Sasa Software

GATESCANNER®

글로벌 Top-class CDR 솔루션

'Malware 예방이 최고의 해결책 입니다'

대부분의 네트워크 공격은 이메일이나 공유파일을 통해 전달되는 악성 페이로드로부터 시작 됩니다. Malware의 진입 자체를 차단하는 것은 해커가 잠재적이며 파괴적인 랜섬웨어 혹은 APT 공격을 시작하는데 필요한 초기 발판을 확보하지 못하게 예방하는 효과가 있습니다.

그러나 Signature-base의 안티바이러스 도구는 고도로 난독화된 제로데이 Malware 를 탐지하지 못하는 반면, Behavior-base 휴리스틱 및 샌드박스는 멀웨어가 트리거된 후에만 작동됩니다.

CDR 기술은 탐지되지 않은 경우에도네트워크에 진입하기 전 첫관문 단계에서 파일기반위협을 직접적으로 제거합니다. 인입되는 컨텐츠는 'Re-Package' 되어 새롭고 깨끗한 파일 혹은 이메일로 목적지에 전달됩니다.

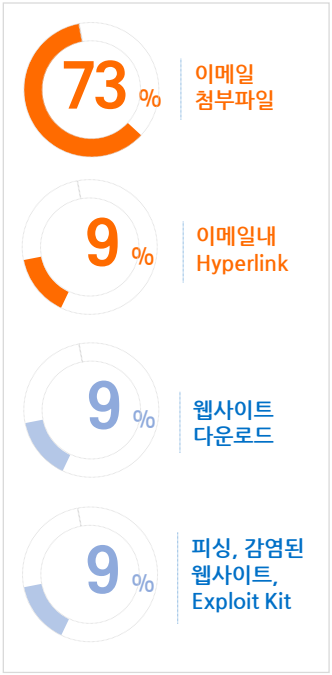
GateScanner® 의 CDR 기술을 통한 File Sanitization (파일살균)은 **"모든 파일 기반 Known / Unknown Malware 모두를 최대 99.9% 차단하는 것이 입증"** 되었습니다.

가트너로부터 '사이버 물리보안 시스템' 분야의 '**2020 Cool Vendor**' 로 인정

CDR 필수인 사이버 환경

이메일을 통한 Malware유입 82%

미국의 사이버보안 기관인 CISA의 2021년 발표에 따르면, 공격자들이 선호하는 Malware 전달 경로는 이메일 이며, 그 수치는 무려 82%에 달합니다.



Source) CISA, 2021

Gartner

" CDR protects against exploits and weaponized content that have not been seen before. "

도전 과제

개방된 컨텐츠 채널 유지와 내부망 및 내부 핵심 디지털 자산 보호라는 상충되는 시장 요구 만족

가장 정교한 네트워크 공격도 초기침투로부터 시작되고, 피싱 이메일 혹은 파일공유, 웹 다운로드, 공개 포털, APP간 통합 혹은 플러그인 USB 장치와 같은 다양한 루트를 통해서 들어오는 감염된 파일을 통해서 자주 이루어집니다.

증가하고 있는 유해한 환경에서, 출처에 상관없이, 내부망으로 인입되는 모든 파일에는, 대규모 공격의 문을 열수 있는 악성컨텐츠가 잠재적으로 포함되어 있다고 의심해야 합니다.

IT 보안팀은 일상적인 운영을 위한 중요한 역량인 전세계로의 개방된 컨텐츠 채널을 유지하는 것이고, 동시에 네트워크 손상을 방지하고 핵심 디지털 자산을 보호해야하는 서로 상충되는 요구사항에 직면해 있습니다.

해결책

글로벌 450여개 이상의 고객으로 부터 검증된 CDR 기술 적용

SASA Software의 GateScanner® 는 특정 임무가 할당된 모듈을 통해 제공되는 강력한 콘텐츠 살균 솔루션으로서, 모든 네트워크 구성 및 사용사례 (Use case)를 실질적으로 충족합니다.

CDR (컨텐츠 해제 및 재구성) 기술은, 원본으로부터 깨끗한 사본은 만들어내는 엄격한 소독 절차를 적용하여, 모든 컨텐츠 경로에 도착하는 파일과 이메일을 포함되는 악성코드 (Malware)를 무해와 (Disarm)합니다.

안전하고, 원본과 동등하고, 기능이 완전히 복원된 파일은 거의 실시간으로 목적지에 투명하게 전달 됩니다.

GateScanner® 는 2013년 부터 정부기관, 국방 조직, 제조업체, 석유/가스회사, 금융기관, 의료 기관 및 중요 인프라를 보호하고 있으며, GateScanner® 에 대한 고객들의 자체적인 Test에서 는 감지할 수 없는 ('Signature-less') 위협을 최대 99.9%까지 차단하는 것이 반복적으로 입증되었습니다.

* CISA : Cybersecurity & Infrastructure Security Agency
* CDR : Content Disarm & Reconstruction (컨텐츠 악성코드 무해화, 재조합)

적용 기술

GateScanner® 의 CDR 프로세스는 인입되는 파일을 가장 기본적인 구성요소로 분해하는 것으로부터 시작합니다.
멀티 Anti-virus 엔진과 AI 기반 탐지엔진이 분해된 파일의 각 구성요소에 개별적으로 적용 되어, '**비교할 수 없는 수준의 위협 탐지를 달성**' 합니다.
다음으로는, **자사 고유의 재조합 기술을 통해 파일을 재조합**하고, **구성요소들을 다시 섞어서 탐지를 교묘히 피해 남아있을 가능성이 있는 위협까지 제거** 합니다. 재조합을 마친 깨끗한 파일은 원본과 동일한 내용과 기능을 유지하고, 내부망으로 파일이 전달되어도 완벽히 안전합니다.

GateScanner® 제품군

GateScanner® Suite 모듈은 하기와 그림과 같이 핵심 CDR 파일 살균 기술과 다양한 적용사례를 수용하는 추가 기능을 제공합니다.

01

Kiosk

이동식 미디어 (USD, CD/DVD)에서 내부보안망의 목적지 Device로 안전하게 파일을 전송/관리합니다.

사전에 설정되고, 보안이 강화된 물리적 스테이션은 독립형 장치 혹은 네트워크 구성으로 작동될 수 있습니다. Mciro PC, 노트북, PC 또는 벽걸이/자립형 함체 형태로 제공할 수 있습니다.

02


API

GateScanner의 REST API 구현을 통해 모든 데이터 스트림에 파일 살균기능을 적용합니다. 타사 어플리케이션과 OEM에 추가 보안계층을 추가합니다.

스캐닝 엔진은 On-premise에 위치하거나, 프라이빗 또는 퍼블릭 클라우드 내의 가상환경 내에서 구현될 수 있으며, 서비스로도 이용 가능합니다.

03

Mail Gateway

Office365, MS exchange로의 직접적인 통합 혹은 메일 전송 에이전트(SMTP bridge), 보안 이메일 게이트웨이와 같은 유연한 설치 옵션을 보유한, 기업 이메일 보안을 위한 완벽한 솔루션 입니다.

이메일 본문과 첨부파일 모두에 대해서 심층 Content URL 분류를 통해 실시간 IP 평판 확인, 피싱 방지, 스팸 방지, 바이러스 검출, 스푸핑 방지 (DKIM,DMARC,SPF) 외부 도메인 차단 목록 (DNSBL) 기능을 제공합니다

04

Security Dome

디지털 금고를 사용하는 웹기반의 안전한 MTF (Managed File Transfer)솔루션입니다.

안전한 파일공유, 안전한 이메일, 자동화된 파일 전송 및 클라우드 스토리지 동기화를 지원하는 완전한 SaaS, 다중 Tenant 플랫폼입니다. URL 분류 기능이 있는 브라우저 플러그인을 제공합니다. 지원되는 파일 소스는 이메일, 금고(Valult), OneDrive, FTP, FTPS, SFTP, UNC 및 로컬 폴더 입니다.

05

Imaging Gateway

방사선 영상 파일(DICOM)을 의료기관의 PACS시스템에 안전하게 업로드하는 기능 제공합니다

CDR 기술을 이용한 자산 고유의 DICOM 위협 스캐닝 엔진은 DICOM 파일을 픽셀 데이터와 메타데이터로 분해하고 멀티 Anti-Virus 엔진으로 스캔하며, 환자의 영상자료의 우발적/의도적 오용을 방지하기 위해 HIS (Health Information Security)를 준수/검증됩니다.

06

Desktop

사용자의 Desktop PC에서 GateScanner Desktop Agent를 설치하여 CDR 스캐닝과 Redaction 기능을 사용할 수 있도록 합니다.

LAN 내부 및 외부 스캐닝을 가능케하고 AD (Active Directory) 와의 통합도 지원합니다. DMZ에 확장 가능한 가상 GateScanner 엔진 그리드를 사용하여 중앙에서 파일을 스캔할 수 있습니다.

07

Multi-Source

분리된 네트워크에 있는 어플리케이션들간의 다중 소스 보안 파일전송을 지원합니다.

GateScanner Injector 단방향 Data Diode와 결합하여, 분할된 에어갭 네트워크를 지원할 수 있습니다. 지원되는 파일 소스/목적지는 FTP, FTPS, SFTP, UNC, SMB, 공유 및 로컬 폴더 입니다.

08

Injector

에어갭 네트워크에 적용되어, 다양한 GateScanner Software 솔루션과 통합 연동되어 중단 없는 데이터 전송 서비스를 제공합니다.

TX/RX 분리형 제품으로 광 Data Diode 기능을 제공하며, 100Mb (~35Gb/hr), 1Gb (~120Gb/hr)의 전송속도를 선택할 수 있고, 지원되는 프로토콜은 SMB, Syslog, SMTP, STMP,TCP, UDP 입니다.

Sasa Software 소개

Sasa Software는 파일기반 공격을 방지를 전문으로 하는 사이버 보안 회사입니다.

Kibbutz Sasa가 Plasan Defense Industry 의 분파로 2013년에 설립한 Sasa Software는 비상장 회사입니다.
모든 수익은 지속 가능한 성장과 소중한 고객의 지속적인 장기적 지원을 보장하기 위해서 R&D에 재투자하고 있습니다.

GateScanner는 전세계 450여 곳 이상의 의 정부기관, 국방 조직, 제조업체, 석유/가스회사, 금융기관, 의료 기관 및 중요 인프라를 보호하고 있습니다.

ISO 27799 ISO 27001

Sasa Software
www.sasa-software.com / sales@sasa-software.co.kr