SHIELDEX

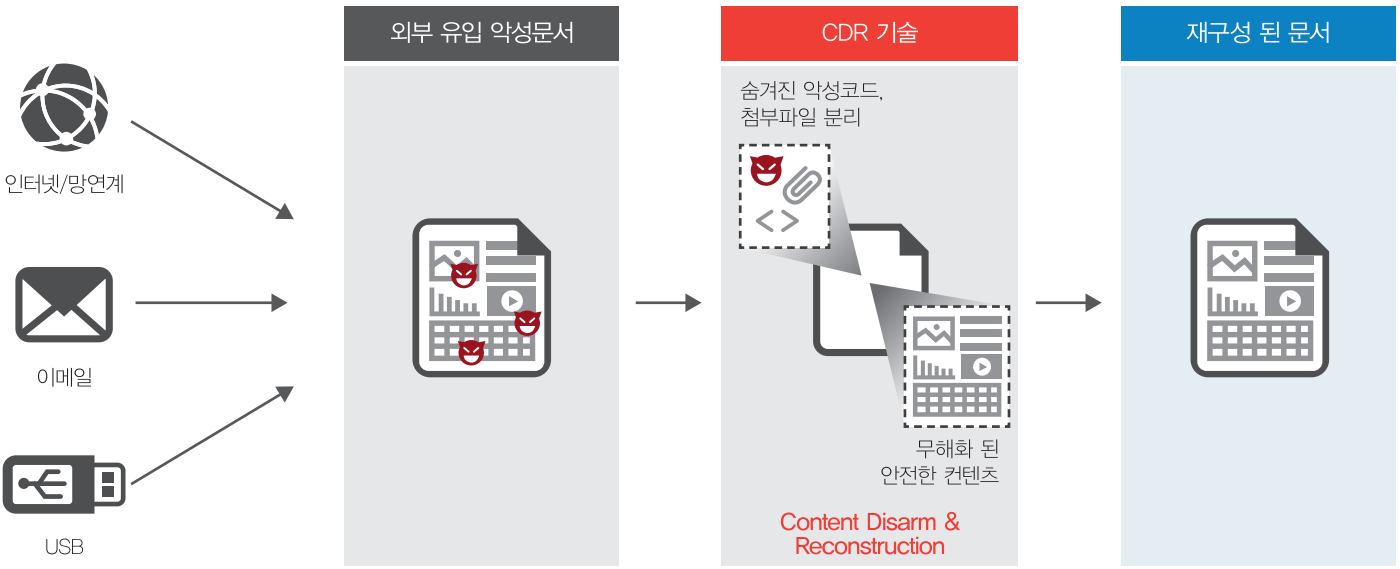
악성 문서파일에 의한 랜섬웨어, APT 공격 언제까지 당하고만 계시겠습니까?

CDR(Content Disarm & Reconstruction) 기술로 랜섬웨어, APT 공격 대응
문서구조 분석방식을 통해 외부에서 유입되는 악성 문서파일 무해화 및 재구성
문서 콘텐츠 내 의심 요소 제거, 안전한 콘텐츠로만 재구성하여 악성코드 원천차단

- 전 세계적으로 APT, 랜섬웨어 사이버위협 증가, 산업전반에 큰 피해 발생
- 기존 패턴 분석, 행위 분석 기반 탐지방식을 회피하는 악성코드 공격이 늘고 있는 상황
- 이메일 첨부파일, 인터넷 다운로드를 이용한 공격 방식이 늘고 있으며, 이에 대한 대응 필요
- 망분리가 도입된 환경이라도 이메일, USB, 망연계 서버로부터 유입되는 파일에 의한 공격 잠재

SHIELDEX

- 기존의 악성코드 탐지방식과는 차별화된 CDR/파일무해화 기술 적용
- 문서구조 분석방식으로 악성 문서파일을 무해화 및 재구성하여 외부유입파일에 의한 위협 방어



망분리 환경 보안 강화

망분리 환경에서 주요 경로를 통해 유입되는 외부유입 파일을 무해화하여 안전한 파일로 재구성

기존 탐지방식 한계점 보완

CDR 기술을 통해 기존 솔루션들이 탐지할 수 없었던 ZeroDay 등 알려지지 않은 악성코드에 대응

랜섬웨어, APT 공격 대응

문서구조 분석방식으로 문서 내 악성요소들을 제거하여 문서파일 형태의 악성코드 원천차단

적용대상

01
망분리 환경에서 외부유입파일에 대한 보안강화를 고려하고 있는 조직

02
APT, 랜섬웨어 등 사이버 위협에 대한 대응 방안을 고려하고 있는 조직

03
ZeroDay 등 알려지지 않은 공격에 대한 강화된 보안대책 마련이 필요한 조직

04
금융/에너지/국방 등 고도화된 사이버 테러 집단의 잠재적 공격 대상 조직

주요기능

문서 구조 스캔 (File Scan)

문서 파일 구조를 Scan 하여 문서 파일의 표준 구조와 다른 의심스러운 부분을 탐지

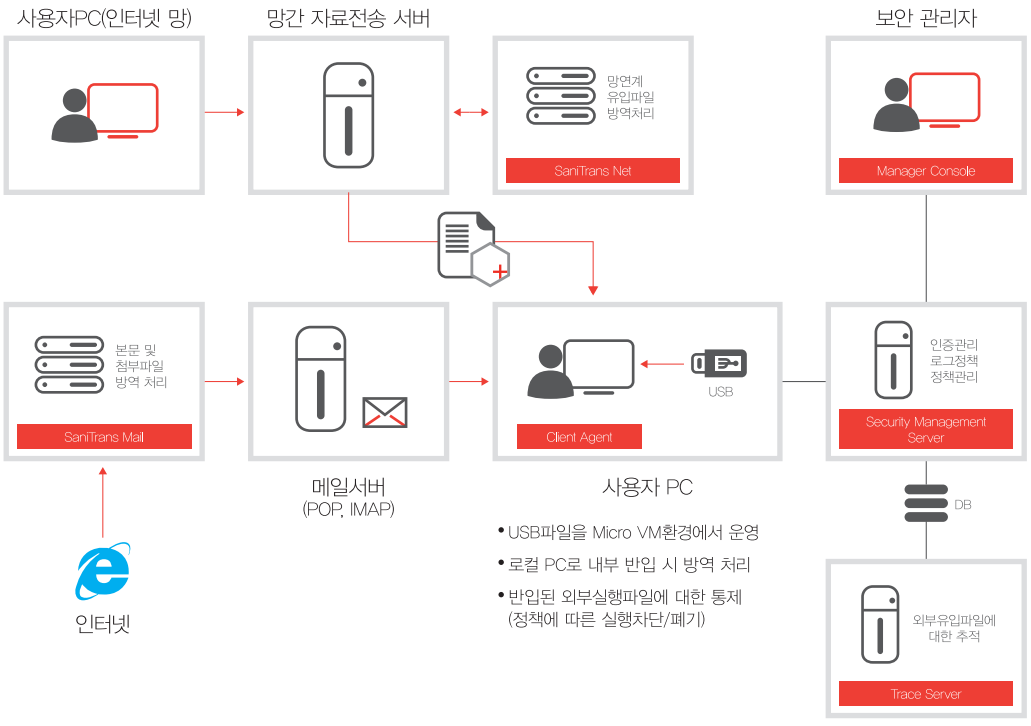
파일 무해화 (Content Disarm & Reconstruction)

무해화 기술을 적용하여 구조에서 의심스러운 부분을 제거하고 안전한 문서로 재구성

이력관리 (Logging)

원본 파일의 Hash 를 기준으로 다양한 무해화 처리 정보를 제공

시스템 구성도



옵션제품

Trace Server
외부유입파일 대한 추적/모니터링 관리 (차단정책 설정)

SaniTrans Net
망간자료전송시스템을 통해 내부망으로 유입되는 파일에 대한 방역 및 통제

SaniTrans Mail
외부 메일 본문 방역 및 첨부파일 방역

Client
외부 유입파일이 실환경에 영향을 끼치지 못하도록 Micro VM을 통한 가상화

외부유입파일의 이용내역 감시 및 PC해심영역 접근차단