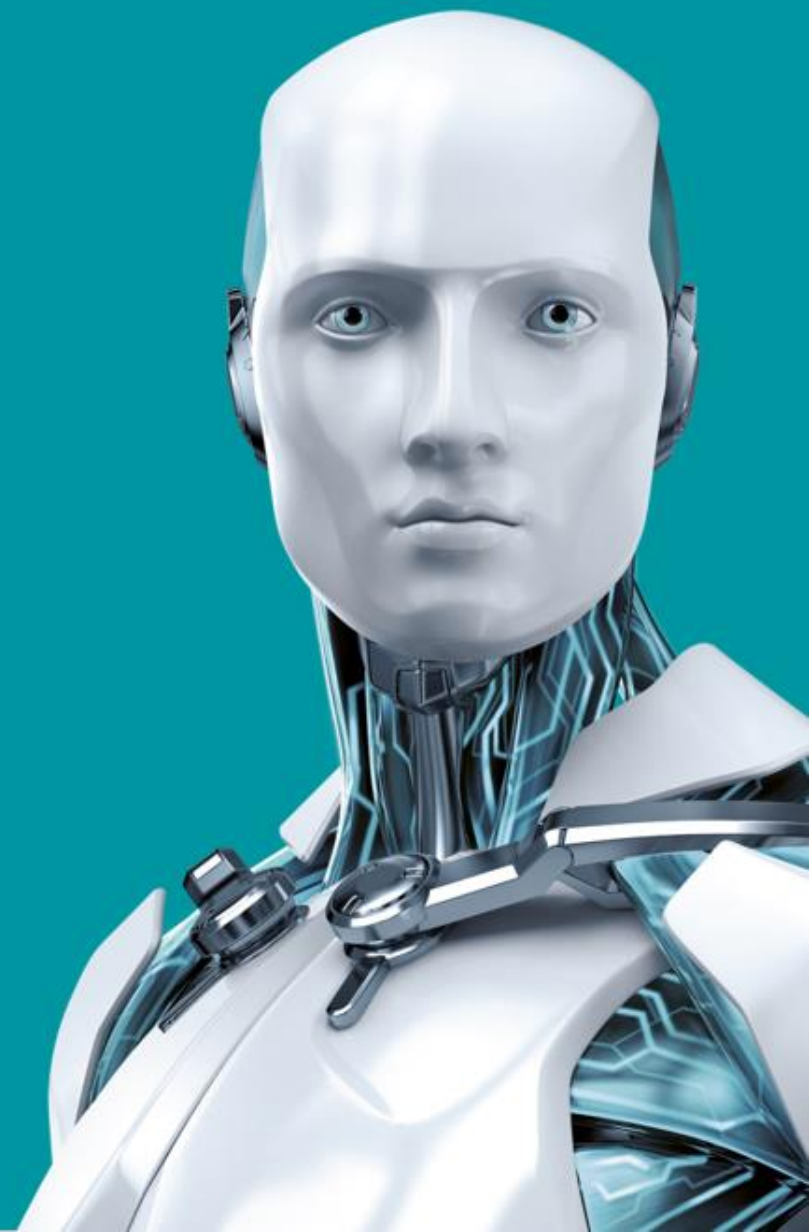
30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ESET DYNAMIC THREAT DEFENSE

클라우드 샌드박스 서비스

ENJOY SAFER TECHNOLOGY™



Index

ENJOY SAFER TECHNOLOGY™

제안 배경

HOME > 뉴스 > 보안

“랜섬웨어, 타깃 맞춤형 공격으로 수익률 높인다”

*** 기자 | 승인 2021.01.11 10:37 | 댓글 0

공격 추이를 살펴보면, 10월과 11월 다소 증가하다 12월 다소 줄어들었다. 랜섬웨어는 2018년 3분기부터 꾸준히 감소하는 추세를 보이고 있지만, APT 공격과 결합해 피해규모는 크게 늘어나고 있는 것으로 보인다. 일례로 지난해 국내 유통기업을 대상으로 한 클롭 랜섬웨어는 사전에 기업 내부 시스템을 조사해 맞춤형 악성 파일을 공격에 사용했으며, 파일 확장명을 변경하는 이전 변종과 달리 원본 파일명을 그대로 사용해 피해자의 의심을 피하는 등 고도화된 수법을 사용했다.

- **시스템 다운으로 인한 업무 불가**
- **생산라인 다운으로 인한 막대한 손실**
- **내부 중요 정보 유출 발생**

WHY EDTD?

필요성	EDTD
최신 악성파일에 대한 방어	샌드박스를 통한 최신 악성파일 발견
AI 머신러닝 등 최신 기술 필요	AI 머신러닝 탑재, 제로데이 위협 탐지
보안/전산 인력 부족	ESET 중앙관리를 통한 통합 관리
고가의 APT 제품	클라우드 샌드박스를 이용한 낮은 비용

WHY EDTD?

High End Solution (EDR, 장비형태)

- 높은 비용
- 전담 엔지니어(분석가) 필요
- 차단을 위한 추가 솔루션 필요
- 추가 에이전트 설치
- 장비에 대한 유지보수 필요

클라우드 기반 샌드박싱 기술을 이용한 APT 서비스 ESET Dynamic Threat Defense

ESET Dynamic Threat Defense

- AI Machine Learning
- Ransomware Protection
- Zero-day Threats Detection
- Automatic Protection
- High End 솔루션보다 낮은 비용
- 백신에 포함되어 있어 추가 에이전트 설치 불필요

EDTD 소개

- ✓ ESET 제품과 연동 가능
- ✓ 머신러닝 기능 탑재
- ✓ 랜섬웨어 보호
- ✓ 제로데이 위협 탐지
- ✓ 모든 엔드포인트 대상 즉시 보호 기능
- ✓ 분석 결과에 대한 상세 리포트 전달

ESET LIVEGRID®

Whenever a zero-day threat such as ransomware is seen, the file is sent to our cloud-based malware protection system – LiveGrid®, where the threat is detonated and behavior is monitored. Results of this system are provided to all endpoints globally within minutes without requiring any updates.

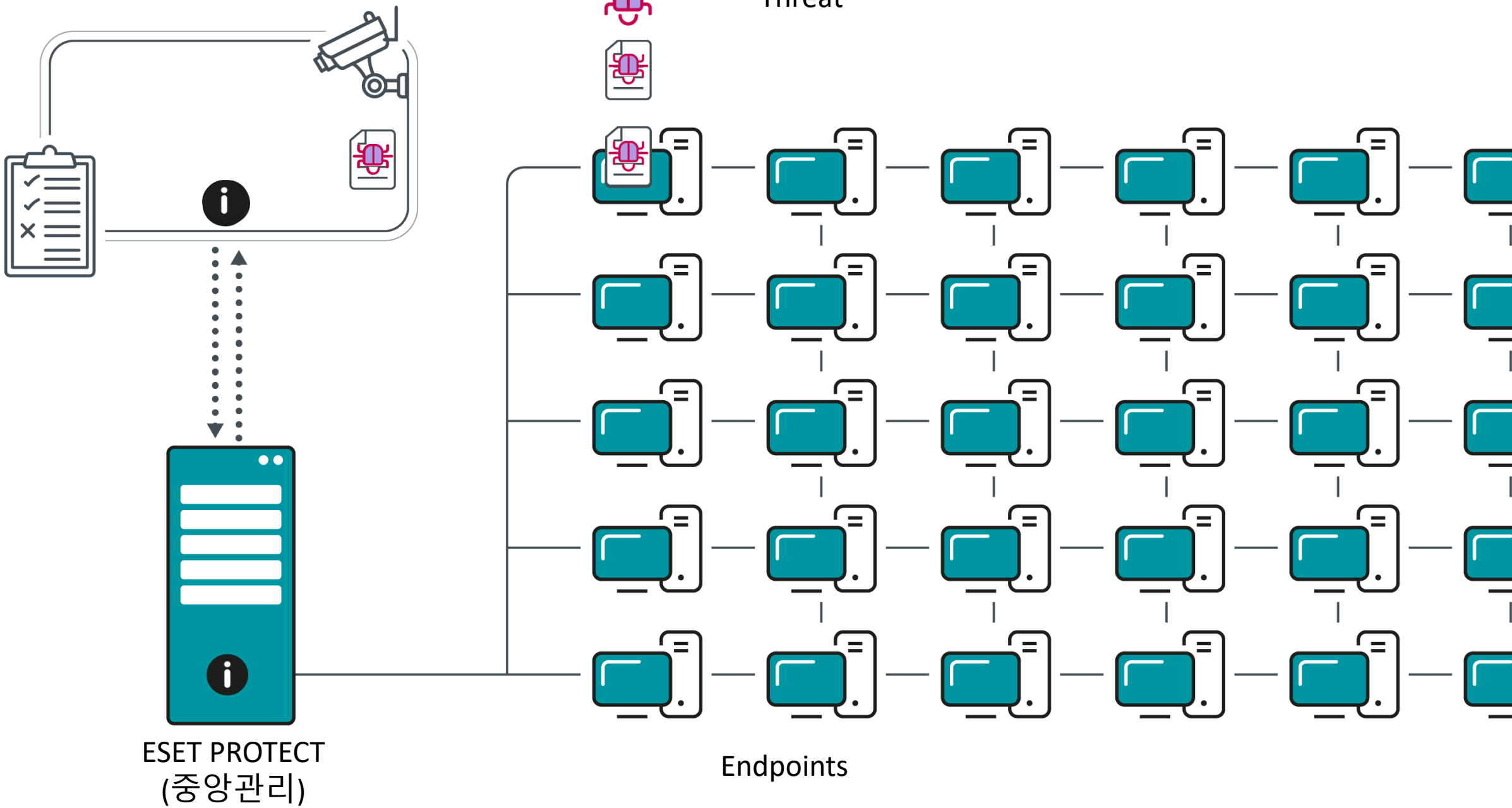
MACHINE LEARNING

Uses the combined power of neural networks and handpicked algorithms to correctly label incoming samples as clean, potentially unwanted or malicious.

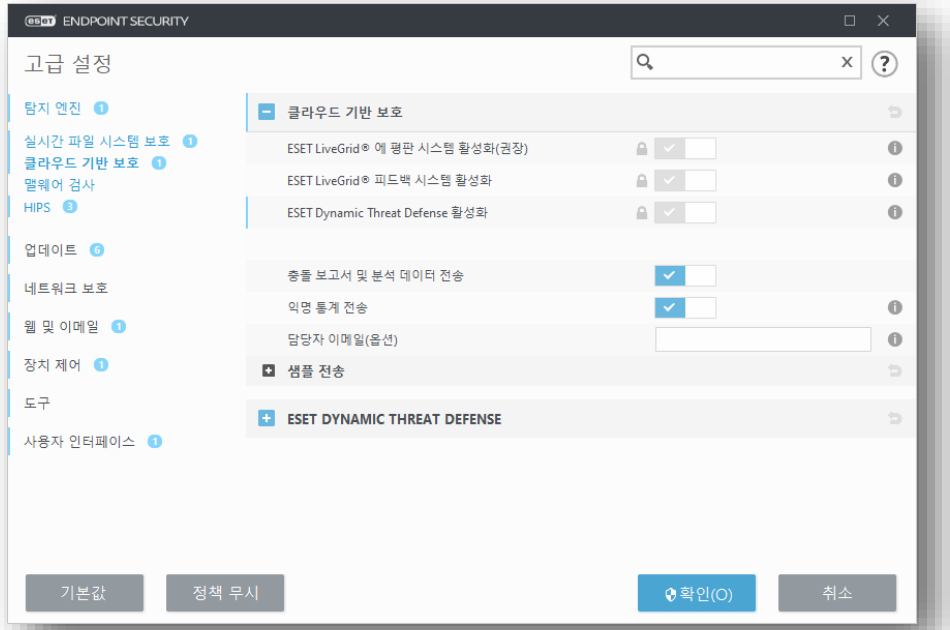
HUMAN EXPERTISE

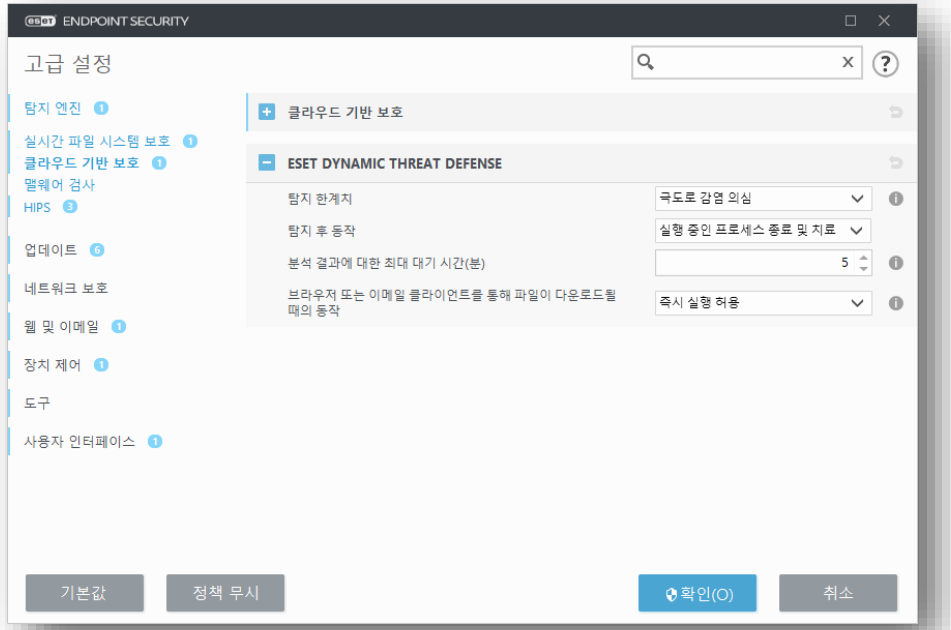
World-class security researchers sharing elite know-how and intelligence to ensure the best round-the-clock threat intelligence.

ESET Endpoint Security with EDTD



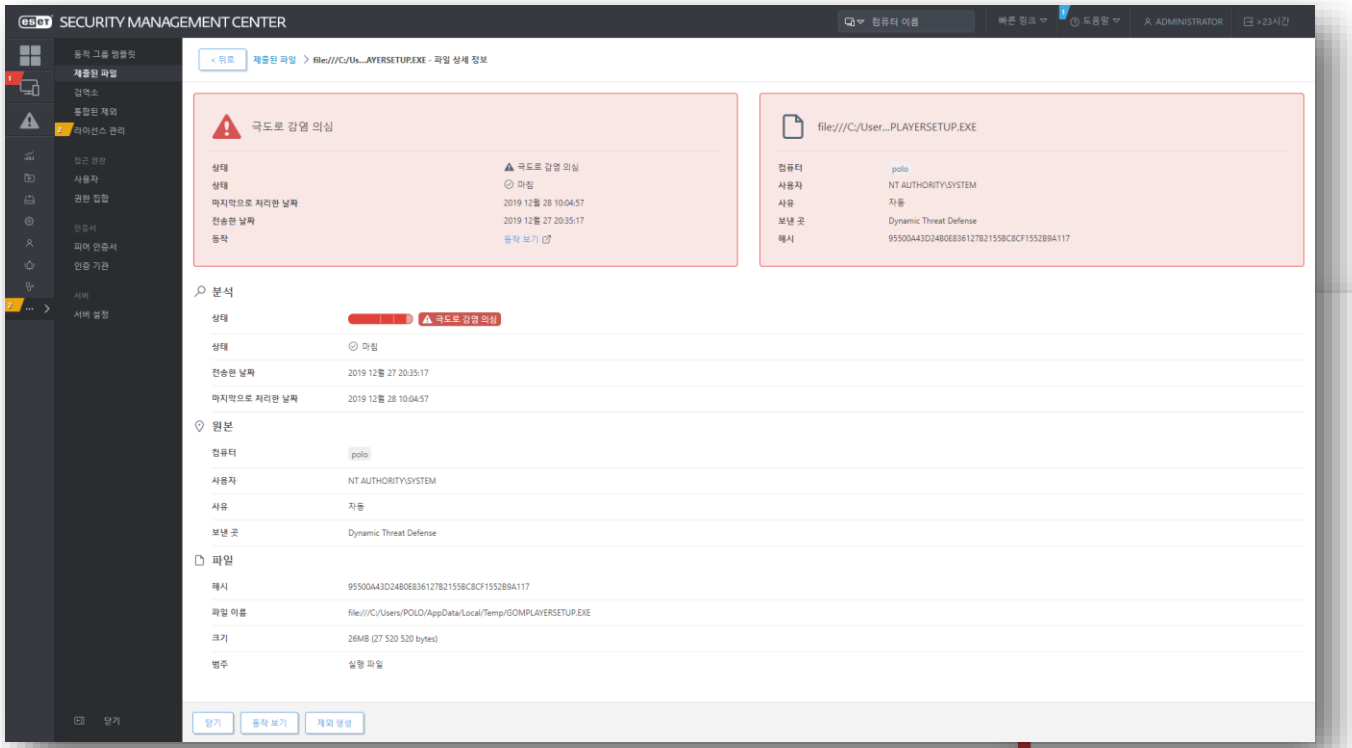
EDTD 소개

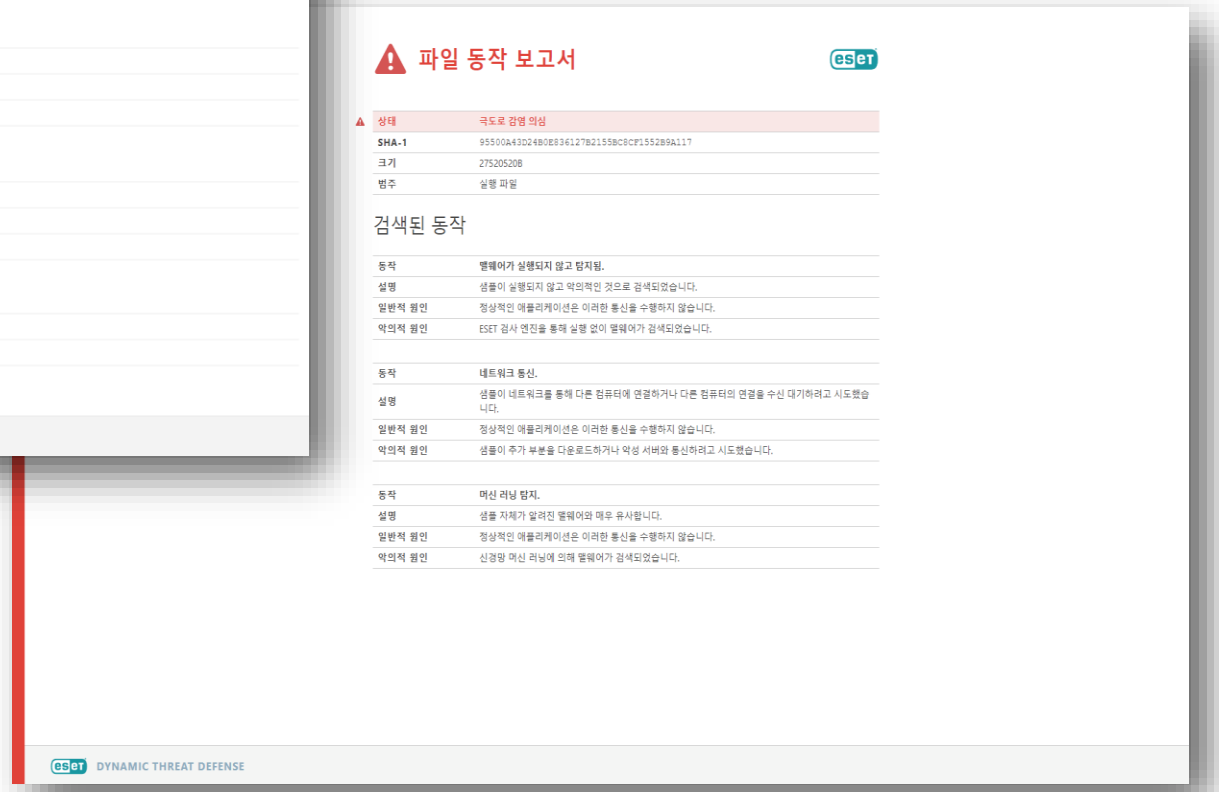




NEW 클라우드 기반 샌드박스	ESET 클라우드 서버에서 머신러닝, 샌드박싱 수행
NEW 제로데이 위협 탐지	DB에 없는, 알려지지 않은 신종 위협의 신속한 탐지 및 제거
NEW EP(중앙관리) 통합	EP(중앙관리)에서 분석된 개체 정보 및 보고서 확인
NEW ESET 제품 연동	EEA/EES/EFSW/EMSX 가 이미 설치된 시스템에서 바로 활성화
NEW 로밍 엔드포인트 지원	회사 네트워크에서 분리된 엔드포인트 호스트도 EDTD 이용에 제약이 없음

EDTD 소개 - 중앙관리 및 보고서





감사합니다.

- ESET –

세상에서 가장 가볍고 빠르고 정확한 백신!!

관리가 쉽고 간단합니다.

Address : 서울시 강남구 논현로 406 4층(역삼동, 요경빌딩)
Tel : 1899-8352
Fax : 02)573-0040
구매 문의 : sales@estc.co.kr
기술 문의 : tech@estc.co.kr
웹사이트 : www.estc.co.kr

ENJOY SAFER TECHNOLOGY™