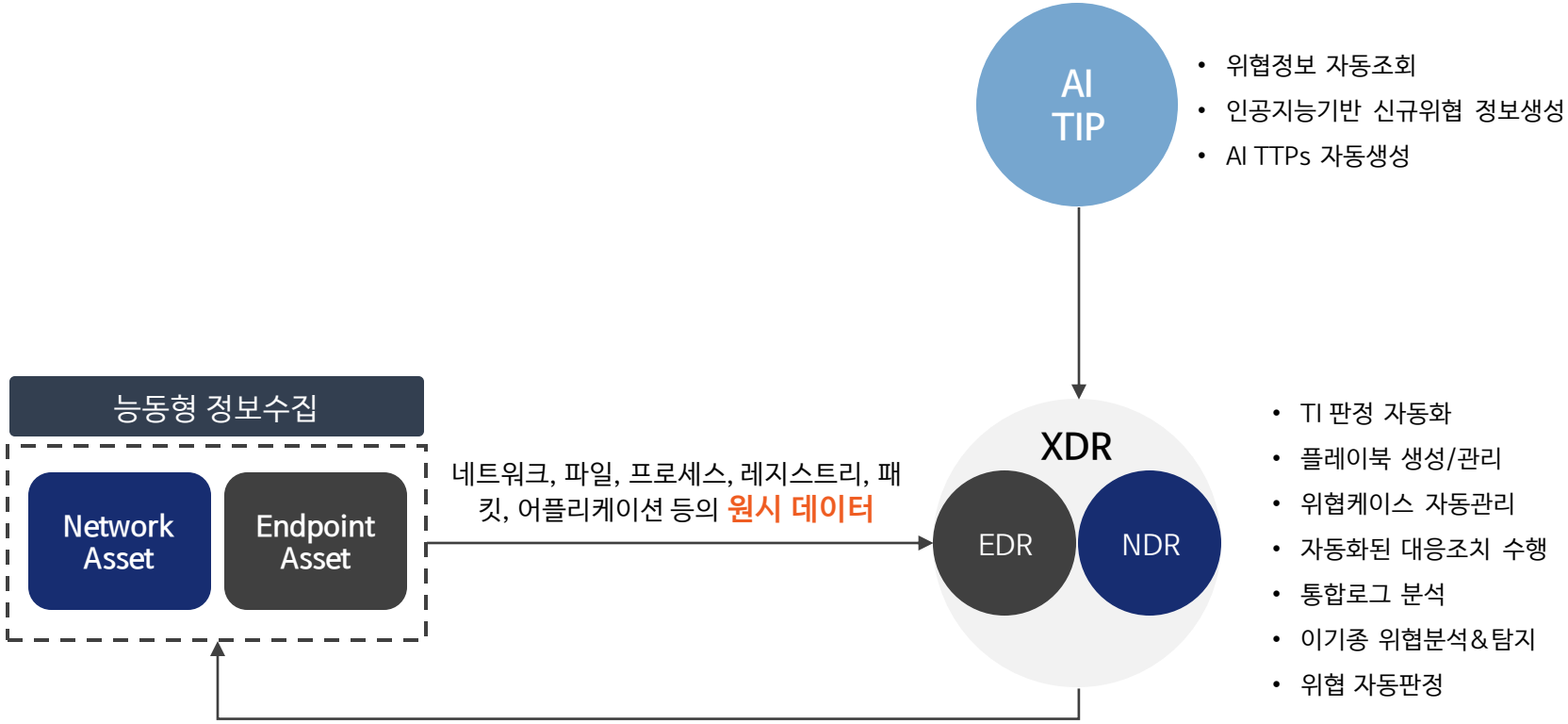
1. 데이터 소스의 상호 연관을 통해 평균 탐지 시간을 단축
2. 분류를 가속화, 조사 및 범위 지정 시간을 줄여서 평균 조사 시간 단축
3. 간단하고 빠르며 관련성이 높은 자동화를 구현, 평균 대응 시간 단축

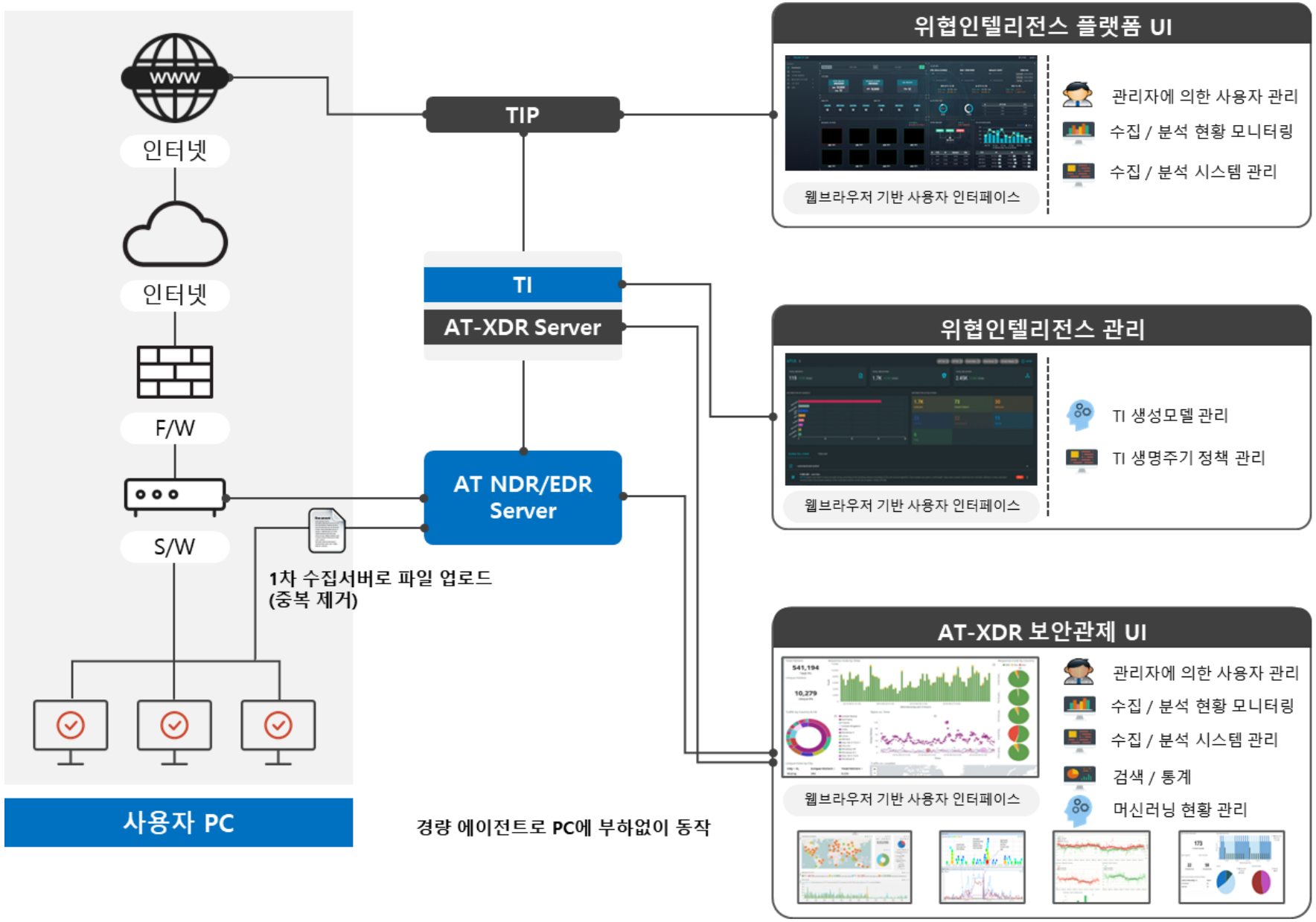
XDR의 장점 - 정보

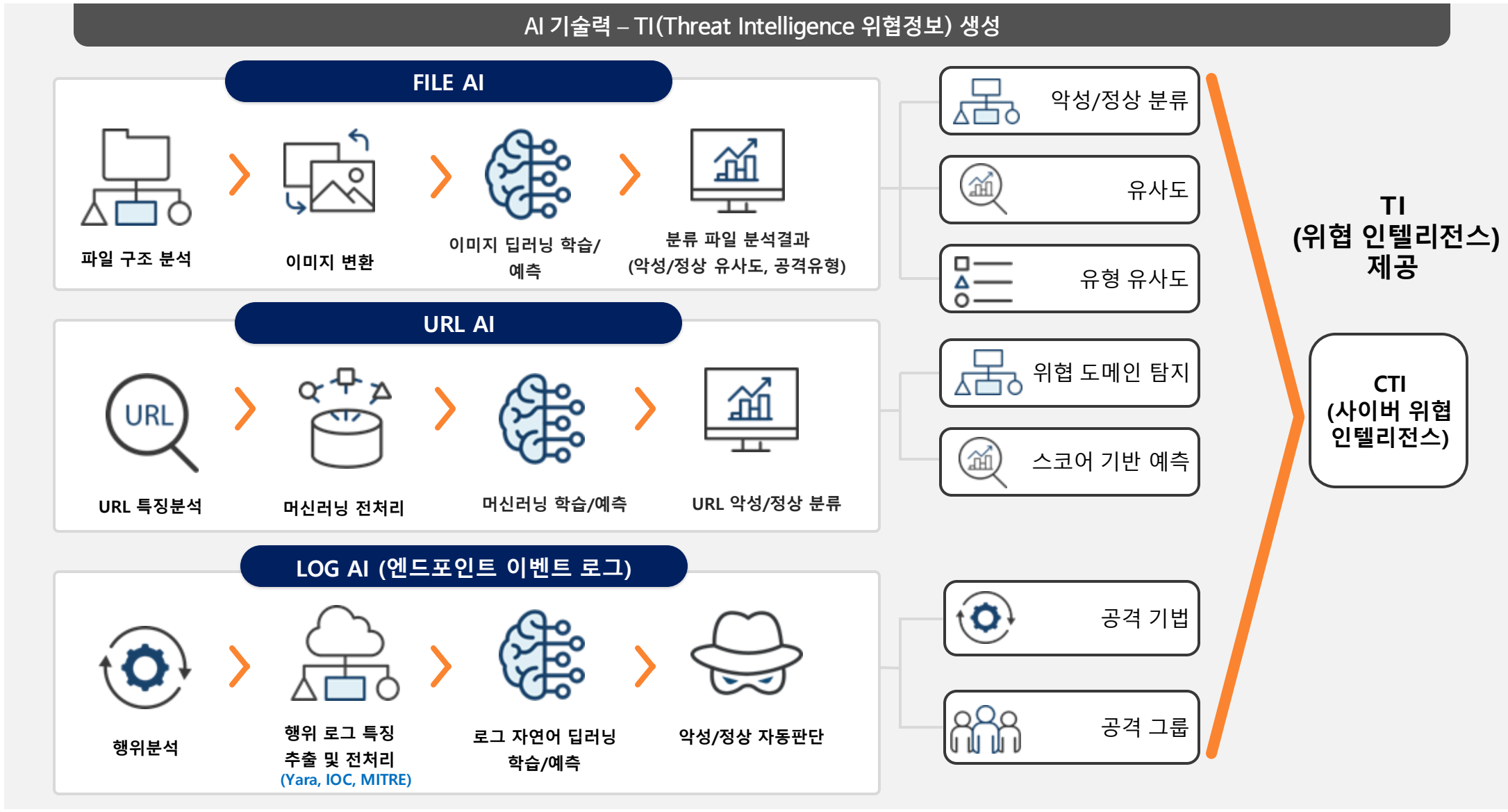
1. 단말 및 네트워크에서 발생 되는 모든 이벤트 수집
2. 각각의 솔루션이 아닌 전체 보안에 대한 가시성 향상
3. 사이버 공격 발생 시, 연동 분석을 통한 공격 현황 파악 및 대응판단

엔피코어의 AT-XDR이란?

트래픽&엔드포인트의 능동형 데이터 수집과 AI기반의 위협인텔리전스가 결합되어 분석가가 없어도 보안 위협을 자동으로 판단하고 대응이 가능한 국내 최초의 AT-XDR 플랫폼







THANK YOU