Data Sheet

Genian Insights E

'Genian Insights E'는 다양한 위협에 대응하기 위해 EDR(Endpoint Detection and Response), AV(Anti-Virus), 안티랜섬(Anti-Ransom), 매체제어(Device Control) 등의 기능이 통합된 통합 단말 보안 플랫폼입니다.

Highlight

이벤트 정보수집 및 연동

- File, Module, Process, Network, Registry 정보
- 외부 저장매체 사용 현황 및 파일 정보
- Syslog, RESTful API, 손쉬운 연동을 위한 XDR 플러그인 지원
- 다양한 Sandbox APT 연동(Trend Micro, Check Point…)

수집정보 검색 및 가시화

- 위협 사냥(Threat Hunting)
- 수집 정보 Full-Text 검색 및 사용자 정의 검색 필터 제공
- 세부 정보 탐색이 가능한 타임라인 차트 지원
- 다양한 분석 위젯 지원 및 위젯 활용 이벤트 분석 정보 제공
- 관리자 정의 다양한 대시보드 설정 가능

최신 위협 인텔리전스 활용

- AV(Anti-Virus), IoC(침해 사고 지표)와 ML(머신러닝), MITRE
- ATT&CK 기반 XBA(행위 기반 엔진)을 통한 최신 위협 및 침해 사고 대응
- 탐지된 위협에 대한 위험도, 신뢰도 , 유사도 및 유형 정보 제공
- 커스텀 Malware Hash/IP, Good Hash/IP 추가 및 관리 기능
- 행위 기반의 Fileless 위협 대응
- 관리자 정의(Custom) Rule 지원

엔드포인트 위협 분석

- 위협 목록 및 분석 화면 제공
- 탐지된 위협의 상세 정보 제공, 의심 파일 수집
- 감염 및 접속 정보 모니터링 기능
- 파일 및 접속 프로세스 분석
- 이벤트 타임라인 및 연관 분석(Chain of Event)

엔드포인트 추적관리

- 이상 행위 프로세스 발생 시점 및 경로 정보 제공
- 위협에 대한 탐지 히스토리 관리
- 접속 프로세스별 추적 기능(사용자, 출발지 IP, 목적지 IP/포트 등)

안티랜섬

- 랜섬웨어 행위(문서 암호화)에 대한 실시간 모니터링
- 랜섬웨어 탐지 시 실시간 파일 백업/복원 기능 제공
- 탐지된 랜섬웨어 파일 및 랜섬웨어에 의해 생성된 파일 즉시 삭제

매체제어

- 이동식 디스크, 외장 하드디스크, CD/DVD 통제 (허용/읽기전용/차단)
- 공유폴더 제어, 안전모드 진입 방지

Challenges

보안위협의 지능화, 고도화

IT 환경이 급변함에 따라 보안 위협 또한 지능화, 고도화되며 다양한 경로를 통해 유입되고 있습니다. 또한 지속적으로 피해를 야기하고 있지만, 많은 기업과 기관들은 여전히 침해 사고에 무방비한 상태입니다.

기존 보안솔루션의 대응 한계

지능화, 고도화된 위협이 엔드포인트에서 실행 또는 은닉, 확산되고 있습니다. 그럼에도 불구하고 대부분의 기업, 기관에서는 Anti-Virus 제품과 네트워크 기반의 방어 체계로 대응하기 때문에 지능화되고 있는 엔드포인트 공격에 효과적으로 대응하기 어렵습니다.

전방위적인 위협 관리 및 대응 필요성

급변하는 위협 동향에 따라 엔드포인트 레벨에서 가시성을 높이고 다양한 탐지 기법을 활용한 악성코드/이상행위에 대해 조사, 분석하고 빠른 대응 체계를 구축하여 네트워크와 엔드포인트 등 내부 인프라 전반에 대한 체계적인 위협 관리 및 대응이 필요합니다.

key Features

지속 확장 가능한 가시성

- 단말의 모든 행위에 대하여 상시 수집
- 수집된 정보로 악성코드/이상행위에 대한 다양한 분석 기법 제공
  - AV(Anti-Virus), IoC(침해 사고 지표), CTI *, ML(머신러닝), XBA(행위 기반)
- 악성코드/이상행위에 대한 체인 이벤트 제공
- 관심 또는 연관성 있는 이벤트 간의 연결 고리 제공

* CTI : 지니언스 평판 시스템

수집된 데이터 기반 관리자 정의 대시보드

수집된 데이터의 분석 및 활용을 극대화하기 위해 관리자가 정의한 위젯을 통해 다양한 대시보드를 제공합니다.

Ecosystem

기업, 기관에서 수집된 위협을 Ecosystem으로 보내 위협에 대한 분석 결과(평판 서비스)를 제공하며 고객사에서 수집된 위협과 예외 처리된 데이터를 확인 및 가공하여 Genian Insights E를 사용하는 기업, 기관에 재배포합니다.

Genians

Components&Deployment

Genian Insights E는 서버와 에이전트로 구성됩니다. 서버는 고성능의 appliance 뿐 아니라 상용서버와 클라우드에서도 설치 운영할 수 있습니다. 에이전트는 사용자 PC(windows, macOS) 와 서버(Windows, Linux)에도 설치하여 보안을 강화할 수 있습니다.

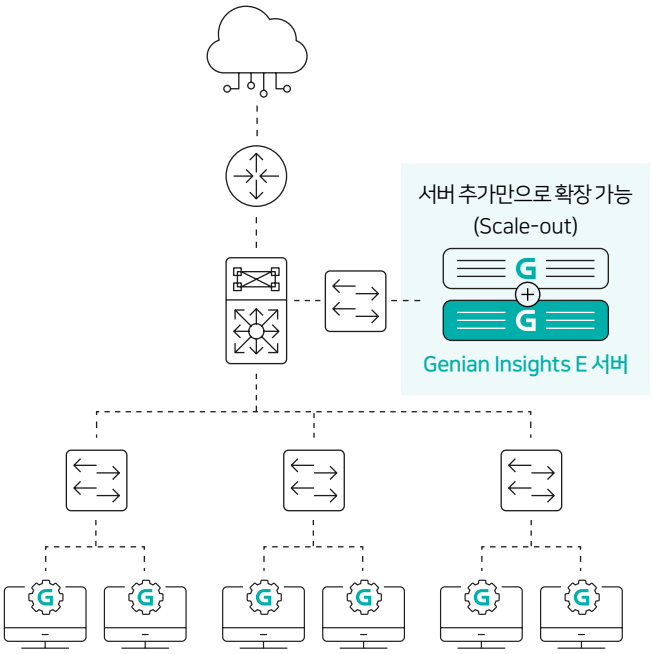
Policy Server

- Data 분석을 통한 위협 및 이상 징후의 탐지
- 탐지된 위협의 상세 내용 분석
- 로그 저장 및 검색 기능 제공
- 이벤트 통합 분석 및 연관 분석, 시계열 분석, 근원 분석 등
- 관리자 단계별 권한 위임을 통한 효율적 관리
- 분석 내용의 보고서, 위젯, 대시보드 등 시각화 및 표출

Agent

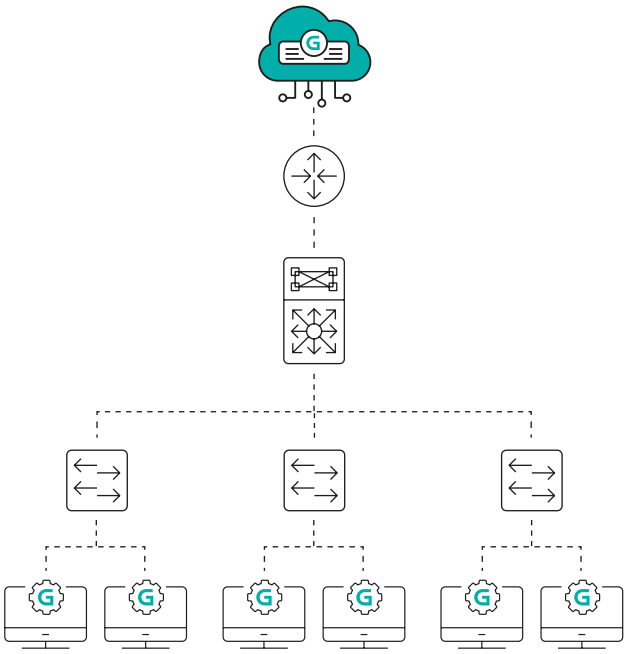
- 단말 주요 행위(파일, 프로세스, 접속, 레지스트리 등)의 모니터링 및 수집
- 추가 분석 필요한 PE 파일 Server 전송(샘플 수집)
- 위협 탐지 시 고지, 차단, 종료 등 단말 수준의 대응
- 위협 대상(파일 등)의 격리 및 사용자 알람, 네트워크 차단
- Off-Line 로그 수집

On-Premise



Genian Insighs E 에이전트

Cloud



Genian Insights E 에이전트

* Genian NAC 사용 시, NAC Agent에 플러그인(모듈) 형태의 간단한 배포와 인증정보 자동 연동 기능 제공

01 Genian EDR(Endpoint Detection & Response)

실시간 행위 기반 탐지 및 위협 대응으로 지능형 공격(APT)에 대한 심층 분석 및 빠른 대응 지원

02 Genian AV(Anti-Virus)

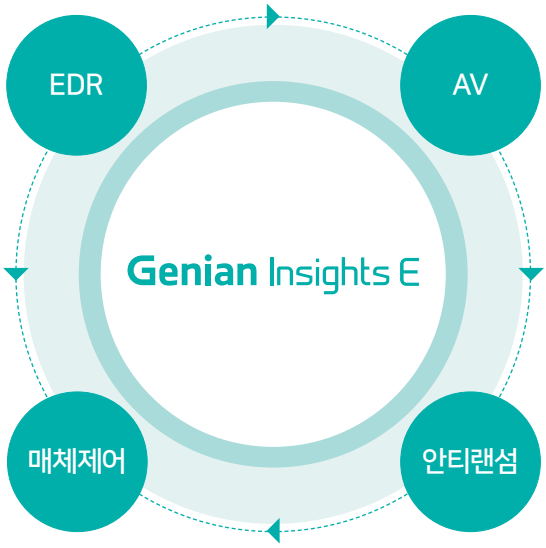
시그니처 기반 진단을 통한 악성코드 탐지 및 자동 치료

03 안티랜섬(Anti-Ransom)

파일 암호화 행위 실시간 차단, 중요 문서 파일 실시간 백업 및 자동 복원 기능으로 랜섬웨어 피해 최소화

04 매체제어(Device Control)

USB, 외장 하드 등 저장매체 사용 제어(read-only/write/block)로 내부 정보 유출 방지



Product Funtion

* 단일 에이전트, 단일 관리 콘솔을 통한 운영 복잡도 감소 및 관리 효율성 향상

(Windows 기준)

Category	Features
정보 수집	· 상시 로그 수집 및 분석 사후 조사와 분석을 위한 상시 정보 수집 · 엔드포인트의 다양한 정보 수집 파일/프로세스/모듈/네트워크 연결/레지스트리 등 · 침해대응 분석을 위한 Artifact 수집 시스템 정보, 윈도우 이벤트 로그, Prefetch 파일, Registry hive 등 · 문서/압축 파일 이동 현황 정보 수집 Web, 메신저, 공유폴더, 외장 저장장치 등 · 사용자 정의 윈도우 이벤트 로그 실시간 수집 · 장기간 Live 검색 데이터 Hot(신규 데이터)+Warm(오래된 데이터) 아키텍처
탐지 / 분석	· 악성코드 탐지 AV(Anti-Virus)와 IoC(침해 사고 지표) 기반의 악성코드 탐지 · Fileless 및 행위 기반 위협 탐지 · 탐지된 악성코드+이상행위에 대한 종합적인 분석 및 시각화 정보 Root Cause/Chain Analysis 등 · Process Tree 및 관련 정보 · 관리자 커스텀 룰 설정 및 탐지 · Remote Shell 원격 접속을 통하여 명령 수행 및 결과를 확인할 수 있는 보안점검 기능 · MITRE ATT&CK 탐지 룰 및 매트릭스 뷰 제공
대응	· 위협 탐지 시 대응 사용자/관리자 알림, 파일 격리/삭제, 프로세스 종료, 네트워크 격리 · 동일한 위협 탐지 시 설정한 대응 정책에 따른 자동 대응 · 랜섬웨어 대응 - Volume Shadow copy Service(VSS)를 활용한 스케줄 백업 및 복원 - 안티랜섬(Anti-Ransom) 엔진을 통한 문서 기반 실시간 백업 및 자동복원 · 탐지 정합성 향상을 위한 예외처리
운영 / 관리	· 관리 기능 인사DB 연동 다양화, 상/하위 그룹관리, 개별/통합 정책관리, 사용자정의 권한관리 · 유연한 대시보드 세분화 된 위젯, Customize, 공유 대시보드(export/import 포함) 등 · 매체제어 - 이동식 디스크, 외장 하드디스크, CD/DVD 통제(허용/읽기전용/차단) - 공유폴더 제어(허용/everyone 권한 제거/공유 해제), 안전모드 진입 방지 · 3rd party 연동 SIEM/SOAR, TI, Sandbox APT등 · 폐쇄망 환경 지원 솔루션 패치, 침해지표 최신화 등 수동 업데이트 기능 제공

Summry

안정성
낮은 리소스 사용
충돌 최소화 기술 적용

시장점유 1위
24/25년 조달 점유 1위
240여 곳 고객사 구축
(2026. 01)

안티바이러스
백신 모듈이 추가되어
더욱 강력한 탐지 기능 제공
(필요에 따라 On/Off)

빠른 성능
고성능의 SSD/ 최적화된 DB
사용으로 1억 건 5초 이내 조회
(빅데이터 필수 사항)

강력한 분석
수집된 정보를 활용
입체적인 분석 가능

안티랜섬
특화된 안티랜섬 기능
실시간 백업/탐지/대응/복원

장기간 로그 저장
로그 서버 추가 시
12개월 이상의 로그 보관
(+Scale Out)

탐지/대응 기본
EDR에서 제공하는 기본 이상의
다양한 기능+정보 제공

Windows	macOS	Linux
· Windows 7(SP2) 이상 · Windows Server 2012 이상	· macOS(BigSur) 11.0 이상	· CentOS : 6.4 이상 · RHEL : 6.4 이상 · Unbuntu : 18.04 이상 · Rocky : 8.4 이상 · Debian : 10 이상 · Fedora : 35 이상

Appliance Line Up

Policy/Log Server

모델명	ES300	ES300W	ES500
모델 이미지			
CPU	Intel Xeon 3.1G(6C12T)	Intel Xeon 3.1G(6C12T)	Intel Xeon 3.2G(16C32T)
Memory	64GB	64GB	128GB
HDD/SSD	1.92TB/4TB	1.92TB/12TB * 3(RAID-5)	3.84TB/16TB
Port	1G UTP * 2	1G UTP * 2	1G UTP * 4

14058 경기도 안양시 동안구 벌말로 66 평촌역 하이필드 지식산업센터 A동 12층
기술지원 : 1600-9750(평일 오전 9시~오후 6시) / 도입문의 : sales@genians.com