

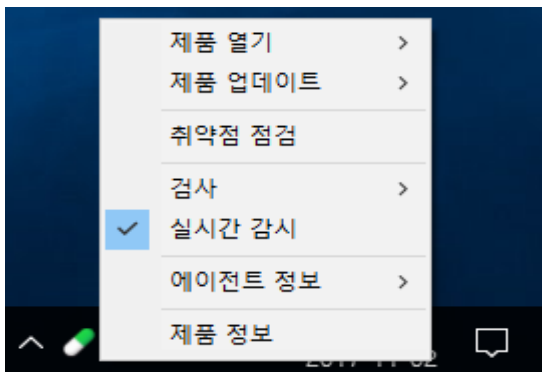
알약 사용자 메뉴얼

통합에이전트

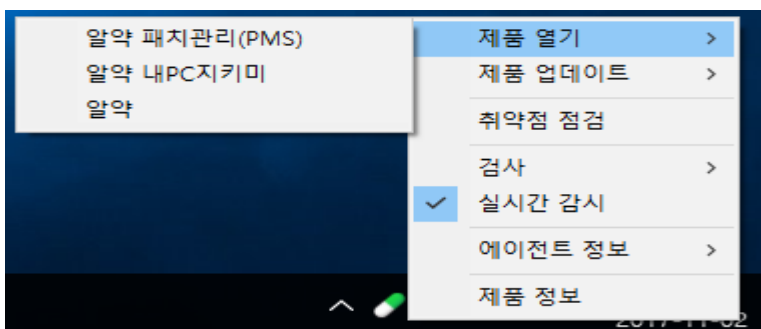
통합에이전트는 각 클라이언트 설치 시 함께 설치되어 ASM 4연동을 위한 서버 정보와 사용자 정보를 관리하고, 설치된 클라이언트들의 업데이트 진행 및 주요 정보를 취합/전송하는 통합 관리 역할을 수행합니다.

주요 기능 소개

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

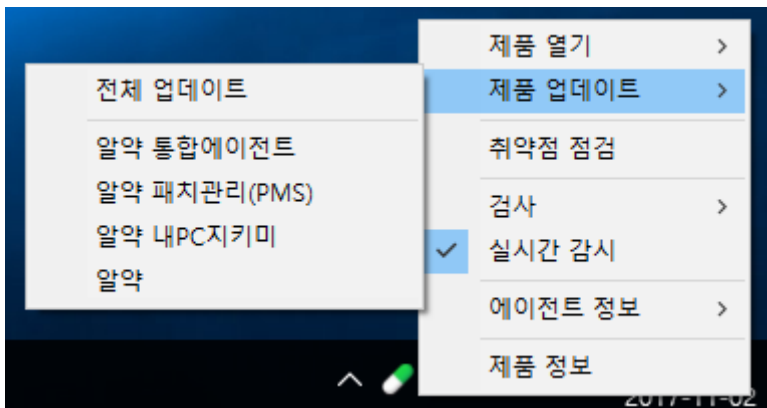


① 제품 열기: 설치된 알약, 알약 패치관리(PMS), 알약 내PC지키미 등 설치된 클라이언트를 실행시킬 수 있습니다.

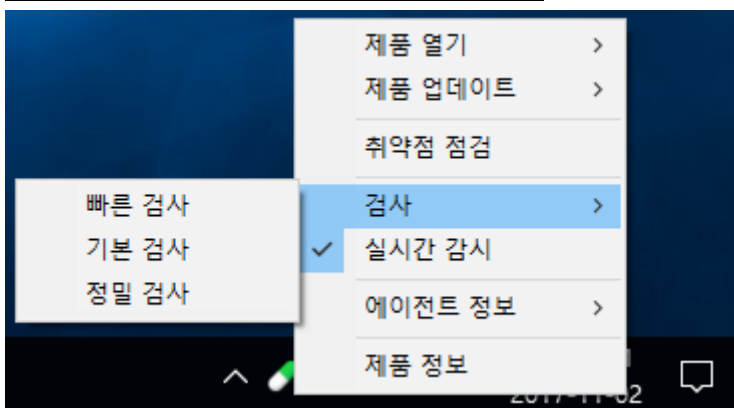
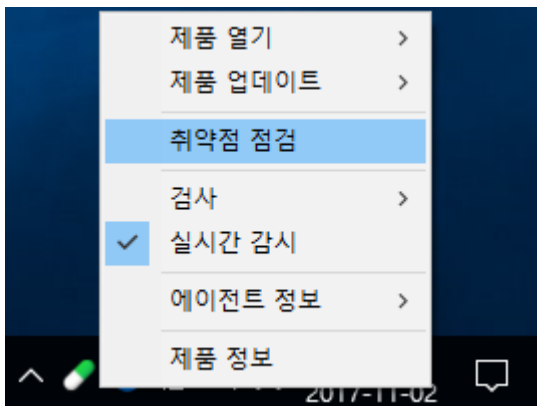


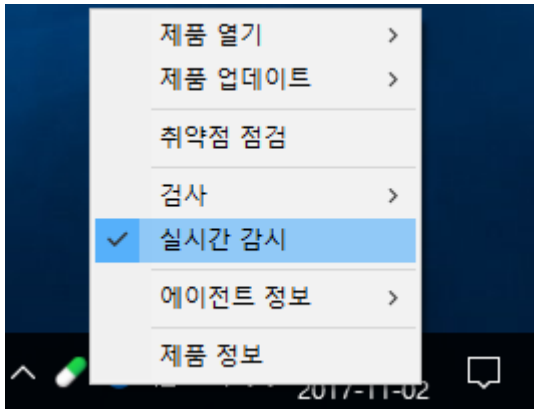
ASM 4 매뉴얼

- ② 제품 업데이트: 알약 통합에이전트와 클라이언트들을 즉시 업데이트 시킬 수 있습니다.
전체 업데이트 선택 시, 설치된 모든 제품 및 알약 통합에이전트가 일괄 업데이트됩니다.

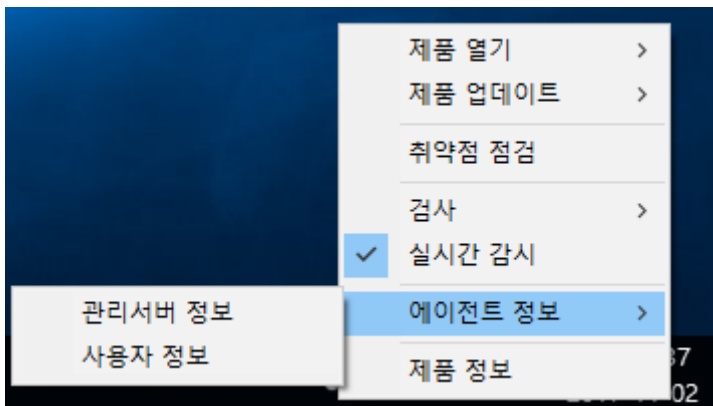


- ③ 제품별 메뉴: 제품별 주요 기능을 바로 사용할 수 있습니다.
- 취약점 점검: 알약 내PC지키미의 취약점 점검을 수행할 수 있습니다.
 - 검사: 알약의 검사 기능을 수행할 수 있습니다.
 - 실시간 감시: 알약의 실시간 감시를 ON/OFF 할 수 있습니다.





④ 에이전트 정보



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

에이전트 정보
✕

관리서버 정보

관리서버 IP (I)

관리서버 Port (S)

에이전트 Port (G)

서버연결 확인

닫기

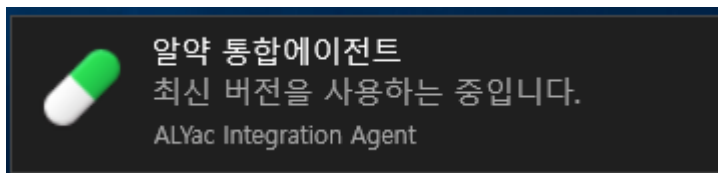
ASM 4 매뉴얼

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

빠른검사 >

- 실행된 프로세스와 관련파일
- 중요 시스템 영역

기본검사 >

- 빠른검사 영역
- 시스템 영역
- 자주 감염되는 위치

정밀검사 >

- 기본검사 항목
- 모든 시스템 영역
- 디스크 파일

검사 - 알약

기본검사

검사 진행상황 : 73090개 (검사시간 : 00:01:10)
 HLMWsoftware\microsoft\windows\currentversion\run [newname]

탐지된 항목: 0개 위험도: ● 아주낮음 ● 낮음 ● 보통 ● 높음 ● 아주높음

⚠ 위험요소 (0)

검사완료 후(△): 지표대기 일시종지(P) 종지(S)

환경설정 - 알약

기본설정

- 실행 설정
- 보안센터
- 로그 및 걸역소
- 업데이트

검사/실시간감시

- 실시간감시
- 마이윙케어
- 검사 옵션
- 검사 설정
- ✓ **예약검사**

네트워크

- 방화벽 설정

시스템

- 시스템 보호

도구

- 레지스트리 정리
- 매체케어

탐지 제외

- 탐지 제외 설정

> 예약검사

> 예약검사 설정(N)

검사종류	검사일정	마지막실행	다음실행

검사종류(K): 기본검사 ▼

검사일정(S): 지정요일 검사 ▼ 월요일 ▼

시간지정(T) 00 시 00 분

검사완료 후(ℳ): 자동지표 ▼

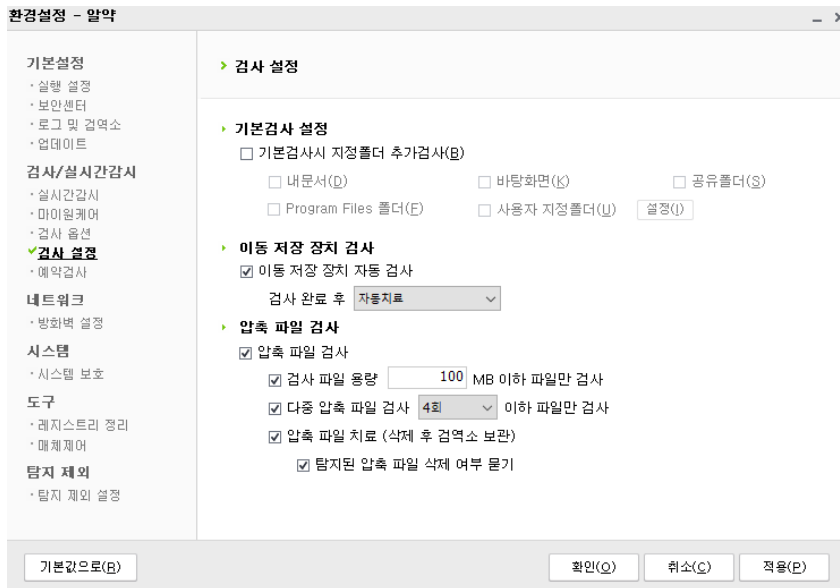
> 검사 시작 시 동작

검사하면 숨김(M)

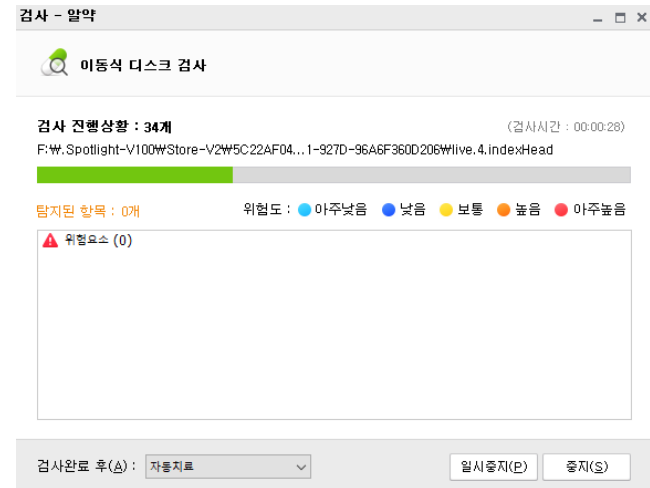
악성코드 검사 ②

- 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 방지함으로써 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

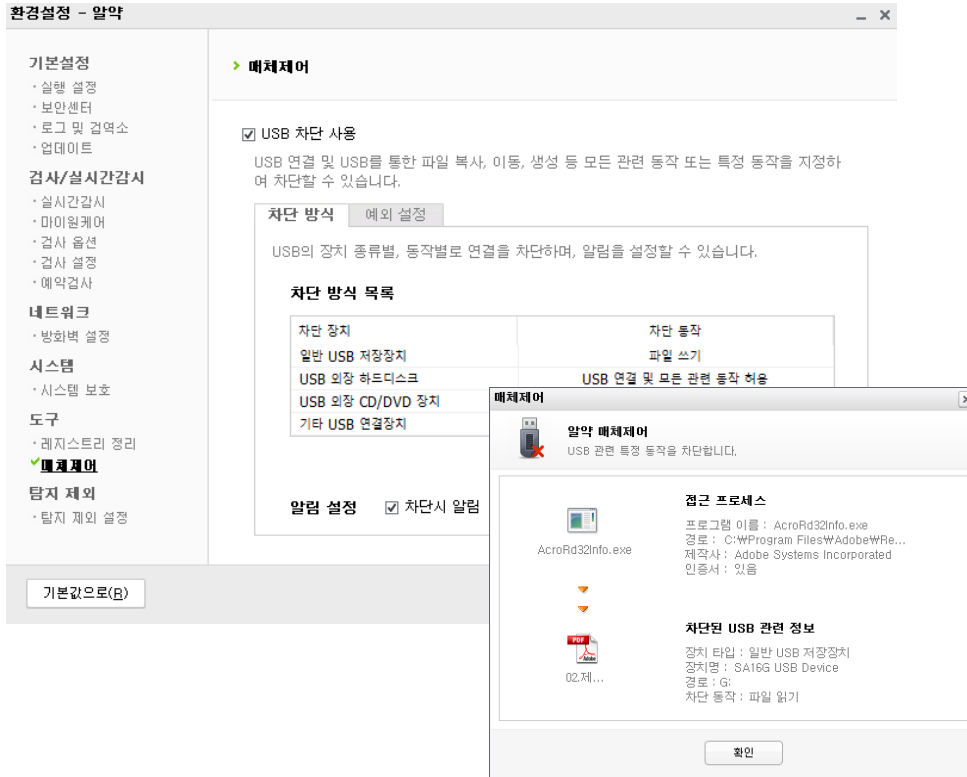
강력한 네트워크 폴더 감시

- 네트워크를 통한 악성코드의 감염이 다양해짐에 따라
다양한 접근 타입에 대해 강력하게 감시

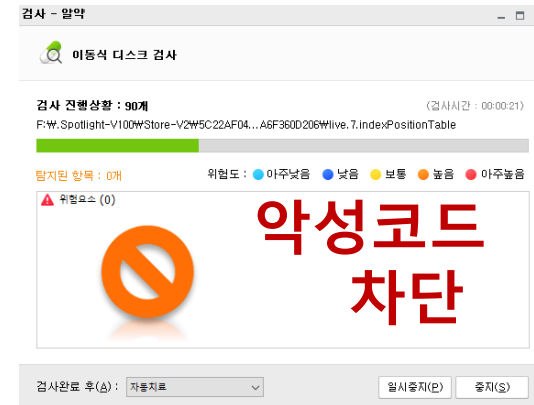
매체 제어

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



다양한 로그 기능

로그

- 알약의 동작 및 보안에 위협이 되는 동작이나 현상을 기록

기록 - 알약

로그 | 알약소 | 미치료 항목

이벤트 로그 | 시작일(년): 2017-09-07 | 종료일(년): 2017-09-07 | 새로고침(B)

전체
 실시간검사
 검사
 치료
 업데이트
 시스템보조
 정보유출방지
 시스템관리
 네트워크(방화벽)
 메세제어
 기타

일시	기능	이벤트 내용	타입
2017-09-07 16:58:24	매제제어	과일 소기 ; 자판	MWR UFD Memore...
2017-09-07 16:55:37	업데이트	업데이트 버전	4.0.0
2017-09-07 16:55:37	업데이트	업데이트종류	67개 성공
2017-09-07 16:55:27	업데이트	업데이트시작	자동업데이트
2017-09-07 15:27:27	외부저장장치검사	외장 메모리, 디스크 점...	176개 항목 검사
2017-09-07 15:27:02	매제제어	과일 소기 ; 자판	MWR UFD Memore...
2017-09-07 15:27:02	매제제어	과일 소기 ; 자판	MWR UFD Memore...
2017-09-07 15:15:13	수동검사(기본검사)	기본검사 중지	0개 항목 검사
2017-09-07 15:14:49	수동검사(기본검사)	기본검사 시작	
2017-09-07 14:55:51	업데이트	업데이트 버전	4.0.0
2017-09-07 14:55:51	업데이트	업데이트종류	37개 성공
2017-09-07 14:55:47	업데이트	업데이트시작	자동업데이트
2017-09-07 13:12:14	외부저장장치검사	외장 메모리, 디스크 점...	0개 항목 검사
2017-09-07 13:11:28	매제제어	과일 소기 ; 자판	MWR UFD Memore...

검역소

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

기록 - 알약

로그 | 알약소 | 미치료 항목

검역소 보관항목 | 시작일(년): 2017-09-08 | 종료일(년): 2017-09-08 | 새로고침(B)

기록일시	항목명	치료항목	로그인사용자
2017-09-08 16:07:12	Misc.TestMessage	TestMess...	est

전체
 위험요소
 예상위험요소(유리신식)
 미치료 프로그램

선택항목 정보

기록 일시: 2017-09-08 16:07:12
 탐지명: Misc.TestMessage
 탐지항목: TestMessage.exe
 위치: C:\ProgramData\Bin\WS-1-5-21-2258917340-1386467061-309034718-1001\WRC4TOVW
 로그인사용자: est

미치료 항목

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

기록 - 알약

로그 | 알약소 | 미치료 항목

미치료 항목 | 시작일(년): 2017-09-08 | 종료일(년): 2017-09-08 | 새로고침(B)

탐지일시	항목명	탐지항목	로그인사용자
2017-09-08 16:05:25	Misc.TestMessage	TestMess...	est

전체
 위험요소
 예상위험요소(유리신식)
 미치료 프로그램

선택항목 정보

탐지 일시: 2017-09-08 16:05:25
 탐지명: Misc.TestMessage
 탐지항목: TestMessage.exe
 위치: C:\ProgramData\Bin\WS-1-5-21-2258917340-1386467061-309034718-1001\WRC4TOVW
 로그인사용자: est

의심파일 신고 기능

알약이 탐지하지 못하는 위협요소, 위협요소가 아님에도 위협요소라고 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

신고하기 - 알약

신고 내용

구분: 정상 파일을 알약이 탐지(N) 탐지한 파일을 치료하지 못
 바이러스, 악성코드를 탐지 못함(D) 알약 기능오류(E)
 기타 문의(Q)

내용(T):

파일첨부(U): 추가 0 KB

이메일 주소(E):

전화번호(P): (선택사항)

고객사명(C): (선택사항)

시스템정보 송신 동의

시스템에서 발생한 문제를 해결하기 위해서 시스템 정보를 수집하여 알약고객센터에 전송할 수 있습니다. 신고한 문제 해결을 위해서만 사용되며 다른 목적으로 이용되지 않습니다. 위 내용에 동의해야만 신고하기 기능을 이용할 수 있습니다.

동의

검사 - 알약

기본검사

검사 완료 : 258225개 (검사시간 : 00:08:49)

탐지된 항목이 있습니다. 치료를 진행 하세요.

탐지된 항목 : 1개 위협도 : 아주낮음 낮음 보통 높음 아주높음

- 위협요소 (1)
- 기타 (1)
- Misc.TestMessage (1)

전체 선택/해제(A) **신고하기(M)** 탐지제외(E)

치료하기(S) 닫기(C) 설정(S)

미치료항목

미치료항목

- 위협요소
- 예상위험요소(유리스틱)
- 미해가 프로그램

시작일(E): 2017-09-08 종료일(T): 2017-09-08 새로고침(R)

탐지일시	탐지명	탐지영역	로그인사용자
2017-09-08 16:05:25	Misc.TestMessage	TestMess...	est

선택항목 정보

탐지 일시 : 2017-09-08 16:05:25
탐지명 : Misc.TestMessage
탐지영역 : TestMessage.exe
위치 : C:\\$Recycle.Bin\WS-1-5-21-2258817340-1386467051-309034718-1001\WS#PC4TOVN
로그인사용자 : est

관련 이벤트로그로 이동(G) **신고하기(M)** 탐지제외(E)

미치료 항목 재검사/치료(C) 미치료 기록삭제(D)

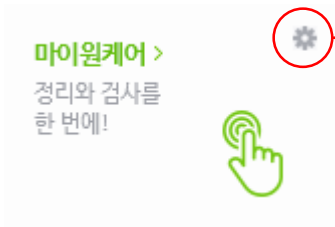
전송하기(S) 취소(C)

마이원케어

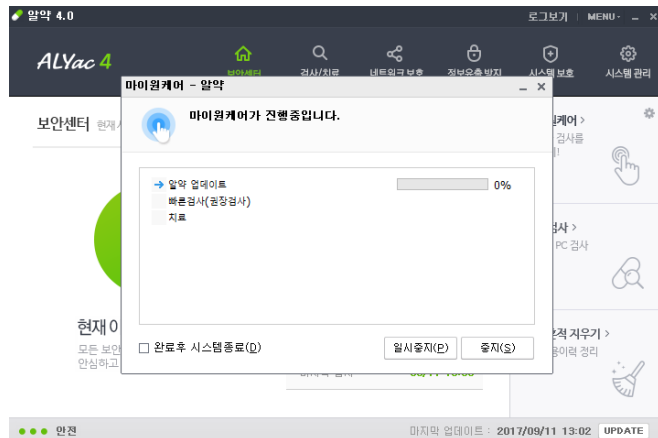
마이원케어란? (타사 백신에 없는 **알약 4.0의 특징!**)

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

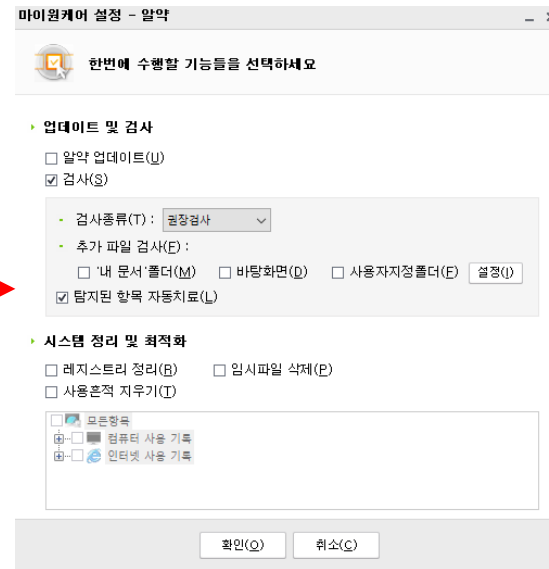
• 알약의 메인 화면에서 “마이원케어” 클릭



• 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

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 설정

방화벽 기능 사용(E)

▶ 기본 설정

- 들어오는 연결 제한(A)
 - 허용/차단 여부 묻기(B)
- 나가는 연결 제한(Q)
 - 허용/차단 여부 묻기(W)
- ICMP(Ping) 응답거부(I)

▶ 규칙 설정

환경설정과는 별도의 방화벽 규칙 화면을 통해 설정할 수 있습니다.

방화벽 규칙설정

• 방화벽 규칙 설정 화면

방화벽 규칙 - 알약

프로그램 규칙(P) 일반 규칙(G)

▶ 목록(S)

연결 상태	연결 방향	프로그램 명	실행파일	실행파일 위치
들어오는연결	차단	Internet Exp...	ieexplore.exe	C:\Program Files\Internet ...

▶ 추가/수정

- 연결 상태(W): 허용
- 연결 방향(Y): 모든 연결(T) 나가는 연결(U) 들어오는 연결(I)
- 프로그램 명(B):
- 실행 파일(M):

추가(A) 수정(E) 삭제(L)

규칙에 의해 통신 제한된 항목 알림(I) 확인(Q) 취소(C)

• 방화벽 기능 알림 화면

방화벽 - 알약

통신시도 (나가는 연결) 방화벽 규칙(E)

chrome.exe 74.125.204.189

통신시도 프로그램 정보

프로그램 이름 :chrome.exe
 인증서 :있음(Google Inc)
 프로그램 경로 :C:\program files (x86)\google\chrome\application

통신정보

연결된 주소 :74.125.204.189
 연결 포트 :443

위험 항목이 아니라면 허용을 선택하세요.

계속적용 허용(E) 차단(D)

레지스트리 검사 및 복구

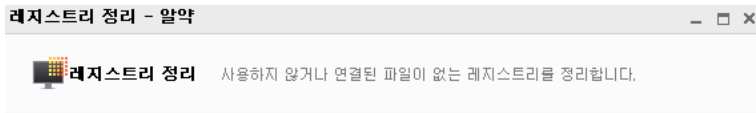
레지스트리 정리 기능을 이용한 레지스트리 복구 기능 (타사 백신에 없는 **알약 4.0의 특징!**)

• 알약>메인화면>시스템 관리

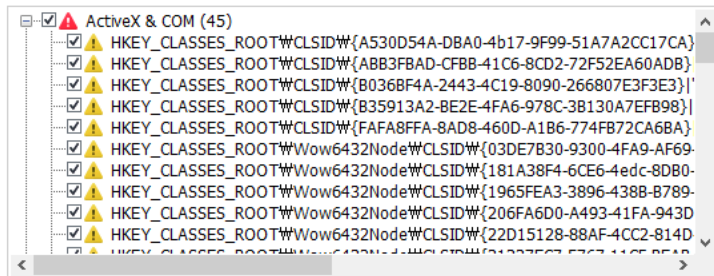
 레지스트리 정리
연결되지 않았거나 불필요하게 존재하는 레지스트리를 삭제할 수 있습니다.



• 레지스트리 검사 화면



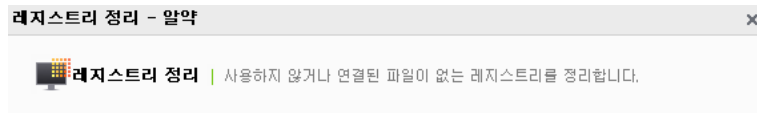
 **검사가 완료되었습니다.** 00:01:27
총 65개의 정리할 항목이 발견되었습니다.
정리를 시작하세요.



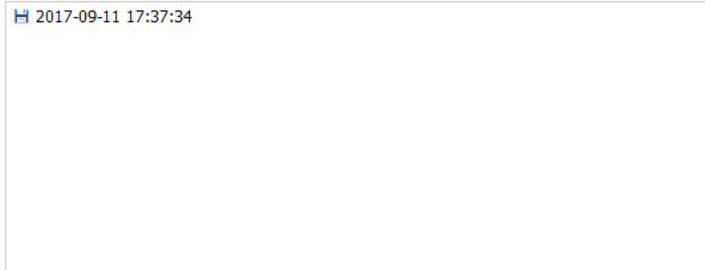
정리할 항목 백업(B)

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

• 레지스트리 복구 화면



복구할 백업항목을 선택하세요.
총 1개의 복구가능 항목이 있습니다.
복구할 항목을 선택한 후 '복구 시작' 버튼을 누르세요.

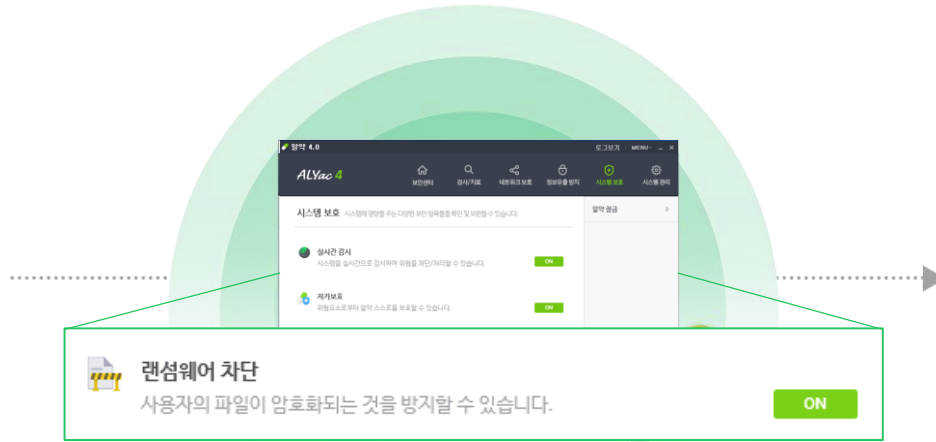


- 복구가능 항목 삭제 가능

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

