Leaflet

Genian Insights E

엔드포인트에서 발생하는 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.

Genian Insights E 필요성

01
백신으로 감지할 수 없는
다양한 신 변종 악성코드의 대응

02
APT(지능형 지속위협) 및
Fileless 공격의 대응

03
내부 위협 확산과 재발 방지를 위한
악성코드 유입 경로 확인 및 내부
정보 유출 확인

04
행위 분석 등 다양한 탐지 방식을
이용한 이상행위 및 악성코드 탐지

Genian Insights E 위협(Threat) 탐지

알려진 악성코드 대응

- AV(Anti-Virus)를 이용한 시그니처 기반 악성코드 탐지
- IoC(침해사고지표)를 이용한 알려진 악성코드 탐지
- 평판 정보를 통한 악성코드 탐지 및 유사도 확인

알려지지 않은 악성코드 및 이상행위 대응

- MITRE ATT&CK 기반의 탐지 룰과 자체 개발한 탐지 룰이 결합된 XBA 행위 탐지 분석 엔진
- ML(머신러닝) 기법을 이용한 악성 의심 파일 탐지
- Custom(사용자 정의) 탐지 룰 설정 기능 제공

Genian Insights E 위협(Threat) 대응

- 위협이 탐지되는 경우 에이전트에서 네트워크 격리, 파일 삭제, 프로세스 종료, 사용자 알림 등의 대응 수행
- 정책(Policy) 기반으로 즉시 작용하므로 확산 방지 등 초동 대응 가능

수집
- File
- Process
- Module
- Network
- Registry

탐지
- 자동 탐지
- 수동 탐지
- 의심

분석
- 유사도지표 분석
- 공격 스토리라인 분석

대응
- 프로세스 종료
- 파일 격리/삭제
- 사용자/관리자 알람경고
- 네트워크 격리
- 프로세스 덤프

자동 대응

수동 대응

Genian Insights E 특장점

EDR 국내 시장점유율 1위 및 국내 최초 보안기능확인서 획득
(인증번호: VSFT-KOIST-20220024)

파일, 프로세스, 레지스트리, 모듈, 네트워크 정보 수집으로
모든 프로세스에 대한 체인 이벤트 정보 제공

엔드포인트로부터 수집된 많은 데이터를 압축 전송 방식으로
사내 네트워크 영향 최소화

단말의 부팅부터 종료까지 모든 I/O 정보 수집으로
악성코드 유입 및 동작 방식 확인

Sandbox APT, SIEM/SOAR 등 위협 분석을 위한
솔루션과의 손쉬운 연동
- Restful API, SNMP, Syslog, XDR 플러그인

랜섬웨어에 특화된 전문 Anti-Ransom 엔진을 탑재하여
보다 정확하게 **랜섬웨어를 탐지/차단 및 복원**

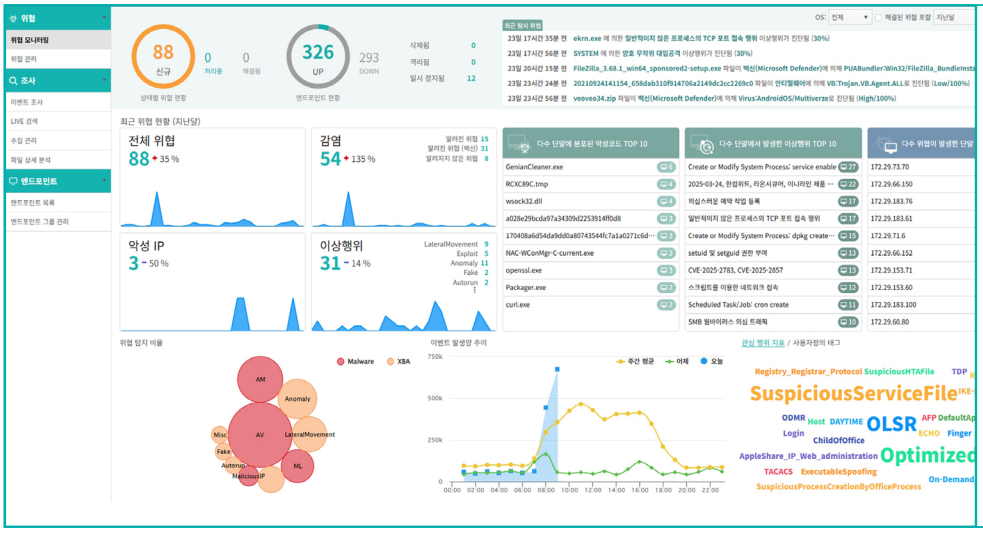
엔드포인트 내의 **다양한 가시성** 및 수집된 로그를
다양한 목적으로 활용할 수 있는 **유연한 대시보드 제공**

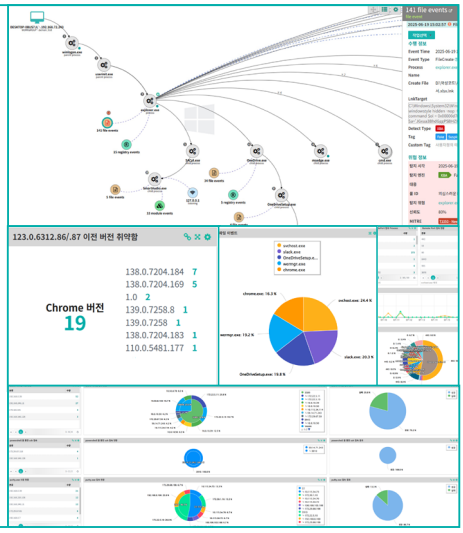
EDR, AV(Anti-Virus), 안티랜섬(Anti-Ransom),
매체제어(Device Control) 기능이 **통합된 에이전트 제공**

단말 부하 및 충돌 최소화한 탐지/분석
- 에이전트는 단말 영향을 최소화하여 이벤트 수집 및 이상행위를 탐지하고 대응 정책을 수행

폐쇄망 및 망분리, 가상화 환경(VDI) 등 다양한 구축
국내 대형 고객사의 **글로벌 법인 및 해외 사무소 구축**

Administrator UI





조달청 디지털서비스몰

※ 다량납품할인율: 25,300,000 이상 20% / 50,600,000 이상 25%

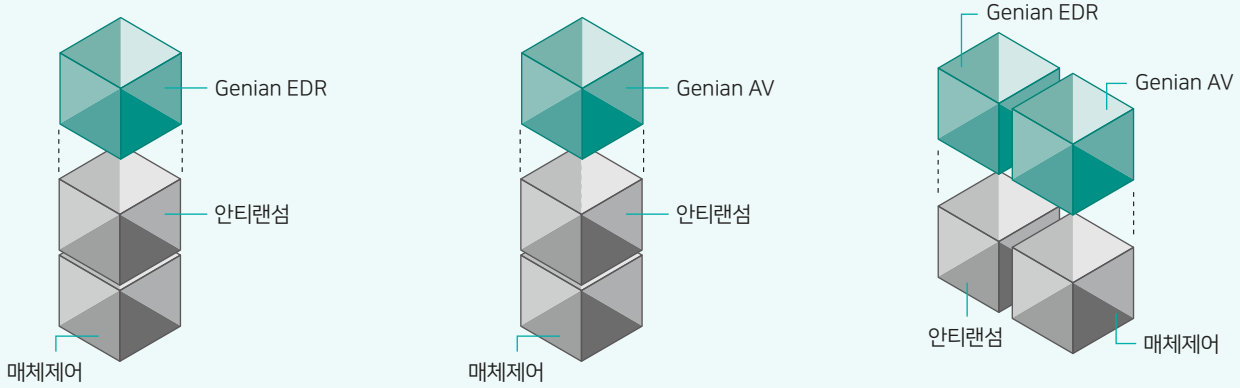
제품군	규격명	조달단가	물품식별번호
EDR 라이선스	Genian Insights E v2.0, Client, 연간라이선스	50,600	23929714

Genian Insights E 제품 구성

서버 & 에이전트 구성

- Genian Insights E 서버와 에이전트의 간단한 구성이며 On-Premise와 Cloud 모두 제공
- On-Premise 환경에서는 Scale-Out 기능을 제공하여 확장이 용이

단일/통합 에이전트



EDR 단독
+(addon)
안티랜섬 / 메체제어

AV 단독
+(addon)
안티랜섬 / 매체제어

EDR & AV
+(addon)
안티랜섬 / 매체제어

Genians

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

Genian Insights E
더 알아보기