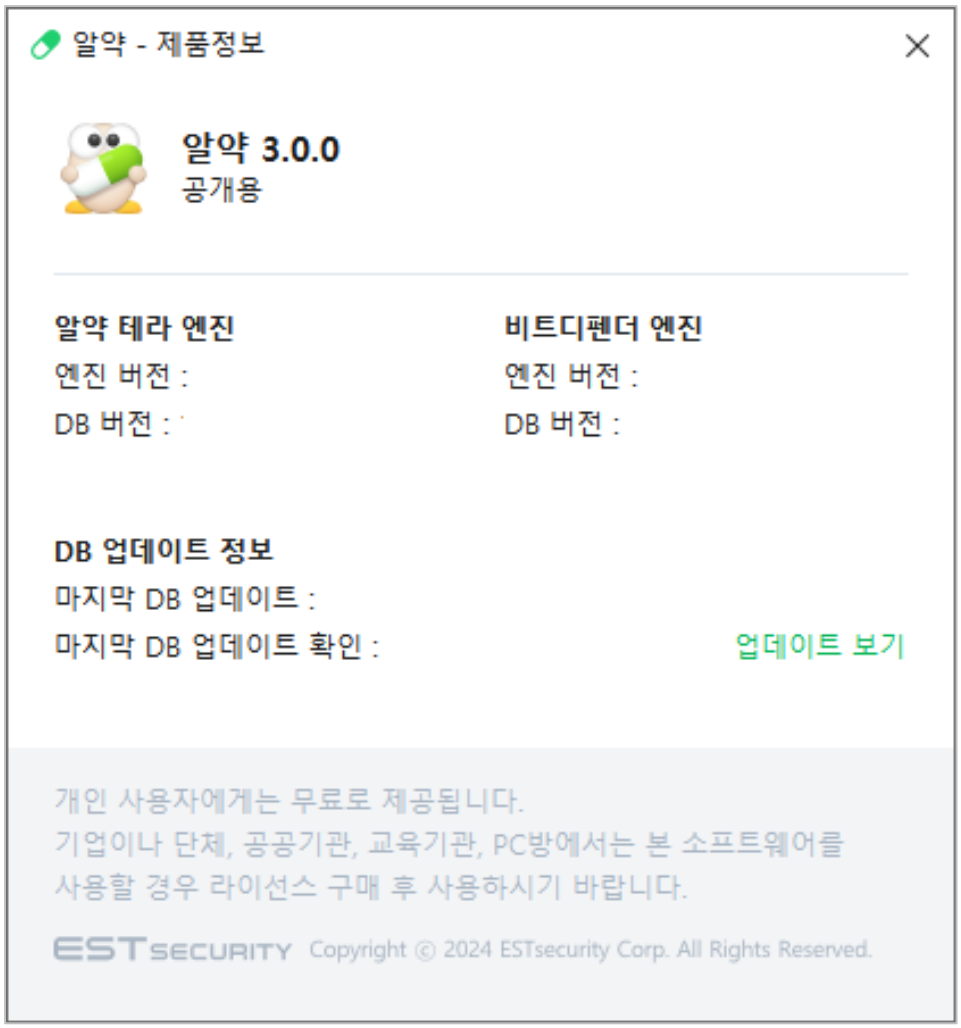
공개용 알약 3.0 도움말

알약은 사용자 PC 내 바이러스와 악성코드를 검사/치료하고, 실시간 감시 기능을 통해 시스템을 안전하게 보호하는 통합 백신 프로그램입니다.

네트워크 사용이 일상화된 환경에서 온라인을 통해 확산되기 쉬운 각종 위협으로부터 사용자의 PC를 지키는 것은 필수적입니다. 알약은 직관적이고 간편한 인터페이스를 제공하여 보안 지식이 많지 않은 사용자도 쉽게 활용할 수 있으며, 다양한 부가 기능을 통해 PC 보안 수준을 한층 강화할 수 있습니다.



알약 3.0 특징

1. 멀티 엔진 기반 탐지력

알약은 자체 엔진 **테라(Tera)**와 글로벌 보안 엔진 **비트디펜더(Bitdefender)**를 결합한 멀티 엔진 구조를 채택했습니다. 이를 통해 국내외에서 발생하는 다양한 악성코드를 높은 정확도로 탐지할 수 있습니다.

2.최적화된 성능

엔진 최적화와 프로그램 경량화를 통해 메모리와 CPU 점유율을 최소화하였습니다. 덕분에 백신 실행 중에도 PC 성능 저하 없이 쾌적하게 사용할 수 있습니다.

3. 스마트 스캔 (Smart Scan)

안전성이 확인된 파일은 **화이트리스트(WhiteList)**로 분류되어 반복 검사를 줄입니다. 검사 횟수가 쌓일수록 검사 속도는 점점 빨라지며, 자주 사용하는 프로그램은 불필요하게 영향을 받지 않습니다.

4. 안정적인 업데이트

알약은 최신 환경에서도 안정적으로 동작하며, 업데이트가 자동으로 이루어집니다. 사용자는 별도의 조치 없이 항상 최신 보안 상태를 유지할 수 있습니다.

알약 3.0 주요 기능

1. 악성코드 검사 및 치료

알약은 바이러스, 스파이웨어, 애드웨어, 루트킷, 트로이목마 등 다양한 악성코드를 손쉽게 검사하고 치료할 수 있습니다. 한 번의 클릭만으로 빠르게 검사가 가능합니다.

2. 실시간 감시

실시간 감시 기능은 악성코드 침입을 즉시 탐지하고 차단합니다. 감염 사실을 사용자에게 알리며, 관련된 파일까지 일괄적으로 치료 또는 삭제해 PC를 안전하게 보호합니다.

3. 신종 악성코드 대응

알약은 기존에 알려지지 않은 신종 악성코드까지 대응할 수 있는 탐지 기술을 적용하여

잠재적인 위협도 사전에 방어할 수 있습니다.

4. 이동장치 검사

USB 등 외부 저장장치 연결 시 자동으로 검사가 실행됩니다. 이 기능은 Autorun을 이용한 악성코드 감염을 사전에 차단합니다.

5. 랜섬웨어 보호

랜섬웨어 의심 행위를 사전에 탐지하고 차단합니다. 이를 통해 사용자의 중요한 파일이 암호화되는 것을 방지하여 데이터를 안전하게 지킬 수 있습니다.

알약 3.0 설치 환경

항목	최소 사양	권장 사양
CPU	Intel 셀러론 이상	Intel Core i3 이상
RAM	1GB 이상	2GB 이상
HDD	800MB 이상 여유 공간	1GB 이상 여유 공간
OS	Microsoft Windows 10/11 (x84/x64)	동일

알약은 최소 사양의 PC 환경에서도 원활하게 작동하도록 설계되었습니다.
다만, 더욱 빠르고 안정적인 사용 경험을 위해서는 권장 사양 이상의 PC에서 사용하시기를 권장합니다.

알약 설치하기

⚠️ 알약 설치 환경 확인

알약을 설치하기 전, 사용 중인 PC 환경이 알약의 지원 범위에 포함되는지 반드시 확인하시기 바랍니다.

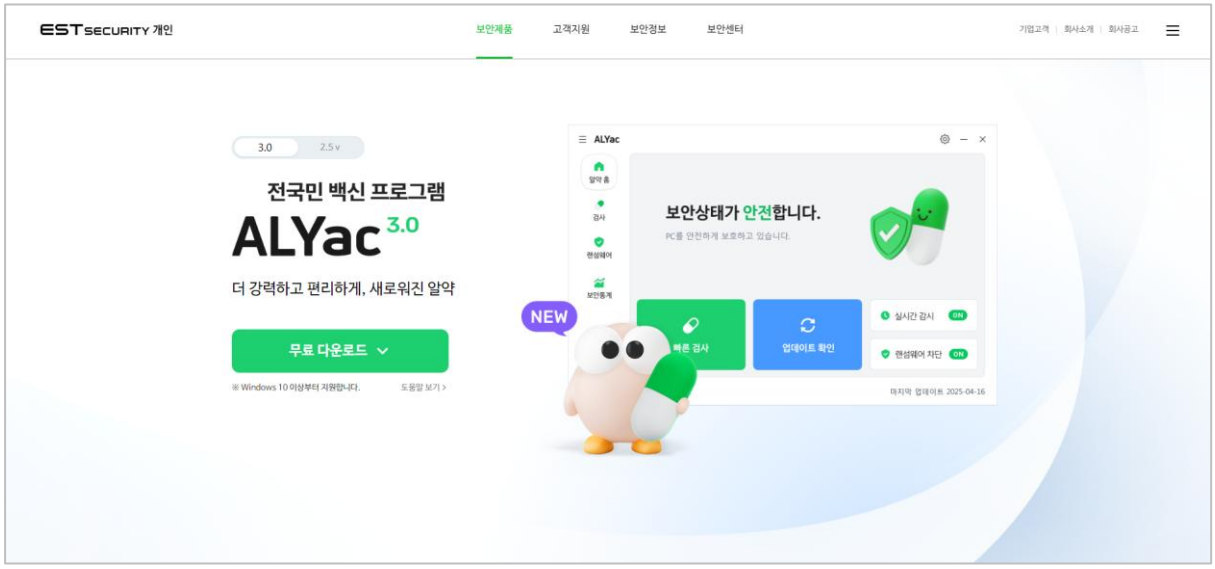
- 지원 운영체제: Windows 10/11 (32bit/64bit)
- 지원 불가 환경: ARM64 기반 기기(예: 갤럭시 북 S, 갤럭시 북 엣지 등)

⚠️ 타사 백신 및 보안 프로그램 제거

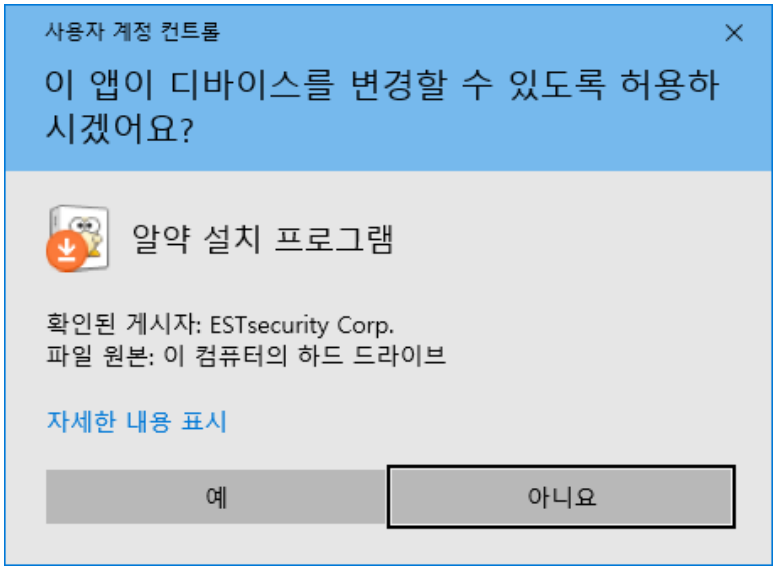
알약 설치 전에 시스템에 이미 설치되어 있는 타사 백신 또는 보안 프로그램을 반드시 제거해 주시기 바랍니다.

🚨 주의
알약을 타사의 백신·보안 프로그램과 동시에 사용하면 정상적으로 동작하지 않을 수 있으며, 프로그램 간 충돌로 인해 오류가 발생할 가능성이 있습니다.

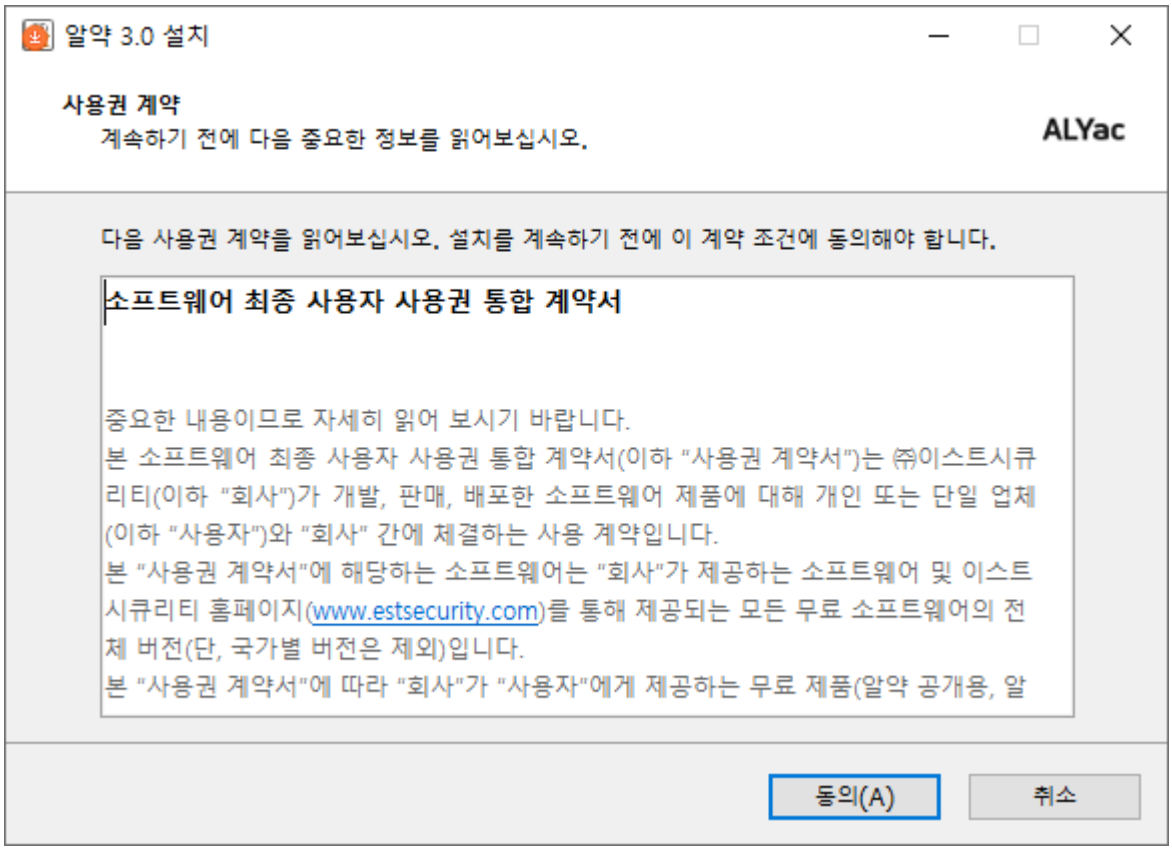
1. [이스트시큐리티 홈페이지](https://www.estsecurity.com/public/product/alyac-3)의 알약 공개용 3.0 메뉴에서 [무료 다운로드] 버튼을 클릭하면 알약 다운로드가 시작됩니다.



2. 다운로드가 완료된 후 알약 설치 파일을 실행합니다.

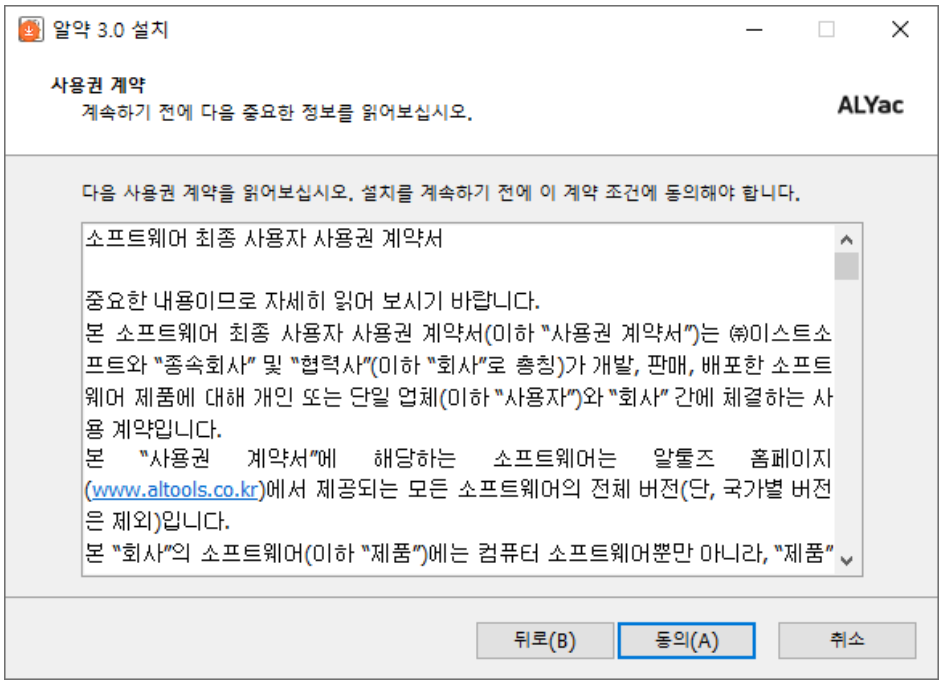


3. 알약 설치 프로그램이 실행되면 이스트시큐리티 소프트웨어 사용권 계약이 표시됩니다. 충분히 읽어 보신 후 [동의]를 클릭합니다.

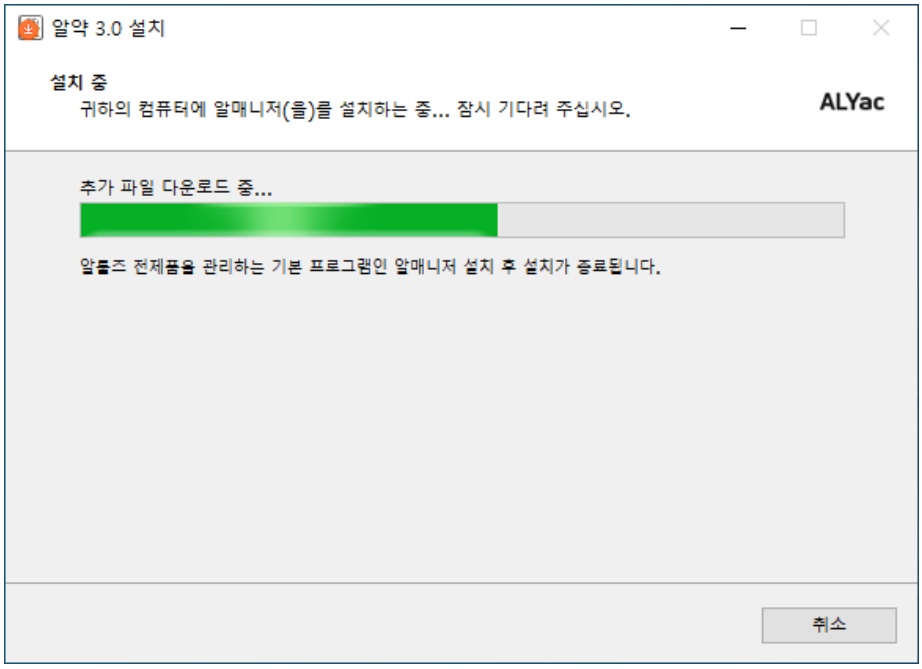


4. 알약은 알툴즈 통합 설치 프로그램인 알매니저를 통해 설치되며, 알매니저 설치 완료 후 알약 설치가 이어서 진행됩니다.
(알매니저가 이미 설치되어 있다면 바로 6번 단계로 진행됩니다.)

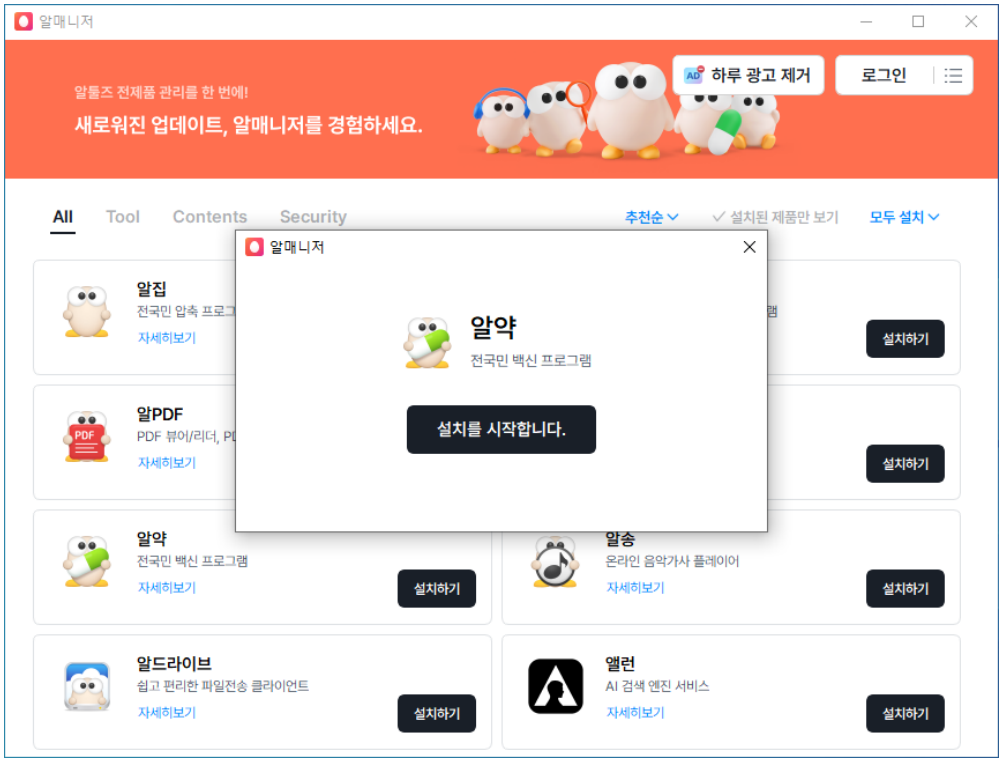
알툴즈 소프트웨어 사용권 계약이 표시됩니다. 충분히 읽어 보신 후 [동의]를 클릭합니다.



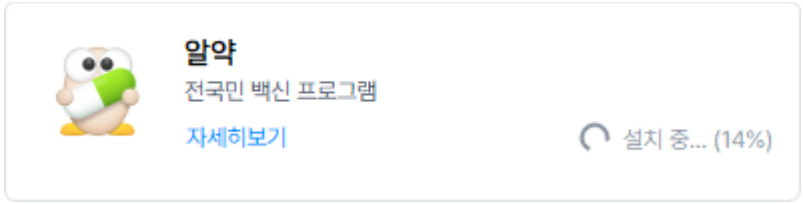
5. 알매니저 설치가 진행 중입니다. 설치가 완료되면 자동으로 알매니저가 실행됩니다.



6. 알매니저가 실행되어 알약 설치를 시작합니다.



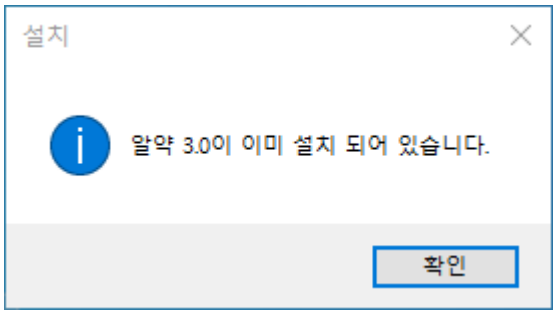
7. 알약 설치가 진행 중입니다.



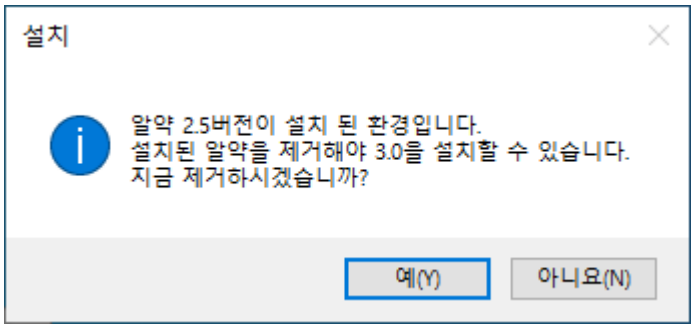
8. 알약 설치가 완료되었습니다.

⚠️ 알약이 이미 설치되어 실행 중인 PC의 경우

알약이 이미 설치되어 실행중인 상태에서는 알약이 설치되지 않습니다.

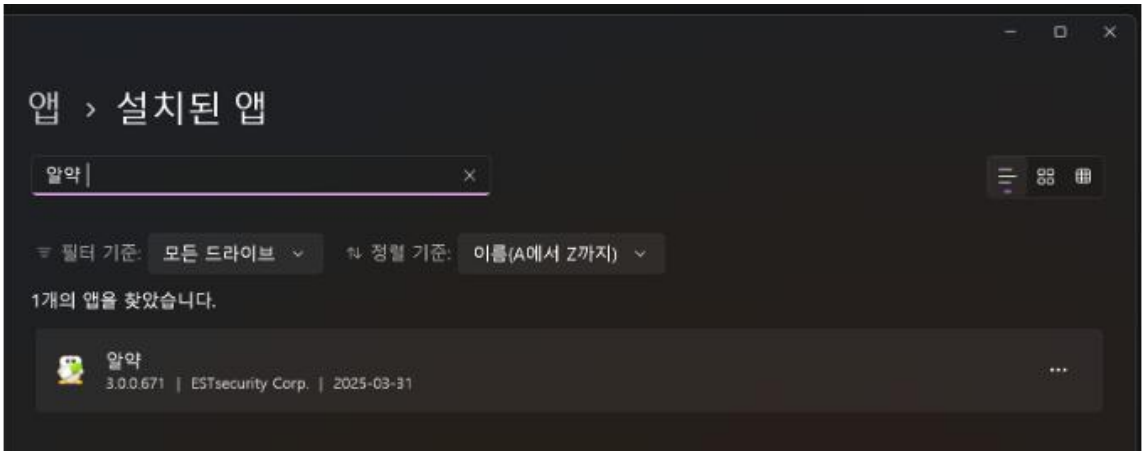


이전 버전의 알약이 설치되어 있는 경우에는 안내에 따라 제거 후 설치해주세요.

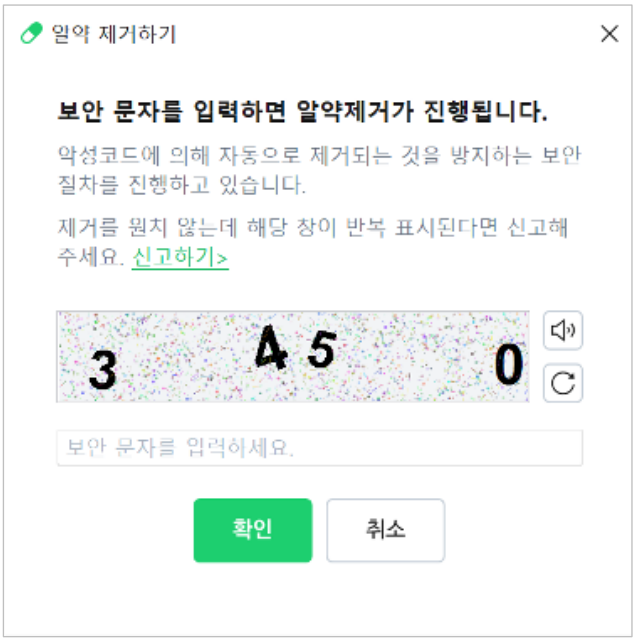


알약 제거하기

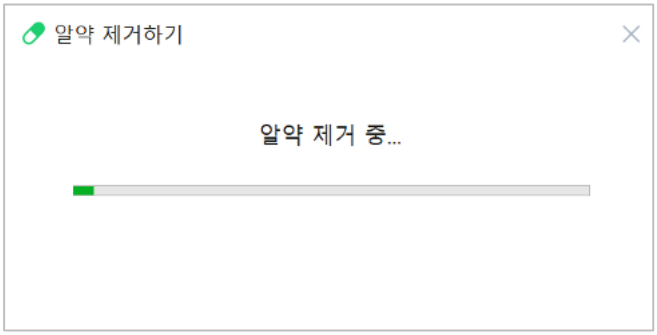
1. 시작>설정>앱>`설치된 앱`에서 알약을 선택한 후 메뉴에서 '제거'를 클릭합니다.



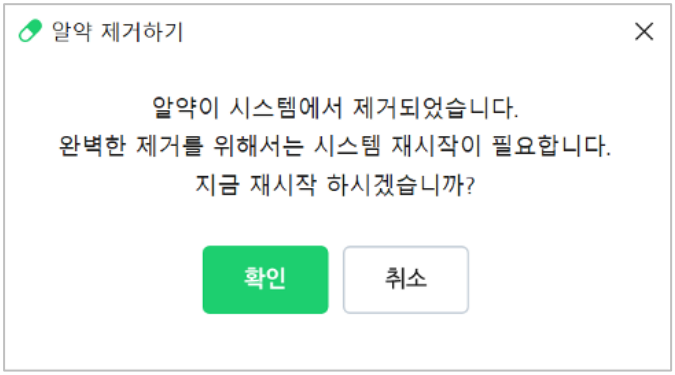
2. 알약 자동 제거 방지를 위한 창에서 숫자를 정확히 입력하고 [확인] 버튼을 클릭합니다.



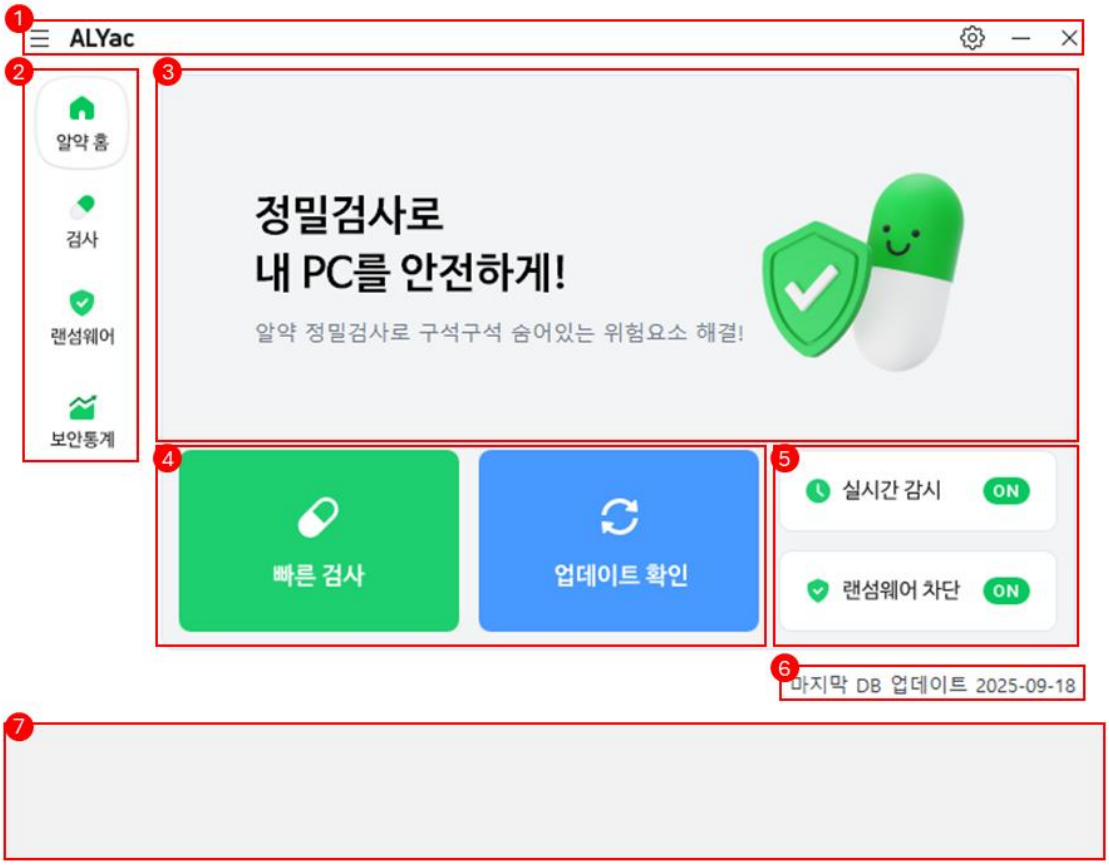
3. 알약 제거가 진행 중입니다. 잠시만 기다려 주시면 제거 작업이 완료됩니다.



4. 알약 삭제가 완료된 후 시스템 재시작을 위해 [확인]을 클릭합니다.



알약 홈(메인)



1. 타이틀 영역

메뉴 버튼과 제품명, 설정, 최소화 닫기 버튼이 포함되어 있는 영역입니다.

- ☰ 메뉴
검역소, 로그보기, 신고하기, 제품 정보 등을 확인하거나 도움말, 알약/알툴즈 홈페이지로 이동할 수 있습니다.

- ⚙ 환경설정
알약의 세부적인 옵션을 설정할 수 있습니다.

- − 최소화
알약 3.0 제품의 화면을 최소화합니다.

- × 닫기
알약 3.0 제품을 닫습니다.

2. 메인 메뉴 영역

알약에서 지원하는 주요 기능으로 이동할 수 있습니다.

- 알약 홈
알약의 메인 화면으로 주요기능과 상태를 확인할 수 있습니다.

- 검사
빠른 검사와 정밀검사 기능을 수행할 수 있습니다.

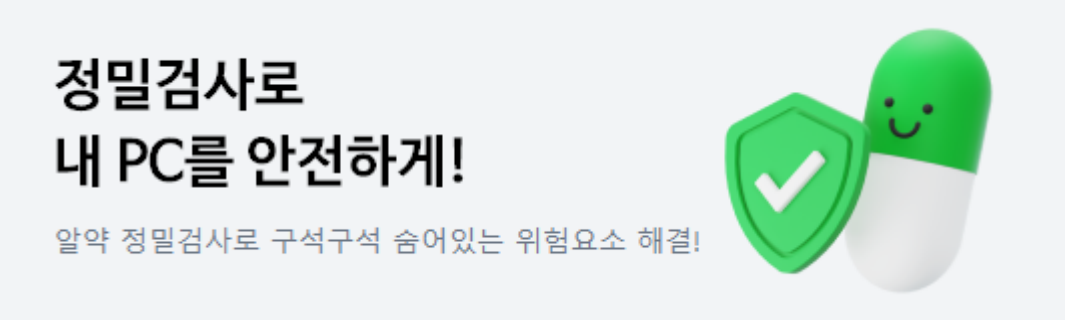
- 랜섬웨어
랜섬웨어 보호 상태를 변경하거나 백업/복구, 차단 제외 기능을 수행할 수 있습니다.

- 보안통계
악성코드 탐지 횟수와 치료 결과를 통계로 확인할 수 있습니다.

3. 커뮤니케이션 영역

PC의 실시간 보안 상태를 표시합니다.

- 정상 문구
실시간 보호와 랜섬웨어 차단 기능이 모두 활성화되어 있고, 최신 제품 버전과 DB 버전을 사용하며 빠른 검사와 정밀 검사를 정상적으로 실행하는 경우 '안전'으로 표시됩니다.



- 실시간 감시 미사용 문구

실시간 보호를 사용하지 않는 경우 다음 문구를 노출합니다.

- 랜섬웨어 미사용 문구

랜섬웨어 차단을 사용하지 않는 경우 다음 문구를 노출합니다.

- 기타 상태 안내 문구

    - 마지막 정밀검사에서 60일이 경과한 경우
      정밀검사로 내 PC를 안전하게! 알약 정밀검사로 구석구석 숨어있는 위험요소 해결!

    - 마지막 업데이트에서 60일이 경과한 경우
      업데이트가 최신이 아닙니다. 매일 새롭게 추가되는 위험요소를 차단하기 위해 업데이트를 수행해 주세요.

    - 마지막 업데이트에서 7일이 경과하거나 마지막 정밀검에서 60일이 경과한 경우
      주의가 필요합니다. 알약으로 PC를 안전하게 보호하기 위해 최신 업데이트 및 검사를 수행해 주세요!

4. 기능 버튼 영역

주요 기능을 빠르게 실행할 수 있습니다.

- 빠른 검사

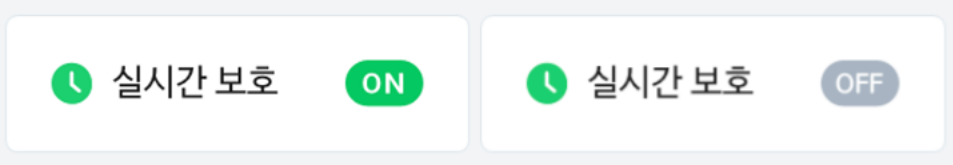
    - 시스템 주요 영역의 악성코드 감염 여부를 빠르게 진단합니다.

- 업데이트 확인

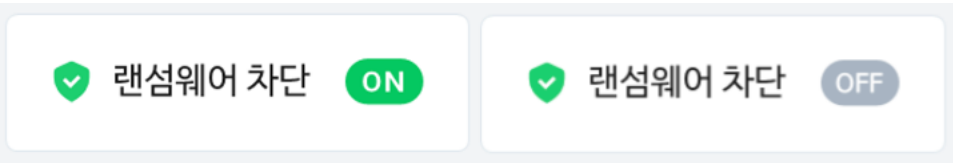
    - 업데이트 상태를 확인하고 수동으로 업데이트를 진행합니다

5. 옵션 버튼 영역

주요 기능의 ON/OFF를 설정할 수 있습니다.



- 실시간 보호
    - 실시간 보호 기능을 ON / OFF 할 수 있습니다.
    - **ON**일 경우 기능이 활성화되며, **OFF**의 경우 비활성화됩니다.



- 랜섬웨어 차단
    - 랜섬웨어 차단 기능을 ON / OFF 할 수 있습니다.
    - **ON**일 경우 기능이 활성화되며, **OFF**의 경우 비활성화됩니다.

6. 업데이트 정보 영역

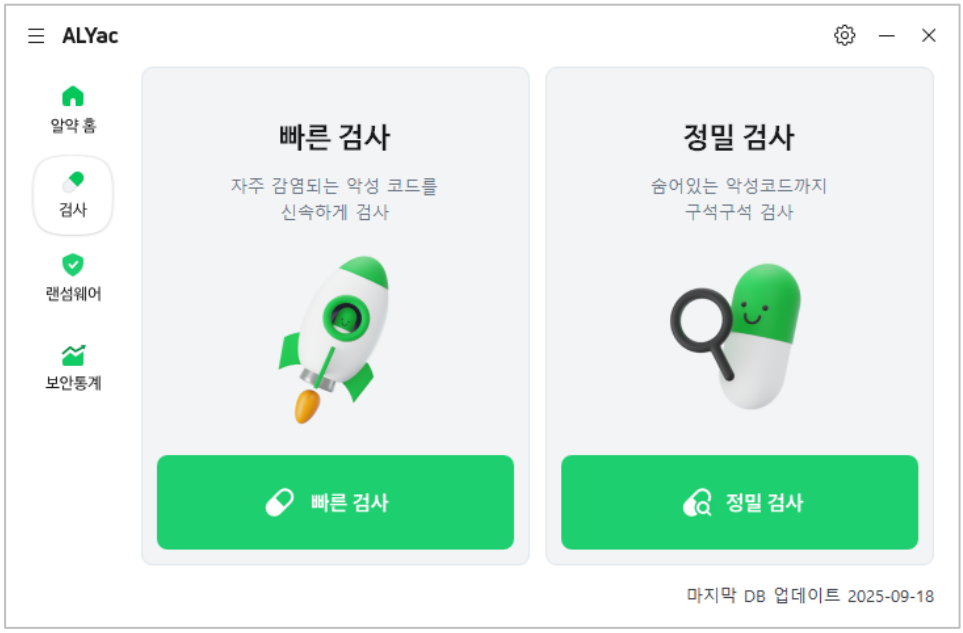
최근 DB 업데이트 진행 일자를 확인할 수 있습니다.

7. 광고 영역

더 나은 서비스 제공을 지원하기 위한 광고가 표시됩니다.

검사

빠른 검사와 정밀검사를 제공하는 영역입니다.



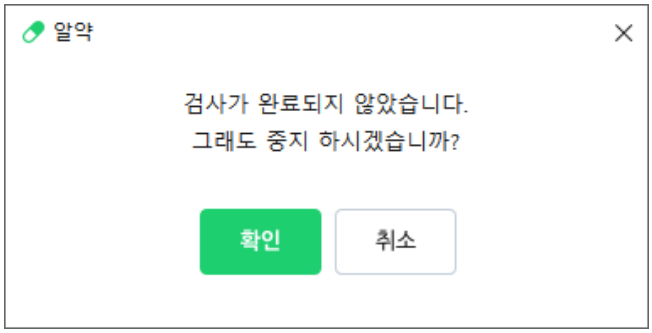
빠른 검사

- 시스템에 즉시 피해를 줄 수 있거나 자주 감염되는 바이러스나 악성코드를 신속하게 검사합니다.

- 사용자 PC의 주요 영역만을 검사하여, 매번 정밀 검사를 실행하지 않더라도 효과적으로 PC를 보호할 수 있습니다.

- **일시 중지** 버튼을 클릭하면 검사가 일시 중지됩니다. 일시 중지된 상태에서는 **계속 진행** 버튼을 클릭하여 검사를 이어 진행할 수 있습니다.

- **중지** 버튼을 클릭하면 의사 확인 후 검사를 완전히 종료합니다.



⚠ 빠른 검사 영역

빠른 검사에서는 아래 사항들을 단계적으로 검사합니다.

1. 프로세스
   - 현재 실행 중인 프로그램의 파일을 검사합니다.
2. 프로세스 모듈
   - 실행 중인 프로세스가 불러온 모듈(라이브러리 및 구성 요소 파일)을 검사합니다.
3. 서비스
   - Windows 서비스로 등록되어 자동 실행 중인 프로그램을 검사합니다.
4. 자동 실행 프로그램 (AutoRun)
   - 시작 시 자동으로 실행되도록 등록된 프로그램을 검사합니다.
5. 자동 실행 설정 파일 (AutoRun.inf)
   - 이동식 디스크 등에 포함된 AutoRun 설정 파일을 검사합니다.
6. 부트 섹터 (Boot Sector)
   - 하드디스크의 부팅 영역(MBR, Master Boot Record)을 검사합니다.
7. 기본 검사 영역
   - 휴지통, Windows 폴더, System32 폴더, 루트 디스크 등 주요 시스템 영역을 검사합니다.

⚠ 추가 검사 영역

사용자가 추가로 검사 영역을 지정할 수 있습니다.

1. 내 문서 (My Documents)
   - "내 문서" 폴더 안에 저장된 파일들을 검사합니다.

2. 바탕화면 (Desktop)
 - 바탕화면 폴더에 위치한 모든 파일을 검사합니다.
3. 공유 폴더 (Shared Folder)
 - 현재 공유 설정이 적용된 폴더 내 파일을 검사합니다.
4. 프로그램 설치 폴더 (Program Files)
 - 기본적으로 프로그램이 설치되는 Program Files 폴더 내 파일을 검사합니다.
5. 사용자 지정 폴더 (Custom Folder)
 - 사용자가 직접 추가로 지정한 폴더 내 파일을 검사합니다.

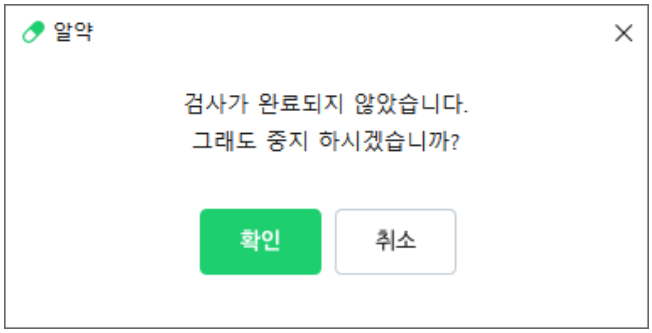
정밀 검사

- 사용자 PC의 모든 하드디스크 또는 사용자가 지정한 폴더 전체를 대상으로 상세하게 검사를 수행합니다.

- 빠른 검사에 비해 오랜 시간이 걸리나, 활동하지 않고 숨어 있는 악성코드까지 탐지할 수 있습니다.

- **일시 중지** 버튼을 클릭하면 검사가 일시 중지됩니다. 일시 중지된 상태에서는 **계속 진행** 버튼을 클릭하여 검사를 이어 진행할 수 있습니다.

- **중지** 버튼을 클릭하면 의사 확인 후 검사를 완전히 종료합니다.



⚠ 정밀 검사 영역

정밀 검사에서는 아래 사항들을 단계적으로 검사합니다.

1. 임시 파일 삭제
- PC 최적화를 위해 불필요한 임시 파일을 삭제하여 시스템 여유 공간을 확보합니다. (환경설정> 검사 설정> 정밀 검사 설정> 정밀 검사 전 임시 파일 삭제 옵션 ON/OFF에 따라 동작)

2. 프로세스 검사
- 현재 실행 중인 프로그램(프로세스)의 파일을 검사합니다.

3. 프로세스 모듈 검사
- 실행 중인 프로세스가 불러온 모듈(라이브러리 및 구성 요소)을 검사합니다.

4. 서비스 검사
- Windows 서비스로 등록되어 실행되는 프로그램을 검사합니다.

5. 자동 실행 프로그램 검사 (AutoRun)
- 시작 시 자동 실행되도록 등록된 프로그램을 검사합니다.

6. 자동 실행 설정 파일 검사 (AutoRun.inf)
- 이동식 디스크 등에 포함된 AutoRun 설정 파일을 검사합니다.

7. 부트 섹터 검사 (Scan Boot Sector)
- 하드디스크의 부트 영역(MBR, Master Boot Record)을 검사합니다.

8. CLSID 레지스트리 검사
- Windows 레지스트리의 CLSID 관련 항목을 검사합니다.

9. 프로세스 메모리 검사
- 실행 중인 프로세스 메모리를 검사합니다. (환경설정> 검사 설정> 정밀 검사 설정> 프로세스 메모리 검사 옵션 ON/OFF에 따라 동작)

10. 안티 루트킷 검사
- 숨겨진 파일 및 루트킷 유형 악성코드를 검사합니다.

11. 호스트 파일 검사
- Windows 시스템의 hosts 파일에 사용자가 직접 추가한 항목을 검사합니다.

12. 기본 검사 영역
- 휴지통, Windows 폴더, System32 폴더, 루트 디스크 등 주요 시스템 영역을 검사합니다.

⚠️ 추가 검사 영역

사용자가 추가로 검사 영역을 지정할 수 있습니다.

1. 내 문서
- My Documents 폴더 안에 위치한 파일들을 검사합니다.

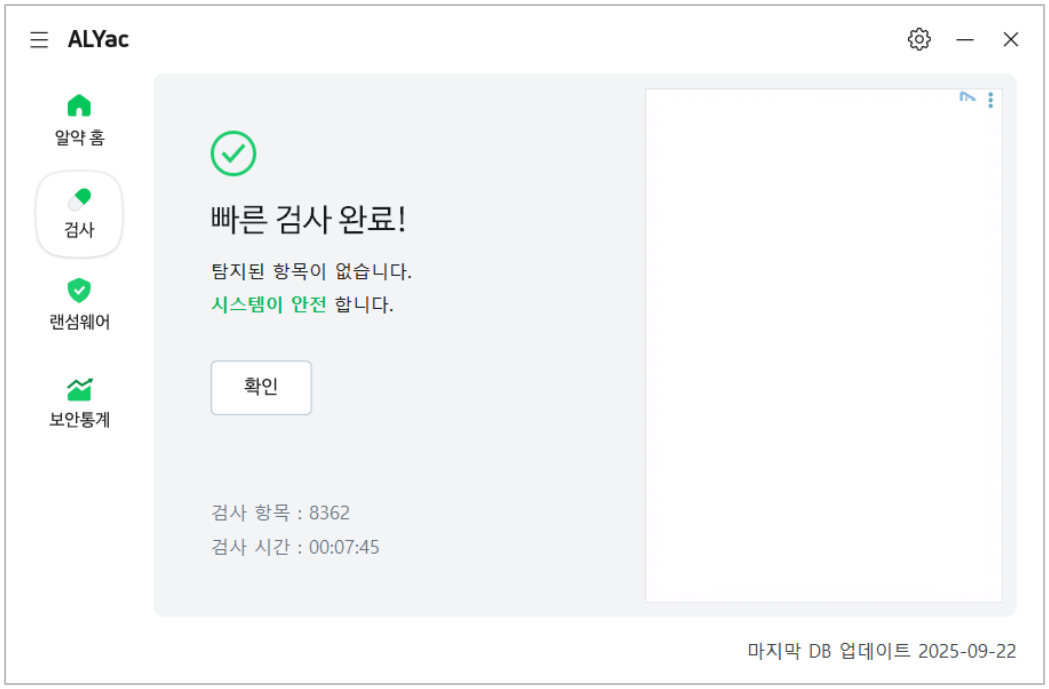
2. 바탕화면
- 바탕화면 폴더 안의 파일들을 검사합니다.

3. 공유 폴더
- 현재 공유 폴더로 지정된 폴더의 파일들을 검사합니다.

4. Program Files 폴더
- 기본적으로 프로그램이 설치되는 폴더인 Program Files 내 파일들을 검사합니다.

5. 사용자 지정 폴더
- 사용자가 추가로 지정한 폴더 내 파일들을 검사합니다.

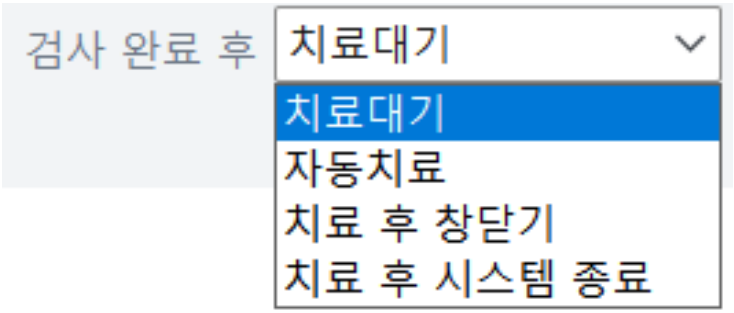
검사 완료



검사가 완료되면 PC의 보안 상태가 **안전** 또는 **주의** 중 하나로 표시됩니다.

- **안전**으로 표시된 경우: 검사 결과 악성코드가 발견되지 않았음을 의미합니다.
- **주의**로 표시된 경우: 탐지된 악성코드가 목록으로 제공되며, 사용자는 해당 항목을 확인한 뒤 치료 또는 삭제와 같은 조치를 진행할 수 있습니다.

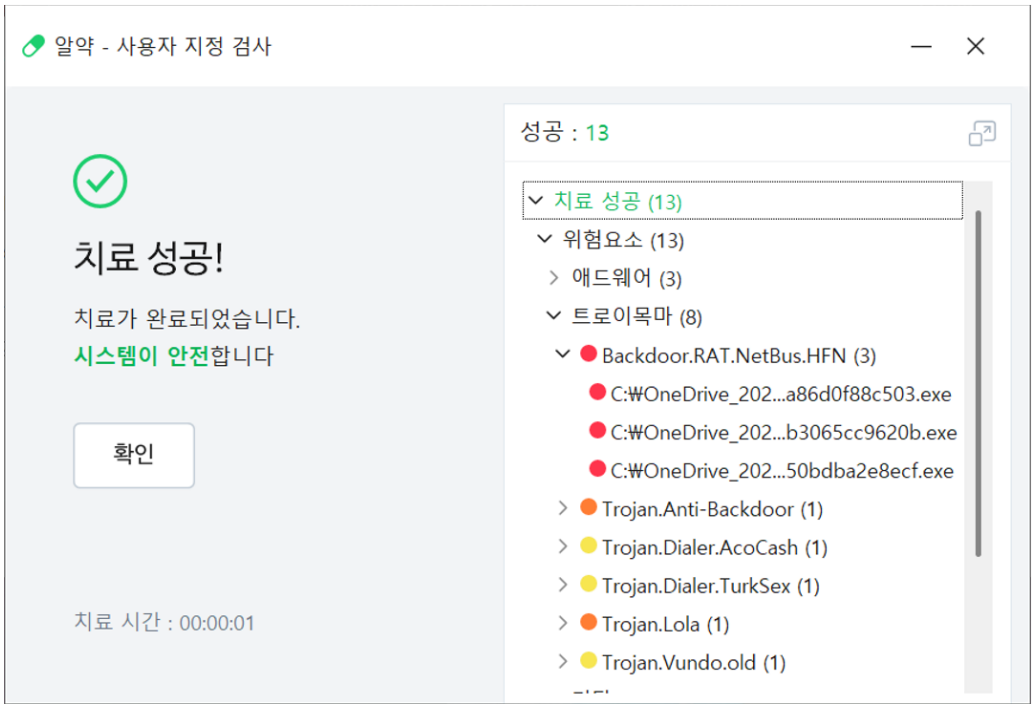
검사 과정에서 악성코드를 탐지했을 때, 사용자가 미리 지정한 방식에 따라 자동으로 처리하거나 선택할 수 있습니다.



각 설정에 따른 동작은 다음과 같습니다.

- 치료대기: 수동으로 치료를 선택하도록 사용자 입력을 대기합니다.

[치료하기] 버튼을 선택 시 치료를 진행하며 치료가 진행된 결과 화면을 보여줍니다.



- 자동치료: 검사 이후 자동으로 치료를 진행합니다.

- 치료 후 창 닫기: 자동으로 치료 후 결과 화면까지 닫습니다.

- 치료 후 시스템 종료: 자동으로 치료 후 시스템을 종료합니다.

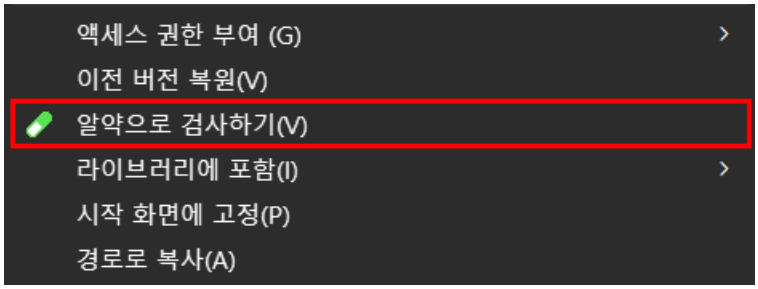
이동식 저장 장치 검사

USB 메모리 등 외부 저장장치가 PC에 연결되었을 때 자동으로 검사를 실행합니다. 이를 통해 사용자가 별도의 조작을 하지 않아도, 이동식 장치를 통한 악성코드 유입을 사전에 차단할 수 있습니다.

특히 자동실행(Autorun) 기능을 악용한 악성코드는 USB 연결과 동시에 실행되어 시스템을 감염시킬 수 있는데, 알약은 이를 즉시 탐지하고 차단하여 안전한 사용 환경을 보장합니다.

사용자 지정 검사

마우스 우클릭 메뉴를 이용해 특정 폴더나 파일만 선택적으로 검사할 수 있는 기능을 제공합니다. 이 기능을 사용하면 전체 검사를 실행하지 않고도, 필요할 때 원하는 항목만 빠르게 점검할 수 있습니다.

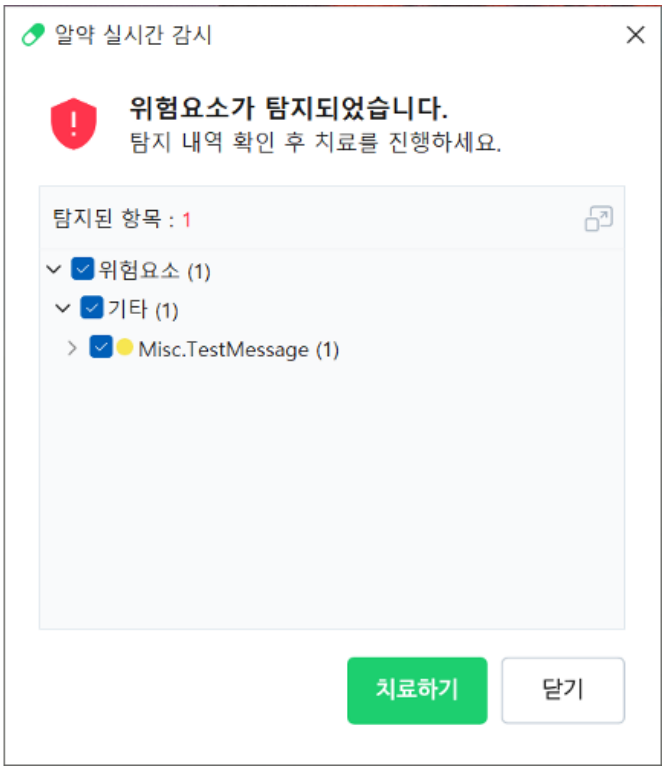


실시간 감시

바이러스나 악성코드가 포함된 파일이 다운로드 되거나 실행될 경우, 즉시 팝업창을 띄워 사용자에게 위협 사실을 알려줍니다.

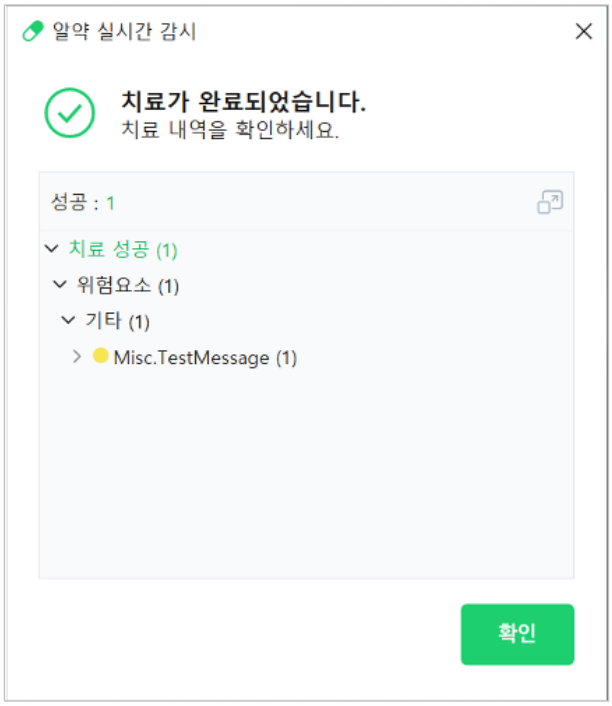
팝업창에서는 탐지된 항목의 정보를 확인할 수 있으며, 사용자가 치료 또는 삭제 기능을 선택해 즉시 대응할 수 있도록 안내합니다.

실시간 감시에서 악성코드 탐지



실시간 감시 기능이 활성화(On) 상태일 경우, 악성코드가 실행되면 알약이 자동으로 차단합니다. 사용자는 알림창에서 다음과 같이 조치할 수 있습니다.

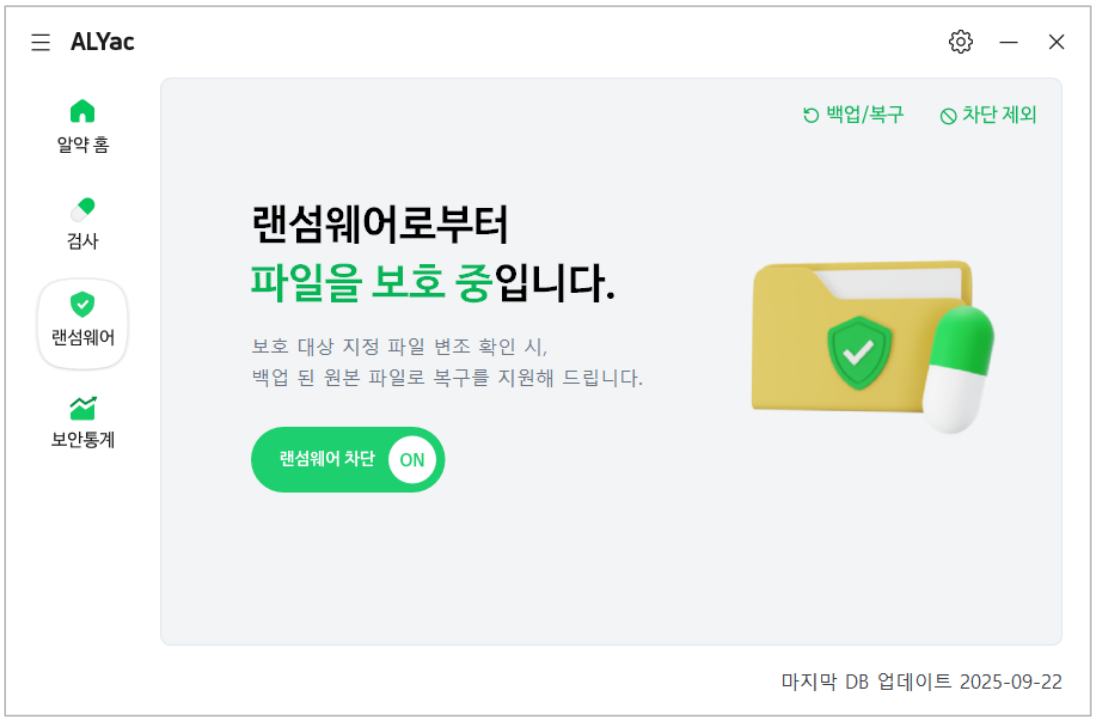
- [치료하기] 버튼
  → 탐지된 악성코드를 치료하거나 삭제합니다.



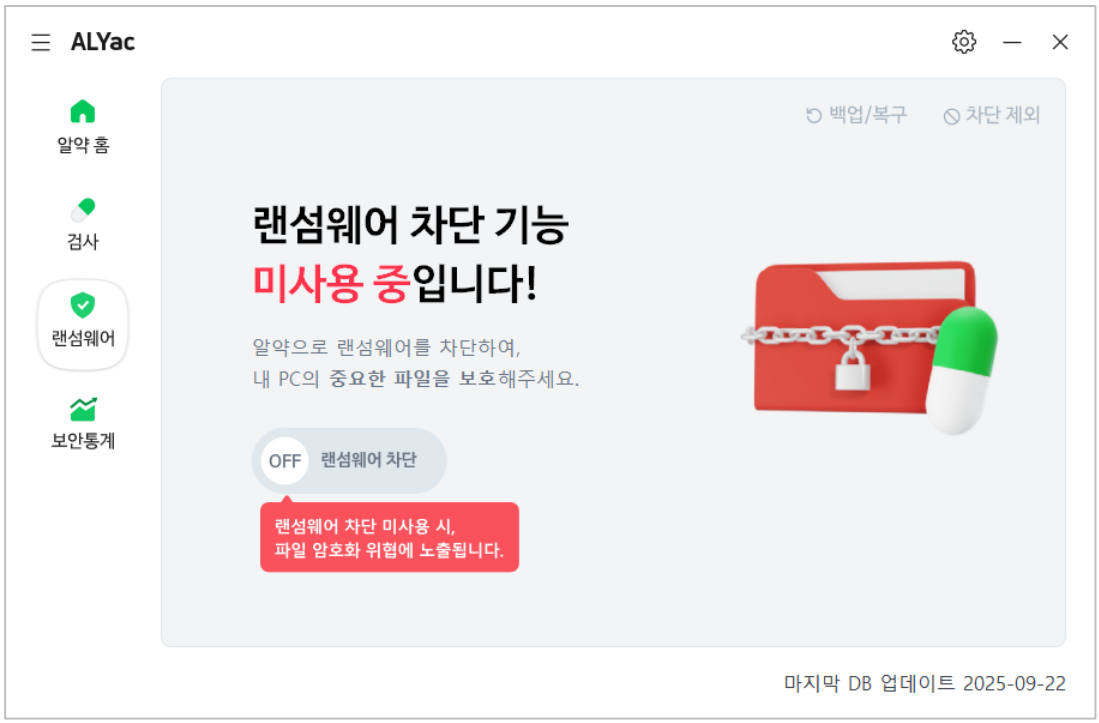
- [닫기] 버튼
  → 악성코드를 치료하지 않고 실시간 감시 알림창을 종료합니다.

랜섬웨어

랜섬웨어는 사용자의 파일을 강제로 암호화한 뒤 금전을 요구하는 악성 프로그램으로, 한 번 감염되면 복구가 어렵기 때문에 사전 예방이 무엇보다 중요합니다.

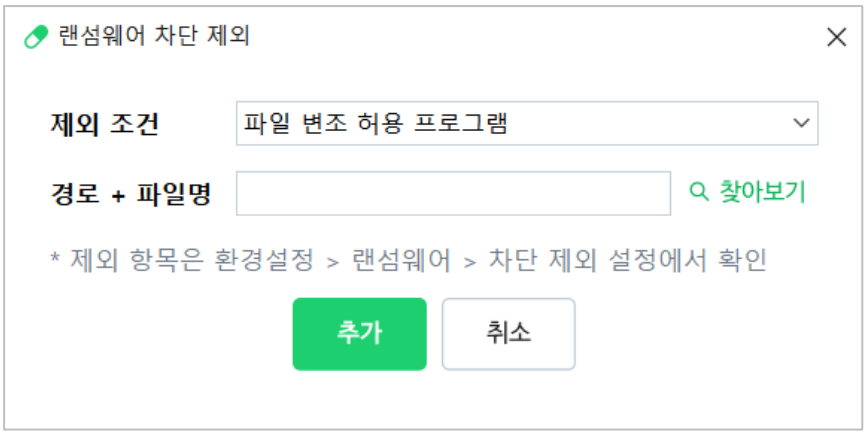


랜섬웨어 차단 기능을 OFF로 변경할 경우, 아래와 같은 안내 문구가 출력됩니다.

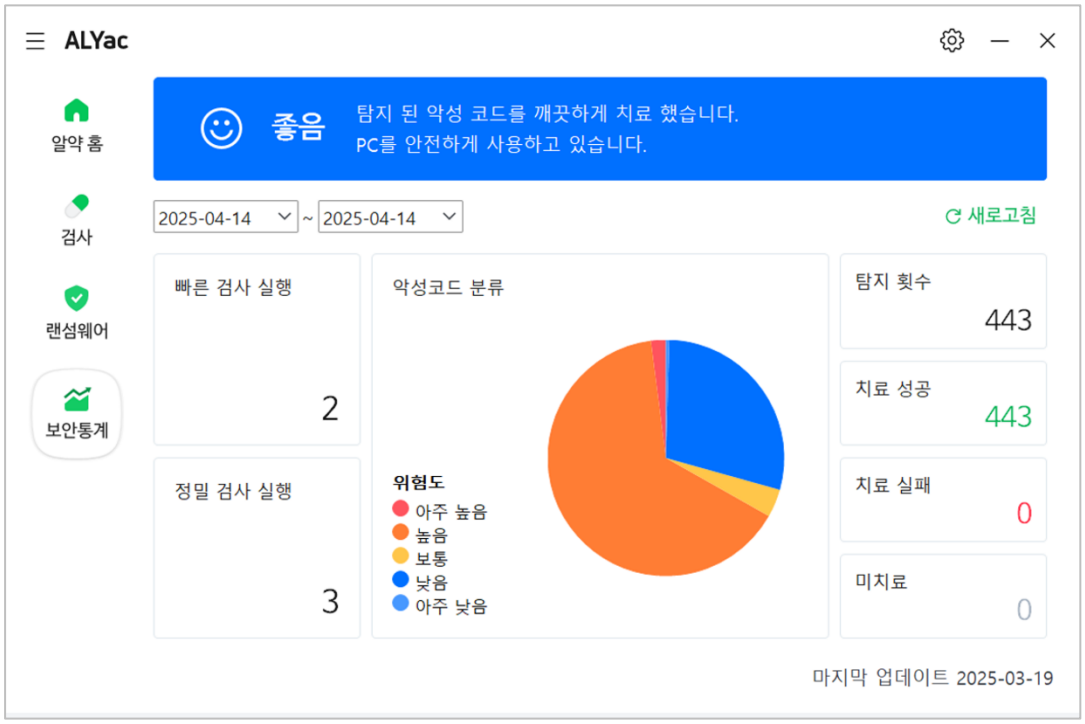


- [백업/복구] 버튼을 선택하면 검역소의 랜섬웨어 백업/복구 창을 오픈합니다.

- [차단 제외] 버튼을 선택하면 다음 창이 열리며 차단제외를 바로 등록할 수 있습니다.



보안통계



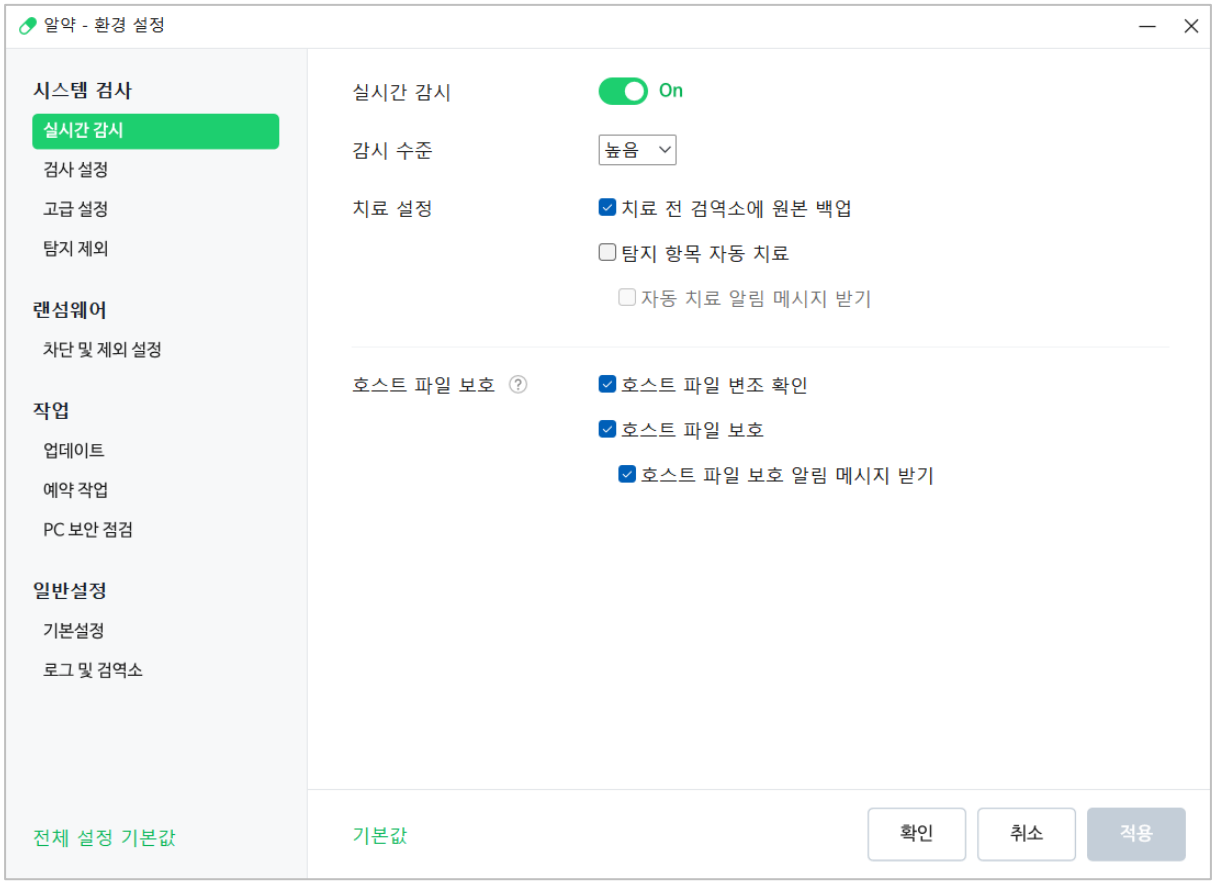
알약 설치 후에는 사용자가 진행한 빠른 검사와 정밀 검사 횟수를 확인할 수 있습니다. 또한 알약이 탐지한 악성코드의 탐지 횟수, 치료 성공 여부, 치료 실패 여부, 미치료 상태를 구분하여 보여줍니다.

추가로, 탐지된 악성코드의 위험도에 따라 분류된 그래프를 제공하여, PC 보안 상태를 한눈에 확인할 수 있습니다.

환경설정

메인 화면에서 ⚙ 아이콘을 클릭하거나, 작업 표시줄의 트레이 메뉴에서 [환경설정]을 선택하면 환경설정 창이 열리며 알약과 관련된 다양한 옵션을 직접 설정할 수 있습니다.

시스템 검사



실시간 감시

기능이 On일 경우 기능이 활성화되며, 비활성화의 경우 Off로 설정하면 됩니다.

감시 수준

높음 (기본값): 모든 시스템 영역을 감시합니다.

보통: 실행 파일만 감시합니다.

치료 설정

치료 전 검역소에 원본 백업 (기본값): 악성코드를 치료하기 전에 원본 파일을 검역소로 복사·백업합니다.

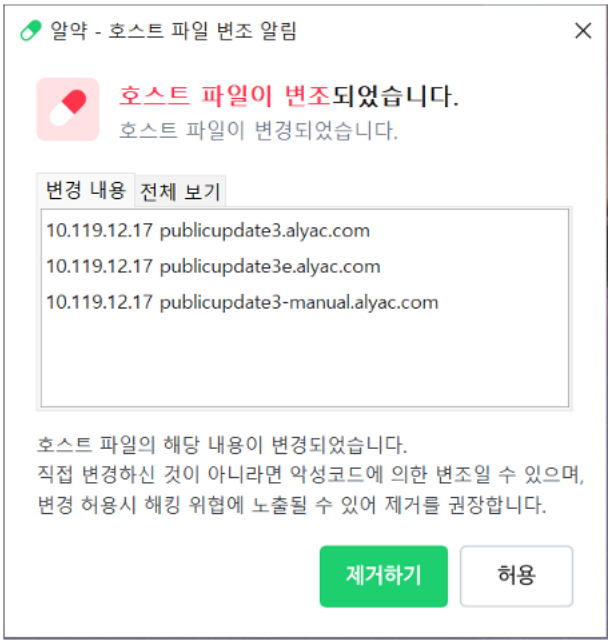
탐지 항목 자동 치료: 탐지된 악성코드를 자동으로 치료합니다.

자동 치료 알림 메시지 받기: 자동 치료가 완료된 경우 알림창을 표시합니다.

호스트 파일 보호

호스트 파일 변조 확인 (기본값): 알약 실행 시, 악성코드에 의한 호스트 파일 변조 여부를 확인 후 사용자에게 알립니다.

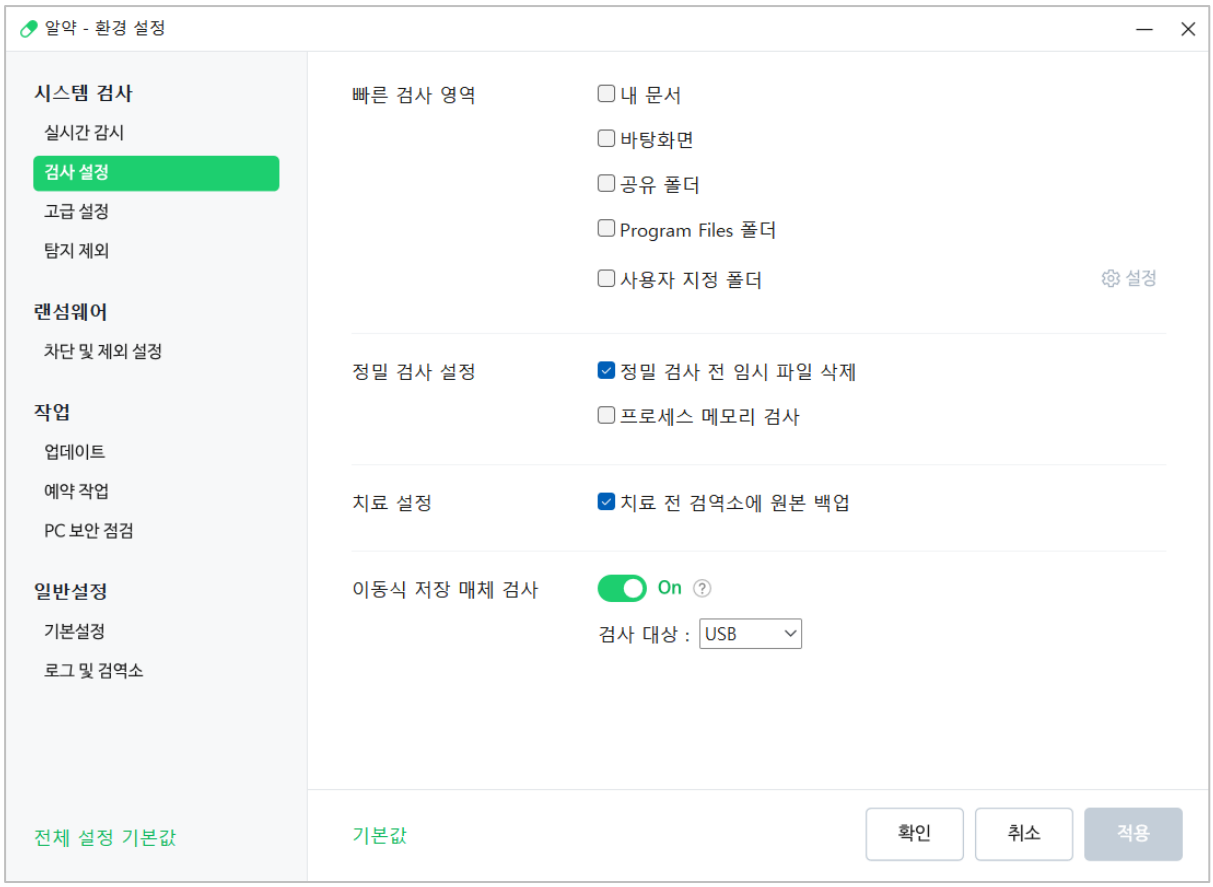
호스트 파일 보호 (기본값): 호스트 파일이 변경되면 사용자에게 알려줍니다.



호스트 파일 보호 알림 메시지 받기 (기본값): 호스트 파일 변경 시도가 감지되면 변경을 차단하고, 알림창을 팝업합니다.

옵션 해제 시: 다음 단계에서 한 번 더 확인 메시지를 표시합니다.

검사 설정



빠른 검사 영역

내 문서/바탕화면/공유 폴더/Program Files/사용자 지정 폴더를 검사하도록 추가로 설정할 수 있습니다.

- 내 문서: My Documents 폴더 안에 위치한 파일들을 검사합니다.
- 바탕화면: 바탕화면 폴더 안의 파일들을 검사합니다.
- 공유 폴더: 현재 공유 폴더로 지정된 폴더의 파일들을 검사합니다.
- Program Files 폴더: 기본적으로 프로그램이 설치되는 폴더인 Program Files의 파일들을 검사합니다.
- 사용자 지정 폴더: 사용자가 추가로 지정한 폴더의 파일을 추가로 검사합니다. 설정 버튼을 통해 빠른 검사 시 사용자 지정 폴더를 검사할 수 있으며, 사용자 지정 폴더는 최대 15개까지 노출할 수 있습니다.

정밀 검사 설정

- 정밀 검사 전 임시파일 삭제 (기본 값): 이 기능을 선택할 경우 정밀 검사 전에 PC 최적화 관점의 임시 파일을 삭제해 시스템 여유 공간을 확보할 수 있습니다.
- 프로세스 메모리 검사: 실행 중인 프로그램의 메모리 영역을 직접 점검하여, 디스크 검사만으로는 발견하기 어려운 악성코드를 탐지하는 기능입니다.

치료 설정

치료 전 검역소에 원본 백업 (기본 값): 악성코드가 발견되어 치료하기 전에 검역소로 원본 파일을 백업하는 기능입니다.

치료 실패나 오탐지의 경우에 원본 파일을 복원할 수 있으므로 "치료 전 검역소에 원본 백업"은 항상 선택 상태로 놓으시기를 권장합니다.

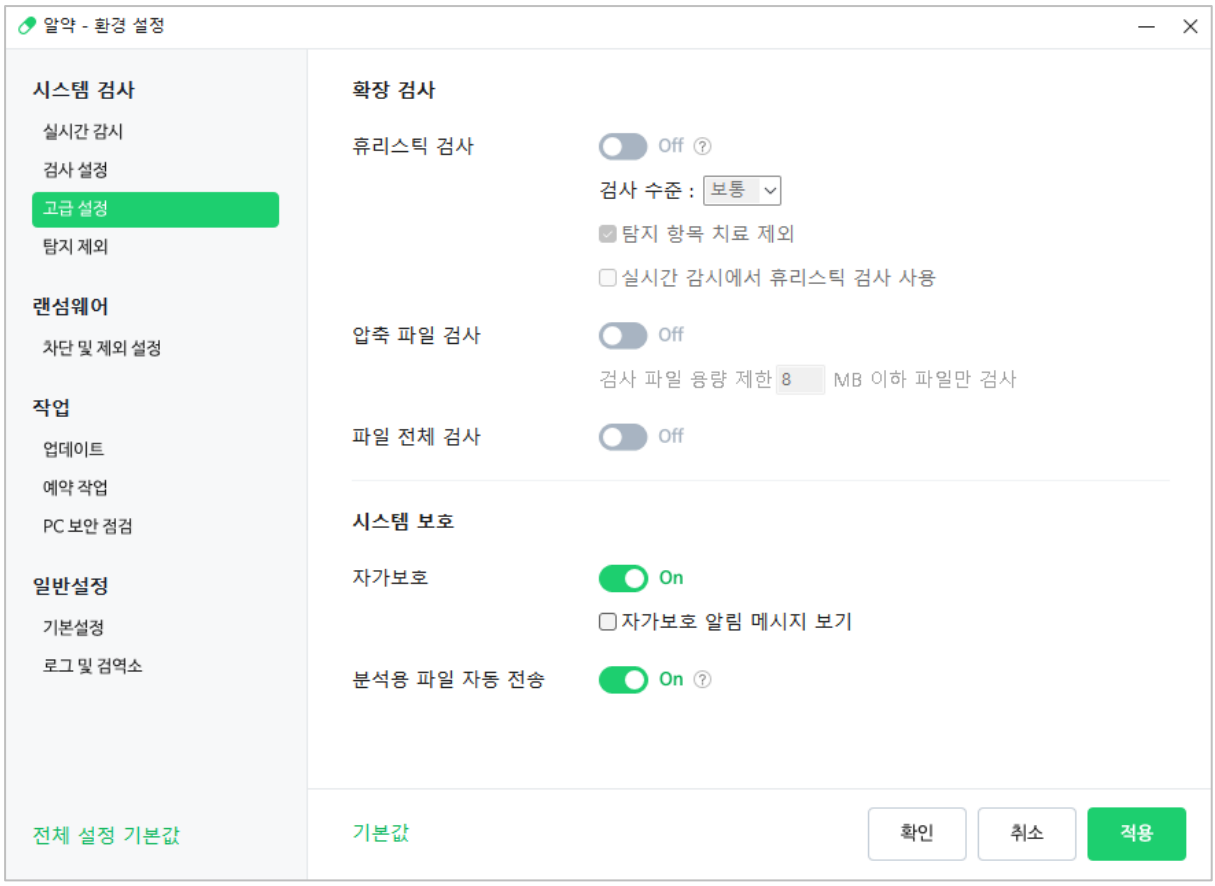
이동식 저장 매체

이동장치검사는 PC에 이동장치(USB/CD 등)를 삽입했을 때, 자동으로 악성코드가 발견되는 주요 영역 검사를 진행하여 자동실행(Autorun) 기능을 악용한 악성코드 감염을 사전에 차단합니다.

검사 완료 후 치료 동작은 실시간 감시의 치료 방식을 따릅니다.

- 검사 대상
  전체: USB 및 CD/DVD 등 이동 저장 장치를 전부 검사합니다.
  USB: 파일이 저장되는 이동식 저장 장치만 해당됩니다.
  CD/DVD: CD/DVD에 대해 검사합니다.

고급 설정



휴리스틱 검사

알려지지 않은 신종 및 변종 악성코드에 대한 진단율이 높아집니다.

- 검사 수준
  높음: 알약 정적 휴리스틱 + YARA 검사(Parser사용) + 비트디펜더 동적 휴리스틱
  보통 (기본 값): 알약 정적 휴리스틱 + YARA검사(Parser사용)
  낮음: YARA 검사(Parser미사용)
- 탐지 항목 치료 제외 (기본 값): 휴리스틱 검사에서는 경우에 따라 정상 파일도 탐지할 가능성이 있으니 탐지 내역을 꼭 확인하고 치료를 진행하기 위해 탐지한 항목을 치료하지 않도록 설정되어 있습니다. 비활성화 시 치료 설정을 따르게 됩니다.
- 실시간 감시에서 휴리스틱 검사 사용: 휴리스틱 검사는 자원을 많이 사용할 수 있어 실시간 감시에서는 사용하지 않도록 설정되어 있습니다. 실시간으로 알려

지지 않은 신종 및 변종 악성코드에 대해 진단하고 싶은 경우 활성화하세요.

압축 파일 검사

압축 파일에 대한 검사를 지정할 수 있습니다.

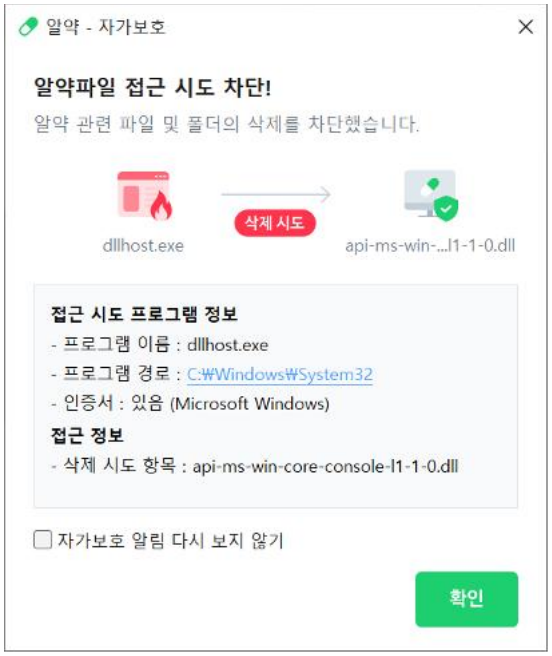
- 검사 파일 용량 제한 8MB 이하 파일만 검사 (기본 값)
  최소 1MB, 최대 1024MB까지 지정 가능합니다.
  다중 압축 파일은 지원하지 않습니다.

파일 전체 검사

디스크 전체 영역의 모든 파일을 대상으로 악성코드 감염 여부를 상세히 진단합니다.

자가 보호

자가보호 알림 메시지 보기 (기본 값)



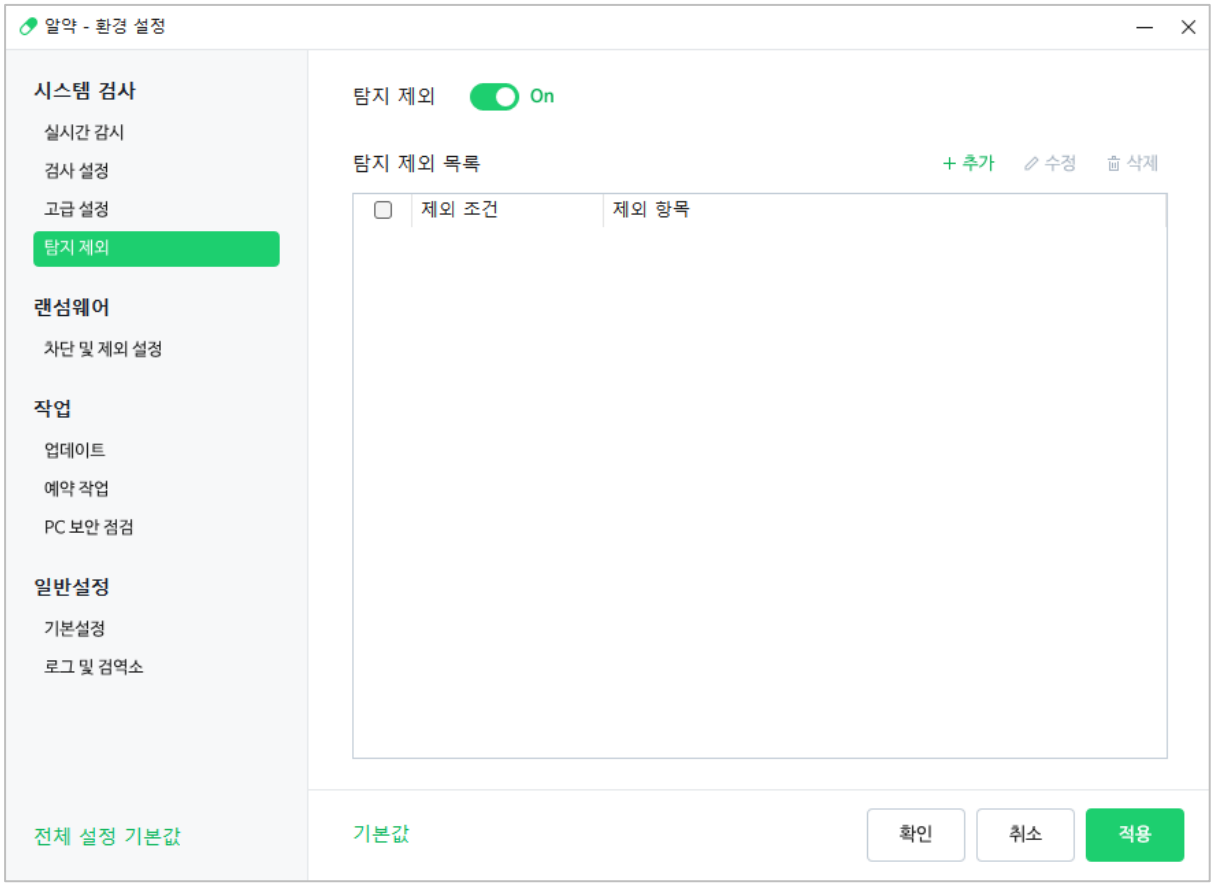
자가보호 알림 다시 보지 않기를 선택 후 확인을 누르면 `고급설정> 시스템 보호> 자가보호> 자가보호 알림 메시지 보기`가 해제됩니다.

분석용 파일 자동

안전하지 않은 파일을 알약 분석센터에 자동으로 전송하여 분석 후 알약 탐지 시스템을

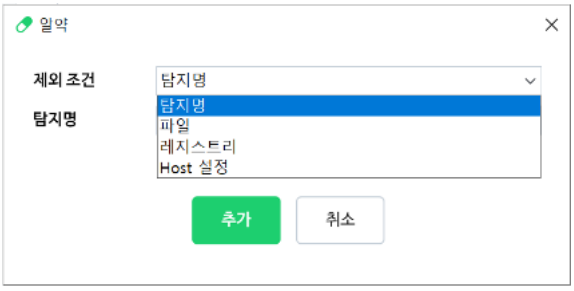
고도화 하는데 활용합니다. 전송되는 파일은 개인을 식별할 수 없으며, AI를 통한 악성코드 정밀 분석 용도로만 사용됩니다.

탐지 제외



실시간 감시 또는 수동 검사에서 해당 항목에 대한 탐지를 제외처리 하게 됩니다.

탐지 제외 목록



- 탐지명: 탐지명 (예:Trojan.Generic.383423)을 기준으로 진단되는 악성코드를 검사 대상

에서 제외할 수 있습니다.

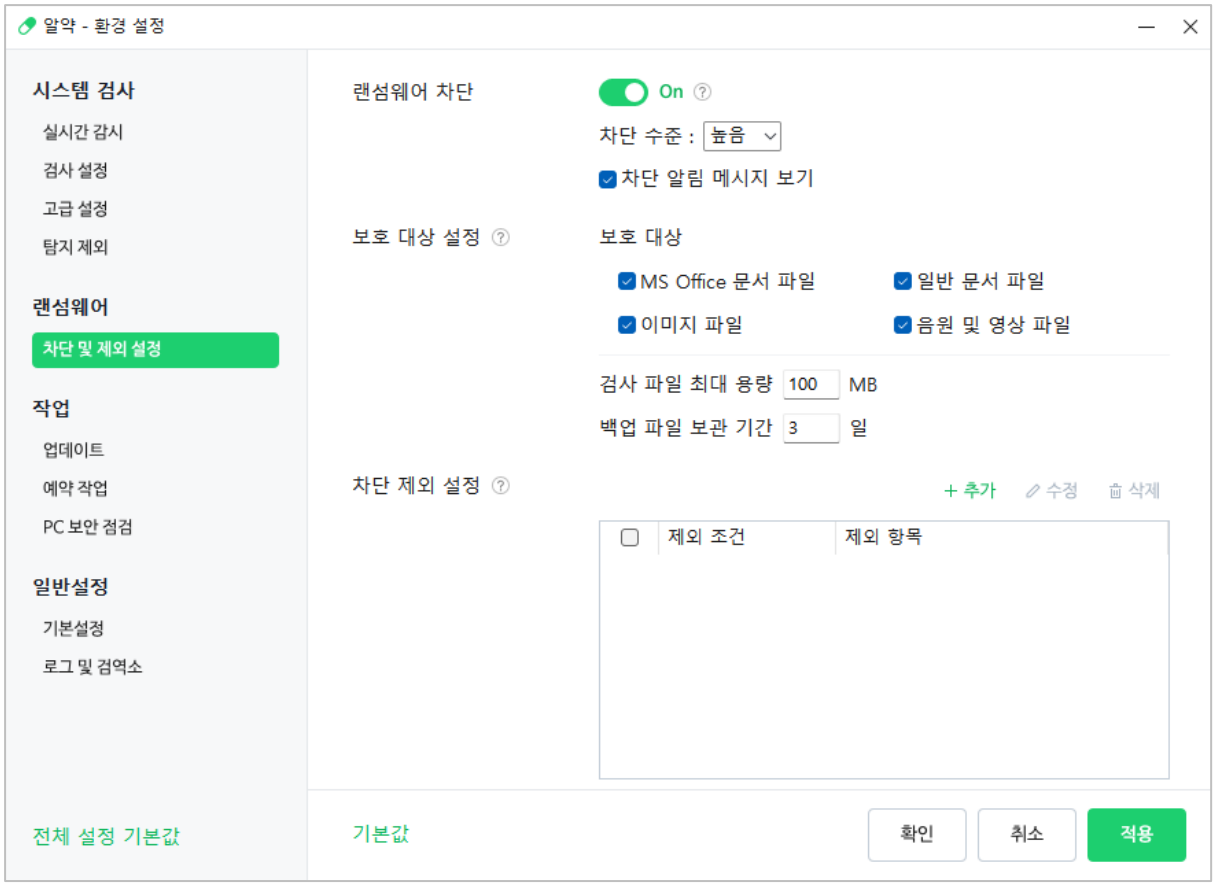
- 파일: 파일이나 폴더 단위 별로 검사 대상에서 제외할 수 있습니다. 루트 디렉토리(예: C드라이브)나 Program Files, Windows 같은 중요 폴더를 제외 방법으로 설정하지 않도록 주의합니다.

- 레지스트리: 레지스트리의 경로나 값을 지정해 해당 항목을 검사 제외처리 합니다.

- Host 설정 : Windows의 Host 파일(Windows₩System32₩drivers₩etc₩hosts)에 사용자가 특별히 추가한 항목(IP와 도메인 주소)에 대해 검사 제외 처리합니다.

랜섬웨어

차단 및 제외 설정



랜섬웨어 차단

랜섬웨어 의심 행위를 차단하여 사용자의 파일이 암호화되는 것을 방지합니다.

- 차단 수준

높음 (기본 값): 트랩 행위는 물론 보호 대상 파일의 암호화를 탐지합니다.

보통: 트랩 행위를 차단합니다.

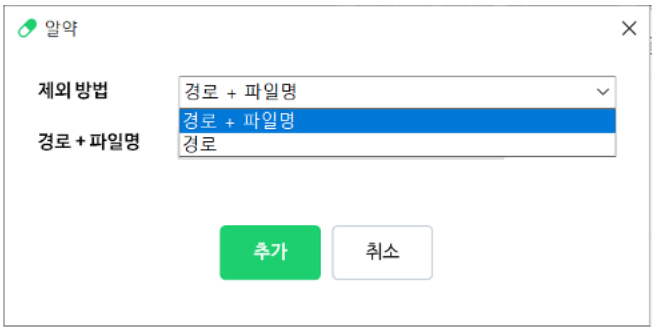
- 차단 알림 메시지 보기 (기본 값)

보호 대상 설정

- 랜섬웨어 차단 수준 높음 일 때 활용됩니다.
- 보호 파일 훼손 시, 원본 파일을 안전한 곳에 보관 후 복구를 제공합니다.
- 보호할 파일의 용량 및 보관 기간을 제한할 수 있습니다.
- 보호 대상
    - MS Office 문서 파일 (기본 값)
    - 일반 문서 파일 (기본 값)
    - 이미지 파일 (기본 값)
    - 멀티미디어 편집 파일 (기본 값)
    - 설계 파일
    - 압축 파일
    - 음원 및 영상 파일
- 검사 파일 최대 용량 100MB (기본 값): 최소 1MB, 최대 1024MB까지 지정 가능합니다.
- 백업 파일 보관 기간 3일 (기본 값): 최소 1일 최대 999일까지 지정 가능합니다.

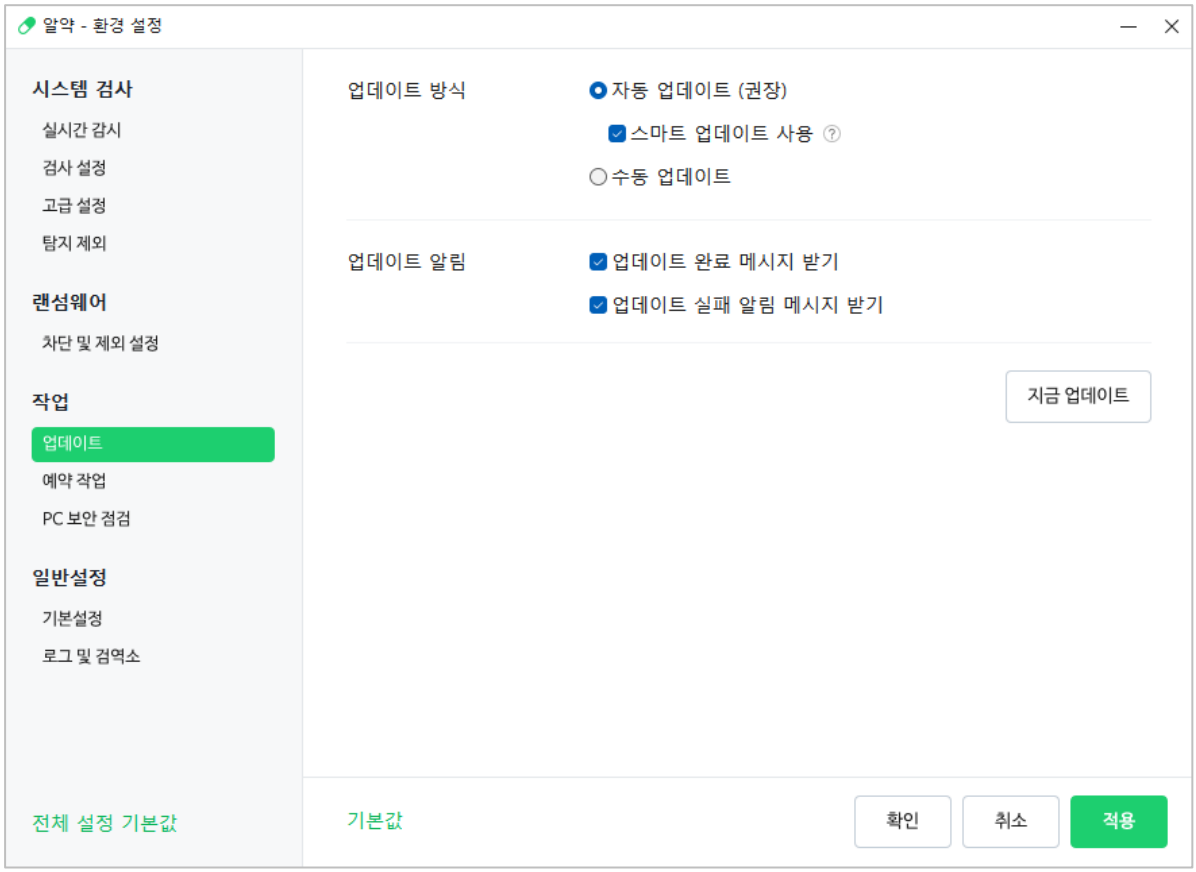
차단 제외 설정

추가된 조건에 따라 랜섬웨어 의심 행위 차단을 제외합니다.



작업

업데이트



업데이트 방식

업데이트 설정에서 자동/수동 업데이트 여부를 선택할 수 있습니다.

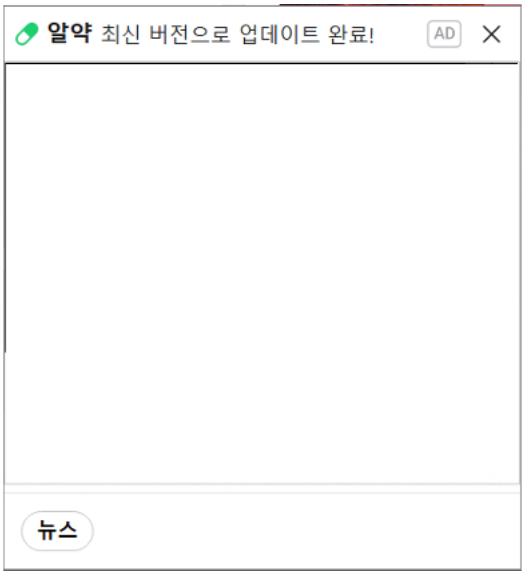
- 자동 업데이트 (권장) (기본 값): 매번 '업데이트' 버튼을 누를 필요 없이 알약이 자동으로 업데이트 과정을 수행합니다.

- 스마트 업데이트 사용 (기본 값): P2P원리의 분산 업데이트 방식으로 서버의 상황과 관계없이 항상 안정적이고 신속한 업데이트를 제공하여 업데이트 실패 확률을 최소화합니다.

- 수동 업데이트: 수동으로 업데이트 합니다.

업데이트 알림

업데이트 완료 메시지 받기 (기본 값): 자동 업데이트가 완료된 후 메시지를 나타나게 합니다. 수동 업데이트를 하는 경우 해당 메시지 받기 옵션과 상관없이 완료 메시지를 제공합니다.



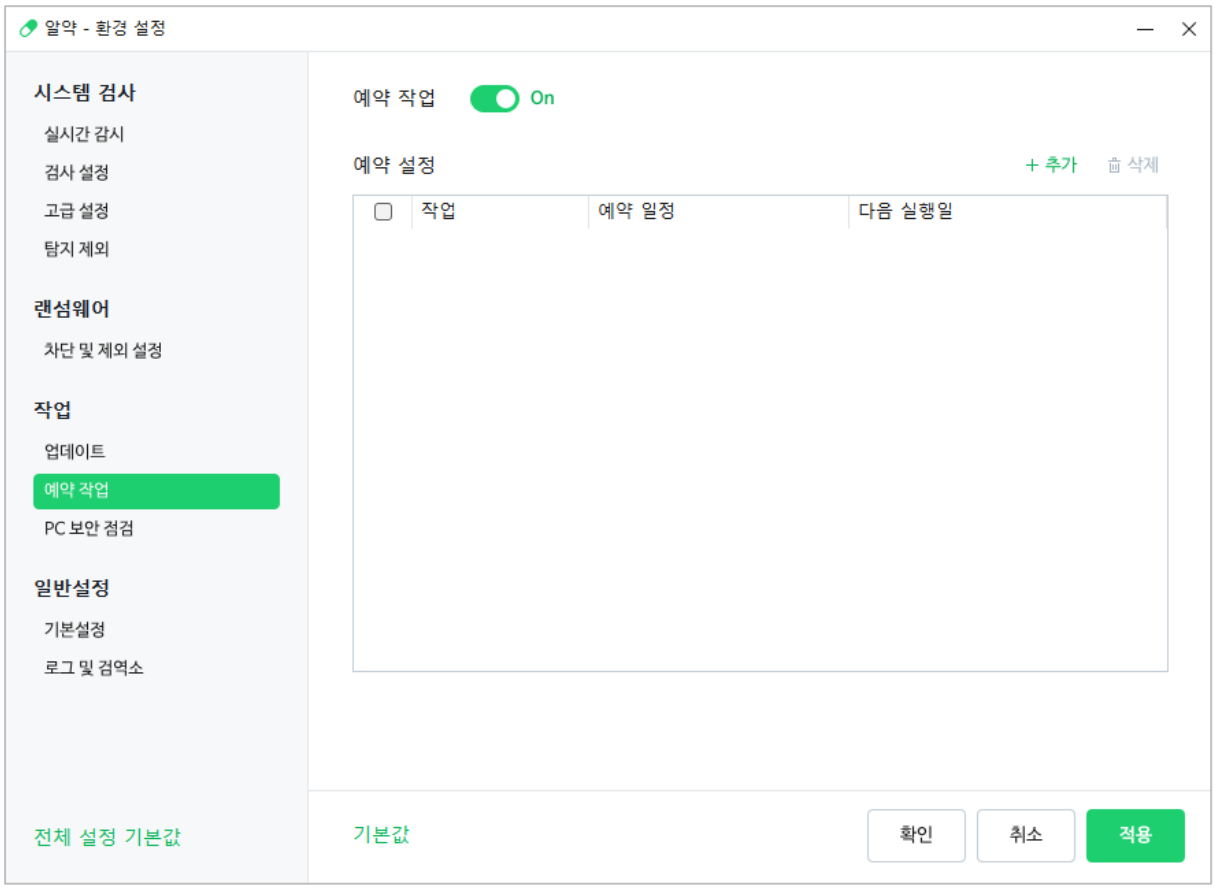
업데이트 실패 알림 메시지 받기 (기본 값): 장기간 업데이트가 진행되지 않을 때 안내 메시지를 나타나게 합니다.

지금 업데이트

버튼을 클릭하면 바로 알약 업데이트를 시작합니다.

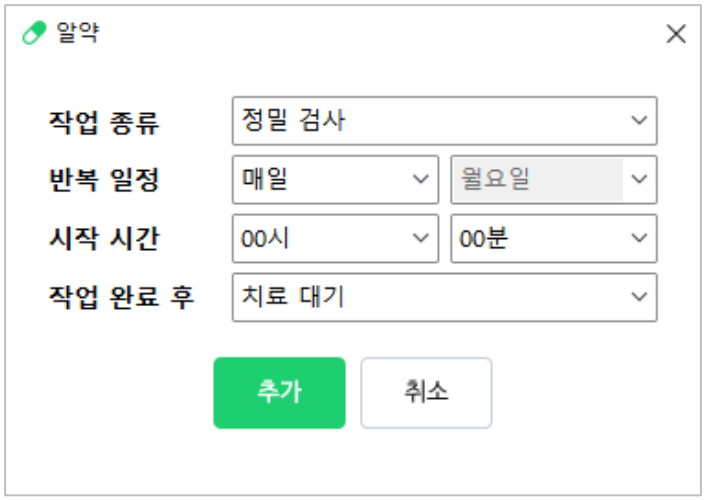
예약 작업

예약 작업을 설정할 수 있습니다.



- **예약 설정**

추가: 버튼을 선택하여 예약 작업을 추가할 수 있습니다.



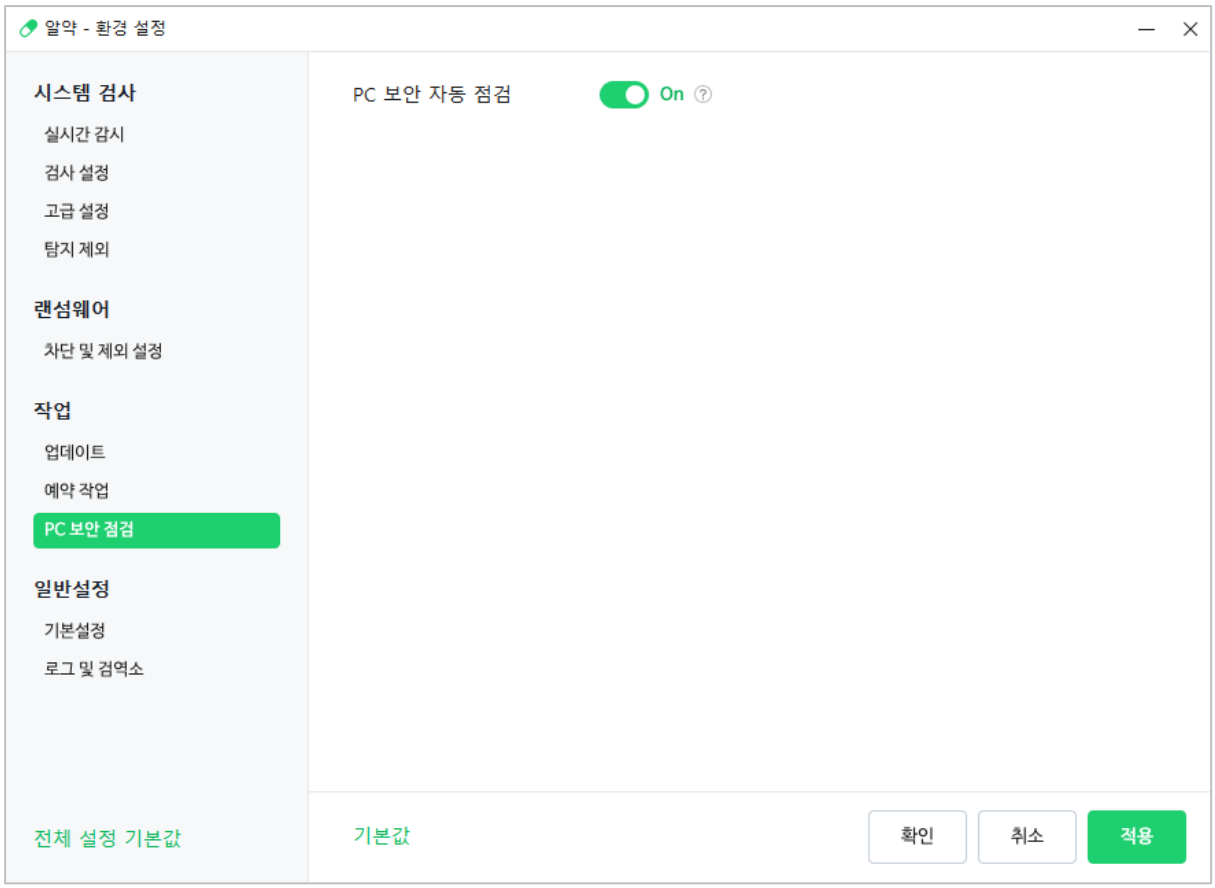
- 작업 종류: 정밀 검사, 기본 검사 중 하나를 선택합니다.

- 반복일정: 매일, 매주, 매월마다 반복하도록 설정합니다. 매주의 경우 요일 선택(월~일)이 가능합니다.

- 시작시간: 작업을 시작할 시간과 분을 설정합니다.

- 작업 완료 후: `치료대기, 자동 치료 후 대기, 창 닫기, 시스템 종료` 중 동작을 선택 가능합니다.

PC 보안 점검

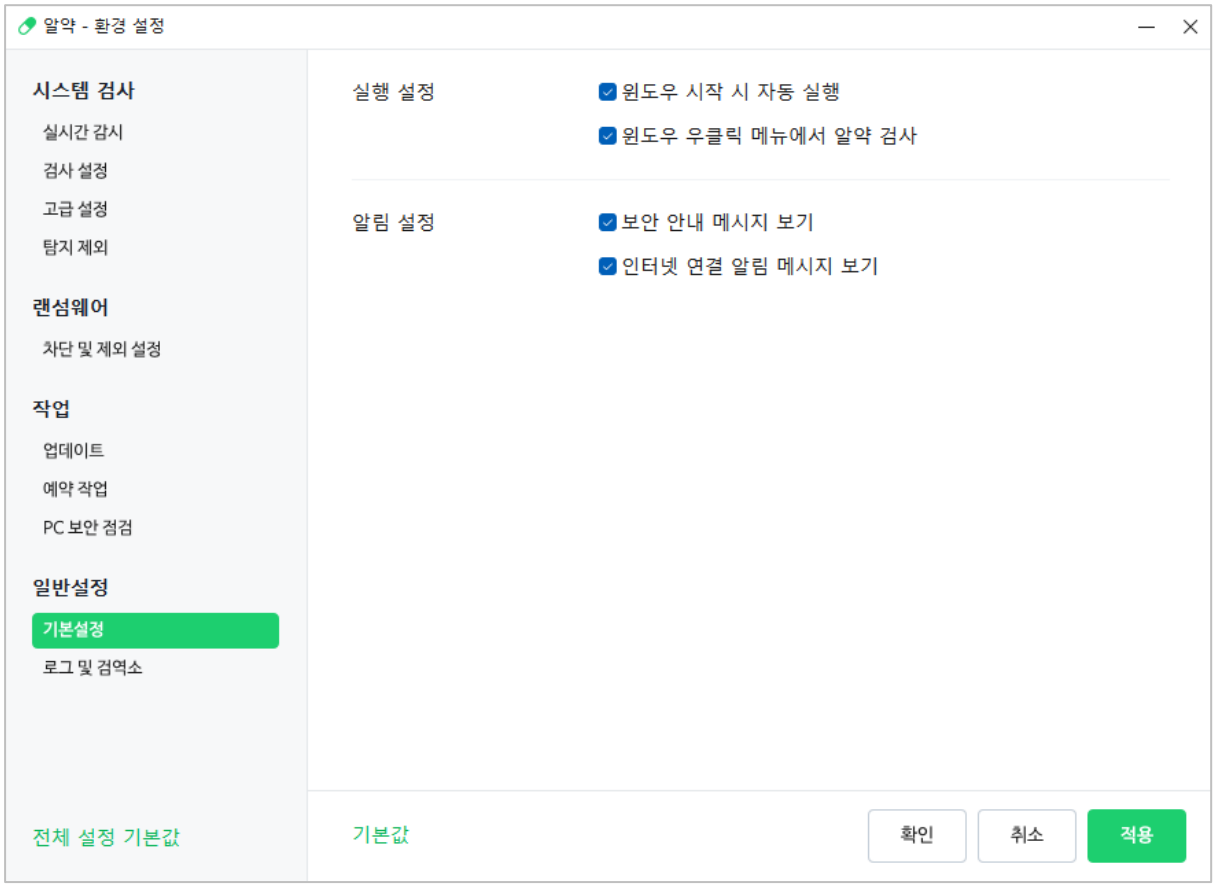


인터넷을 이용하는 개인 PC를 대상으로 보안 점검 서비스를 제공합니다.

기능이 On일 경우 기능이 활성화되며 매월 1회 자동 점검을 수행합니다. 비활성화의 경우 Off로 설정하면 됩니다.

일반설정

기본설정



실행 설정

- 윈도우 시작 시 자동 실행 (기본 값): 윈도우 시작 시에 알약을 자동으로 실행합니다.

- 윈도우 우클릭 메뉴에서 알약 검사 (기본 값): 마우스 우클릭 메뉴를 이용해 선택한 폴더/파일을 검사하는 기능입니다.

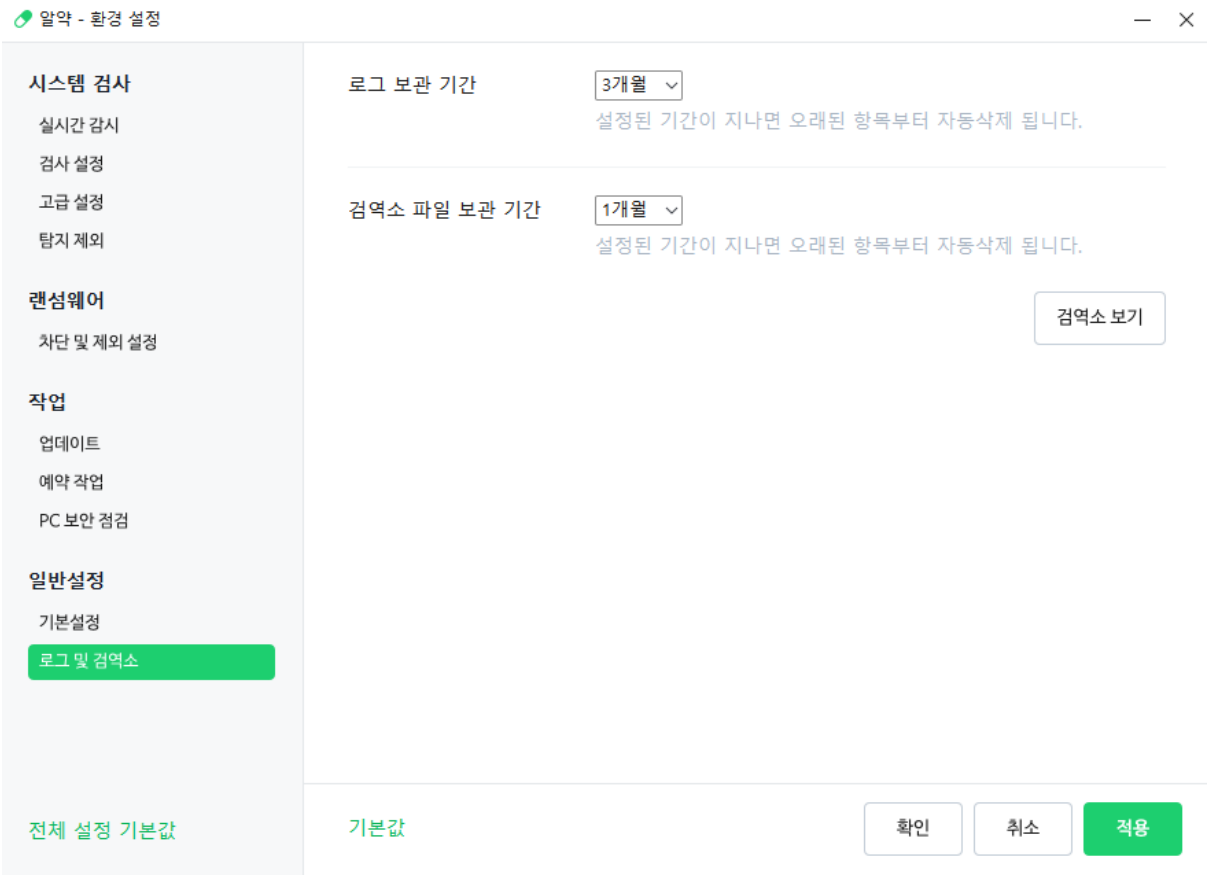
알림 설정

알약의 이벤트 발생 시 사용자에게 이벤트를 알려주는 안내 창이 나옵니다.

- 보안 안내 메시지 보기 (기본 값)

- 인터넷 연결 알림 메시지 보기 (기본 값)

로그 및 검역소



알약은 로그 및 검역소 파일로 인한 하드디스크 용량 소모를 줄이기 위해 지정된 날짜보다 오래된 로그와 검역소 파일부터 자동 삭제합니다.

로그 보관 기간

알약에서 생성되는 로그의 관리 기간을 선택합니다.

- 3개월 (기본 값), 1개월, 2개월, 6개월, 1년 중 선택 가능합니다.

검역소 파일 보관 기간

알약에서 관리하고 있는 검역소 파일의 관리 기간을 선택합니다.

- 1개월 (기본 값), 2개월, 3개월, 6개월, 1년 중 선택 가능합니다.

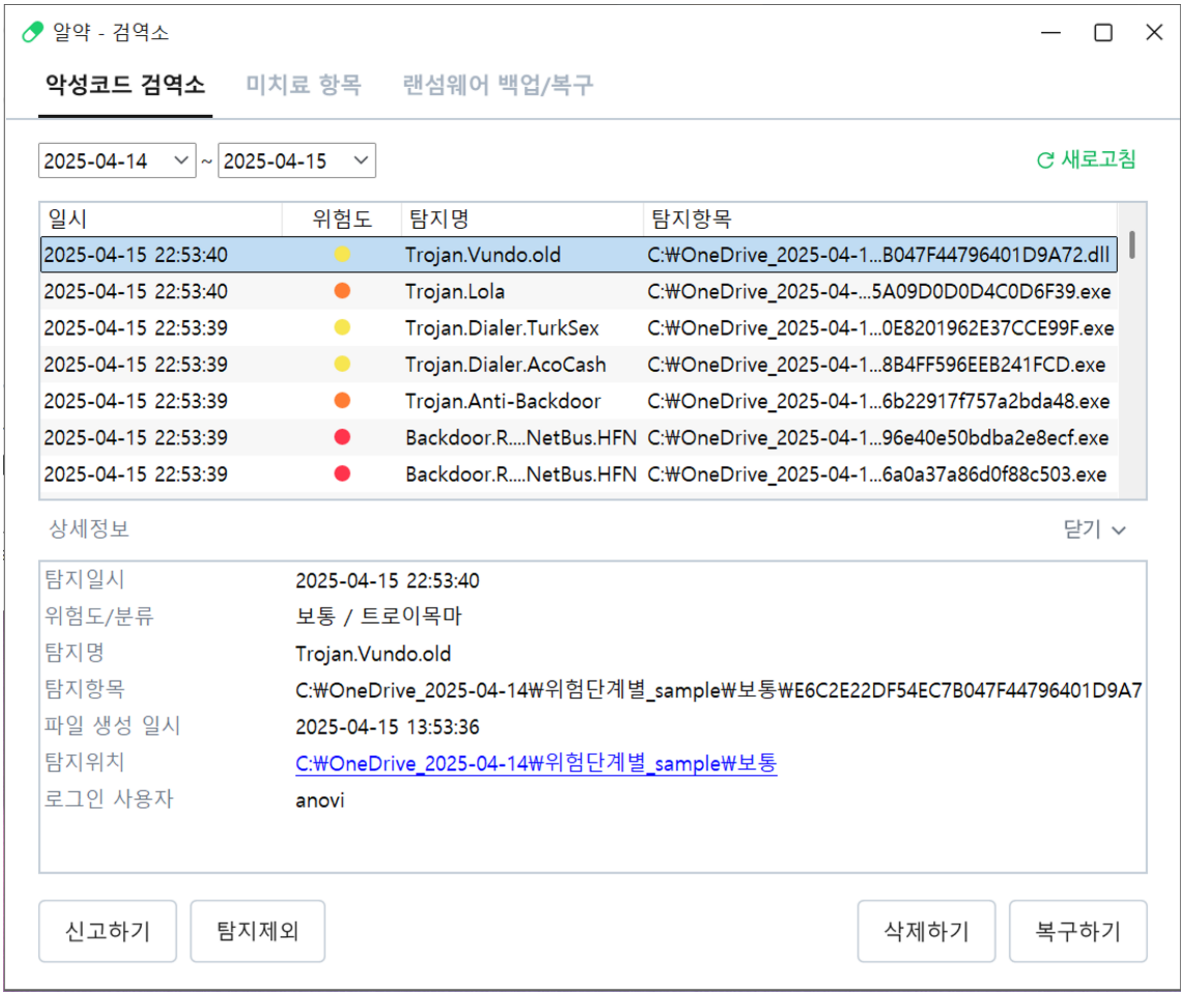
검역소 보기

선택 시 검역소 창을 실행합니다.

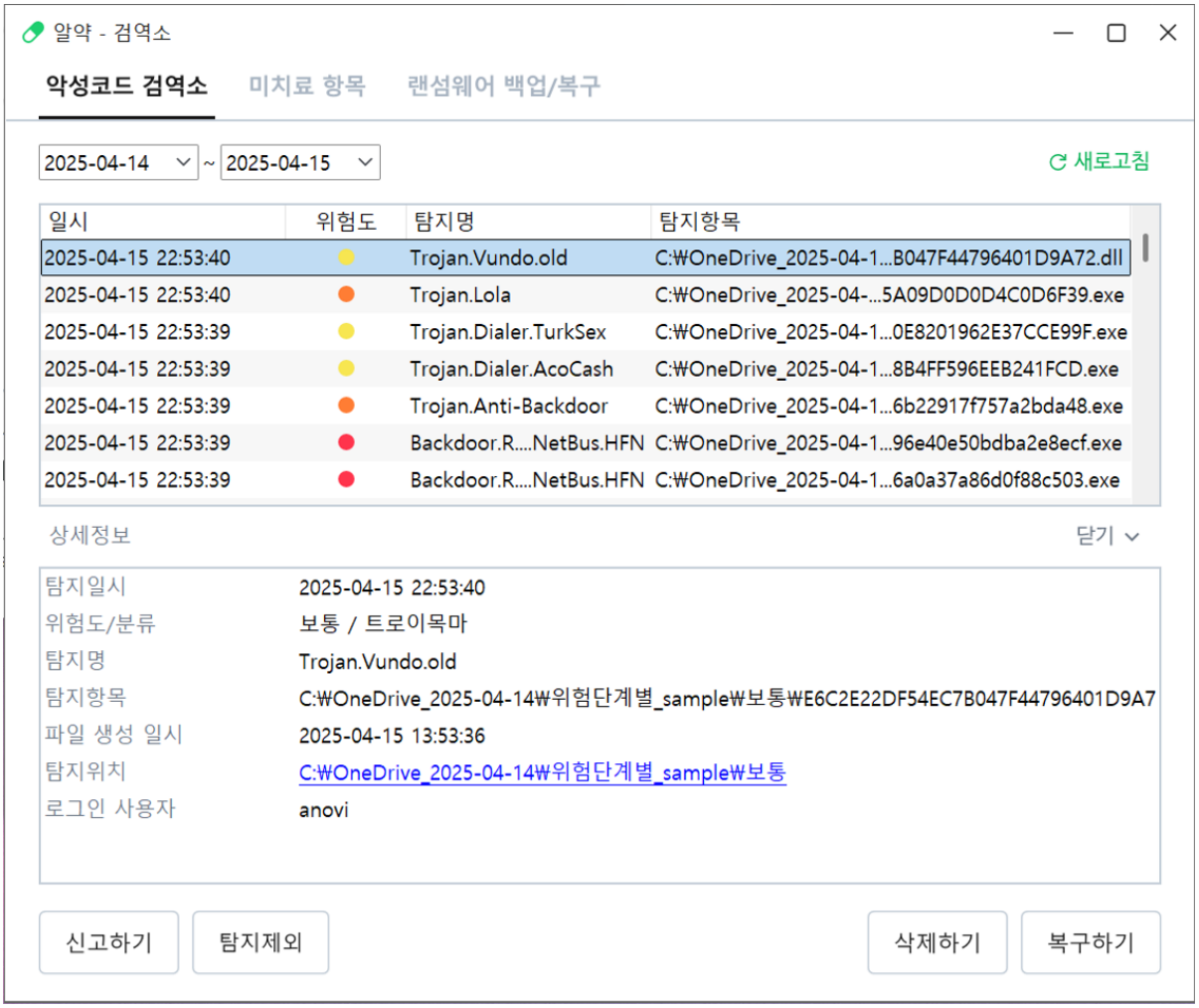
검역소

악성코드 검역소

실시간 감시 및 수동검사 중에 탐지된 악성파일들을 암호화하여 안전하게 보관되는 곳입니다.

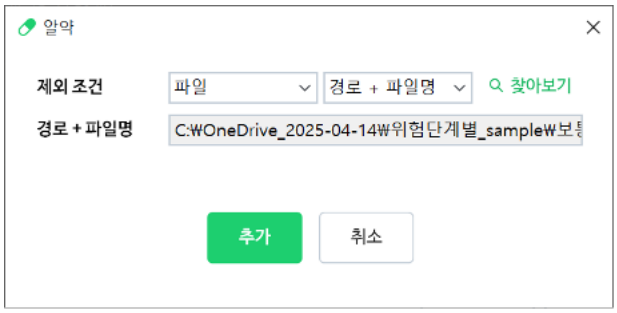


항목을 선택하면 상세정보 확인과 함께 다음 기능을 사용할 수 있습니다.



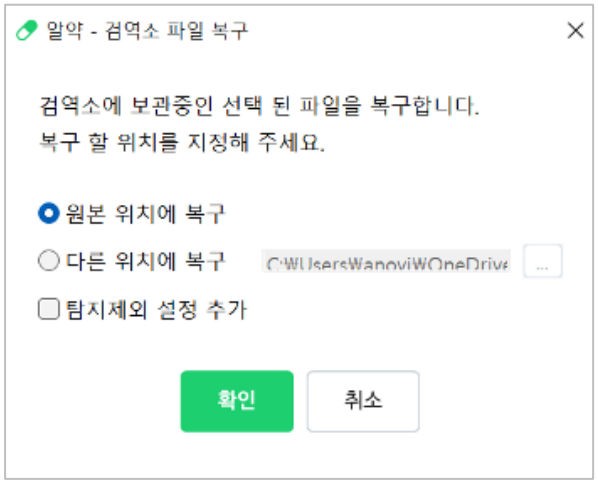
- [신고하기] 버튼을 누르면 알약의 신고하기 화면이 나옵니다.

- [탐지제외] 버튼을 누르면 탐지 제외 창이 실행되며 등록 시 파일을 더 이상 악성코드로 탐지하지 않습니다.



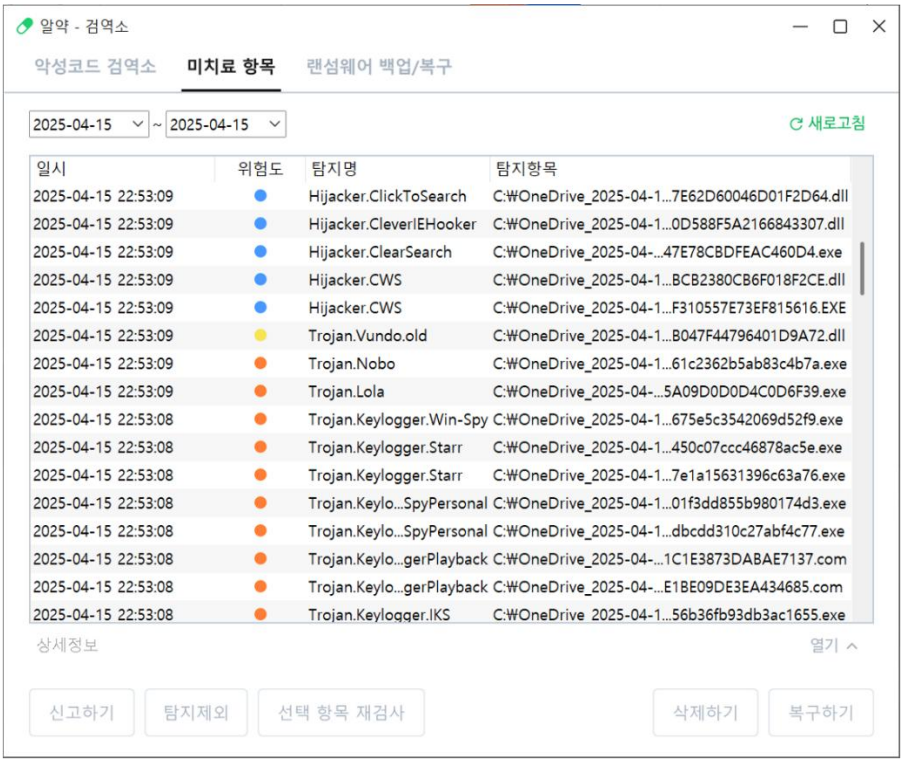
- [삭제하기] 버튼을 누르면 삭제 알림창이 노출되며 확인을 누르면 해당 항목의 파일을 삭제합니다. 삭제한 파일은 복구할 수 없습니다.

- [복구하기] 버튼을 누르면 이 파일의 원래 위치로 복원시키거나 별도의 위치로 복원시킬 수 있습니다.

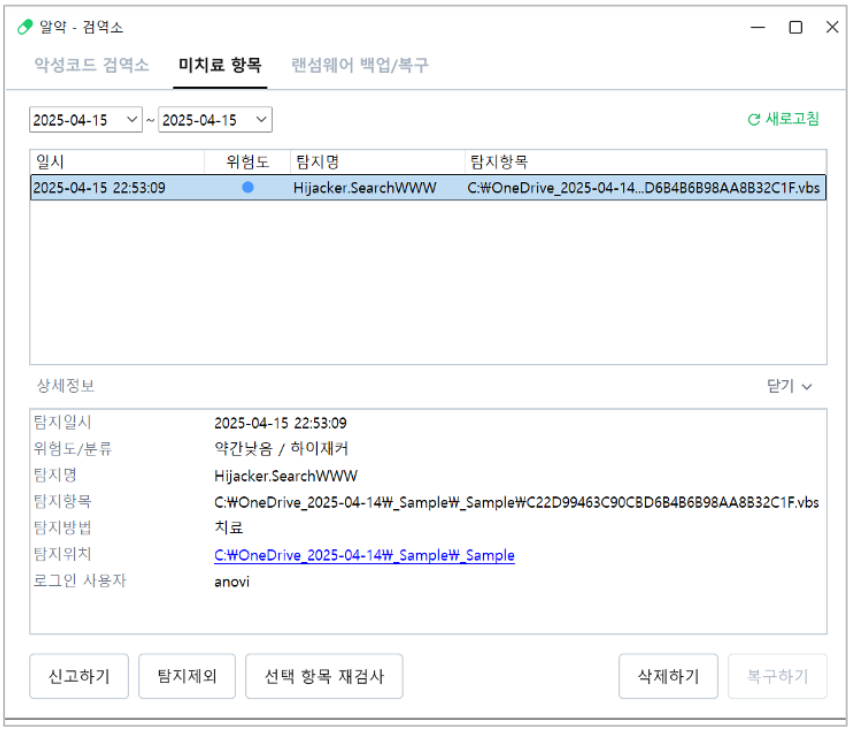


미치료 항목

실시간 감시 및 수동검사 중에 탐지된 악성파일들을 치료하지 않은 항목을 암호화하여 안전하게 보관되는 곳입니다.

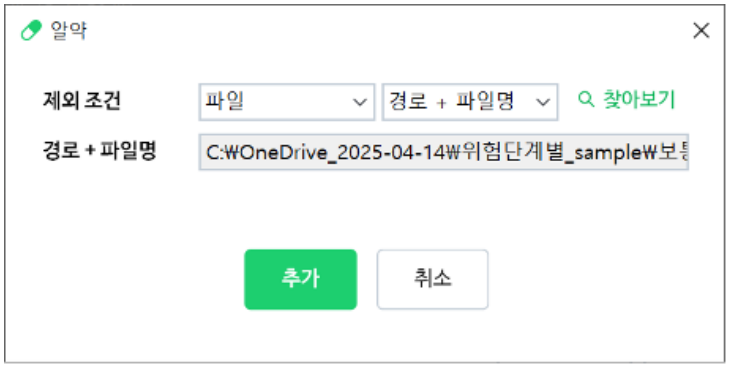


항목을 선택하면 상세정보 확인과 함께 다음 기능을 사용할 수 있습니다.



- [신고하기] 버튼을 누르면 알약의 신고하기 화면이 나옵니다.

- [탐지제외] 버튼을 누르면 탐지 제외 창이 실행되며 등록 시 파일을 더 이상 악성코드로 탐지하지 않습니다.



- [선택 항목 재검사] 버튼을 누르면 선택 항목에 대한 사용자 지정 검사(우클릭 검사)를 수행합니다.

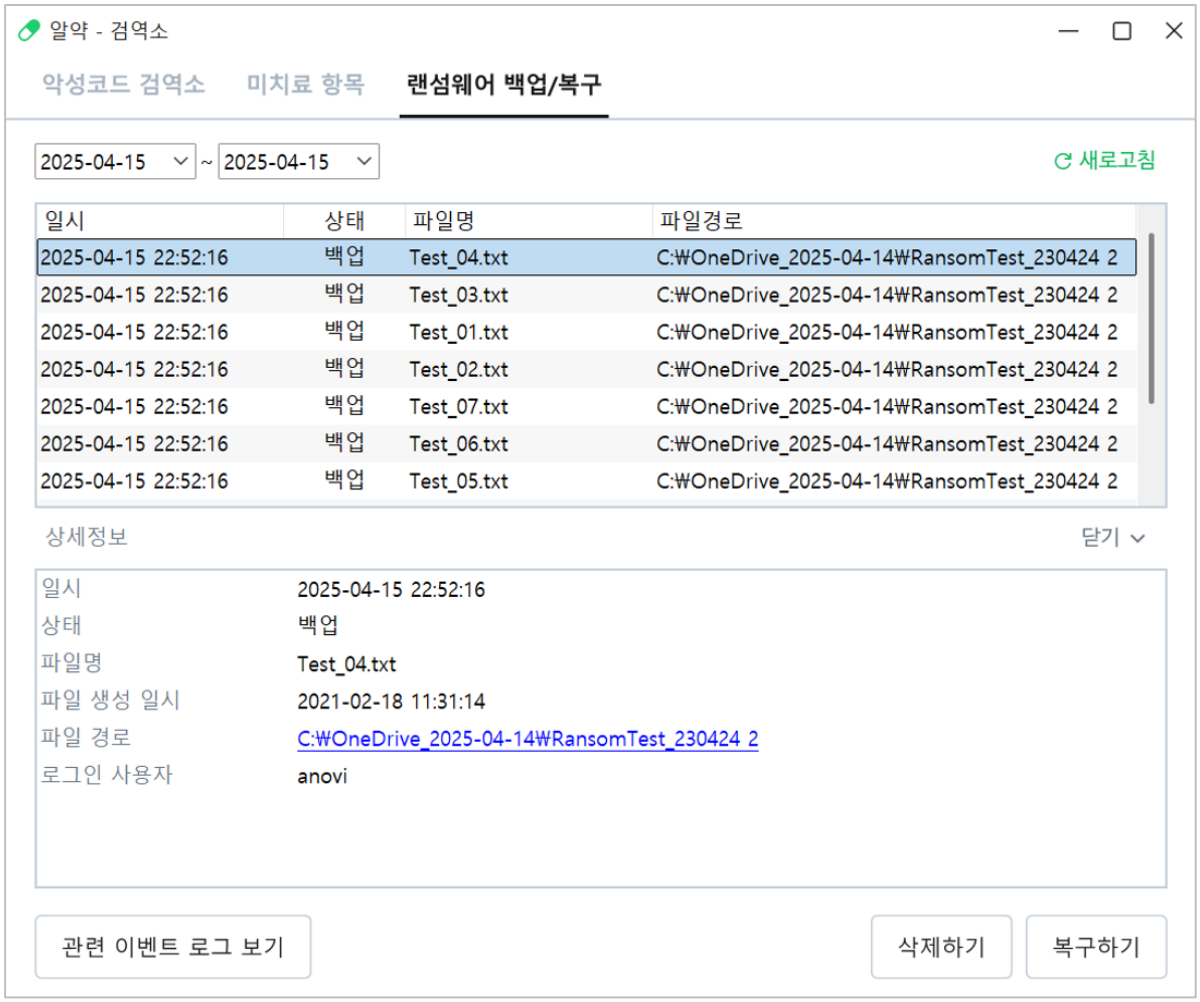
- [삭제하기] 버튼을 누르면 삭제 알림창이 노출되며 확인을 누르면 해당 항목의 파일을 삭제합니다. 삭제한 파일은 다시 복구할 수 없습니다.

- [복구하기] 버튼은 현재 비활성화 되어 있습니다.

랜섬웨어 백업/복구

랜섬웨어 수준이 높음 상태에서 차단이 발생했을 때 원본파일을 백업 후 복구하는 기능을 제공합니다.

항목을 선택하면 상세정보 확인과 함께 다음 기능을 사용할 수 있습니다.



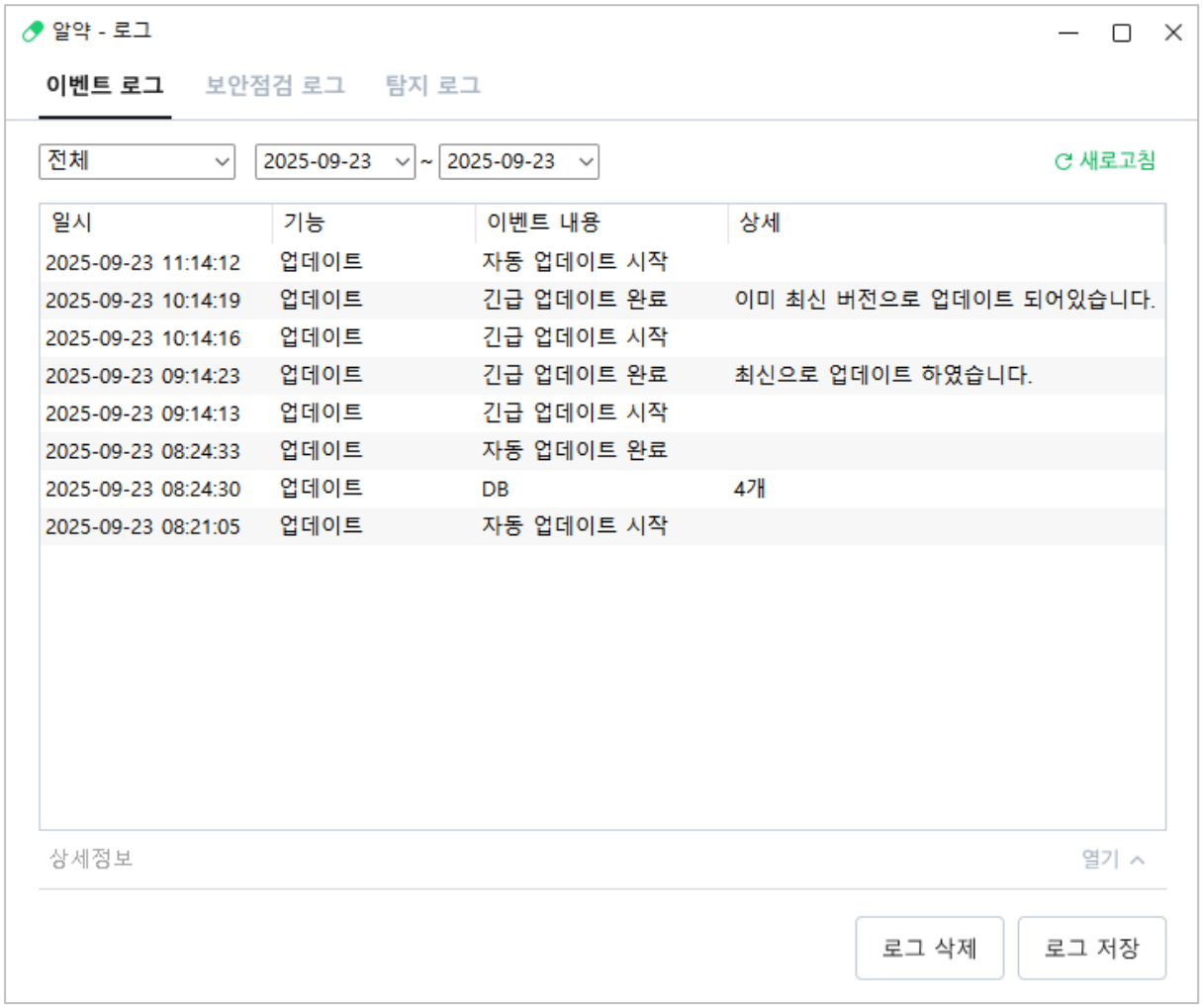
- [관련 이벤트 로그 보기] 버튼 클릭 시 로그보기 창의 이벤트 로그 창을 노출하며, 선택된 항목의 랜섬웨어 차단 이벤트 로그를 노출합니다.

- [삭제하기] 버튼을 누르면 삭제 알림창이 노출되며 확인을 누르면 해당 항목의 파일을 삭제합니다.

- [복구하기] 버튼을 누르면 이 파일의 지정된 경로에 복원시킬 수 있습니다.

로그보기

이벤트 로그



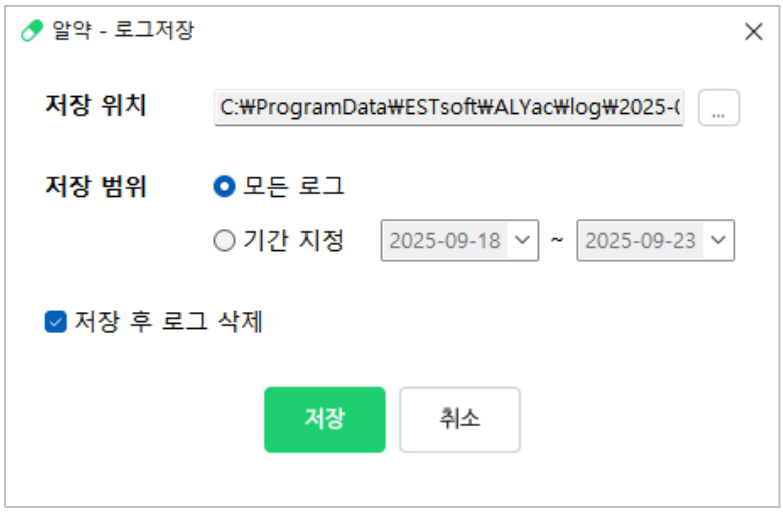
옵션 선택을 통해 전체, 실시간 감시, 검사, 치료, 업데이트, 랜섬웨어.,자가보호, 탐지제외, 기타 로그를 확인 가능합니다.

로그가 기록된 일시 범위 조정을 통해 특정 일시의 로그를 조회 가능합니다.

보안점검 로그

보안점검 로그가 기록됩니다.

- [재점검] 버튼을 누르면 즉시 보안점검을 수행합니다.
- [로그 삭제] 버튼을 누르면 로그가 삭제됩니다.
- [로그 저장] 버튼을 누르면 다음창이 오픈됩니다.



- 저장 위치: 로그 파일이 저장되는 위치를 지정합니다.

- 저장 범위: 모든 로그 또는 기간을 지정하여 저장할 수 있습니다.

- 저장 후 로그 삭제 (기본 값)이 선택되어있으면 로그를 파일로 저장 후 저장 범위에 해당하는 로그를 삭제합니다.

- 항목을 선택 후 상세정보에서 상세결과를 [열기]를 클릭하면 보안점검 상세 결과 창이 오픈됩니다.

보안점검 상세 결과

1. 취약점 점검 요약 결과

   전체 보안점검 항목 수와 취약 항목 수를 확인할 수 있습니다.

2. 사용자 정보

   보안점검 날짜 및 사용자 PC의 간략한 정보를 확인할 수 있습니다.

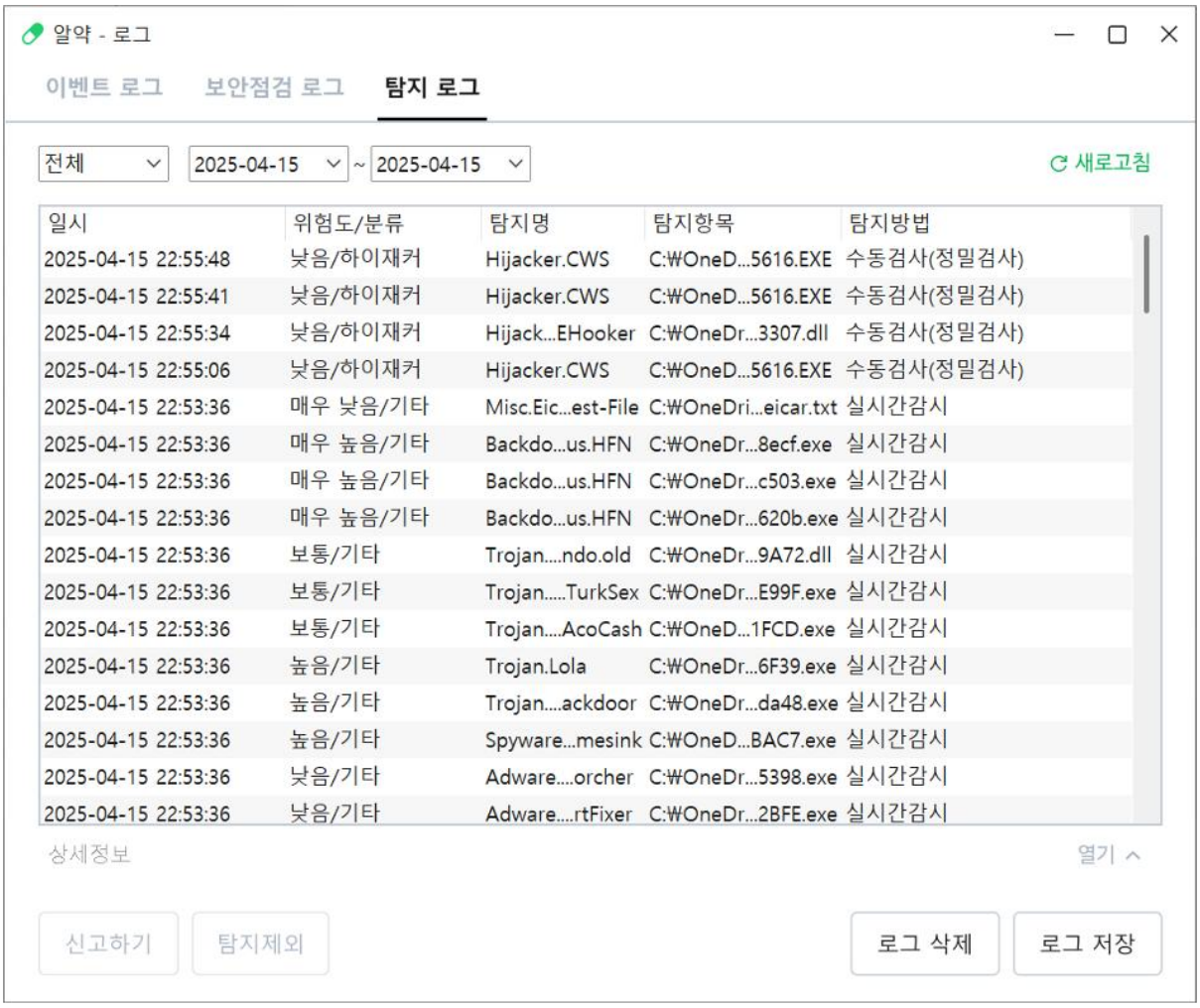
3. 점검 항목 목록

   점검 항목에 대한 간략한 설명과 점검 결과를 확인할 수 있습니다.

4. 조치매뉴얼 바로가기

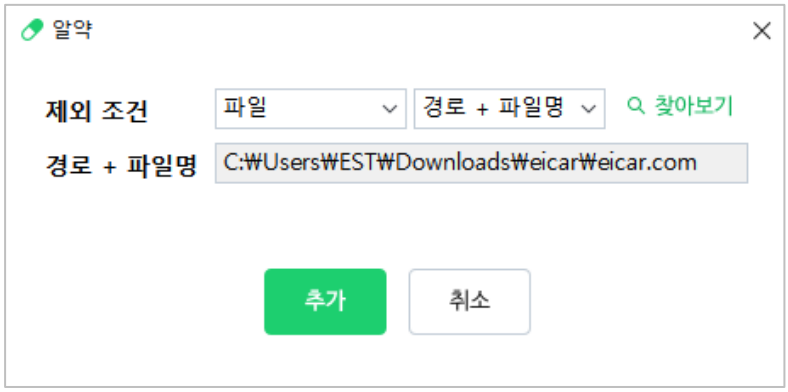
   취약한 점검 결과의 조치를 위한 상세 매뉴얼을 확인할 수 있습니다.

탐지 로그



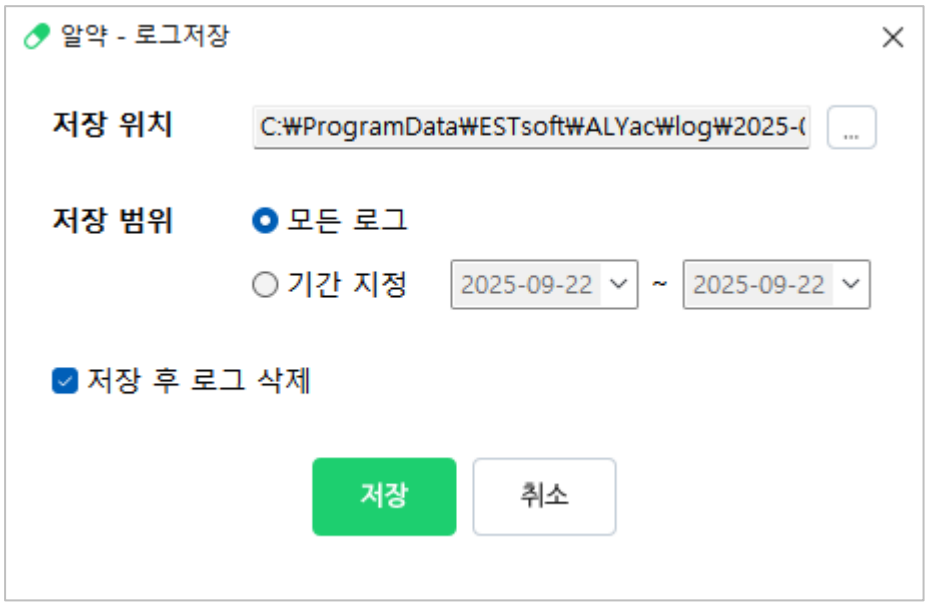
- [신고하기] 버튼을 누르면 알약의 신고하기 화면이 나옵니다.

- [탐지제외] 버튼을 누르면 탐지 제외 창이 실행되며 등록 시 파일을 더 이상 악성코드로 탐지하지 않습니다.



- [로그 삭제] 버튼을 누르면 로그가 삭제됩니다.

- [로그 저장] 버튼을 누르면 다음창이 오픈됩니다.



- 저장 위치: 로그 파일이 저장되는 위치를 지정합니다.

- 저장 범위: 모든 로그 또는 기간을 지정하여 저장할 수 있습니다.

- 저장 후 로그 삭제 (기본 값)이 선택되어 있으면 로그를 파일로 저장 후 저장 범위에 해당하는 로그를 삭제합니다.

알약 사용 중에 문제가 발생하거나 문의 사항이 있으신 경우 아래의 지원 채널을 이용하시기 바랍니다.

- 전화 문의 : 1544-8209
- 이메일 문의 : help@alyac.co.kr
- 홈페이지 : https://www.estsecurity.com/
- 주소 : 서울시 서초구 반포대로 3 ㈜이스트시큐리티
