kaspersky

kaspersky THE POWER OF PROTECTION

KASPERSKY SECURITY FOR BUSINESS PORTFOLIO

Twitter.com/ Kaspersky

Facebook.com/ Kaspersky

Youtube.com/ Kaspersky

이메일 | sales@kaspersky.co.kr

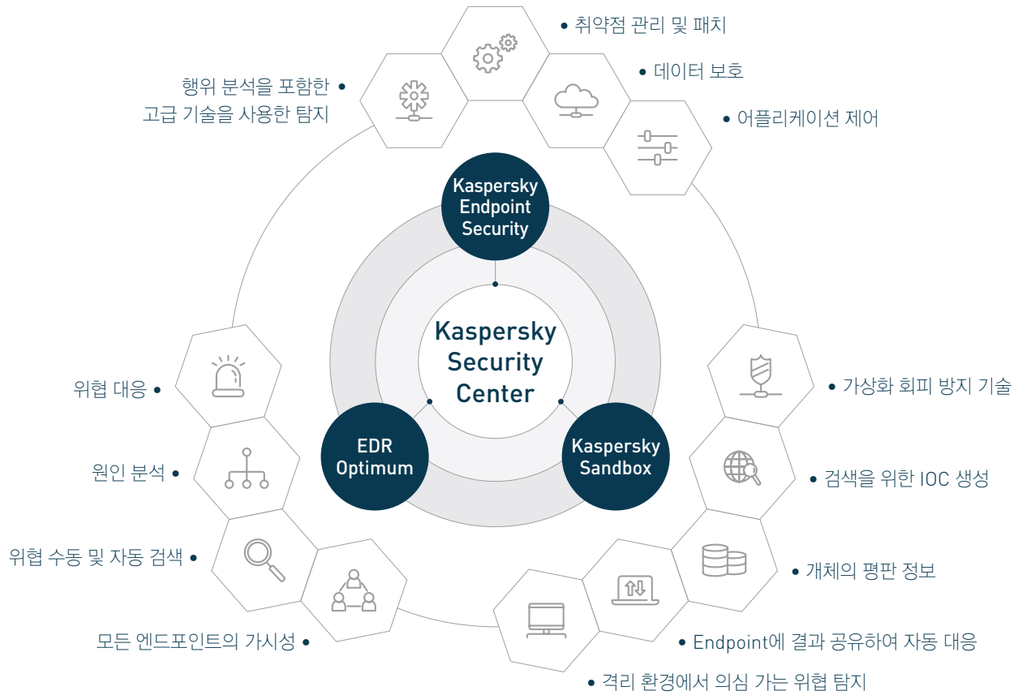
다양한 보안 정보 | www.securelist.com

파트너 찾기 | http://www.kaspersky.co.kr/partners

Kaspersky Lab Korea | www.kaspersky.co.kr

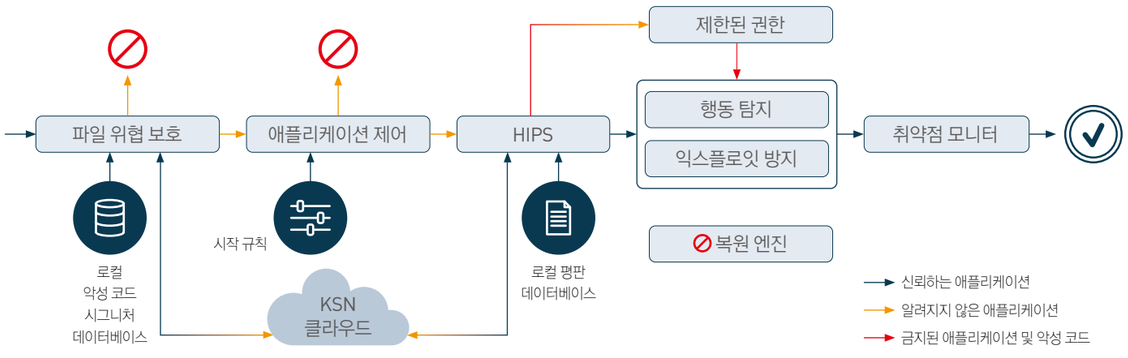
카스퍼스키 엔터프라이즈 솔루션

카스퍼스키가 제안하는 엔드포인트 보안 전체 개요



Kaspersky Endpoint Security

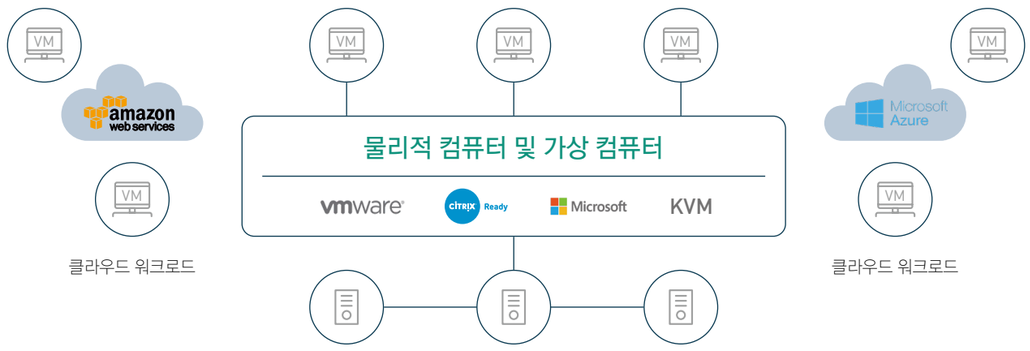
다양한 수상 경력으로 입증된 업계 최고 수준의 Kaspersky 검사 엔진이 운영 체제의 여러 레벨에서 동작하여 악성 코드를 효과적으로 차단합니다. 또한, 클라우드 기반의 Kaspersky Security Network(KSN)를 통해 새로운 보안 위협으로부터 사용자를 실시간으로 보호합니다.



KASPERSKY HYBRID CLOUD SECURITY

최고의 보호 성능과 데이터센터의 운영 유형에 상관없이 통합 관리할 수 있는 하이브리드 클라우드 보안 솔루션

사내 설치형 인프라 운영과 함께 퍼블릭 클라우드 리소스와 호스팅 클라우드 리소스를 결합하면 비용 효율성이 우수한 IT 환경을 구축할 수 있지만 보안과 관련해서 새로운 문제가 발생할 수 있습니다. 하이브리드 클라우드 환경 전반에 동일한 보안 기준을 엄격히 적용해야 하기 때문입니다. 이를 성공적으로 실현하지 못할 경우 기업의 가장 귀중한 자산인 데이터를 잃게 될 수 있습니다.
Kaspersky Hybrid Cloud Security는 통합 운영되는 맞춤형 사이버 보안 체계를 실현해줍니다. 무중단으로 운영되며 탁월한 효율성을 최적의 조합으로 제공하기 때문에 프라이빗 클라우드나 퍼블릭 클라우드에서 중요한 비즈니스 데이터를 처리하거나 저장할 때 시스템 성능 저하 없이 최신 위협은 물론 알려지지 않은 미래의 위협으로부터 기업의 인프라를 보호할 수 있습니다.



STEP1. 물리적 환경, 가상 환경 및 클라우드 환경을 모두 아우르는 차세대 보안

카스퍼스키의 특허 기술과 다양한 수상 경력으로 입증된 보안 엔진을 사용해 운영 환경에 관계 없이 모든 워크로드를 보호합니다. 머신 러닝이 지원되는 실시간 다계층 보안으로 새로운 위협으로부터 데이터, 프로세스 및 애플리케이션을 보호할 수 있습니다. 새로운 데이터 보호 규정인 PCI-DSS, 개인정보보호법, EU GDPR 등을 완벽하게 준수합니다.

STEP2. 리소스 효율성이 우수한 하이브리드 클라우드 보안

퍼블릭 및 관리형 클라우드 보안 통합을 통해 최소한의 리소스만으로도 애플리케이션, OS, 데이터 처리, 사용자를 모두 보호할 수 있습니다. 가상 컴퓨터 기술 기반의 Agentless 버전과 Light Agent 버전을 통해 시스템 성능 저하 없이 하이퍼바이저를 사용하는 프라이빗 데이터 센터를 안전하게 보호합니다. 물리적 리소스와 가상 리소스의 관리 통합을 실현하여 관리 효율성이 우수합니다.

STEP3. 통합관리 및 운영

효율적인 관리 기능과 보안 운영이 다양한 클라우드 환경에서 동작합니다. 최신 위협에 대한 완벽한 가시성과 제어 기능, 포괄적인 보호 기능 덕분에 모든 환경에서 워크로드가 안전하게 운영됩니다. 하이브리드 클라우드 환경 전반에 보안 서비스를 보다 쉽게 구축하고 정책 기반 운영을 실현할 수 있습니다.

다양한 장점을 가진 탁월한 기술

완벽한 가시성

- 통합 보안 운영 방식으로 사무실, 데이터센터, 클라우드에서 사용되는 엔드포인트나 서버 등 모든 기업 컴퓨터의 사이버 보안 관리를 하나의 콘솔에서 수행할 수 있습니다.
- 클라우드 API를 사용해 퍼블릭 AWS 및 Azure 환경과 완벽하게 통합 되기 때문에 인프라 검색, 에이전트 배포 자동화 및 정책 관리가 가능하여 보안 시스템 구축 작업을 더욱 손쉽게 수행할 수 있습니다.
- 유연한 관리 옵션이 제공되므로 멀티 테넌시 기능, 권한 기반 계정 관리 및 역할 기반 접근 제어를 구현할 수 있습니다. 그 결과, 유연성과 함께 하나의 관리 서버에서 통합 운영의 이점을 모두 누릴 수 있습니다.

클라우드 워크로드 보호

- 애플리케이션 제어 기능을 갖추고 있어서 시스템 보안 강화를 위해 화이트리스트 운영 모드를 지원하여 하이브리드 클라우드 워크로드 전체의 보안을 강화할 수 있습니다.
- 매체 제어 기능을 활용하여 각 클라우드 워크로드 별로 접근할 수 있는 가상 미디어 장치를 제어할 수 있으며 웹 제어 기능으로는 불필요한 인터넷 접속과 인터넷 기반 사이버 위협으로부터 시스템을 보호할 수 있습니다.
- 네트워크 별 관리 기능은 하이브리드 클라우드 인프라 네트워크에 대한 가시성과 자동화된 보호를 제공합니다. 또한 특정 네트워크나 포트 검사, VMware NSX와 같은 소프트웨어 정의 네트워크 플랫폼과의 통합도 지원합니다.
- 취약점 차단 기능을 제공하여 패치가 적용 안된 취약점을 악용한 지능형 악성 코드와 제로데이 위협으로부터 시스템을 보호합니다.

AI 지원 런타임 보호

- 수상 경력으로 입증된 안티 맬웨어 엔진이 모든 클라우드 워크로드를 악성 코드로부터 실시간으로 보호합니다.
- 클라우드 기반의 카스퍼스키 인텔리전스를 이용하여 신속하게 신종 위협을 식별하고 자동으로 대응 정보를 업데이트 받습니다.
- 메일 보안과 안티 스팸 기능이 클라우드 워크로드에서 이메일 트래픽을 보호합니다.
- 웹 보안과 안티 피싱 기능이 감염 가능성이 높은 웹사이트와 스크립트를 차단하여 위협을 방지합니다.
- 파일 무결성 모니터링 기능은 중요한 파일과 시스템 파일을 보호하며, 운영 체제 로그 파일을 검사하는 기능을 통해 운영 표준을 준수할 수 있습니다. 이는 PCI-DSS, EU GDPR, 개인정보보호법 등의 규정을 준수합니다.
- 동작 분석 엔진은 애플리케이션과 프로세스를 모니터링하여 지능형 위협과 파일리스 (Fileless) 악성 코드까지 차단하며, 필요한 경우 악성 코드로 인한 클라우드 워크로드 내부의 변경 사항을 원래대로 복구합니다.
- 취약점 방지 기능은 시스템 동작, 프로세스 및 애플리케이션 동작을 감시하여 취약점을 악용하는 지능형 위협을 차단합니다.
- 안티 랜섬웨어 기능은 랜섬웨어 공격으로부터 클라우드 워크로드에서 운영하는 로컬 컴퓨터의 파일뿐만 아니라 공유 폴더를 보호합니다.
- HIPS/HIDS는 클라우드 기반 자산에 대한 네트워크 공격을 탐지하고 차단하는 역할을 합니다.

다양한 클라우드를 아우르는 통합 보안

퍼블릭 클라우드
- AWS (Amazon Web Services)
- Microsoft Azure

프라이빗 데이터센터
- VMware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM

VDI 환경
- VMware Horizon
- Citrix XenDesktop

물리적 서버
- Windows
- Linux

Kaspersky EDR(Endpoint Detection and Response) & KATA(Kaspersky Anti Targeted Attack)

기업들은 현재 지능형 위협과 최신 사이버 공격에 대한 대응으로 보안 전략을 개선하고 있습니다. 주요 공격 대상은 여전히 엔드포인트이지만 오늘날의 지능형 위협은 기존의 엔드포인트 보안 솔루션을 회피하기 위해 계속적으로 진화하며 비즈니스 항상성을 손상시키고 생산성이 악화시키며, 이는 운영 비용의 증가로 이어집니다.

Kaspersky EDR

적응형 위협 대응

광범위한 자동 대응 기능이 포함되어 있으므로 다운타임이나 생산성 저하와 같은 문제를 야기하는 기존 치료 프로세스 (완전 삭제 및 백업/복구)에 의존할 필요가 없습니다.

직관적인 웹 인터페이스

사용이 간편한 Kaspersky EDR의 브라우저 기반 인터페이스는 보안팀이 통합 화면으로 가시성을 확보하여 탐지, 조사, 방지, 경고, 보고 등의 기능을 제어할 수 있습니다. 단일 인터페이스를 통해 매우 다양한 기능을 모니터링 및 제어할 수 있기 때문에 보안팀이 더욱 효율적이고 효과적으로 보안 업무를 수행할 수 있으며 별도의 도구와 여러 개의 콘솔을 옮겨가며 사용할 필요도 없습니다.

KATA 와 Sandbox 와의 통합

Kaspersky Anti Targeted Attack Platform과 통합되어 있어, EDR로부터 수집한 사건 관련 데이터뿐만 아니라 네트워크로부터 수집한 데이터를 통합 분석하여 사건의 전후 맥락 히스토리를 완벽 제공합니다.
또한 Kaspersky Sandbox와 통합되어 있어, 의심스러운 File은 자동으로 Kaspersky Sandbox를 이용하여 분석 후 위협 정보를 제공합니다.

KATA

다각적인 고급 탐지

Kaspersky Anti Targeted Attack Platform은 Kaspersky EDR의 탐지 정보와, 여기에 추가로 네트워크 트래픽으로부터 수집한 정보를 연계한 데이터를 기반으로 종합적인 상관관계 분석을 수행합니다. 최고의 보안 인텔리전스와 첨단 머신러닝 기술을 기초로 네트워크와 엔드포인트 데이터, 샌드박스와 인텔리전스 분석을 결합하여 사건의 상관관계를 파악하고 침해 지표(IoC)를 검색하며 매우 복잡한 표적형 공격을 탐지합니다. 사건을 구성하는 다양한 요소들을 연결하여 전체 공격 체인을 총체적으로 밝혀 냅니다.

지능형 위협 자동 예방 종합적 대응

Kaspersky Anti Targeted Attack Platform은 기존 카스퍼스키 보안 솔루션과 자동으로 탐지 정보를 공유합니다.
Kaspersky Anti Targeted Attack Platform, Kaspersky Security for Mail Gateway, Kaspersky Endpoint Security, Kaspersky Endpoint Detection and Response 등이 네트워크 및 엔드포인트에 이르기까지 긴밀하게 통합되어 있어 사건이 발생하면 충분한 정보를 바탕으로 전 영역에서 즉시 대응을 시작합니다.

기존 엔터프라이즈 보안 기능과 통합

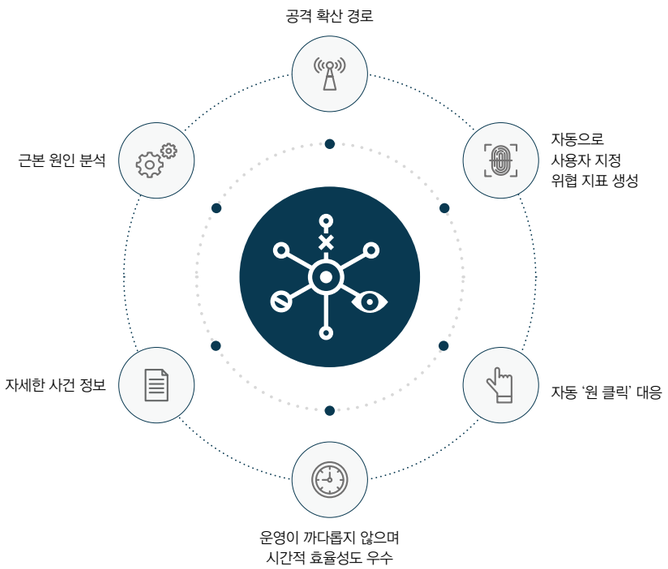
조직의 기존 보안 솔루션은 새로운 침해 정보와 탐지 정보를 공급받아 위협을 차단하는 데 협업할 수 있습니다.
차단 규칙을 NGFW(차세대 방화벽)으로 전송할 수 있으며 침해 이벤트 데이터는 SIEM(보안 정보 및 이벤트 관리 시스템)으로 전송되어 분석되며, 침해 URL은 NGFW, IPS, SWG에 추가 될 수 있습니다.

Kaspersky EDR Optimum

중소형 기업을 위해 최적화된 EDR 솔루션으로 엔드포인트 제품과 연계해 의심스러운 공격에 대한 추가적인 위협 정보를 제공하여 최적의 가시성을 제공하며, 자동으로 위협을 검색할 수 있는 위협 지표를 생성하여 엔드포인트에 적용 합니다.

주요목표

- 사건을 가시적으로 더욱 분명하게 확인 가능
- 솔루션 구축 관련 경비 절감
- 간단하게 사용할 수 있는 조사 도구 제공
- 복잡하고 모호한 위협에 신속하게 대응하여 더 큰 피해 발생 방지



Kaspersky Sandbox

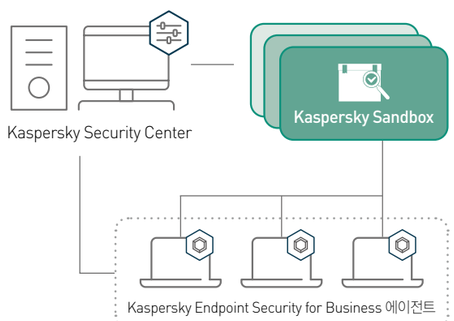
기업에 침투한 의심스런 파일을 엔드포인트에서 Sandbox 로 자동 전송하고 분석하여 악성여부를 판별하며 자동으로 그 위협을 처리합니다. 기존 엔드포인트의 탐지 및 대응 능력을 강화함으로써 알려지지 않은 위협에 더욱 빠르게 대응 할 수 있습니다.

Kaspersky Endpoint Security for Business의 기능을 확대하여 복잡한 위협을 파악 및 차단

- 지금까지 알려지지 않은 악성 코드
- 신종 바이러스 및 랜섬웨어
- 제로데이 익스플로잇 등

사용 사례

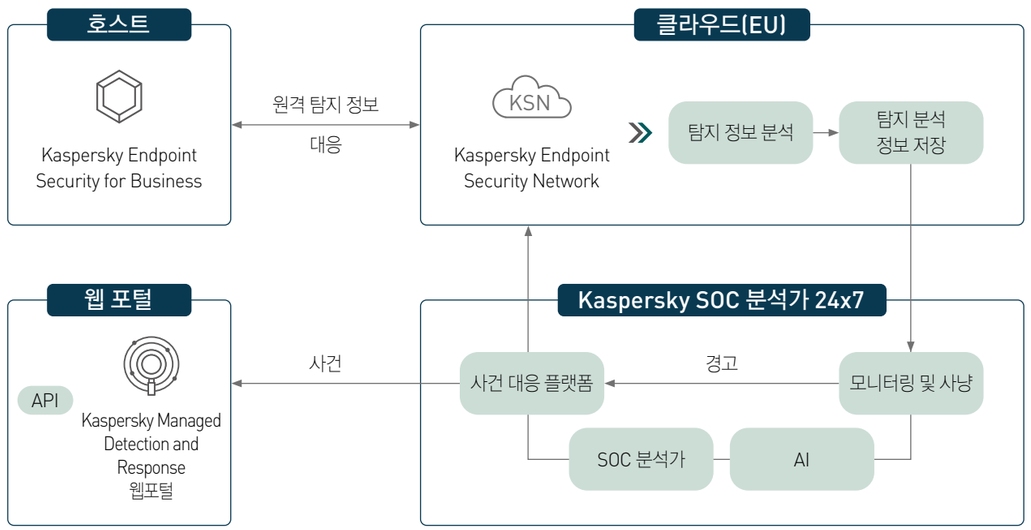
- Kaspersky Endpoint Security for Business의 행동 탐지 모듈을 종료한 상태에서도 고부하 터미널 서버를 보호
- Kaspersky Security Network와 연동 안 된 엔드포인트 보호
- API를 통해 고객 인프라의 타사 애플리케이션과 통합 가능



리소스 제약으로 인해 엔드포인트에서 수행할 수 없는 동작 기반 탐지에 대한 추가 탐지 계층

Kaspersky MDR 서비스

카스퍼스키 Managed Detection and Response (MDR) 은 카스퍼스키 SOC 팀에서 직접 EDR 이벤트에서 위협을 찾아주는 관리형 서비스 입니다. 고도로 자동화 된 머신러닝 기반으로 고객에게 완벽한 가시성과 사건 대응 방안을 MDR 웹 포털을 통해 자동화 하여 제공합니다.



Kaspersky MDR 라이선스 구성

Kaspersky Managed Detection and Response

추가 옵션

- 규제 및 포렌식/e-검색 요구사항에 맞추기 위한 유연한 저장 및 유지 옵션
- 추가적인 SOC 분석가 시간

서비스

- 위협 평가
- SOC 분석가를 위한 실습 교육
- 사건 대응 자문

Optimum

- 24시간 선제적 모니터링
- 위협 사냥 및 사건 조사
- 대응 계획서 및 자동 IR
- 보안 상태 점검 및 자산 확인 기능
- 대시보드 및 보고서가 제공되는 MDR 웹 포털
- 사건 기록 저장 1년
- 원시 데이터 저장 1개월

Expert

- 24시간 선제적 모니터링
- 위협 사냥 및 사건 조사
- 대응 계획서 및 자동 IR
- 보안 상태 점검 및 자산 확인 기능
- 대시보드 및 보고서가 제공되는 MDR 웹 포털
- 사건 기록 저장 1년
- 원시 데이터 저장 3개월
- 카스퍼스키 SOC 전문가와 연결
- Threat Lookup에 대한 요청 연간 1000회, Cloud Sandbox에 대한 요청 연간 500회
- 데이터 다운로드용 API

위협 인텔리전스 서비스

사이버 범죄는 경계 없이 어디서나 발생하고 기술적 역량도 빠르게 향상되고 있습니다. 사이버 위협의 빈도 및 복잡성 측면에서도 꾸준히 발전하고 있으며 조직의 보안을 무력화 시키기 위한 새로운 시도가 계속적으로 이루어집니다.
공격자들은 복잡한 킬 체인과 맞춤형 전술, 기법, 절차 (TTP: Tactics, Techniques and Procedures)를 공격에 적용해 비즈니스에 손상을 입히고 중요 지적 자산을 탈취하거나 조직의 명성에 악영향을 줍니다.
그러나 오랫동안 조직의 보안 전략은 네트워크 경계 및 워크스테이션 보호와 같은 수동적 전략에 머물러 있었습니다. 지능형 공격과 표적형 공격의 피해를 입는 기업이 점차 늘면서 이제는 위협 인텔리전스를 바탕으로 하는 새로운 보호 방법이 필요합니다.
페타바이트 규모의 풍부한 위협 데이터와 독보적인 글로벌 전문가 풀을 갖춘 카스퍼스키는 사이버 공격으로부터 조직을 보호합니다.

카스퍼스키가 제공하는 위협 인텔리전스 서비스는 다음과 같습니다.

카스퍼스키 위협 데이터 피드

조직은 매일같이 다양한 보안 제품에서 생성하는 수많은 보안 경고를 분석해야 합니다. 하지만 보안 분석가는 선제적 위협 사냥 및 대응에 집중하는 것이 아니라, 오탐지 분류에 업무 시간의 절반 이상을 소모하며 이로 인해 탐지 시간이 크게 지연됩니다. 이러한 정보 과잉으로 다수의 경고가 분석처리 과정에서 제외/누락 되며, 결국 전체 사건의 약 50%가 조사되지 않고 있습니다.

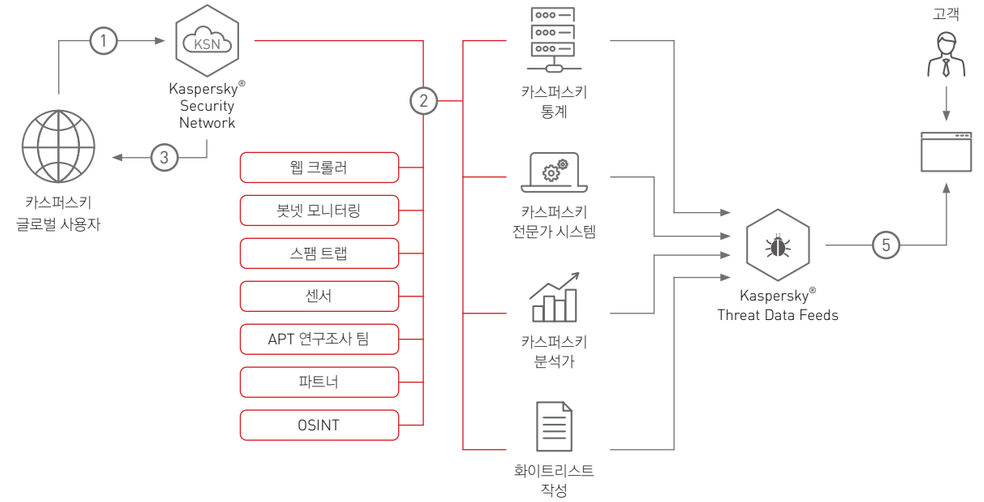
카스퍼스키 위협 데이터 피드는 의심스럽거나 위험한 IP, URL, 파일 해시 정보를 담고 있으며, 10분마다 업데이트되는 위협 인텔리전스 피드를 SIEM 시스템과 같은 기존 보안 제어 솔루션에 통합하여 보안팀에서 초기 사건 심사 프로세스를 자동화합니다. 또한 이를 통해 사건에 대한 충분한 배경 정보가 제공되므로 각 사건에 대해 추가 심층 조사가 필요한지 여부를 즉시 파악할 수 있습니다.
카스퍼스키 위협 데이터 피드는 SIEM과 연동하여 반복 분석작업을 자동화하고 보안 인프라에 대한 오케스트레이션을 제공합니다. 덕분에 보안 전문가는 더욱 스마트한 업무 처리와 빠른 대응이 가능하며 방어 역량도 크게 강화됩니다.

각 데이터 피드의 모든 기록은 실제로 활용 가능한 배경 정보와 함께 제공됩니다 (위협 명칭, 타임스탬프, 지리적 위치, 해결된 감염 웹 리소스 IP 주소/URL, 해시, 빈도 등). 배경 정보를 갖춘 데이터는 '전체적인 상황' 파악에 도움이 되기 때문에 더욱 심층적으로 유효성 검사를 수행할 수 있고 데이터의 광범위한 활용을 지원합니다. 배경 정보가 있으면 더욱 손쉽게 데이터를 사용하여 공격 주체, 내용, 장소, 시기를 파악할 수 있으며 이를 통해 악의적 사용자를 파악하며 시기 적절한 의사결정을 내리고 조치를 취할 수 있습니다.

- 20개 이상의 피드를 제공하며 대표적으로는 다음과 같은 요소가 있습니다.

IP 평판 피드	의심스러운 호스트 및 악성 호스트 관련 배경 정보와 함께 제공하는 IP 주소 세트
악성/피싱 URL 피드	악성/피싱 링크 및 웹사이트 정보
봇넷 C&C URL 피드	공격자 C&C 서버 및 관련 악성 개체 정보
모바일 봇넷 C&C URL 피드	모바일 봇넷 C&C 서버 정보. C&C와 커뮤니케이션하는 감염된 시스템을 파악
랜섬웨어 URL 피드	랜섬웨어 개체를 호스팅하는 링크 또는 이러한 개체를 통해 접근하는 링크 정보

취약점 데이터 피드	다양한 보안 취약점과 관련 위협 인텔리전스(취약한 앱/익스플로잇 해시, 타임스탬프, CVE, 패치 등)
APT IoC 피드	APT 공격 수행에 사용되는 악성 도메인, 호스트, 악성 IP 주소, 악성 파일 정보
IoT URL 피드	IoT 장치를 감염시키는 악성 코드의 다운로드에 사용된 웹사이트 정보
악성 해시 피드	가장 위험성이 높고 보편적으로 발견되는 신종 악성 코드 정보
모바일 악성 해시 피드	Android 및 iOS 모바일 플랫폼을 감염시키는 악성 개체 탐지 기능 지원
P-SMS 트로이목마 피드	SMS 메시지의 탈취, 삭제, 응답을 비롯하여 모바일 사용자에게 고액 요금을 부담시킬 수 있는 SMS 트로이목마 탐지 기능 지원.
화이트리스트 작성 데이터피드	합법적 소프트웨어에 대한 체계적 정보 제공



카스퍼스키 위협 인텔리전스 리포팅

• ATP 인텔리전스 리포팅

- ▶ 사이버 스파이 공격에 사용된 전술 및 방법 설명
- ▶ 공격자 프로필과 사용한 TTP(전술, 기법, 절차)
- ▶ 관련 TTP를 MITRE ATT&CK에 매핑 - 실제 경험을 바탕으로 하는 악의적 TTP 지식 기반
- ▶ 위험에 노출된 정보 자산 및 시스템, 침해로 인한 잠재적 영향, 그에 따른 우선순위 지정 방법을 파악
- ▶ 정보 보안 전략 조정을 비롯하여 잠재적 공격 벡터 처리 관련 특정 기술, 인력, 프로그램에 대한 투자 계획 및 타당성 입증

• Financial 위협 인텔리전스 리포팅

- ▶ 금융 부문 공격에 사용된 전술 및 방법 설명
- ▶ ATM 또는 POS 기기와 같은 특정 인프라 공격 관련 정보
- ▶ 다양한 지역의 다크넷 커뮤니티 및 포럼에서 사이버 범죄자들이 사용, 개발, 판매한 금융 네트워크 공격용 맞춤형 특정 도구 관련 정보

• 맞춤형 위협 인텔리전스 리포팅

- ▶ 고객 맞춤형 취약점 및 공격 위험 분석
- ▶ 소속 조직을 공격하는 활성 또는 비활성 악성 코드 샘플 파악, 모니터링, 분석
- ▶ 고객의 브랜드를 공격하는 피싱 위협
- ▶ 특히 한 기업의 고객, 파트너, 공급업체를 공격하는 위협 및 봇넷 활동의 증거

KASPERSKY EMBEDDED SYSTEMS SECURITY

Kaspersky Embedded Systems Security는 결제 시스템에 특화된 보안 솔루션입니다.

임베디드 시스템은 지리적으로 분산되어 있어 관리가 어렵고 업데이트가 자주 이루어지지 않아 보안이 취약한 영역 중 하나입니다. 현금과 신용카드 자격 증명을 다루는 ATM 및 POS 기기는 사이버 범죄의 표적이 되기 쉬우며, 따라서 이러한 기기에 특화된 보안을 제공하는 지능형 솔루션이 필요합니다.
PCI DSS(결제카드산업 데이터보안표준)에서는 수많은 기술적 요구사항과 신용카드 데이터 기반 시스템의 운영 방법을 규정합니다. 하지만 ATM 및 POS 장치의 보안 규정에는 안티 바이러스 기반의 보안만 정의되어 있습니다. 최근의 공격 유형은 안티 바이러스 접근법만으로는 오늘날의 ATM/POS 위협에 효과적으로 대응할 수 없습니다. 이제는 '매체 제어' 나 '애플리케이션 시작 제어'와 같이 입증된 보안 기술 접근법을 함께 사용하여 중요한 임베디드 시스템을 보호해야 합니다.

제품 특징

• 화이트리스팅 방식의 애플리케이션 시작 제어

지난 10년 간 Tyupkin, Skimer, Carbanak 계열을 비롯해 ATM과 POS를 겨냥하여 개발된 악성 코드가 증가했습니다.
대부분의 일반 안티 바이러스 솔루션은 이렇게 특정 대상을 노리는 최신 위협을 완전히 방어할 수 없습니다.
'기본 거부' 기능을 사용하면 소프트웨어 보안 기능을 제외한 어떤 실행 파일이나 드라이버, 라이브러리도 보안 관리자의 승인 없이 실행되지 않습니다.

• Windows XP ~ Windows 10 지원

Windows XP Embedded는 2016년 1월 12일에, Windows Embedded for Point of Service는 2016년 4월 12일에 지원이 종료되었습니다. 따라서 Windows XP 운영 체제는 더 이상 보안 업데이트나 기술 지원이 제공되지 않습니다.
하지만 Kaspersky Embedded Systems Security는 Windows XP 계열도 100% 지원하고 있습니다.

• 임베디드 시스템 하드웨어 맞춤형 설계

Kaspersky Embedded Systems Security는 대부분의 ATM 및 POS 하드웨어의 특징인 저사양 시스템에서 원활하게 동작할 수 있도록 설계되었습니다. Windows XP 계열 제품의 RAM 최소 요구 사항이 256MB밖에 되지 않기 때문입니다. 또한, 안티 바이러스 모듈은 수동 검사 또는 예약된 바이러스 검사 시에만 하드웨어 리소스를 사용하도록 구성했습니다.

• Kaspersky Security Network와 안티 바이러스

PCI DSS 규정에 따라 신용카드 또는 직불카드를 다루는 모든 시스템은 안티 바이러스를 설치하여 정기적으로 업데이트해야 합니다. Kaspersky Embedded Systems Security는 악성 코드 시그니처에 대해 정기적인 자동 업데이트와 필요에 따른 수동 업데이트 방식을 모두 지원하여 효과적인 안티 바이러스 보호 기능을 제공합니다.
또한, ATM 및 POS 시스템에서 발견되는 악성 코드의 과반수가 제로데이/제로세컨드 취약점을 통해 침입하는 만큼, 취약점 기반의 보안 위험을 예방 및 경감하고 대응 시간을 최소화하려면 클라우드 기반의 Kaspersky Security Network를 통한 지능형 보안을 적용하는 것이 좋습니다.

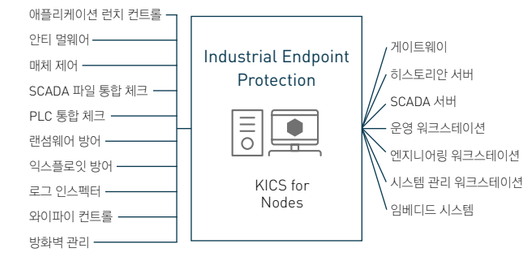
• 효율성 최적화 - 통합 관리

Kaspersky Embedded Systems Security를 사용하면 모든 엔드포인트를 완벽하게 파악하고 제어할 수 있습니다.
Kaspersky Security Center를 통해 하나의 콘솔에서 인벤토리와 라이센스, 원격 문제 해결 및 정책까지 전부 관리할 수 있습니다.
하나의 콘솔에서 관리자가 다양한 네트워크에 있는 모든 보안 에이전트를 관리할 수 있으므로 외부 접속이 차단된 폐쇄형 ATM과 POS 네트워크 환경에서 특히 유용합니다.

Kaspersky Industrial CyberSecurity (KICS)

카스퍼스키 KICS 주요 구성

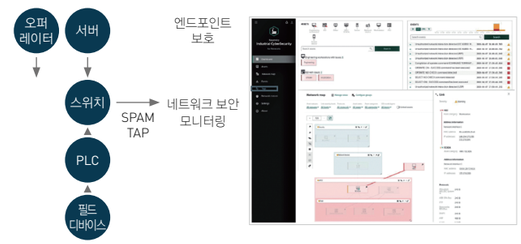
KICS for Nodes 주요 기능과 지원하는 엔드포인트



• KICS for Nodes
복잡한 OT/ICS 엔드포인트 보호로 공격 원천 차단

- ▶ 화이트리스트 기반 또는 블랙리스트 기반의 보안 정책 선택 적용
- ▶ 매우 낮은 리소스 점유율의 고급 안티 멀웨어 엔진과 랜섬웨어 방어 기능
- ▶ 다양한 매체 환경 제어 및 파일 무결성 모니터링
- ▶ Windows XP SP2부터 모든 Windows, Server 및 Linux 환경에서 사용 가능

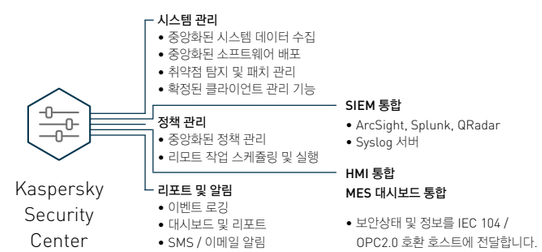
KICS for Networks



• KICS for Networks
OT/ICS 네트워크 영향 없이 네트워크 이상 행위 탐지

- ▶ 네트워크 트래픽 미러링을 통한 네트워크 및 사용자 이상행위 탐지
- ▶ 모든 네트워크 자산 관리 및 알려지지 않은 장치의 커뮤니케이션 탐지

Kaspersky Security Center



• Kaspersky Security Center
폐쇄망에서도 사용 가능한 중앙 보안 관리 시스템

- ▶ 중앙화된 시스템 관리 및 정책 관리
- ▶ 다양한 이벤트 로깅 및 리포트, 알림 제공
- ▶ SIEM 및 HMI, MES 대시보드 통합

Kaspersky Anti-Virus SDK

KASPERSKY ANTI-VIRUS® SOFTWARE DEVELOPMENT KIT (KAV SDK) V8은 여러분의 소프트웨어 및 하드웨어 솔루션에 안티 바이러스 기능을 추가하는 가장 신뢰할 수 있는 방법입니다. 간편하고 유연한 통합을 위해 Windows 및 Linux에서 사용 가능한 교차 플랫폼 API를 제공하며, 빠르고 원활한 통합을 위한 High Lever API와 세부적이고 유연한 통합을 위한 Low Lever API 세트를 제공합니다.

애플리케이션 영역

- 바이러스, 트로이목마, 웜 및 기타 악성코드, 스파이웨어 및 애드웨어
- 루트킷, 부트킷 및 기타 복합 위협
- 키로거, 화면 캡처 악성 코드에 의한 개인정보 도용
- 본넷 및 PC를 하이재킹하는 여러 가지 불법 행위
- 제로 데이 공격 및 알려지지 않은 보안 위협
- 드라이브 바이 다운로드 감염
- 기타 여러 사이버 보안 위협

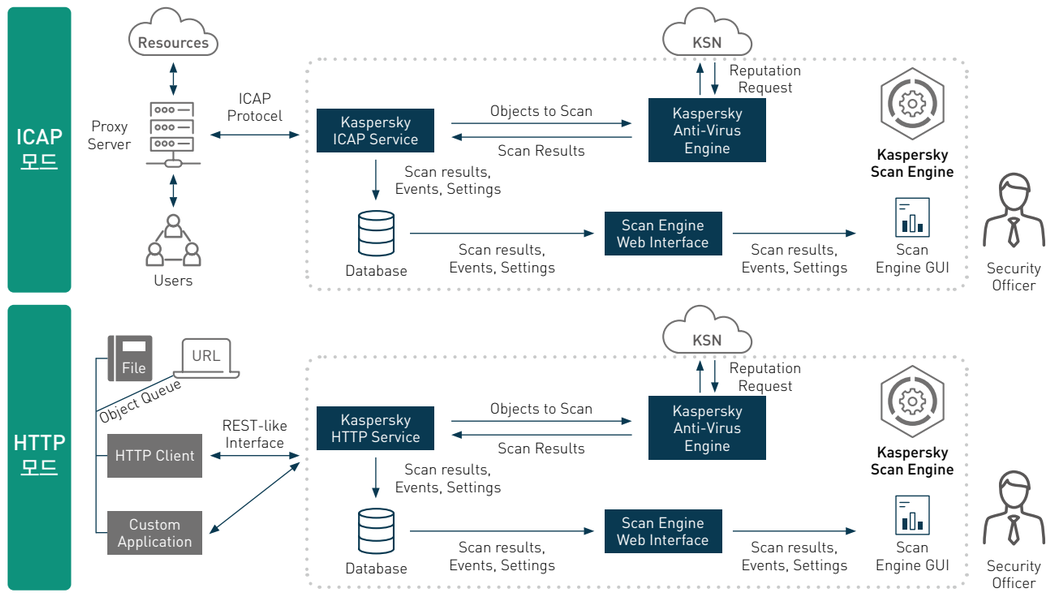
보호방법

- 오랜 히스토리를 가지고 있는 시그니처 분석
- 변종 탐지를 위한 제네릭 탐지
- 24x7x365 안티바이러스 연구소
- 가장 많은 수의 압축 유형 지원
- 자동 실행 파일의 의심스런 동작을 탐지하는 고급 휴리스틱

KAV SDK 외에도 Web Filter, Anti-Spam SDK, Mobile Security SDK, Online File Reputation, Anti-Virus for UEFI, DeepUnpack, SafeStream II와 같이 다양한 OEM 형태의 라이브러리를 전세계 유수의 고객에게 제공하고 있습니다.

Kaspersky Scan Engine

Kaspersky Anti-Virus SDK v.8 기반으로 개발되었으며 별도의 코딩이 필요하지 않은 기업 시스템의 안티 말웨어 솔루션으로 적합한 엔진입니다. 포털이나 트래픽 검사, 스캐너, 파일과 같은 사용자 지정 데이터 소스를 사용하는 맞춤형 시스템에 적합하며 ICAP, HTTP와 같은 표준 프로토콜 지원으로 빠르게 개발할 수 있으며 웹 UI 및 보고서 기능을 가지고 있습니다.



kaspersky

KASPERSKY 회사소개

Kaspersky는 세계 최대의 독립 보안 소프트웨어 업체입니다.

Kaspersky는 강력한 악성 코드 방지 도구, 유연한 제어 도구, 암호화 기술은 물론
시스템 관리 도구까지 포함하는 종합 솔루션을 통해 귀사의 조직에 가장 적합한 IT 보안을 제공합니다.

Kaspersky 보안 소프트웨어는 엔드포인트에서 서버와 게이트웨이까지 아우르는 폭넓은 범위에 걸쳐 제공되며,
Kaspersky의 독자적인 기술 개발을 통해 인프라의 규모에 관계없이 물리 장치, 가상 장치 및 모바일 장치 등
다양한 장치에 대한 보안 관리 및 제어 작업을 하나의 중앙 관리 콘솔에서 통합 관리할 수 있습니다.
또한 Kaspersky 기술은 전 세계에서 업계를 선도하는 여러 IT 제조업체 및 판매업체의 제품과 서비스에 널리 사용되고 있습니다

Kaspersky Mission

Kaspersky는 가정 내 컴퓨터 사용자부터 대기업이나 정부 기관에 이르기까지 모든 사용자가 중요한 정보와 자료를 보호할 수 있어야 한다고 생각합니다. 개인 정보, 가족, 재무 정보, 고객, 사업의 성공, 중요한 인프라 등 사용자에게 중요한 모든 것을 안전 하게 지키는 것을 기업 사명으로 삼고 있습니다.

Eugene Kaspersky Chairman and CEO, Kaspersky