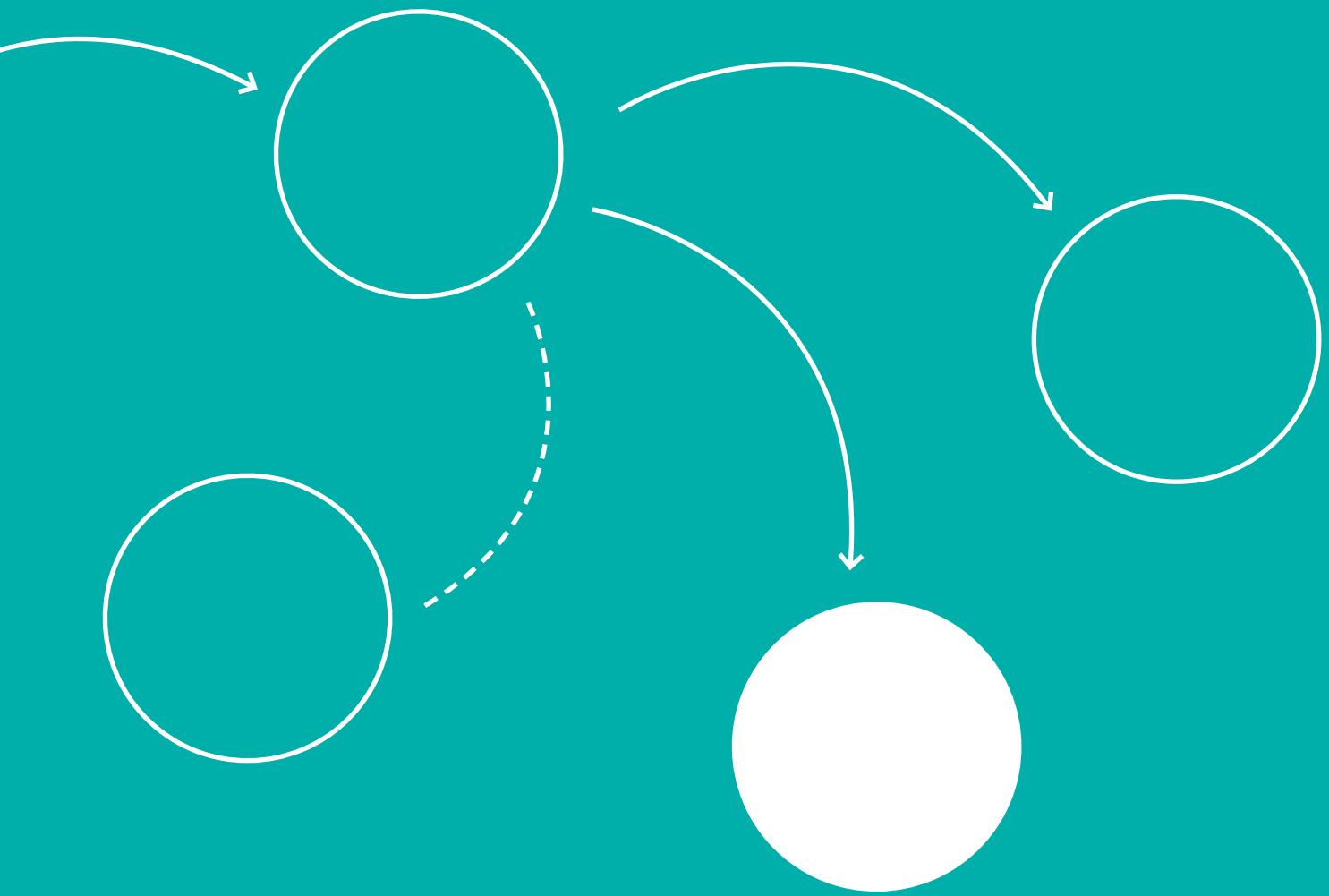
통합 단말 보안 플랫폼

Genian Insights E

v 3.X



Genians

Genian Insights E

Overview

APT(지능형 지속 위협) 및 랜섬웨어 등의 보안 위협은 기하급수적으로 확산되고 있습니다.
이러한 악성코드를 활용한 공격은 단순한 보안 위협 수준을 넘어, 실질적이고 심각한 경제적 손실을 초래하고 있는 상황입니다. 날로 지능화되는 APT, 랜섬웨어 등은 전통적인 보안솔루션을 통해 탐지하고 대응하기 어려운 것이 현실입니다. 운영 중인 다양한 보안솔루션으로도 찾기 어려운 내부 이상 행위 및 침해 사고를 탐지하고 발생한 보안 위협에 빠르게 대응할 수 있는 단말 기반 지능형 위협 대응 솔루션이 필요합니다.

'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.

악성코드 및 이상 행위를 최신 침해 사고 지표 (IoC), 백신 (AV)과 머신 러닝(ML) 행위 기반 엔진(XBA)을 활용해 신속하게 탐지하여 APT, 랜섬웨어 등의 공격을 실행단계에서 차단할 수 있습니다.

1. 단말 행위 모니터링/수집	2. 위협의 탐지	3. 위협의 대응	4. 탐지 위협의 조사/분석
· File, Module, Process, Network, Registry 정보 · 사용자 및 단말에서 발생하는 이상 행위 · 외부 저장매체 사용 현황 · 다양한 대시보드 제공	· AV(Anti-Virus)와 IoC*(침해사고지표) 기반의 알려진 위협 탐지 · ML(머신러닝)기반의 알려지지 않은 위협 탐지 · 행위 기반의 Fileless 위협 탐지 · YARA를 이용한 사용자 설정 기반의 심층조사	· 탐지된 위협 대상의 고지, 종료, 삭제, 네트워크 격리 · 알려진 위협 사전 대응 · 분석 후 대응(대응 시 동일 이벤트 자동 대응) · 샌드박스, SIEM 등 기존 보안 솔루션 연동	· 탐지된 위협의 상세 정보 제공, 의심 파일 수집 · 통합 검색 및 연관 검색 · 이벤트 타임라인 및 연관 분석(Chain of Event) · Ecosystem(평판 서비스) 제공

* IoC: Indicators of Compromise, 악성코드 및 접속 C&C 등 침해 사고의 흔적들에 대한 정형화된 데이터

통합 엔드포인트 보안

'Genian Insights E'는 엔드포인트를 노리는 다양한 사이버 위협에 대응하기 위해, 다음과 같은 보안 기능이 통합된 솔루션을 제공합니다.

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)**

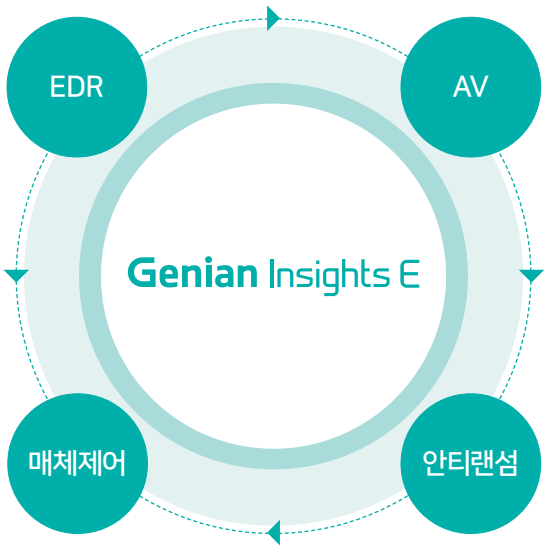
시그니처 기반 진단을 통한 악성코드 탐지 및 자동 치료

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



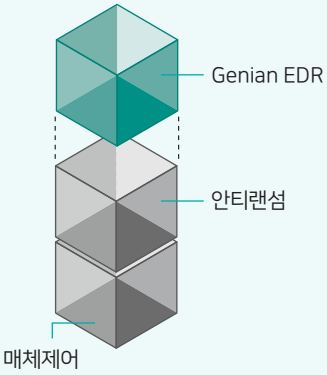
Key Features

에이전트 설치 및 운용

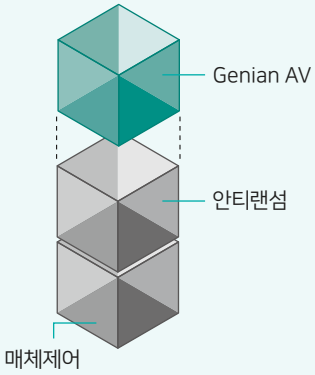
에이전트는 단말 부하를 최소화한 탐지/분석/대응과 EDR(Endpoint Detection and Response), 백신(Anti-Virus), 안티랜섬(Anti-Ransom), 매체제어(Device Control) 기능이 통합된 에이전트 제공으로 에이전트 혼잡을 줄이고 관리 효율성을 극대화할 수 있습니다.

단일/통합 에이전트 제공

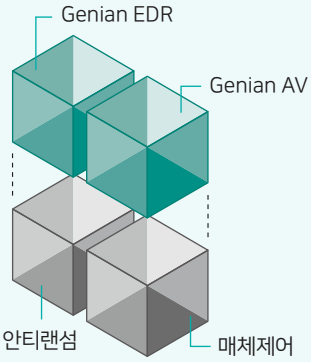
- Genian EDR, Genian AV 단일 설치 및 운영
- Genian EDR, Genian AV, 안티랜섬, 매체제어 통합 에이전트 제공
- 에이전트 설치/배포/운용 등 도입에 따른 부담 최소화
- 단일 에이전트 , 단일 관리 콘솔을 통한 운영 복잡도 감소 및 관리 효율성 향상



EDR 단독
+(addon)
안티랜섬 / 메체제어



AV 단독
+(addon)
안티랜섬 / 매체제어



EDR & AV
+(addon)
안티랜섬 / 매체제어

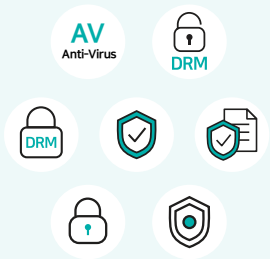
단말 부하 및 충돌 최소화한 탐지/분석

- 단말에 설치된 모듈을 통해 각종 정보 수집 후 서버에 전송
- 분석은 서버에서 이루어지며 사용자 단말 부하 최소화
- 타 프로그램의 동작에 영향을 주지 않도록 충돌 최소화 기술 적용

Agent
- 단말의 정보 수집
- 악성코드 및 이상행위 탐지
- 위협 대응

수집/대응 — 저장/분석

Server
- 수집 정보의 저장/검색
- 위협 분석/표출
- 정책 및 설정 관리



문서중앙화	PMS
매체제어	데이터 복원
DLP	프린터 보안
NAC	메신저
개인정보보호	소프트웨어 관리
SSO통합인증	

No problem!

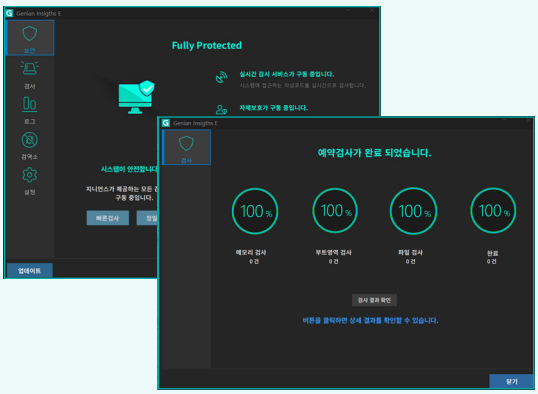
Key Features

보안 시너지, EDR + AV

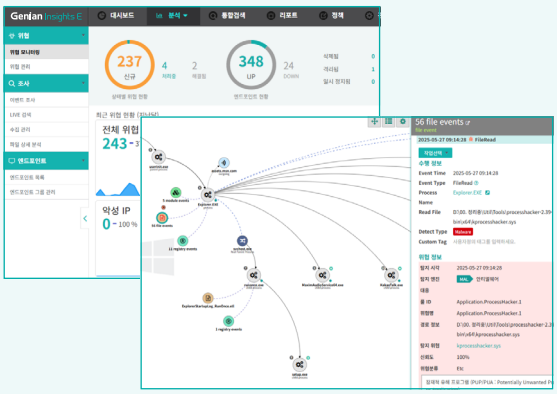
Genian EDR과 Genian AV를 함께 사용하면 알려진 악성코드는 AV로 빠르게 차단하고, 알려지지 않은 고도화된 공격은 EDR로 탐지·분석·대응할 수 있어 보안의 깊이와 범위를 동시에 강화할 수 있습니다. 이를 통해 사고 대응 속도, 가시성, 자동화 수준까지 크게 향상됩니다.

Genian AV는 사전 대응, Genian EDR은 실시간 탐지 및 대응을 담당하며, 전방위 보안 구현

악성코드 사전 대응

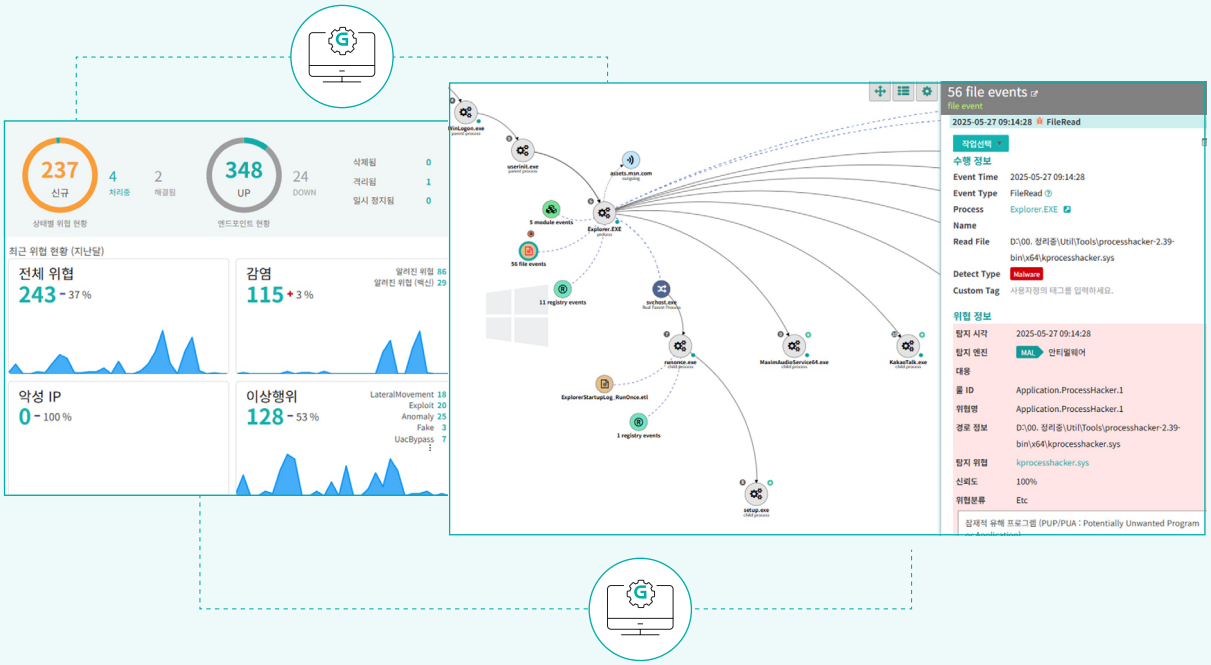


이상행위 실시간 대응



Genian AV 탐지 내역에 대한 체인 이벤트 기반 분석

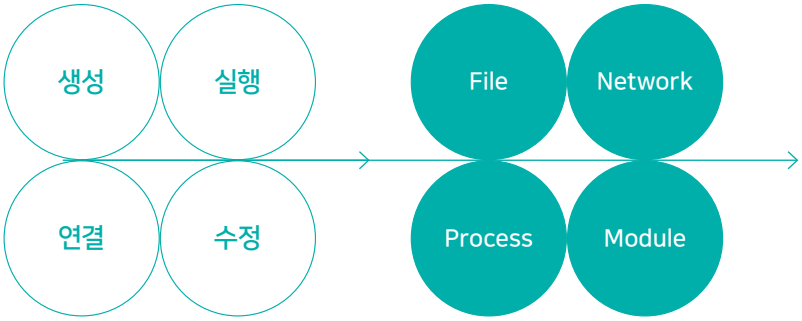
- Genian AV 탐지 내역에 대해서도 Genian EDR의 로그와 분석 기능을 통해 위협 헌팅 수행 가능
- 개별 행위 간의 관계를 시간 순으로 연결하여 전체 공격 시나리오 파악
- 감염 경로 추적 및 사후 분석 기능 제공



Product Function

단말 행위 모니터링

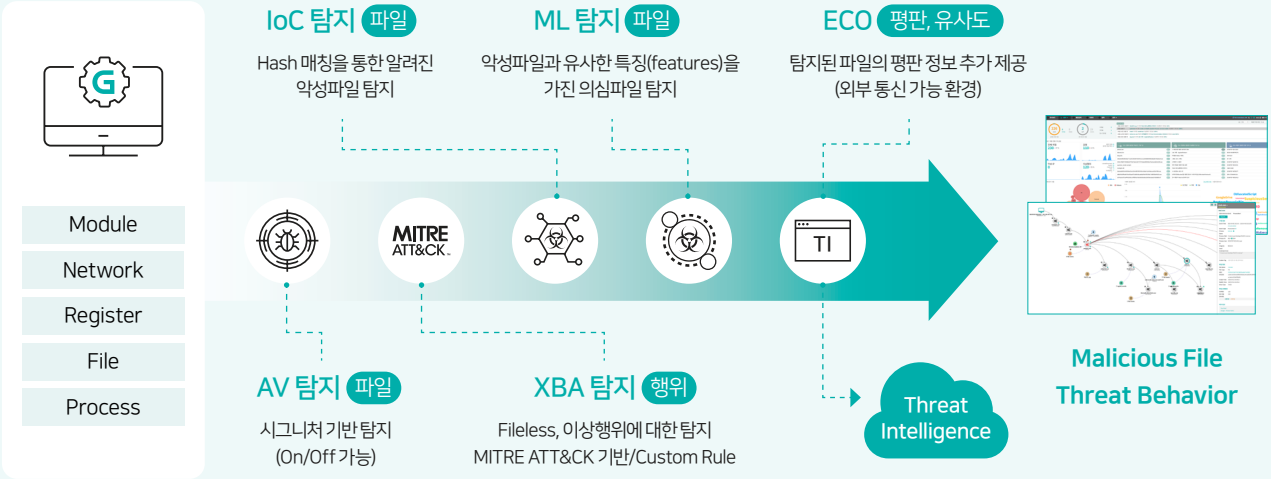
단말에서 발생하는 주요 행위를 모니터링하고 실시간 저장 후 분석합니다. 이를 통해 지능형 위협 등을 사전에 탐지/예방하고, 사후 감사 증적(Audit)이 가능합니다.



- 사용자, 단말의 행위 분석 및 이상행위 탐지
- APT, 랜섬웨어 등 지능형 위협의 탐지
- 탐지된 위협 및 이상행위 대응(Response)
- 침해 사고 및 이상행위의 감사 증적(Audit)

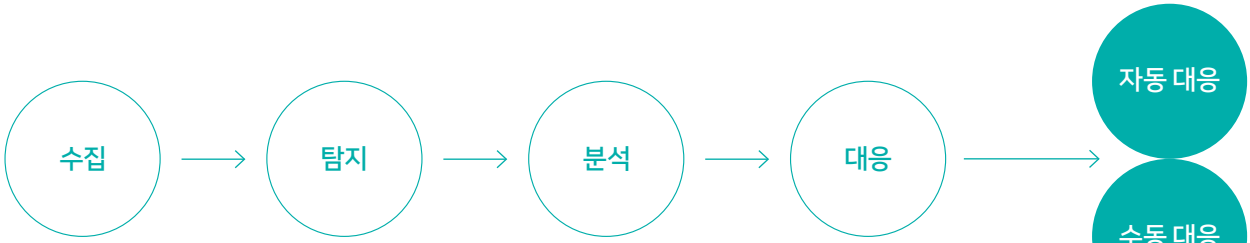
위협(Threat) 탐지

위협 파일은 AV, IoC, ML 기반 탐지로 식별되며, 이상 행위는 MITRE ATT&CK 기반의 XBA 엔진을 통해 탐지됩니다. 관리서버가 외부 통신이 가능할 경우, 제조사 TI와 연동하여 추가 위협 정보를 조회할 수 있습니다.



위협(Threat) 대응

위협이 탐지되는 경우 에이전트에서 네트워크 격리, 파일 삭제, 프로세스 종료, 사용자 알림 등의 대응을 합니다. 정책(Policy) 기반으로 즉시 작용하므로 확산 방지 등 초동 대응이 가능합니다.



- 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

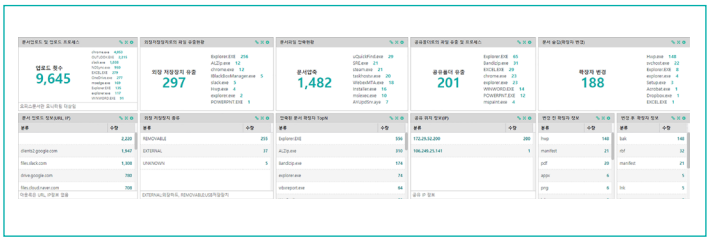
Product Function

Endpoint Discovery

위협 탐지를 위해 상시 수집한 로그는 다시 활용하여 기존에 알 수 없었던 단말에서 행해지는 다양한 행위를 모니터링 할 수 있습니다. 또한, 수집된 로그를 다양한 목적으로 활용할 수 있는 유연한 대시보드를 제공합니다.

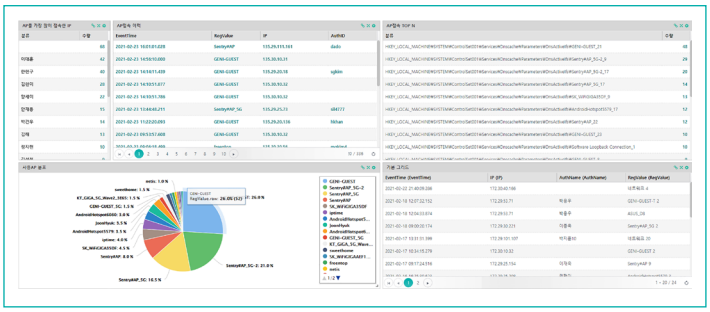
문서 현황 모니터링

- 문서/압축 파일 업로드(Web, SNS 등)
- 외장 저장장치(USB, HDD 등) 복사/이동에 대한 세부 내용
- 문서 압축, 확장자 변경 등



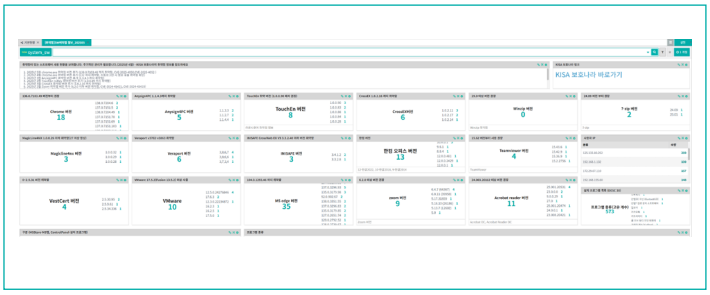
네트워크 접속 현황

- AP 접속 현황
- 원격 접속 현황(원격 데스크탑, 원격 터미널, Putty, SecureCRT 등)
- 오픈 포트 및 프로세스
- 세션을 통해 송/수신한 byte 량
- 외부 IP 접속 프로세스 등



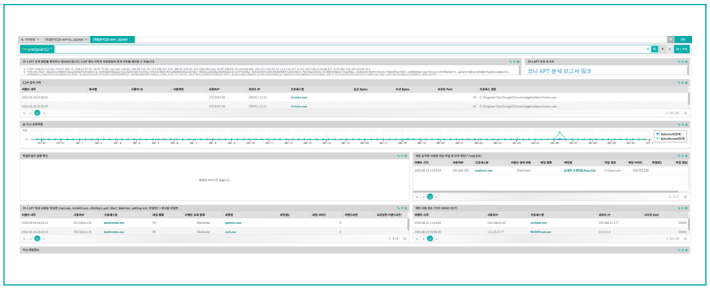
설치된 소프트웨어 버전 확인

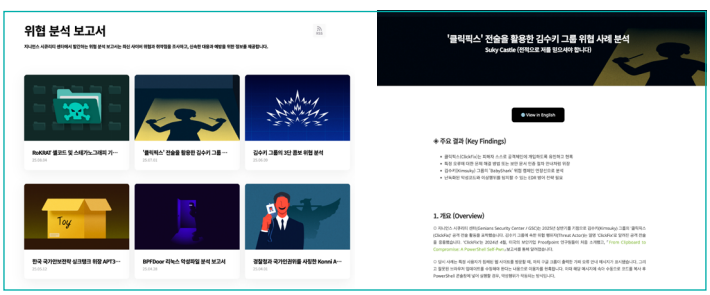
- KISA 보호나라와 다양한 취약점 정보 이용하여 대시보드 구성
- 취약점이 있는 소프트웨어 버전 사용 현황
- 단말 별 취약한 버전 사용 현황
- IP, 사번, 사용자명, 설치 프로그램 상세 정보



위협 분석보고서를 활용한 대시보드

- GSC(Genians Security Center) 위협 분석 보고서를 활용한 대시보드 제공
- 위협 인텔리전스 기반 상세 분석 정보 연계
- 해킹 공격에 사용된 의심 파일 정보
- 이벤트 발생 시각, 사용자 IP 등 상세 정보
- C2IP 접속 이력
- 해킹 사용 포트



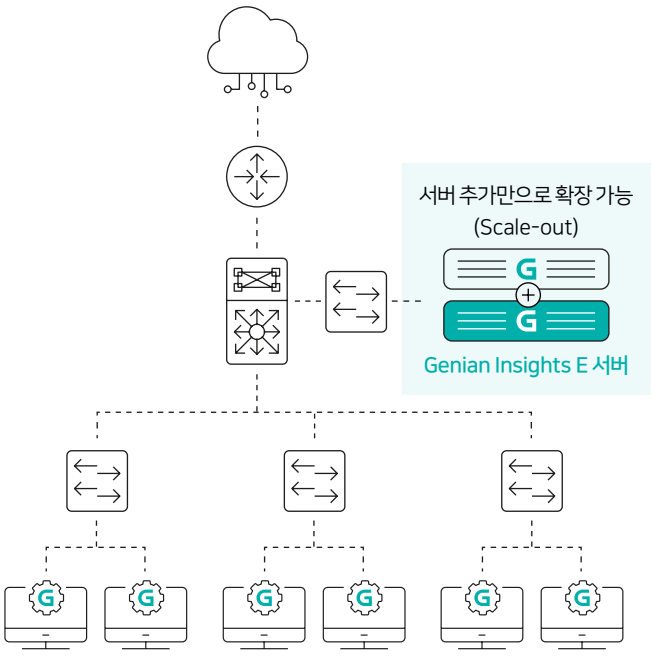


Operating Mode

구성

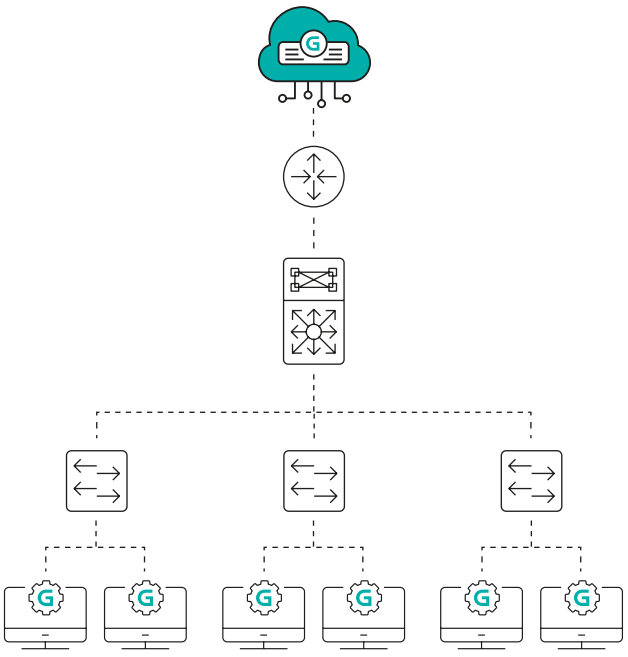
Genian Insights E 서버와 에이전트의 간단한 구성이며 On-Premise와 Cloud 모두 제공합니다.
On-Premise 환경에서는 Scale-Out 기능을 제공하여 쉽게 확장 할 수 있습니다.

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

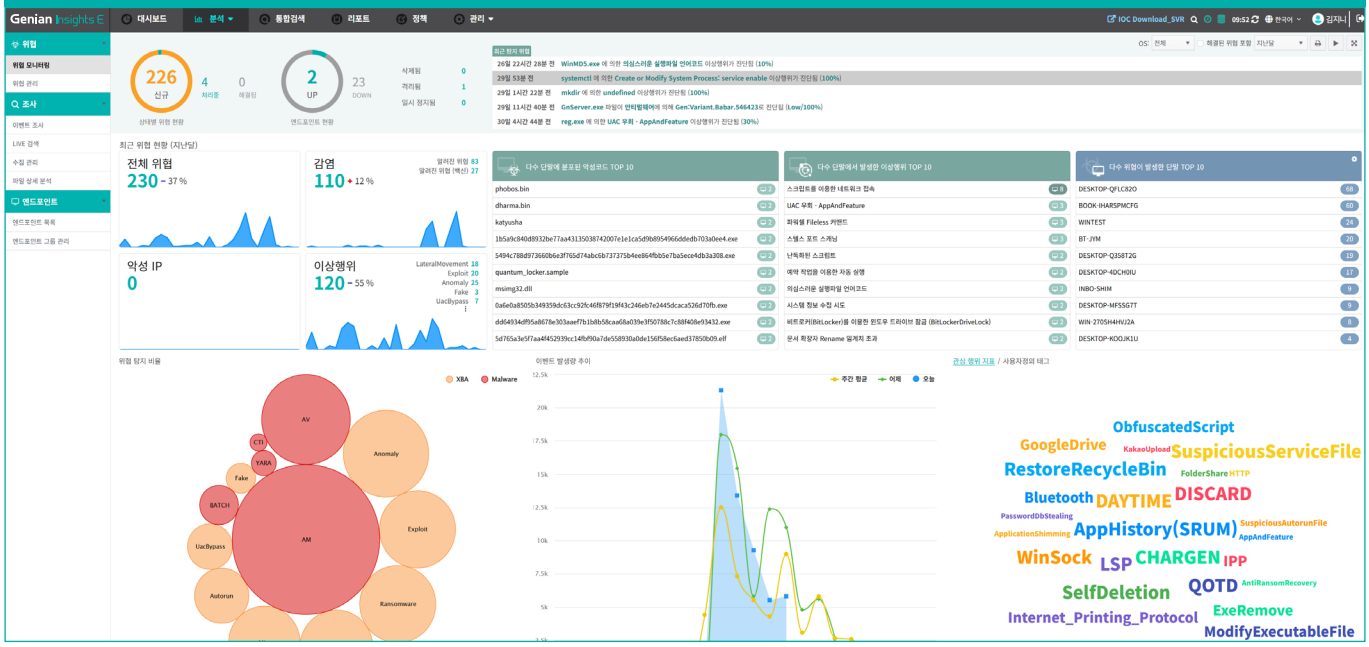
도입 효과

기존 보안 체계의 한계를 효과적으로 보완하고 개선할 수 있습니다.

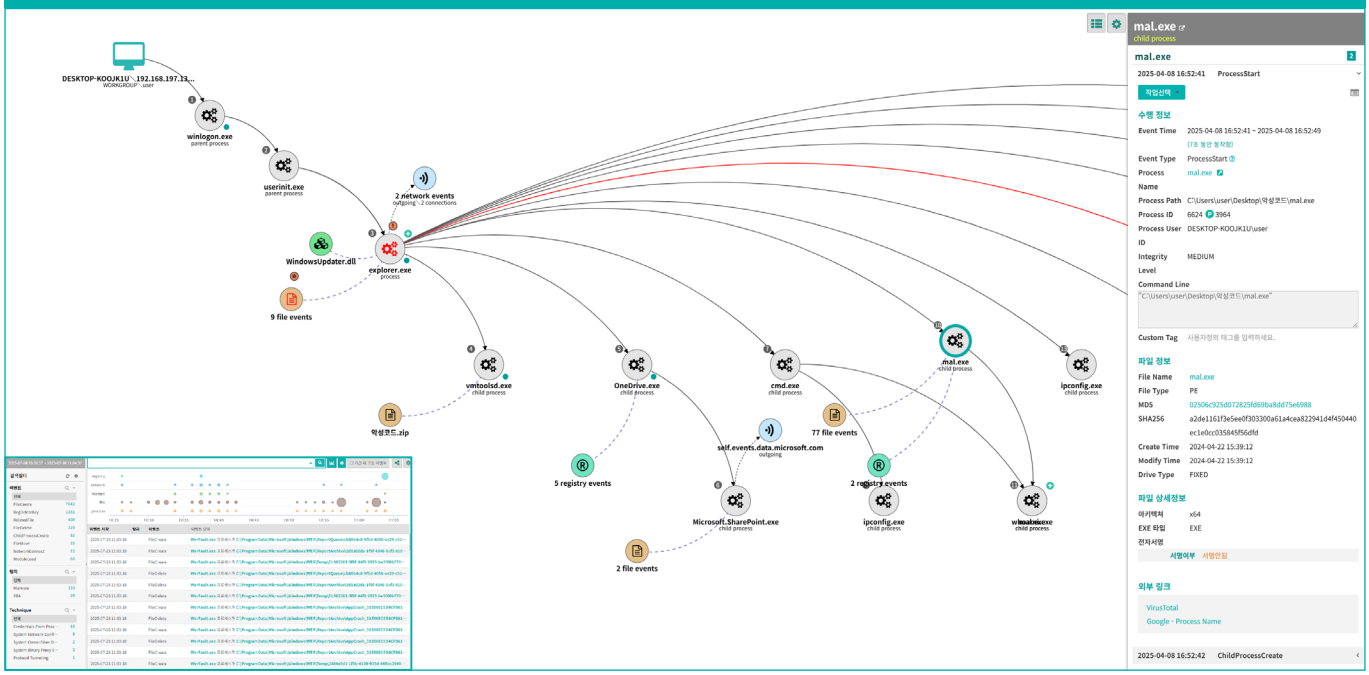
AS-IS (기존 보안 체계)	TO-BE (Genian Insights E 도입 후)
Anti-Virus의 한계 · 백신에서 탐지할 수 없는 신종 악성코드 및 Fileless 형태의 공격 증가	**행위 탐지** · 기존 백신으로 탐지하기 어려운 신종 악성코드 및 Fileless 기반 공격 탐지
가시성 부족 · 엔드포인트 내에서 어떤 활동이 일어나는지 실시간 파악 불가	**가시성 확보** · 엔드포인트 내에 CCTV 가 설치 된 것처럼 실시간 확인 및 조회
정확한 원인 분석 어려움 · 침해사고 발생 후 포렌식에 시간/인력 낭비	**원인 분석 가능** · 빠른 추적과 분석으로 원인을 찾아 대응
취약한 S/W 버전 확인 어려움 · 설치된 S/W 확인 및 취약점이 있는 프로그램 사용 여부 확인 어려움	**취약한 S/W 버전 확인 가능** · 프로그램을 통한 위협 의심 행위 확인
대응 속도 느림 · 이상 징후 발생 후 대응까지 수일 또는 그 이상 소요	**대응 속도 빠름** · 이상 징후 발생 후 분석 및 대응까지 수 시간 내에 가능

Administrator UI

위협 모니터링



공격 스토리 라인



Windows

- Windows 7(SP2) 이상
- Windows Server 2012 이상

macOS

- macOS (BigSur) 11.0 이상

Linux

- Centos : 7 이상
- RHEL : 7 이상
- Unbuntu : 18.04 이상
- Rocky : 8.4 이상
- Debian : 10 이상
- Fedora : 35 이상

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

Genians