

SHIELDDEX

Remote Browser

사이버 공격의 80%는 브라우저 보안 문제로 발생, 어느 것도 신뢰하지 마십시오.

극강의 제로 트러스트 Remote Browser 로 인터넷의 모든 것을 격리하세요.

브라우저 보안 문제를 엔드포인트로부터 분리하여 대응하는 웹 격리 서비스 (Browser as a Service) 웹 브라우저를 이용하는 사용자 경험에 영향은 주지 않으면서, 위협요소가 없는 새로운 보안 가치 제공
탐지가 불가능한 표적 공격에 대해 모든 콘텐츠를 사전 격리해 조직에 안전한 '제로 트러스트' 실현
사이트 소스 코드 분석 방식으로 나타나는 화면 깨짐 없이, 비주얼 스트리밍 방식으로 고도의 정합성 담보

- 조직 네트워크에 있어 외부 네트워크 접속은 악성 감염원이며, 80% 이상은 인터넷 통해 발생
- 피싱(Phishing) 사이트를 통한 개인정보 탈취 공격 증가
- 웹 격리는 보안 아키텍처에서 사이버 공격을 방지하기 위한 중요한 예방 전략
- 고도의 지능화, 악성코드 은닉 기법 다양화로 기존 보안 솔루션 우회 피해 사례 증가
- 조직/기업 내 웹 브라우저, 이메일을 통해 유입되는 파일과 링크에 대한 위협 잠재
- 기업을 대상으로 한 웹 기반 공격 노출의 확대에 따른 대응책 시급



SHIELDEX Remote Browser

웹 브라우저를 통한 사이버 공격, 이제는 '제로 트러스트' 웹 격리로 실현

외부 보안 공격의 98%는 인터넷을 통해 전송되며, 80%는 웹 트래픽 또는 URL을 사용하는 사용자를 타깃 해킹 공격의 거점이 될 수 있는 웹 브라우저 자체를 100% 격리함으로써 공격 노출면 자체를 제로화

소스 코드 분석 방식이 아닌, 사진을 찍는 듯 비주얼 스트리밍으로 고도의 정합성 보장

HTML, Javascript 등 소스 코드 분석방식으로 발생하는 화면 깨짐 없이, 비주얼 스트리밍 방식으로 정합성 보장 텍스트, 이미지, 동영상처럼 해커가 악용할 수 있는 콘텐츠(Contents)를 안전하게 격리

독자적인 격리 기술로 사용자는 원본 느낌 그대로를 보지만, 이미 내 PC는 100% 격리된 안전한 화면 수신

비디오 신디사이징 테크놀로지(VST, Video Synthesizing Technology)와 렌더링 인포 핸들러(Rendering InfoHandler)와 같은 소프트캠프의 독자적인 렌더링 기술로 사용자 PC에 안전한 콘텐츠 전송

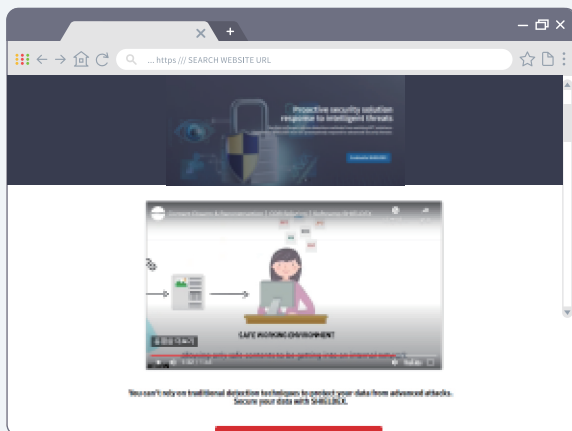
사이트별 대응이 아닌, 크로미엄 엔진 기반으로 선제적 기술 적용

가상화 된 브라우저 서비스를 제공하며, 최신의 크로미엄(Chromium) 기반의 엔진으로 상시 업데이트하여 유지보수 시, 안전하고 빠른 기술을 선제적으로 대응 가능

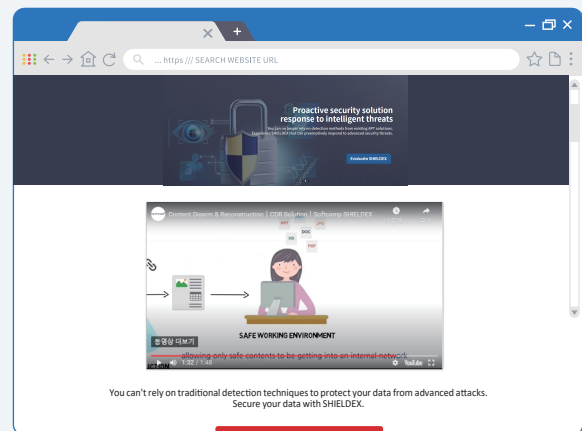
적용 대상

- 1 웹 기반 사이버 공격에 대응책이 필요한 조직
- 2 인터넷망을 통한 침투 방지 대책이 필요한 조직
- 3 보안 강화 차원에서 안전한 망 분리 방안에 대해 검토하고 있는 조직
- 4 보다 능동적인 새로운 사이버보안 방안에 대해서 고민하는 조직

SHIELDEX Remote Browser 의 우수한 정합성



타사



SHIELDEX Remote Browser

Gartner 차세대 기술 제안

원격 브라우저 제품 및 서비스를 통해 최종 사용자의 기기에서 벗어나 각종 위협을 방어할 것을 권장 (Innovation Insight for Remote Browser Isolation, 2018. 03)