악성 코드 탐지 및
제거 통합 솔루션

Kaspersky Scan Engine

kaspersky 미래를 실현하세요

소개

Kaspersky Scan Engine(KSEn)은 대부분의 애플리케이션에 적용할 수 있는 최고의 위협 탐지 솔루션을 제공합니다.

Kaspersky Scan Engine(KSEn)은 웹 포털과 애플리케이션, 프록시 서버, 네트워크 탑재 스토리지, 메일 게이트웨이를 대상으로 포괄적인 보호를 제공합니다.

관리도 쉬우며, HTTP 및 ICAP를 통해 독립 실행형 서비스나 확장 가능한 클러스터, Docker 컨테이너로 쉽게 배포할 수 있습니다. KSEn은 최신 탐지 방식을 사용하여 트로이목마, 피싱 위협, 웜, 루트킷, 스파이웨어, 애드웨어와 같은 악성 코드를 탐지하고 제거합니다.

통합 시나리오

웹 포털 및 클라우드 서버

파일 서버

네트워크 장착 스토리지

메일 서버

웹 및 프록시 게이트웨이

앱 스토어 및 마켓

핵심 기능

두 가지 주요 모드

클라이언트 앱에서 HTTP 요청을 받고, 이 요청에서 통과한 개체를 검사하고, 검사 결과와 HTTP 응답을 회신하는 REST식 서비스.

프록시 서버 / NAS / 웹 애플리케이션 방화벽 / NGFW / ICAP 프로토콜을 통해 통신하는 기타 솔루션을 통과하는 HTTP 트래픽 검사 ICAP 서비스. 이 통합 모델은 사용자가 요청한 URL을 검사할 수도 있습니다. 이에 따라 악성 코드, 피싱, 애드웨어 콘텐츠가 있는 웹 페이지가 필터링됩니다.

KSEn for Linux

Linux Docker 컨테이너로도 이용 가능(HTTP & ICAP 모드에서). Docker Swarm, Kubernetes, AWS EKS, 그리고 기타 유사한 클라우드 환경에 개별 컨테이너로 배포할 수 있습니다.

GUI

Kaspersky Scan Engine은 제품의 동작을 쉽게 설정하고, 서비스 이벤트와 검사 결과를 검토할 수 있는 웹 기반 그래픽 사용자 인터페이스를 포함합니다.

사용 사례

모든 네트워크 솔루션과 통합

다양한 기능의 REST식 API와 오픈 소스 코드로, 사용하는 네트워크의 솔루션 대부분에 Kaspersky Scan Engine을 통합할 수 있습니다.

악성 코드 업로드로부터 웹 포털 보호.

악성 콘텐츠 업로드로부터 공용 (AWS S3 bucket 등) 및 사설 (Nextcloud, ownCloud, 그 외 기타) 클라우드 스토리지 보호.

악성 앱 업로드로부터 앱 스토어와 소프트웨어 마켓 보호.

Windows/Linux 파일 스토리지에서 악성 코드 검사.

제삼자 웹/메일 게이트웨이를 위한 악성 코드 방지 플러그인. 완료된 통합 목록은 요청 시 확인 가능하며, 꾸준히 업데이트됩니다.

기업 문서 관리 시스템, 소프트웨어 개발 파이프라인, 그 외 파일 악성 코드 검사가 필요한 기타 시스템에 대한 악성 코드 방지 모듈.

주요 기능

수상 경력에 빛나는 악성 코드 방지

수상 경력에 빛나는 Kaspersky 악성 코드 방지 기술은 최고의 악성 코드 탐지율을 제공하며 새로운 위협에도 즉시 대응할 수 있습니다.

필터링

악성, 피싱, 애드웨어 URL을 필터링합니다.

탐지

다중 실행 압축 개체 탐지.
광범위한 실행 압축 및 압축 형식 지원.

플랫폼 커넥터

Amazon S3, Nextcloud, ownCloud, Kubernetes 등, 다수의 제삼자 플랫폼을 자체 지원 또는 커넥터를 통해 지원합니다.

파일 치료

감염된 파일, 압축 파일, 암호화된 개체 치료. 탐지된 모든 위협은 한 번에 제거하거나, 악성 페이로드만 제거하고 나머지 파일을 안전하게 보존할 수 있습니다.

업데이트

업데이트 가능한 안티 바이러스 엔진으로 안티 바이러스 데이터베이스 정기 업데이트를 통해 탐지 기술과 처리 로직을 업그레이드하거나 수정할 수 있습니다.

고급 기능

고급 휴리스틱 분석과 머신 러닝 기반 탐지 기술.

빅 데이터

빅 데이터를 기반으로 Kaspersky Security Network에서 파일과 웹 리소스의 평판 정보를 확인하여 더 빠르고 정확한 탐지를 보장합니다.

확장성

Kaspersky Scan Engine은 최고의 성능을 제공하며 확장도 아주 쉽습니다.

형식 인식기

형식 인식기 구성 요소로 추가 필터링 레이어를 구성할 수 있습니다. 이 구성 요소를 사용하여 검사 절차에서 특정 형식의 파일을 인식하고 건너뛸 수 있습니다. 실행 파일, 오피스, 미디어, 압축 파일 등 광범위한 형식을 지원합니다.

TLS 지원

REST식 서비스 모드 실행 시 TLS 프로토콜을 통한 통신을 지원합니다.

클러스터 모드

Kaspersky Scan Engine은 클러스터 모드로 실행이 가능합니다. Kaspersky Scan Engine의 인스턴스 다수를 같은 네트워크에 배포하고 웹 UI를 통해 관리할 수 있습니다.

Kaspersky Scan Engine 2.1의 새 기능

2022년 6월 기준

안전 및 규정 준수

다중 사용자 모드와 역할 기반 액세스 제어 작업 감사 API 토큰을 통한 HTTP 클라이언트 인증 지원 웹 UI에서 암호 무차별 공격 방지.

구조적 변경

Scan Engine은 개별 릴리스 가능한 2개 모듈로 나뉩니다. (1) AV engine (KAV SDK) 과 (2) 기본 제품 기능(KAV SDK에 Scan Engine을 래퍼로 사용).

문서 개선

SIEMs와의 통합 매뉴얼(MicroFocus ArcSight, Splunk). Oracle Solaris VScan, F5 Application Security Manager, GoAnywhere MFT, Dell Isilon OneFS 와의 통합 매뉴얼.

작업 개선

서비스 사용 시 Systemd를 완전히 지원. (start/ stop/status/ restart)

클러스터 모드 개선

클러스터에서 유휴 상태 노드 자동 제거 및 형식이 다른 클러스터(HTTP 및 ICAP) 지원.

syslogging 변경

다중 대상
이벤트 필터 전송.

수상 경력

독립 테스팅 랩에서 Kaspersky 제품의 최근 수상

더 보기

Kaspersky Scan Engine

30일간 무료 체험해 볼 수 있습니다!
아래 링크를 클릭하고 KSEn 체험 요청을 보내주십시오.

더 보기

www.kaspersky.co.kr

#kaspersky
#bringonthefuture