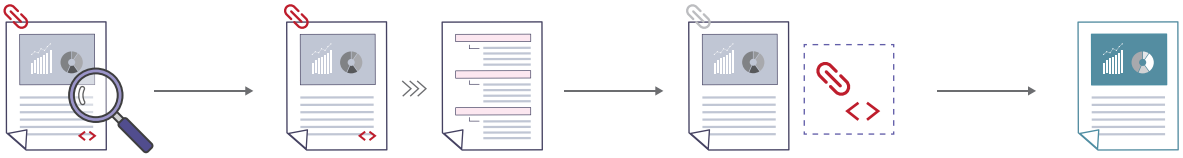
SHIELDEX

문서형 악성코드 선제적 대응
잠재적 위협요소 원천 제거하는 파일 무해화

CDR(Content Disarm & Reconstruction) 기술로 문서 콘텐츠 내 의심 요소 완전 제거
이메일, USB, 망연계 서버 등 외부에서 유입되는 모든 악성 문서파일 무해화 및 재구성
원본 포맷 그대로 깨끗한 콘텐츠로 구성된 파일만 내부로 안전하게 반입

문서파일을 매개체로 악성코드를 위장, 은닉하여 공격하는 사이버 위협 증가
이메일 첨부파일, 인터넷 다운로드 파일 등 다양한 경로를 통해 악성코드 유입
고도의 지능화, 우회적인 방식으로 기존 백신, 샌드박스 탐지 기술 회피하여 공격
망분리 환경이라도 업무 협업을 위해 외부로부터 유입되는 파일에 대한 위협 잠재



Format Verification

문서 포맷 확인

문서 헤더 구조 검사

Structure Analysis

문서 구조 분석

텍스트, 도형, 그림, 표 등
모든 문서 구성요소 구조 검증

Component Extraction

구성요소 추출 및 검증

올바른 구성 요소만 추출
추출된 콘텐츠 검증

Reconstruction Verification

재구성 및 검증

추출된 구성 요소로만 원본
포맷으로 문서 재구성 및 검증

완성도 높은 CDR 기술

20년 이상 문서보안에 특화된 기술력으로 CDR 기술 자체 개발
다년간의 경험으로 완성도 높은 문서 무해화 및 재구성 기술 구현

문서형 악성코드 위협 대응

문서를 기반으로 하는 랜섬웨어, APT 공격
알려지지 않은 악성코드, Zero-Day 공격 대응에 최적화

SHIELDEX

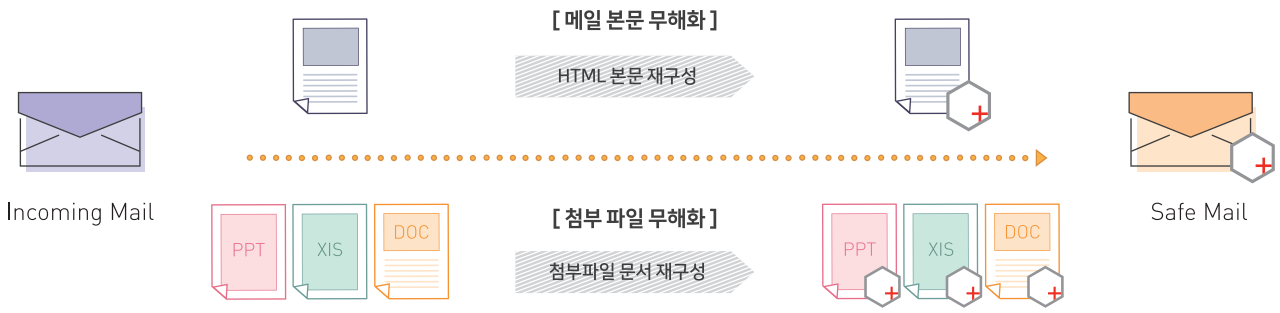
문서파일 클린존 구축

망분리 환경서도 외부에서 유입되는 모든 파일 무해화
깨끗한 문서파일만 내부망으로 반입하여 안전성, 보안성 확보

다양한 클라우드 환경 지원

현지 클라우드 업무 환경에 맞춰 적용 가능
원하는 클라우드 환경에 맞춰 유연하게 구축

SHIELDEX SaniTrans Mail

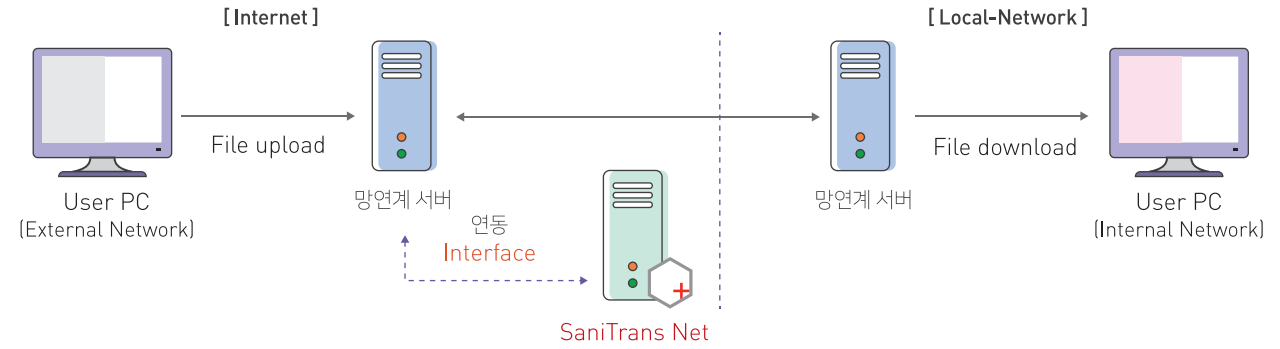


메일 본문 무해화 메일 본문 HTML 내 Script, Hyper Link, Linked Image 확인 및 제거하여 무해화

첨부 파일 무해화 메일에 첨부된 파일을 무해화 및 재구성, 원본 포맷 형태로 전달

결과 리포트 제공 무해화 처리 결과 제공, 악성파일, 매크로 제거 등 상세정보 확인 가능

SHIELDEX SaniTrans Net



망분리 환경에 최적화 망연계를 통해 유입되는 파일을 무해화 및 재구성, 망분리 환경 보안 강화

자체 망연동 모듈 도입 자체 개발한 망연동 모듈 탑재 All-in-One 제품으로 구성, 인터넷 분리상태 유지

망연계 보안체계 강화 문서반입 승인시스템과 연동, 문서파일 반입 시 관리자의 승인 후 반입 가능

Gartner 차세대 기술 제안

가트너 보고서에서는 현재의 APT 대응 기술은 딜레마에 빠져 있으며, 샌드박스를 사용하는 행위 분석방식에 의존하는 대신 새로운 아이디어 CDR 기술을 도입할 것을 제안하고 있다. (2017.02)

CDR 기술은 기존 APT 대응 솔루션에서 막지 못하는 알려지지 않은 악성코드 대응에 최적화된 신기술