Digital Transformation Partner

kt Enterprise

kt Secure 지능형위협메일차단

KT Bigdata 기반 AI 분석 기술로 더욱 강력해진 기업 위협 메일 차단 솔루션

1 서비스 배경

지능화된 악성 이메일 공격으로 기업 금전적·영업적 피해 증가

최근 이메일을 통해 지능화된 해킹공격이 증가 하면서, 기업 대상 이메일 사이버공격 피해가 매년 빠르게 증가하고 있습니다. '22년 침해사고 분석 결과, 악성코드 공격의 75%가 이메일을 통해 전파 되었으며, 특정 기업을 타겟한 사칭·위장 메일 또한 고도화 되어 기업에 막대한 금전적·영업적 피해를 끼치고 있습니다.

고객사칭 이메일 랜섬웨어 감염으로
콜센터 3일 업무정지
('19.12)

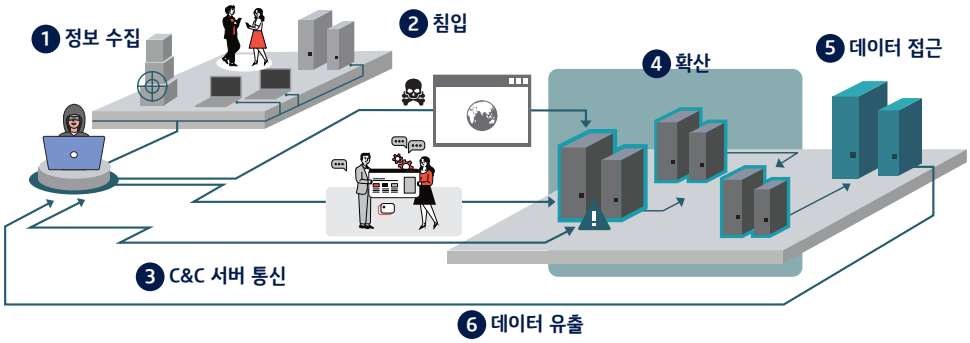
사칭메일 유포
고객 개인정보 수만 건 유출
('19.12)

위장메일에 오송금
61억원 금전적 손실
('20.03)

코로나19 發 해킹
중형 기업 총 1,100억원 피해
('21.08)

2 기존의 한계

패턴 기반 솔루션으로 방어할 수 없는 위협적인 사이버 공격, "APT"



APT는 지능적이고 지속적인 공격(Advanced Persistent Threat)의 약자로, 최근 국내에서 연이어 발생했던 금융권,쇼핑업, 대형게임사 대상 개인정보 유출 및 랜섬웨어 피해사고의 대부분이 APT의 속성을 가지고 있습니다.

APT공격의 가장 큰 특징은 오랜 시간에 걸쳐 미리 정해 둔 표적의 정보를 꾸준히 모아 약점을 파악한뒤, 사용자가 열어볼 수 밖에 없게끔 정상적인 메일로 위장하는 사회공학적 방식을 사용한다는 점입니다. 위장 방식이 정교화 되어 **사람의 눈으로는 거의 구분이 어렵고**, 악성 첨부파일의 경우 **시간차 공격 등으로 SandBox** 환경을 회피하여 기존의 SPAM·APT 솔루션만으로는 대응이 어렵습니다.

3 기업의 고민

더욱 강력한 기업 메일 보안이 필요하신가요?

최근 고도화된 악성 메일, 랜섬 웨어 등
다양한 사이버 공격으로부터 안전하게
지켜줄 수 있는 보안 서비스가
필요합니다!

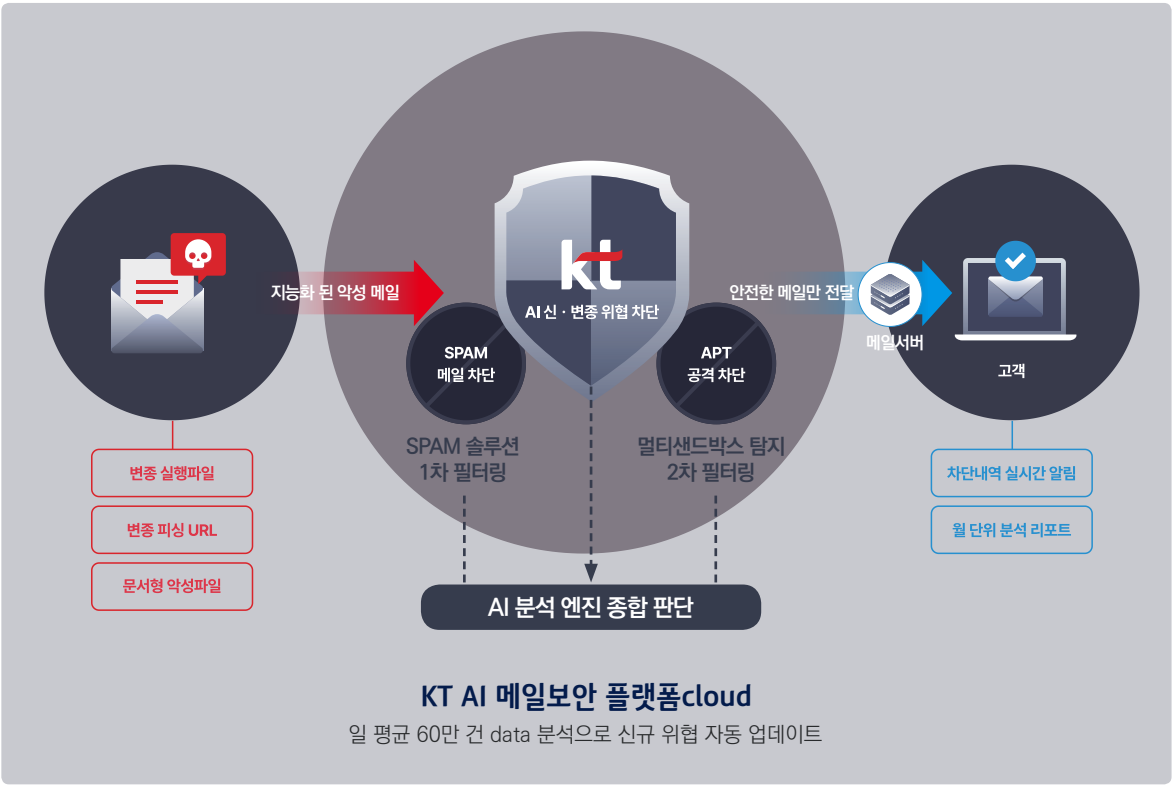
기업 메일보안 솔루션을
별도 장비 투자/운영 필요 없는
Cloud형으로 이용하고
싶은데 방법이 있을까요?

메일 계정 수에 따라 필요한 만큼만
신청하는 유동적인 메일보안
솔루션은 없을까요?

4 서비스 소개

지능형위협메일차단 서비스란?

KT Bigdata 기반의 AI 분석기술을 적용하여, 지능화·고도화 된 신·변종 위협 메일로부터 기업 자산을 안전하게 지킬 수 있으며 별도 장비구축 없이 이용할 수 있는구독형 AI 메일보안 솔루션입니다.



KT AI 메일보안 플랫폼cloud

일 평균 60만 건 data 분석으로 신규 위협 자동 업데이트

5 서비스 구성

고객 니즈에 따라 다양한 구독형 서비스 이용 가능

Basic

Basic 서비스

SPAM차단 솔루션
(WorkingHour 대응)
+ AI APT 대응 솔루션

Premium

Premium 서비스

SPAM차단 솔루션
(1년 365일 24시간 대응)
+ AI APT 대응 솔루션

+

Option

APT 1종 추가

APT 1종 추가로 멀티 샌드박스 적용

· SPAM+AI APT 1종 기본 구성, APT 추가 희망 시 옵션 선택 가능

· 샌드박스(Sandbox) : 가상환경을 만들어 그 안에서 악성파일을 실행 후 악성 행위 분석 및 탐지하는 솔루션

· APT : Advanced Persistent Threat

6 파트너 소개

KT secure 지능형위협메일차단 서비스 파트너를 소개합니다.

AhnLab MDS

독자적 기술의 멀티 엔진을 이용해 고도화된 지능형 위협을 정밀하게 탐지하는 샌드박스 기반 APT탐지 솔루션

시큐레터 MARS SLE

이메일로 유입되는 악성 문서파일 위협(비실행형 파일) 탐지 및 차단에 특화된 리버스 엔지니어링(어셈블리 레벨분석) 위협 탐지 솔루션

지란지교시큐리티 SPAMSNIPER

스팸 바이러스 메일 차단 기능으로 스캠/랜섬웨어등을 대응하는 스팸차단 솔루션

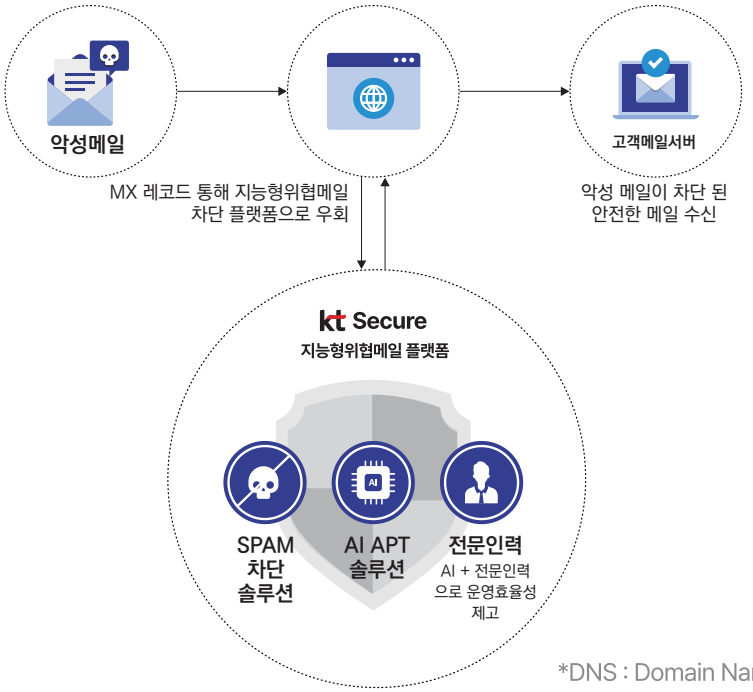
넷엔씨큐 SPAMOUT

Non-Contents 필터링과 Contents 필터링을 동시 수행하는 하이브리드 엔진, 필터링 엔진 탑재 스팸차단 솔루션

7 제품 특장점

7-1 트래픽 우회 방식으로 별도 인프라 구축 불필요

기업 MX 레코드(도메인 IP) 변경을 통해 장비 구축 없이 손쉬운 서비스를 제공하며, AI+전문 인력으로 운용 효율성 제공

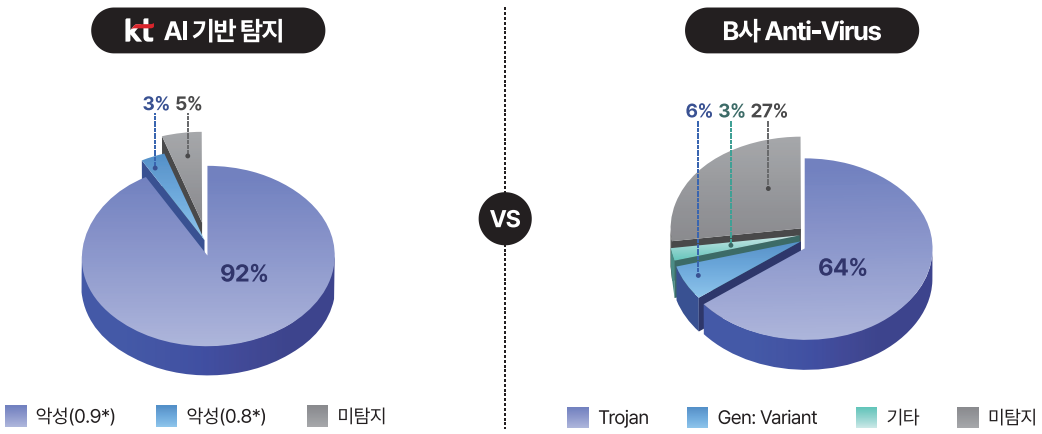


*DNS : Domain Name System

7-2 글로벌 벤더사 대비 최대 22% 더 높은 탐지율

국내 특화 DB기반 AI모델 적용으로 B사의 Anti-Virus 대비 최대 22% 더 높은 악성 파일 탐지

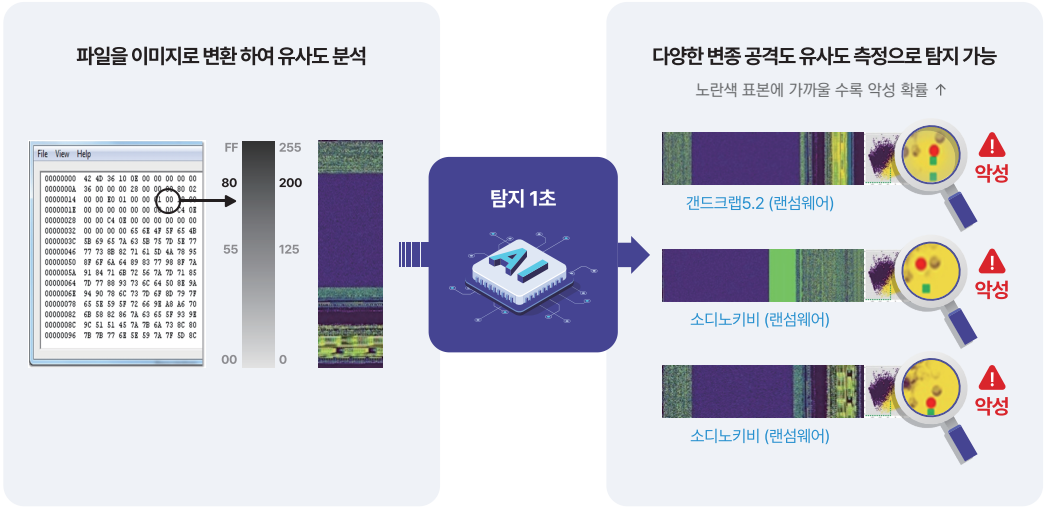
KT이메일 서비스로 유입된 악성코드 2,286개 대상 탐지율 비교(기간 : 3개월)



* 괄호안의 Score가 1.0 에 가까울 수록 악성 파일과의 유사도가 높은 탐지 건으로, 악성 파일로 분류됨

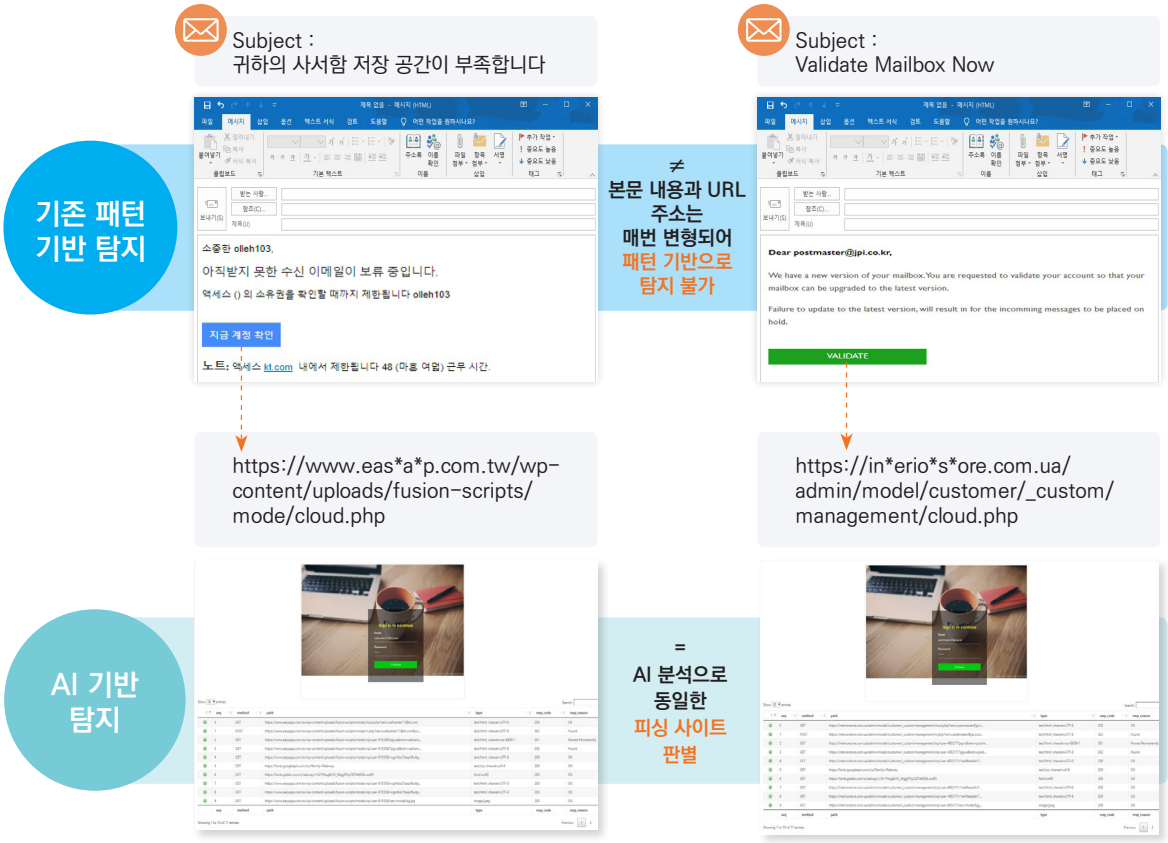
7-3 행위분석 기술대비 180배 빠른 탐지, 높은 정확도

악성파일을 이미지 변환 후 탐지하는 방식으로, 기존 Sandbox(동적분석)대비 변종 악성코드 탐지속도 180배 향상, 벡터 기반 유사도 측정 방식으로 다양한 변종 공격도 높은 정확도로 탐지



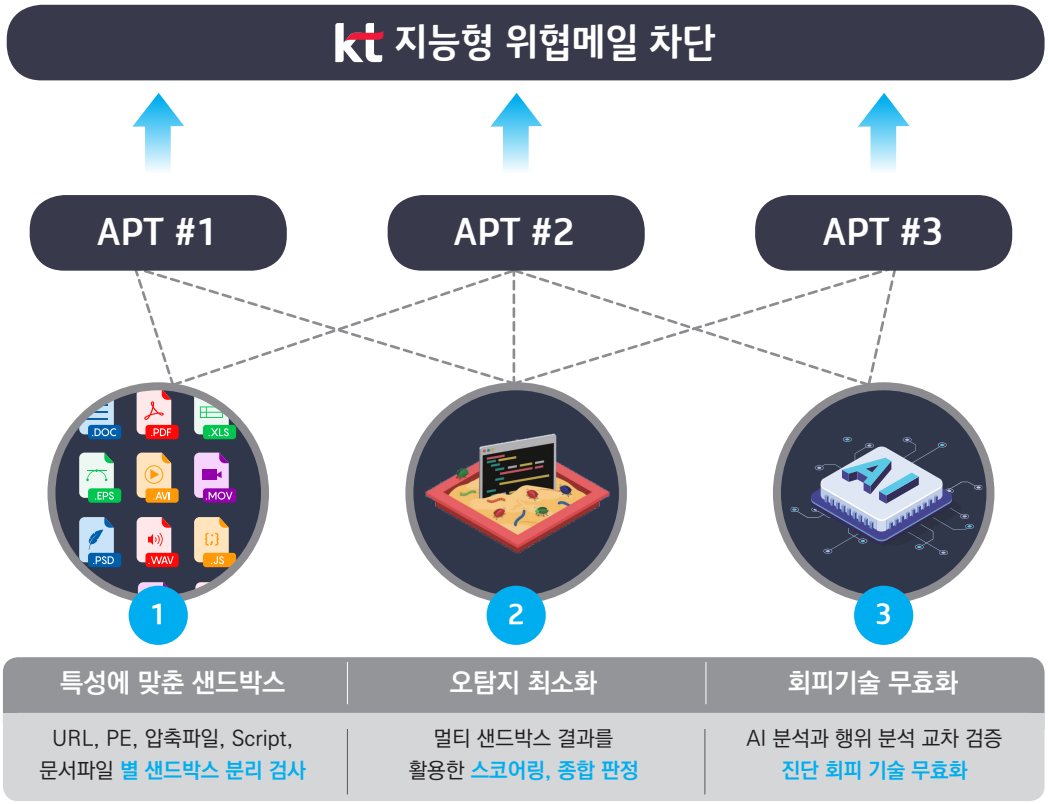
7-4 패턴 기반 솔루션의 피싱 URL 탐지 한계를 AI 기술로 극복

피싱메일 본문의 텍스트와 피싱URL 주소는 매번 변형되기 때문에, 기존 패턴기반 기술로는 탐지가 어려우나, AI 분석은 AI 비전 기술을 통해 전문분석가가 해당 사이트에 직접 접속하여 분석하듯이 사이트 유사성 등을 판단하여 변종 피싱 사이트 탐지 가능



7-5 멀티 샌드박스 기반 동적분석 및 종합 판단으로 정탐율 향상

멀티 샌드박스 구성 및 특성에 따라 최적의 동적 행위 분석 / 종합 판단을 통해 악성 검출 및 정탐율 향상



❶ 실제 PC 유사 환경 파일 실행

- WIN 7, 10, 11 지원
- MS Office, 한글 HWP포함 (공식 라인선스)
- Edge, Chrome 브라우저
- 실제 파일 실행 스크린샷 제공

❷ 프로세스 행위 분석

- 행위정보(악성/일반)
  파일, 프로세스, 레지스트리, 스레드, 디스크, 디렉터리, 디버깅, 후킹, 라이브러리, 메모리, 익스플로잇, 암호화등
- 웜, 트로이목마
- 다운로더, 스파이웨이등

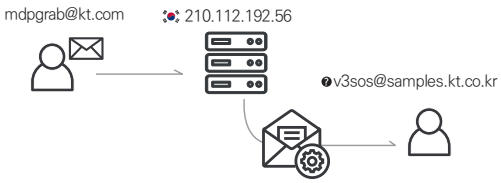
❸ 네트워크 행위분석

- API호출/C&C 서버 호출
- TCP/UDP/HTTP/HTTPS
- URL 분석/이상 트래픽 식별
- PACP 파일 다운로드 제공

❹ Dropped파일 분석

- 이벤트로 인해 생성된 파일 정보
- 특정 파일 핀포인트 분석 제공

❺ 공격 흐름도 분석



❻ 분석 요약 / 레포트 제공

- 위험도 : High, Medium, Low, Grey등
- 진단명, 감염 경로, 탐지 대상, 공격자
- 백신 진단 내역
- 탐지 원인 및 대응방안 제공

kt Enterprise

kt Enterprise | ㈜케이티 서울시 송파구 잠실로 209, KT송파빌딩
Enterprise.kt.com