화이트리스트 실행통제

iMON LOPE 제품 소개

제품 개요

도입 배경

- Malware (악성코드)로 인한 피해 발생
- 신종/변종 출현으로 기존 백신 엔진으로 예방효과 미비
- 해킹 수법 지능화로 과거 패턴에 의한 대응 속도 한계

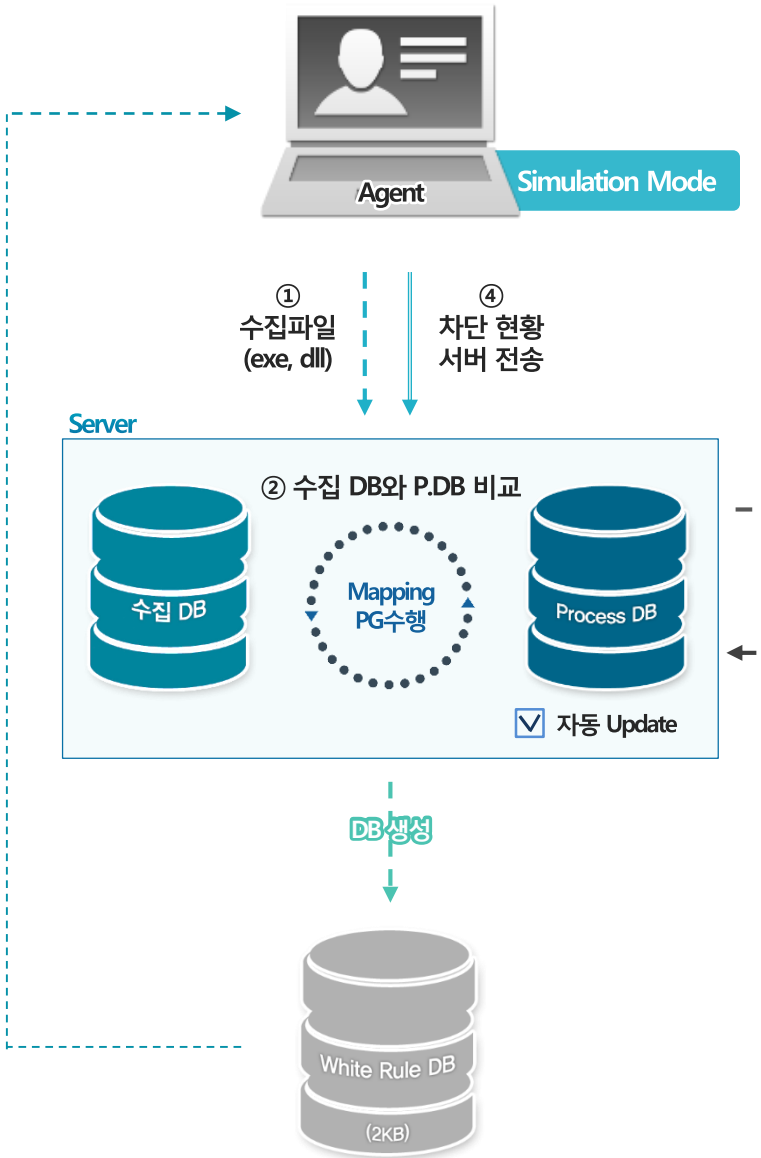
White List 통제 솔루션

iMON LOPE란?

EXE, Script Files (DLL) 실행 전 허용 여부를 판단한 후 허용 외 비인가 파일을 통제하여 실행 시 유입 가능성이 있는 해킹 프로그램 및 악성코드 (Malware) 차단

- White 통제 시 **관리자 업무 프로세스의 불편함을 자동화로 해결**
- P.DB (기준정보) 실시간 혹은 정기 업데이트 서비스 제공
- P.DB의 모든 파일 (1,100,000개)은 전 세계 56개 백신 검사를 통해 안전성 검증
- 모든 수집된 파일은 실시간 바이러스 검사 수행 가능 (i-SCAN Center)
- 저작권 사별 EXE, DLL 파일 정보 제공

Flow_모든 Process 자동화



변경정보 (파일/ 해쉬)

매일 1회 업데이트로 최신 상태 정보 요청

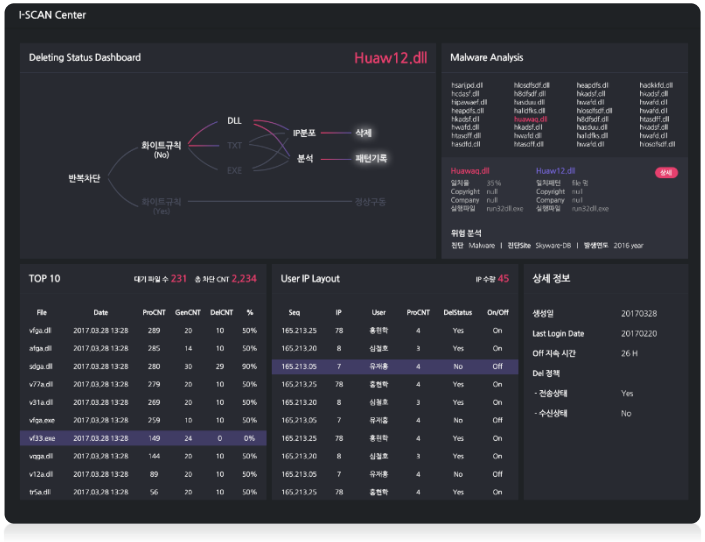
최신 백신 검사 및 추가 내용 전송

*** Simulation Mode**

: 시뮬레이션 모드로 에이전트 배포 및 영향도 결과 안내 관리자 확인 후 ① ~ ④ 수행

*** White 통제 정책 자동화 운영**

① Agent 설치 후 모든 PC의 파일 (exe, dll) 수집
② 수집 DB와 P.DB (기준정보) 매핑 알고리즘 작동
③ White 정책을 모든 에이전트에 전송
④ White 통제로 인한 차단 현황 서버로 전송

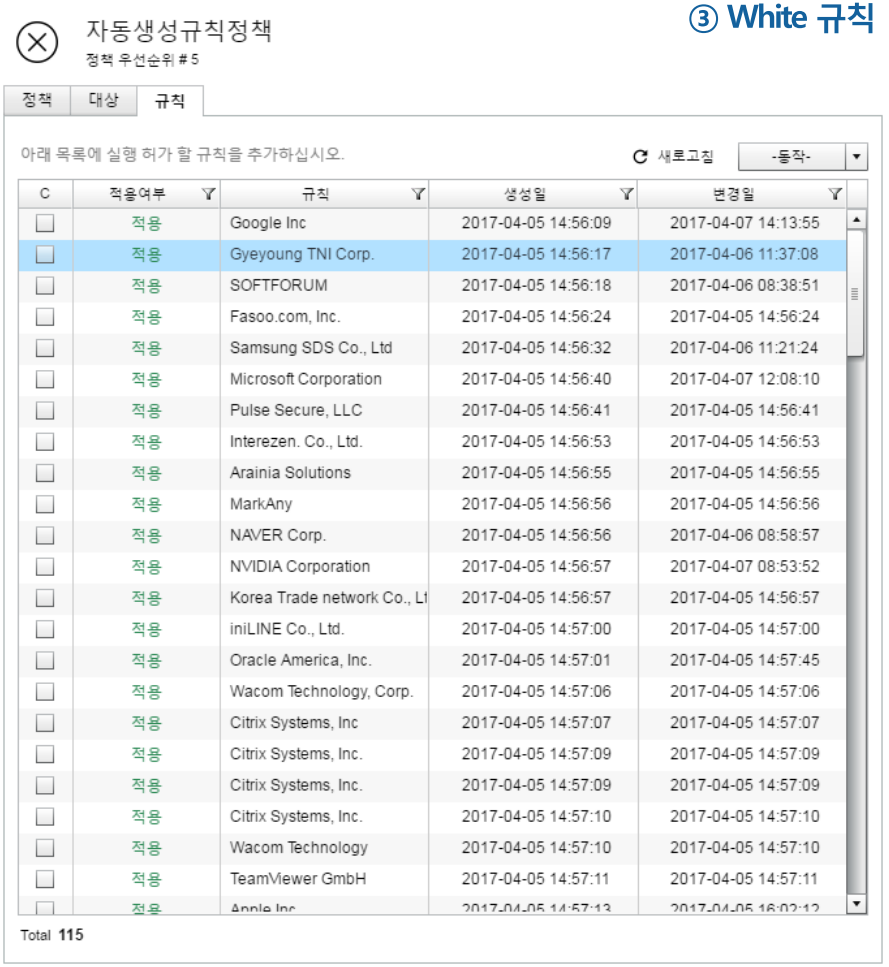


*** i-SCAN Center**

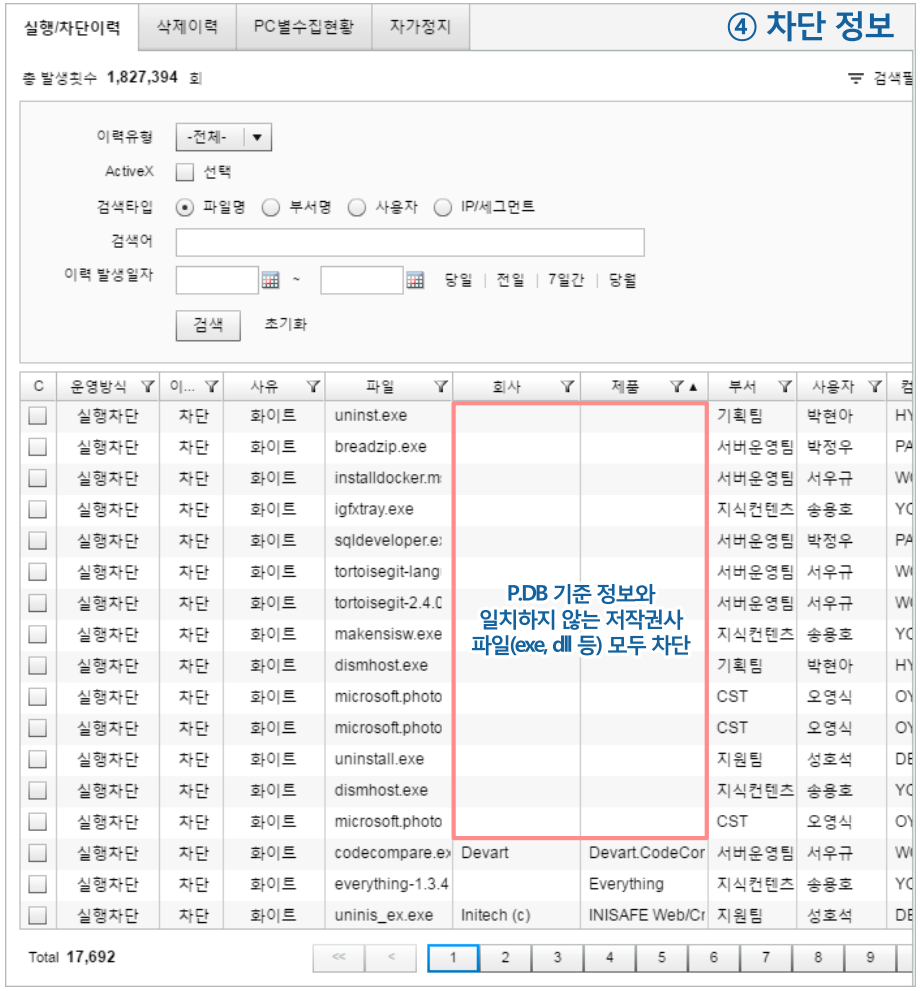
P.DB 정보 갱신 센터 (개발사 운영)로 정기 P.DB 업데이트, 실시간 자동 백신 검사 진행

Flow_모든 Process 자동화

③ White 규칙



④ 차단 정보



[자동으로 생성된 White 규칙]

- 안전성이 검증된 범용 SW의 저작권 제품은 자동 White 규칙 생성
- 저작권사별 디지털서명이 여러 개일 경우 모두 등록
- White 규칙 생성의 경우 제품별 패치 및 업데이트 영향 無

[자동화 White 통제 운영 시 차단 현황]

① 회사 및 제품명 정보가 없는 경우
② 디지털서명이 없는 경우

※ ①, ② 정보는 있으나 P.DB에 없는 제품은 차단

특장점

최근 악성코드 스크립트 방식

* 사용자 1PC에서 수집한 현황

스크립트 유형	Windows 7 C:Windows/	C:efriendPlus	C:programfiles	- - -	Total
해당 저작권사	MS,폰트,K-defence	한국투자증권	안랩,DVDPlayer,Google	- - -	
DLL	27,406	601	2,188	- - -	34,723
TXT	875	213	0	- - -	1,276

□ 악성코드 유형 분석

□ 악성코드 특징

1) 스크립트 방식으로 악성코드 유포
2) Rundll32.exe (정상 프로그램) 을 이용하여 악성코드를 실행시킴
3) Script Files를 자동으로 통제하는 White 통제 솔루션

특장점

iMON LOPE 기능

□ **백신 검사**

- 수집된 모든 파일은 안전성 진단 수행 (P.DB)
- 바이러스 안전성은 온라인 검사 기능으로 진단 가능

□ **시뮬레이션 기능**

- 강제 통제 정책 적용 전 시뮬레이션 모드를 통해서 사전 문제점 도출 및 문제 해결 가능

□ **자동화 기능**

- "자동 모드" 설정하면 안전성이 검증된 파일 기준으로 **자동으로 화이트 규칙 목록에 추가**
- 매월 P.DB 업데이트 자동 실현
- 수집된 DB의 새로운 파일에 대해서는 **자동으로 바이러스 안전성 진단 수행**
- 통제 정책으로 차단되는 파일은 **자동으로 "파일 삭제" 기능**