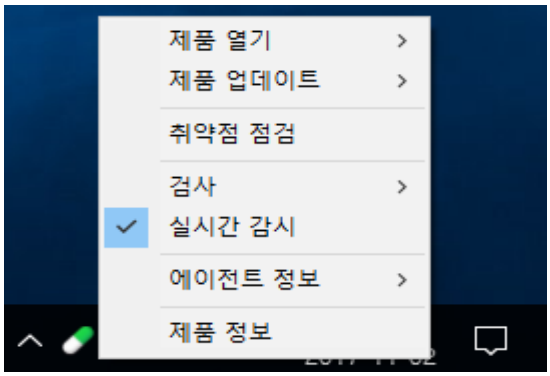
알약 사용자 메뉴얼

통합에이전트

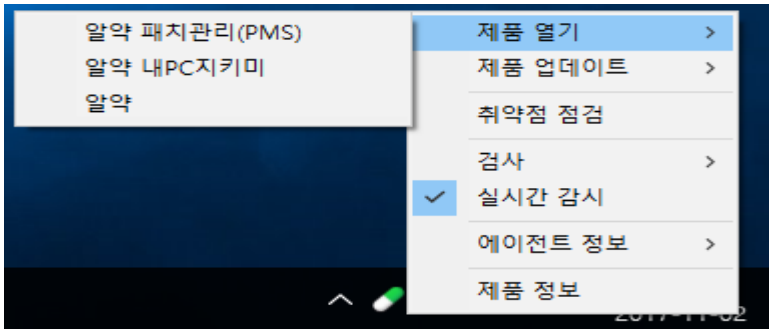
통합에이전트는 각 클라이언트 설치 시 함께 설치되어 ASM 4연동을 위한 서버 정보와 사용자 정보를 관리하고, 설치된 클라이언트들의 업데이트 진행 및 주요 정보를 취합/전송하는 통합 관리 역할을 수행합니다.

주요 기능 소개

시스템 트레이 상에 위치하며, 설치된 클라이언트에 따라 트레이 알림을 확인하고 주요 기능을 즉시 실행할 수 있습니다.

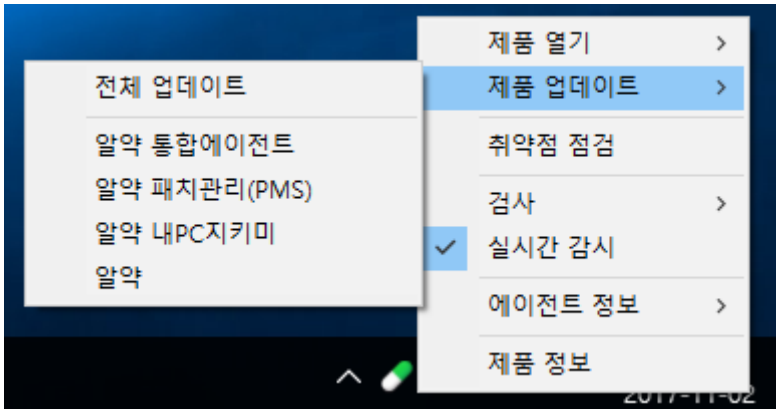


① 제품 열기: 설치된 알약, 알약 패치관리(PMS), 알약 내PC지키미 등 설치된 클라이언트를 실행시킬 수 있습니다.



② 제품 업데이트: 알약 통합에이전트와 클라이언트들을 즉시 업데이트 시킬 수 있습니다.

전체 업데이트 선택 시, 설치된 모든 제품 및 알약 통합에이전트가 일괄 업데이트됩니다.

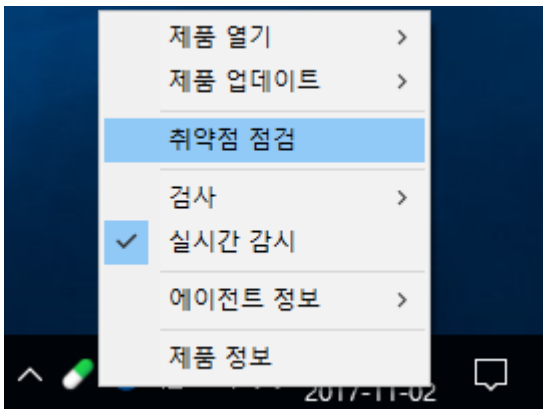


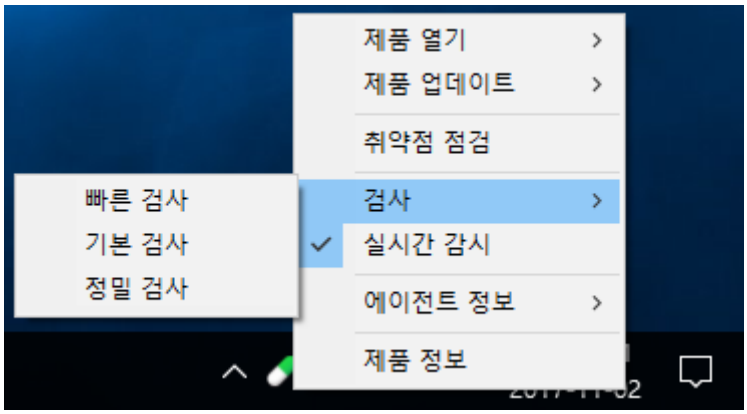
③ 제품별 메뉴: 제품별 주요 기능을 바로 사용할 수 있습니다.

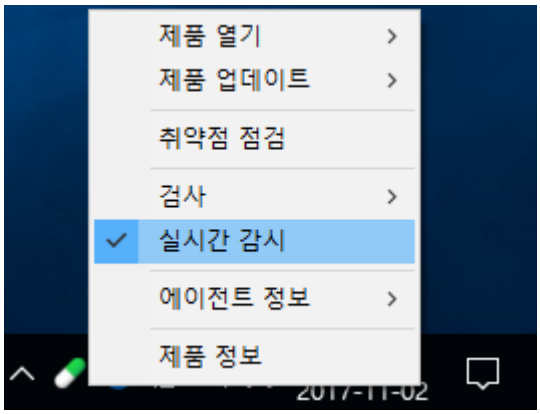
- 취약점 점검: 알약 내PC지키미의 취약점 점검을 수행할 수 있습니다.

- 검사: 알약의 검사 기능을 수행할 수 있습니다.

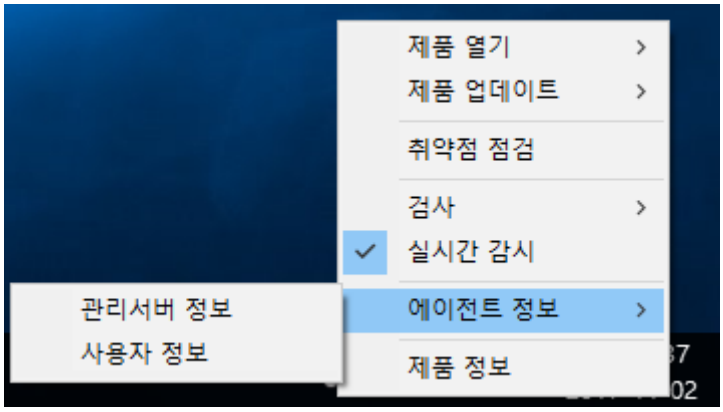
- 실시간 감시: 알약의 실시간 감시를 ON/OFF 할 수 있습니다.



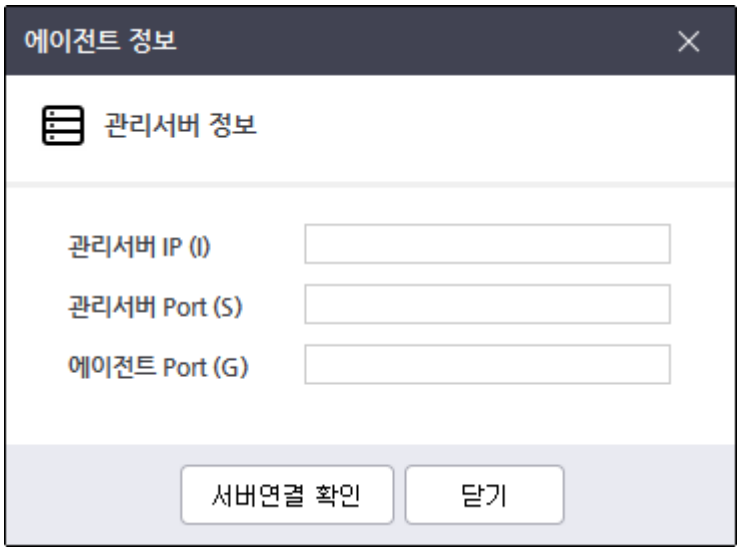




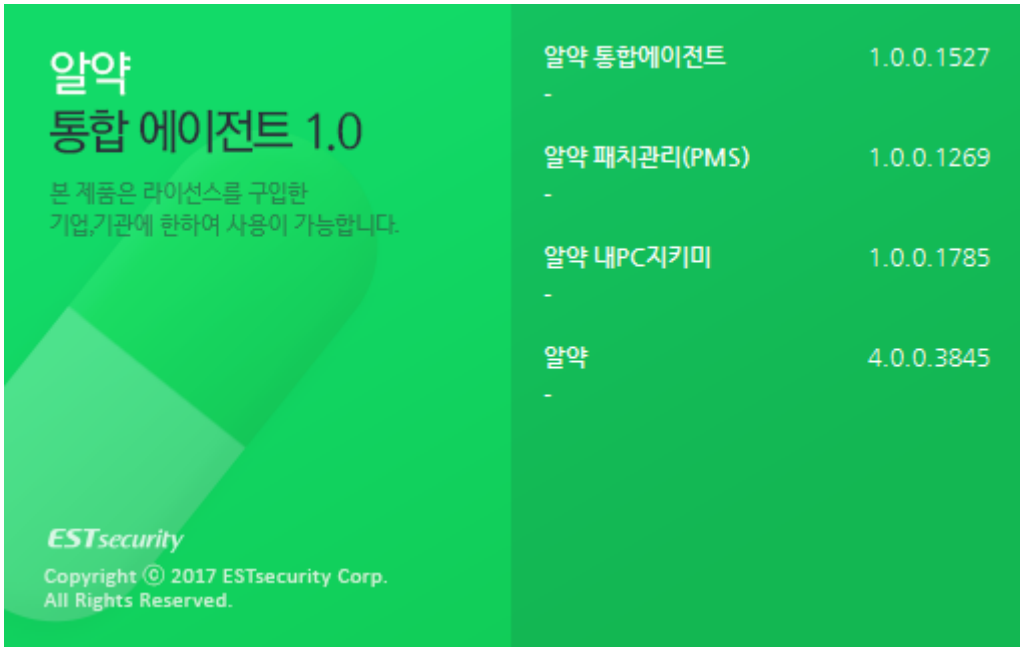
④ 에이전트 정보



- 관리서버 정보: 관리 서버 정보가 자동으로 입력되며, 신규 연결이 필요할 때 서버 연결을 확인할 수 있습니다.

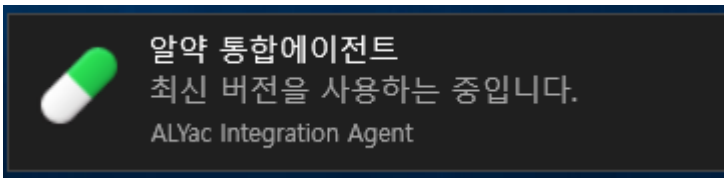


⑤ 제품 정보: 알약 통합에이전트와 설치된 제품의 제품 정보 및 제품 버전이 나타납니다.



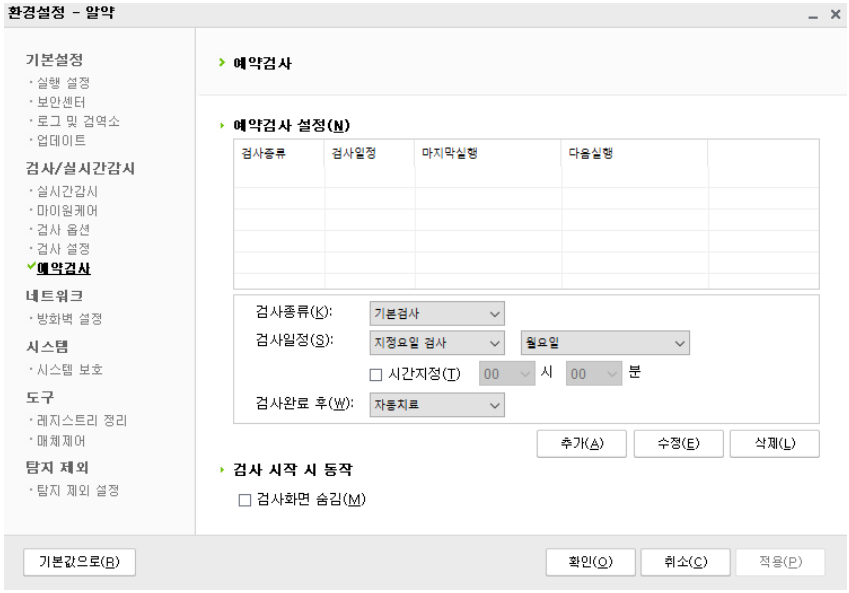
⑥ 트레이 알림: 제품 업데이트, 검사 완료 등 설치된 제품의 주요 알림을 표시합니다.

알약 패치관리(PMS) 설치 시 패치 자동 적용/미적용 설정 여부에 따라 최신 패치 설치/확인이 트레이 알림으로 나타납니다.



악성코드 검사 ①

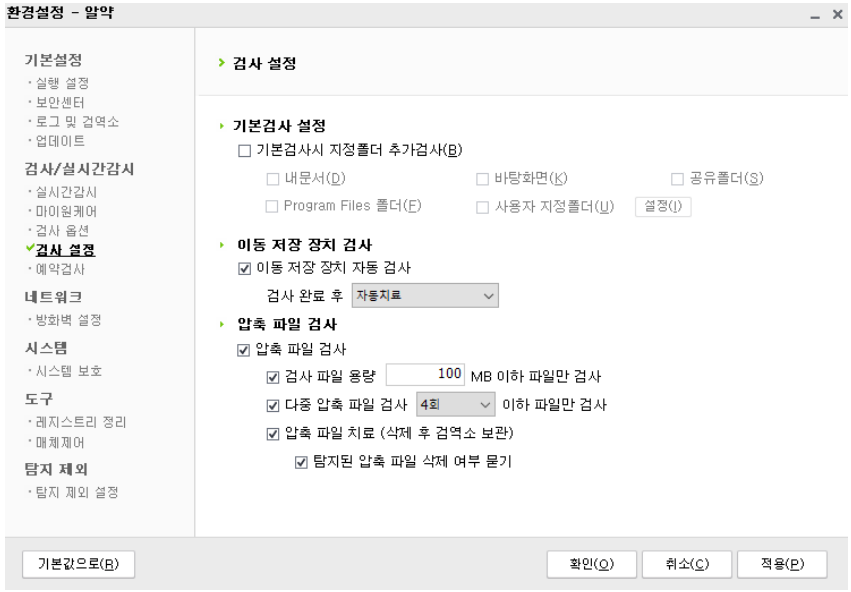
- 트리플 엔진과 스마트 스캔 기능을 기반으로 다양한 검사 기능 제공
- 수동 검사: 빠른 검사-기본 검사-정밀 검사 3단계로 구성된 수동 검사 기능 제공
- 예약 검사: 사용자가 설정한 날짜나 주기에 검사를 자동으로 진행하게 하는 검사 기능
- 로그오프 검사: 예약 검사의 경우 검사가 진행되어야 할 시간에 시스템이 로그오프 상태여도 검사가 진행



악성코드 검사 ②

- 이동 저장 장치 자동 검사: 이동 저장 장치를 통한 악성코드 감염/확산 사전 방지
- 압축파일 검사: 검사 시 압축파일을 검사하여 위험요소를 탐지 및 치료(압축 파일의 용량과 압축 횟수 제한 가능)

- **알약>환경설정>검사 설정**



- **이동식 디스크 검사화면**

악성코드 검사 ③

시스템을 실시간으로 감시하여 위험요소에 노출되는 위험을 실시간으로 차단/처리하며,
웹서핑시 바이러스나 악성코드에 노출되는 것을 방지함으로서 사용자의 시스템과 개인정보 보호

실시간 감시 검사항목 설정

- 모든 시스템 영역 감시

  : 파일의 새로 생성/변경/복사/이동 여부를 감시

- 실행 파일만 감시

  : 새로 실행되는 프로세스만 감시

강력한 네트워크 폴더 감시

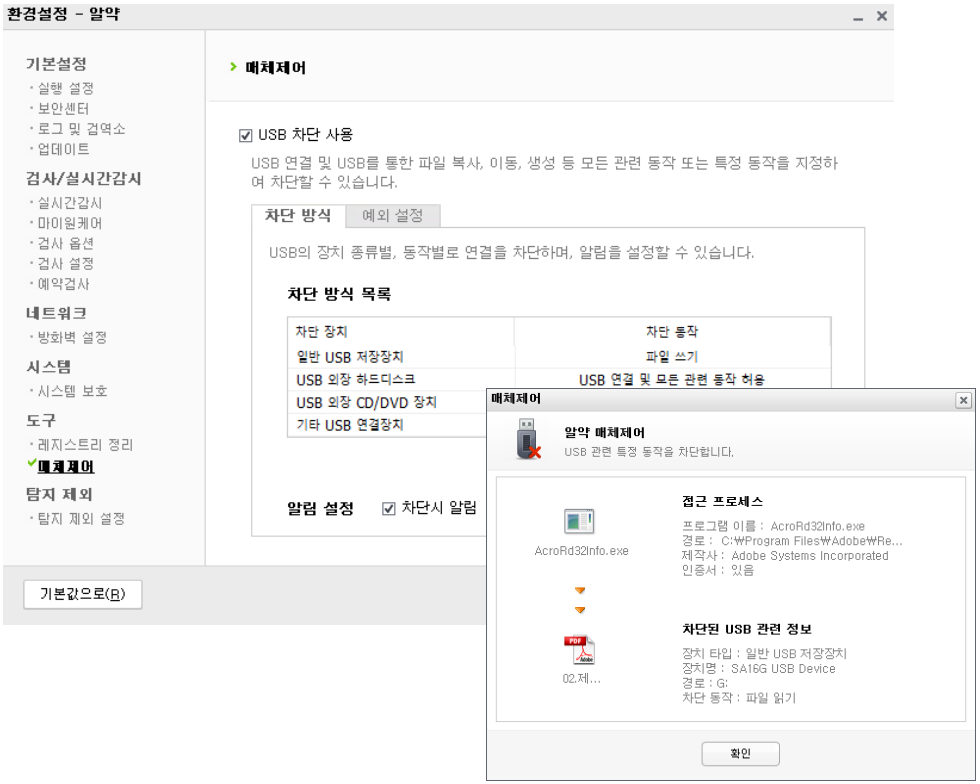
- 네트워크를 통한 악성코드의 감염이 다양해짐에 따라

  다양한 접근 타입에 대해 강력하게 감시

매체 제어

매체 제어 기능을 통해 USB 등 다양한 이동식 저장 장치를 통한 자료 유출/입 차단

- 파일 실행: exe와 같이 실행 가능한 파일 실행 차단
- 파일 읽기: 각종 오피스 외 미디어 파일들을 열지 못하도록 차단
- 파일 쓰기: USB 내에서 파일 복사, 생성 및 수정하는 것을 차단



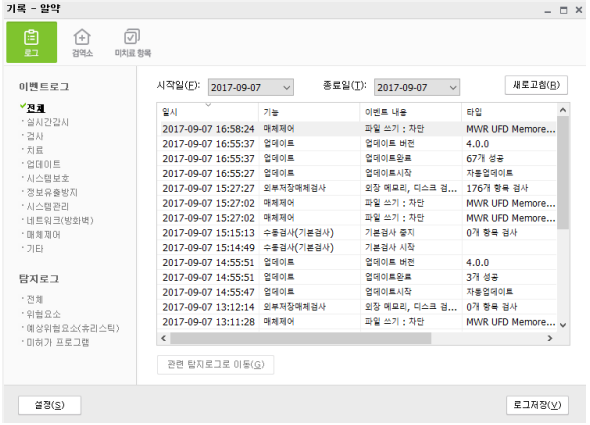
다양한 매체를 통한
위험요소 유입

ESTsoft

다양한 로그 기능

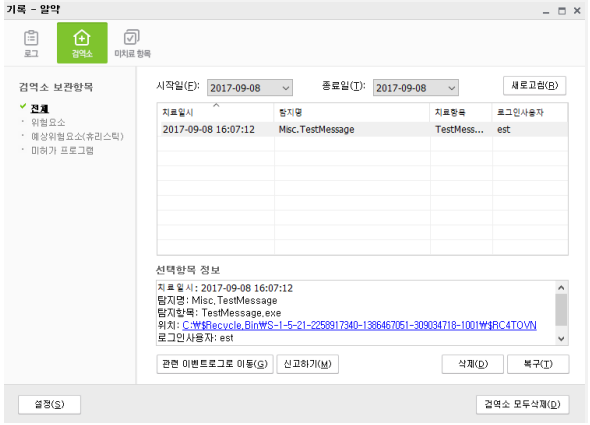
로그

- 알약의 동작 및 보안에 위협이 되는 동작이나 현상을 기록



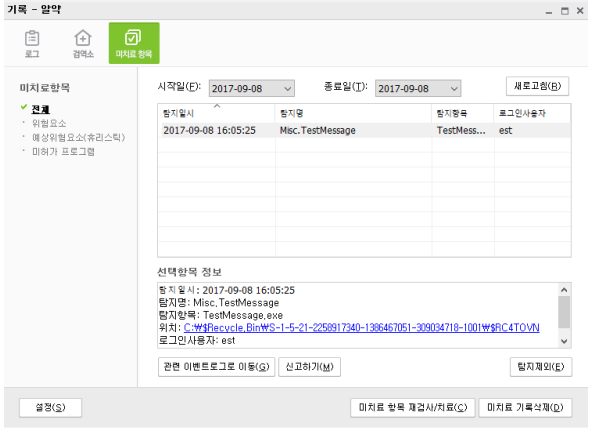
검역소

- 알약으로 치료했던 위험요소를 항목별로 안전하게 격리하여 보관
- 오류가 발생하거나 주요 문서 및 개인 정보가 손상되었을 경우 치료했던 항목을 복원 가능



미치료 항목

- 탐지된 항목 중 치료하지 않은 탐지 항목
- 미치료 항목은 위험요소로 유추하여 재검사 및 치료, 신고하기 가능



의심파일 신고 기능

알약이 탐지하지 못하는 위험요소, 위험요소가 아님에도 위험요소라고 탐지하는 경우

알약의 신고하기 기능 활용 → 알약 긴급대응 팀을 통한 신속한 처리

- 신고하기 기능은 알약 메인화면 상단의 MENU>'신고하기' 이용
- 검사 완료 화면, 검역소, 미치료 항목 화면에서 '신고하기' 버튼 클릭

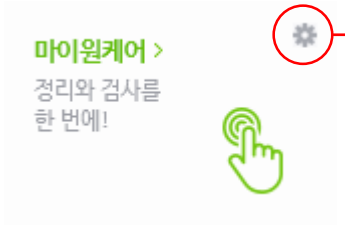
ESTsoft

마이원케어

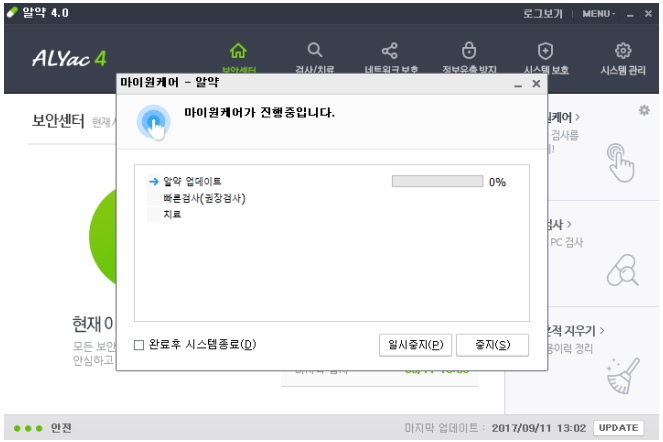
마이원케어란? (타사 백신에 없는 알약 4.0의 특징!)

사용자가 설정한 여러 기능을 한 번의 클릭으로 진행하는 '원 클릭 맞춤 검사'

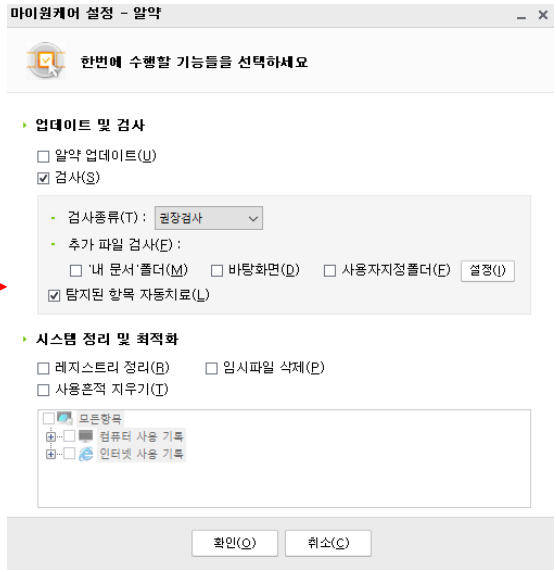
- **알약의 메인 화면에서 "마이원케어" 클릭**



- **마이원케어 진행화면**



- **마이원케어 설정화면**



1. 업데이트 및 검사
- 알약 업데이트
- 검사(알약이 권장하는 검사, 빠른검사, 기본검사, 정밀검사)
- 탐지된 항목 치료

2. 시스템 정리 및 최적화
- 레지스트리 정리
- 임시파일 삭제
- 사용흔적 지우기

ESTsoft

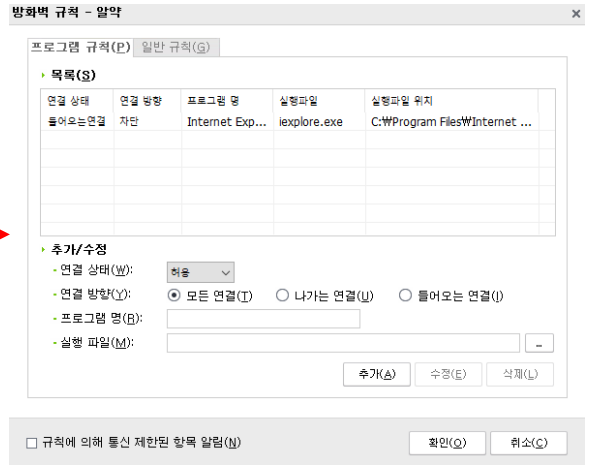
네트워크 차단(방화벽)

실행중인 모든 프로그램의 네트워크 통신 상태를 감시하여 위험 요소의 네트워크 접근을 차단

- 네트워크를 통해 들어오고 나가는 모든 연결 감시
- 통신시도 항목과 원격지 정보 확인
- Process, IP, Port 별 규칙 설정 가능
- 실시간으로 통신항목 모니터링 가능

- **알약>환경설정>방화벽 설정 화면**

- **방화벽 규칙 설정 화면**



- **방화벽 기능 알림 화면**

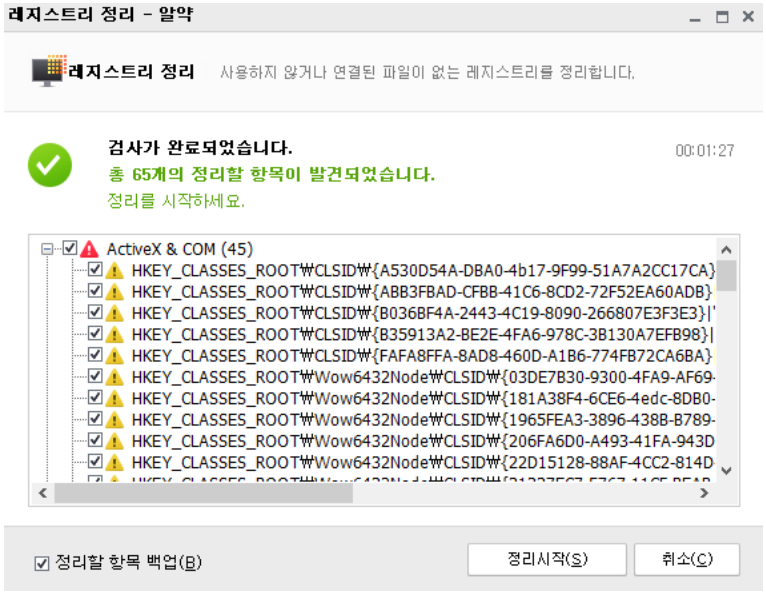
ESTsoft

레지스트리 검사 및 복구

레지스트리 정리 기능을 이용한 레지스트리 복구 기능 (타사 백신에 없는 알약 4.0의 특징!)

- **알약>메인화면>시스템 관리**

- **레지스트리 검사 화면**



- **레지스트리 복구 화면**

- 정리 항목 백업 가능
- 정리 항목 백업 횟수 제한 가능(환경설정)

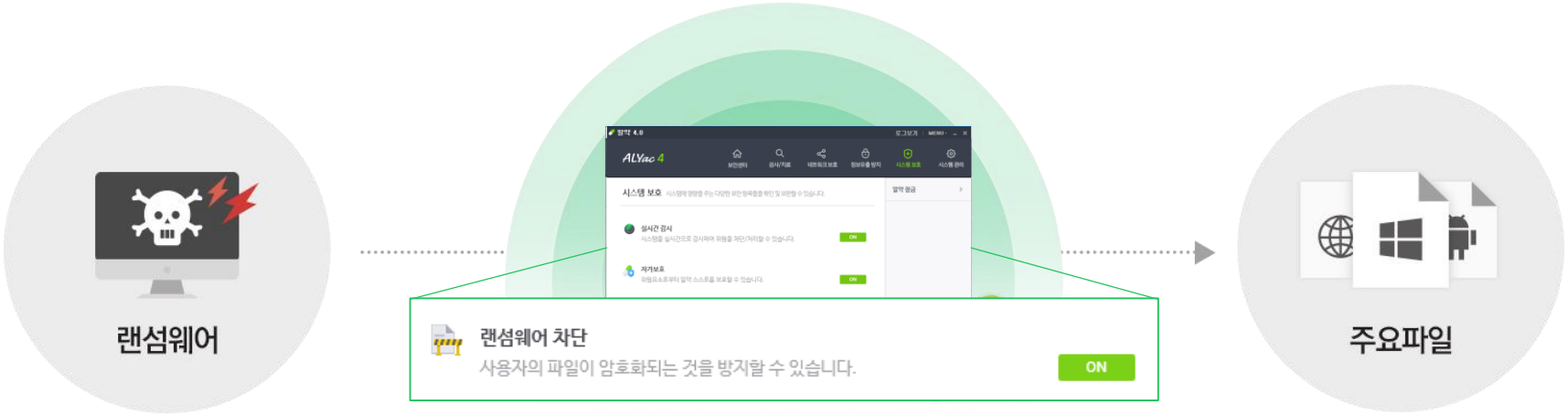
- 복구가능 항목 삭제 가능

ESTsoft

랜섬웨어 차단

랜섬웨어 의심 행위를 사전에 탐지하고 차단하여 사용자의 파일이 암호되는 것을 방지합니다.

- 랜섬웨어 차단 기능은 알약 메인화면 '시스템 보호' 탭 ON/OFF 이용
- 환경설정>기본 설정>시스템 보호 내 옵션 이용



주요 파일 암호화 시도
동작 감지 및 차단

ESTsoft