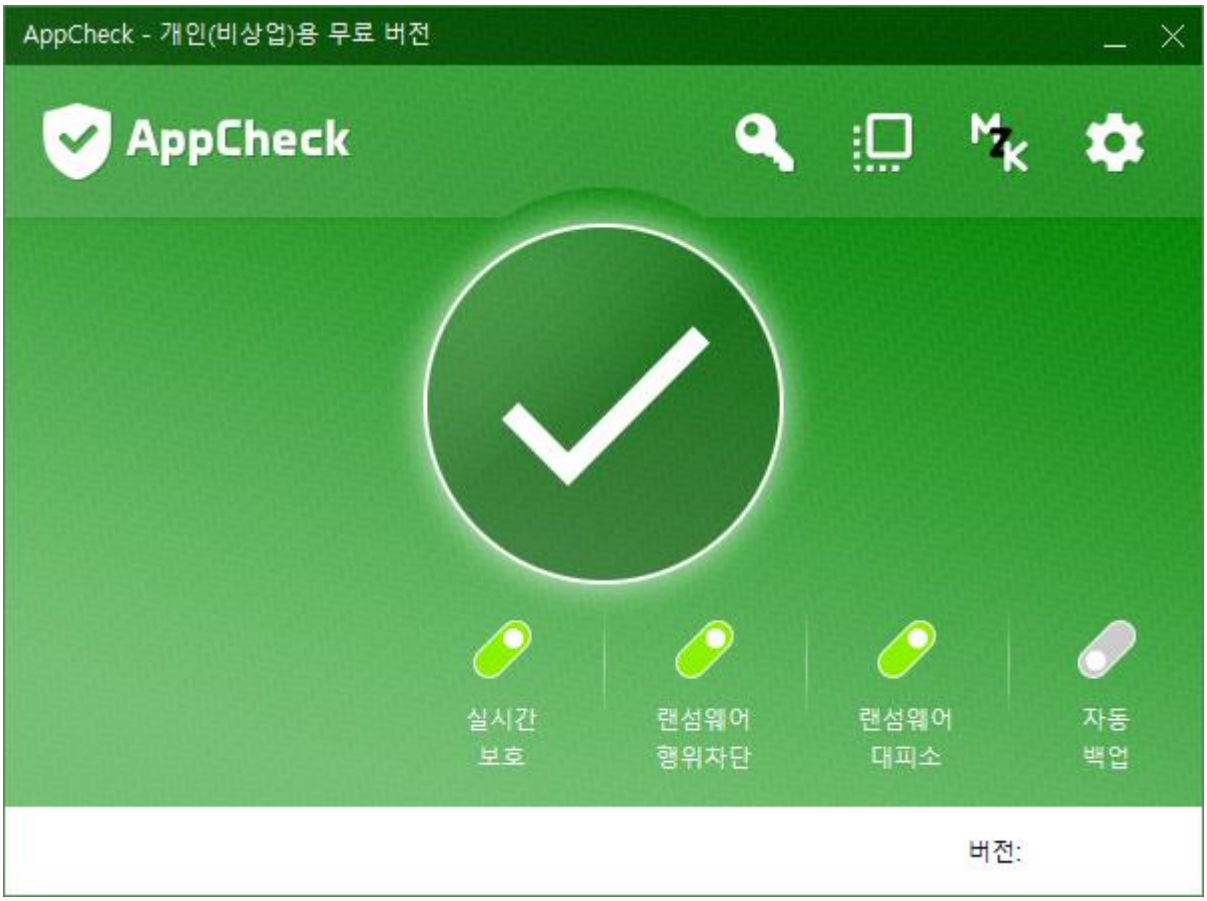
AppCheck 안티랜섬웨어 도움말

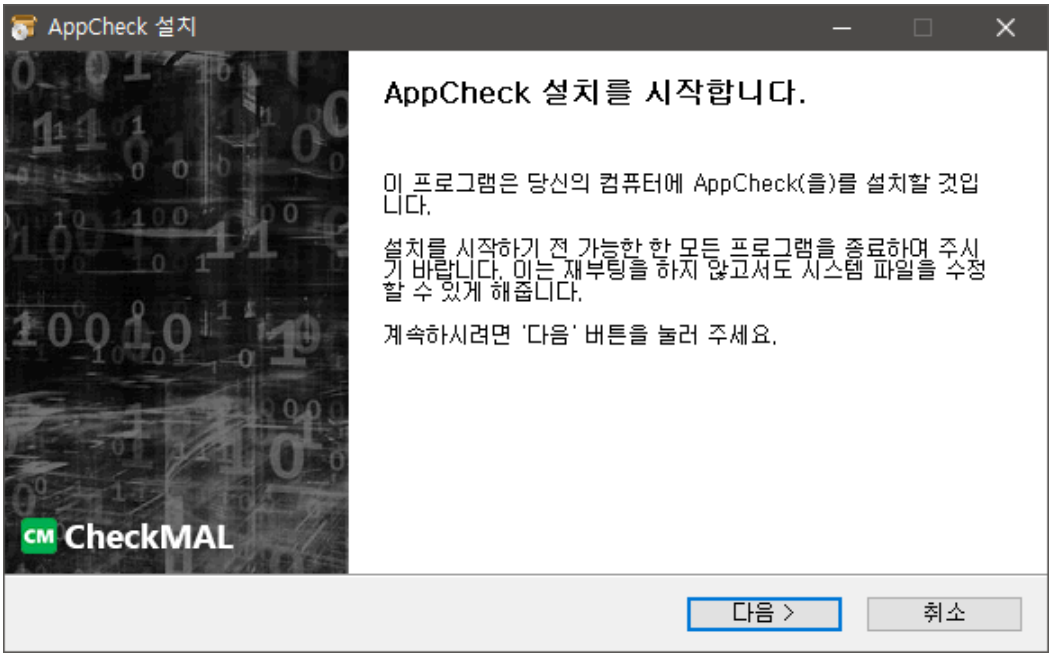


CHECKMAL

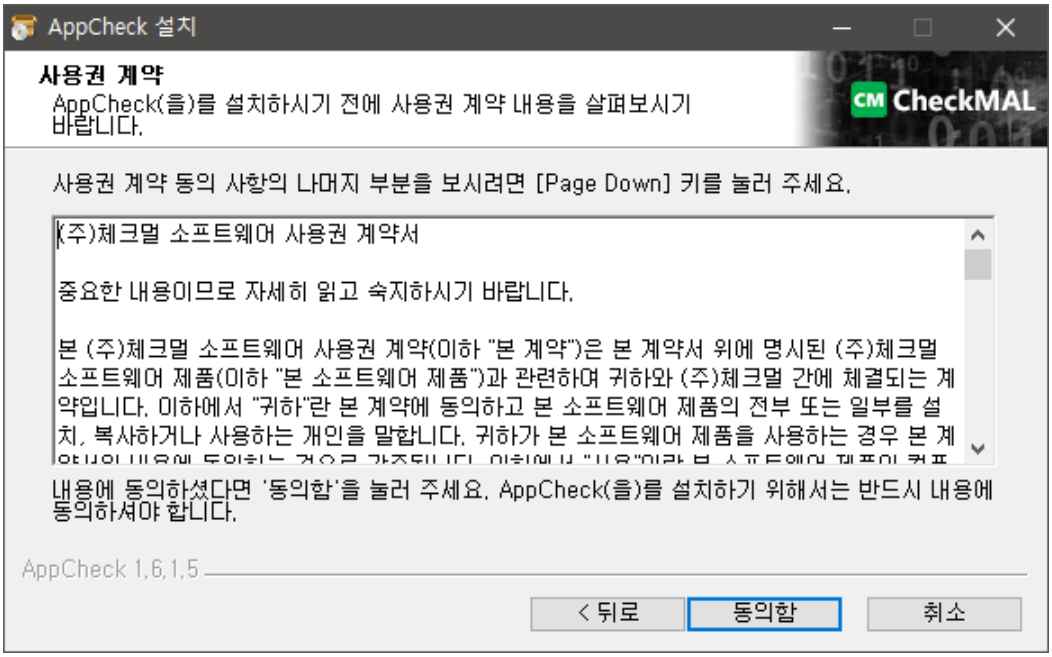
앱체크(AppCheck) 안티랜섬웨어 : 설치하기

앱체크(AppCheck) 안티랜섬웨어(이하 앱체크)는 Windows 7 (32/64bit) 이상의 운영체제에서 설치할 수 있으며, 한국어/영어/일본어 운영체제 환경에 따라 해당 언어를 지원합니다.

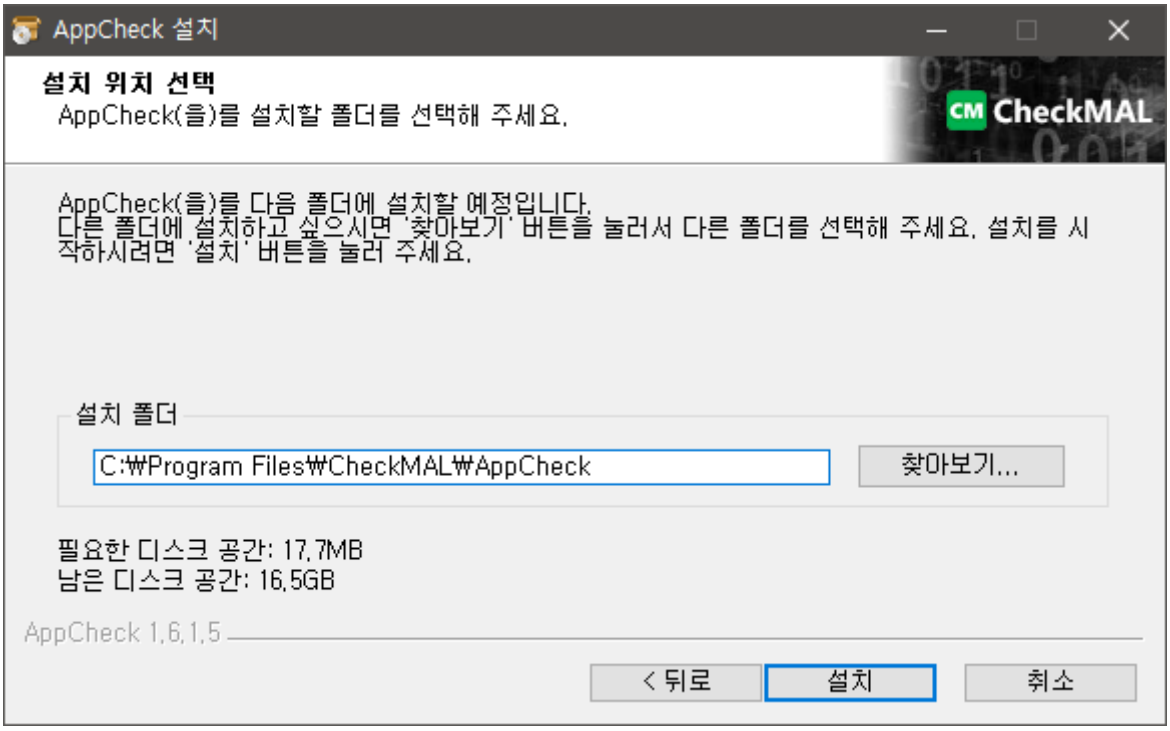
(1) 앱체크를 설치하기 전 실행 중인 모든 프로그램을 종료한 후 설치를 진행하시기 바랍니다.



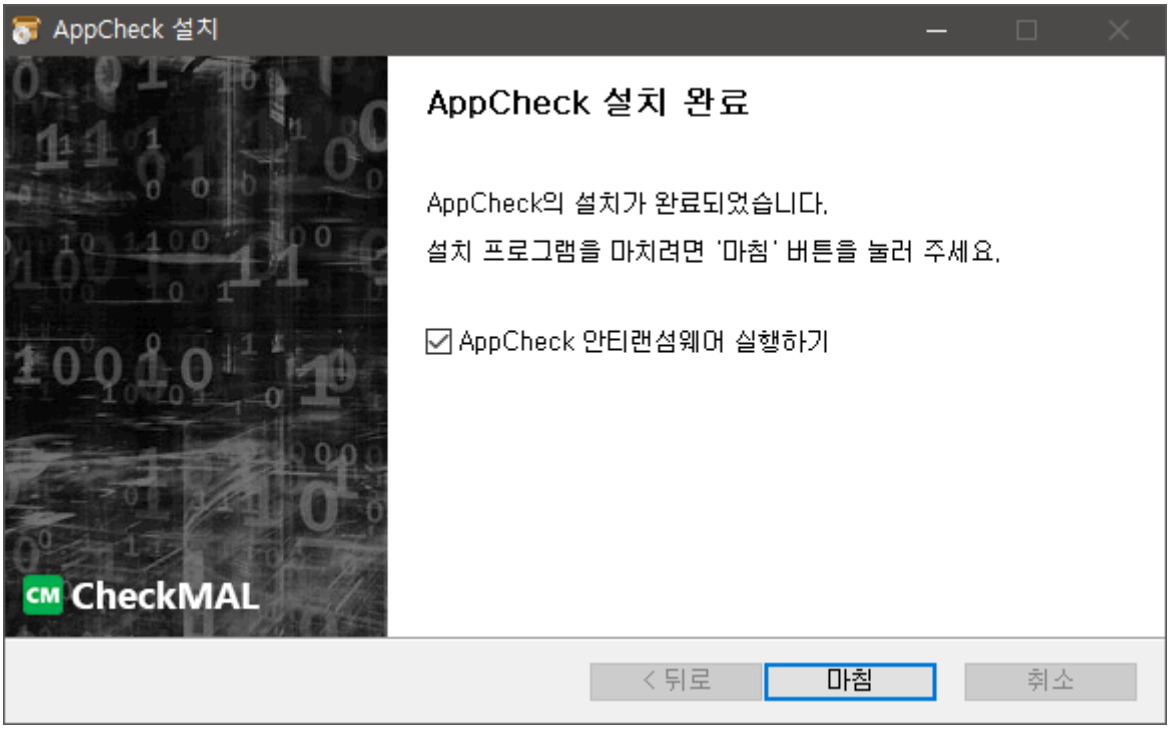
(2) ㈜체크멀 소프트웨어 사용권 계약서 내용에 동의할 경우 "동의함" 버튼을 클릭하시기 바랍니다.



(3) 앱체크는 "C:₩Program Files₩CheckMAL₩AppCheck" 기본 설치 폴더(32/64bit 공통)에 프로그램을 설치합니다.

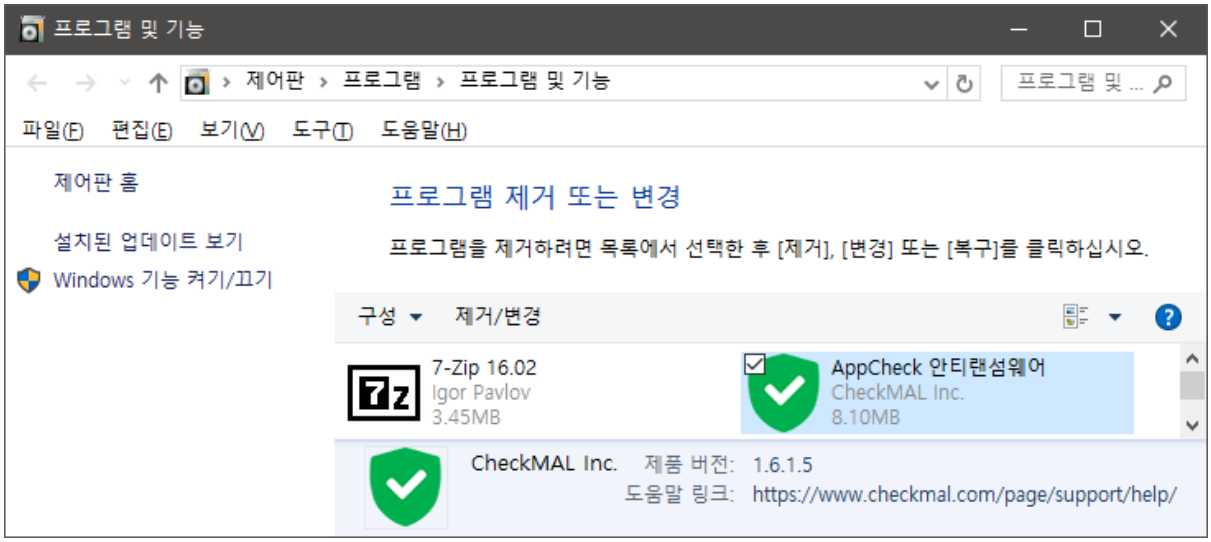


(4) 설치가 완료된 후 "마침" 버튼을 클릭하시면 AppCheck 안티랜섬웨어 프로그램이 자동 실행됩니다.

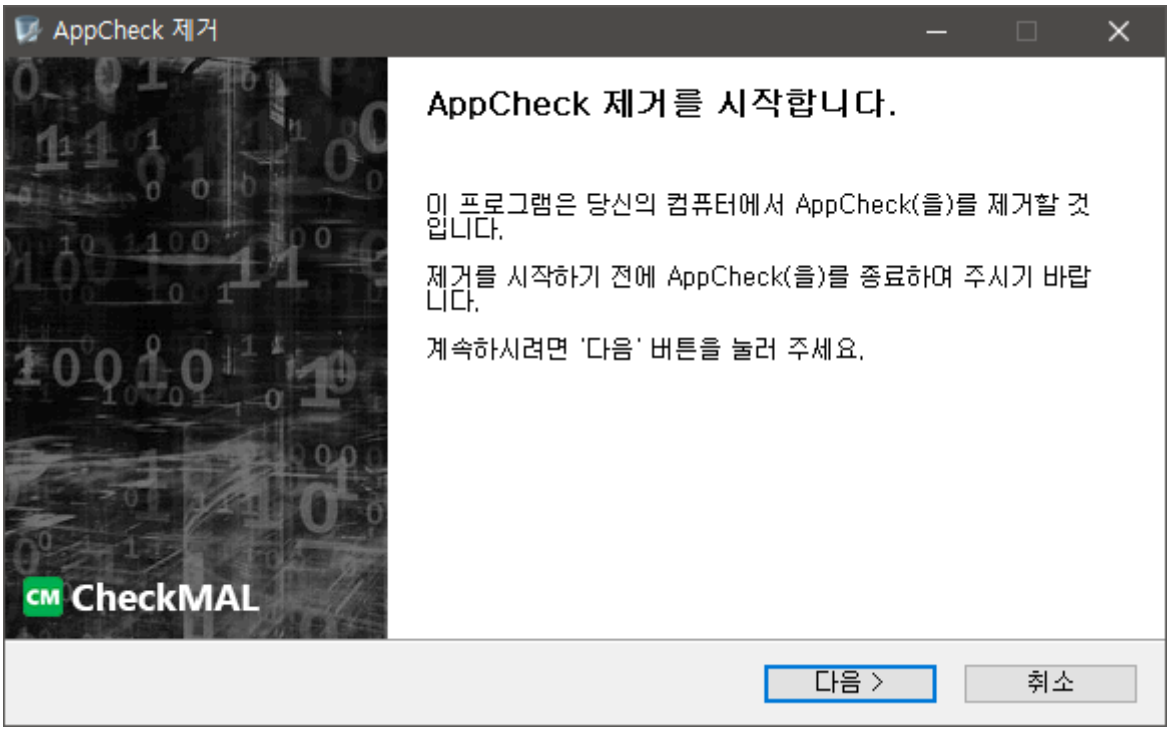


앱체크(AppCheck) 안티랜섬웨어 : 제거하기

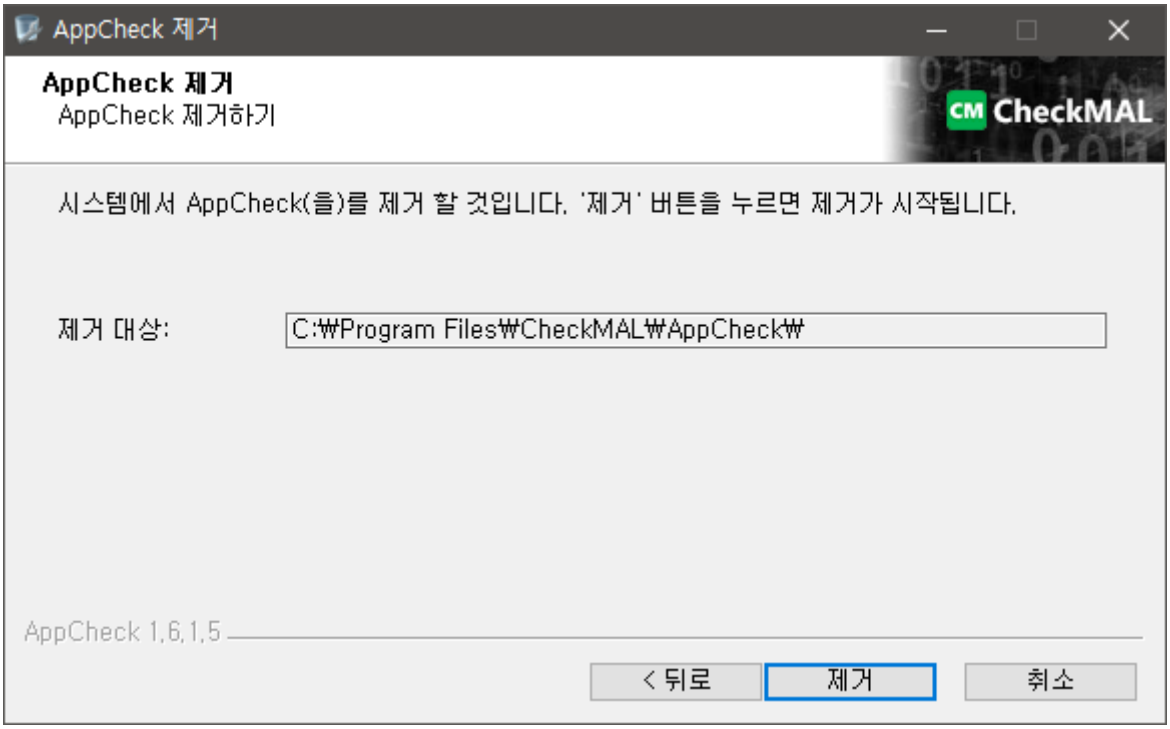
(1) 앱체크를 제거하기 위해서는 제어판의 "프로그램 및 기능"에 등록된 "AppCheck 안티랜섬웨어" 항목을 찾아 제거/변경 메뉴를 실행하시기 바랍니다.



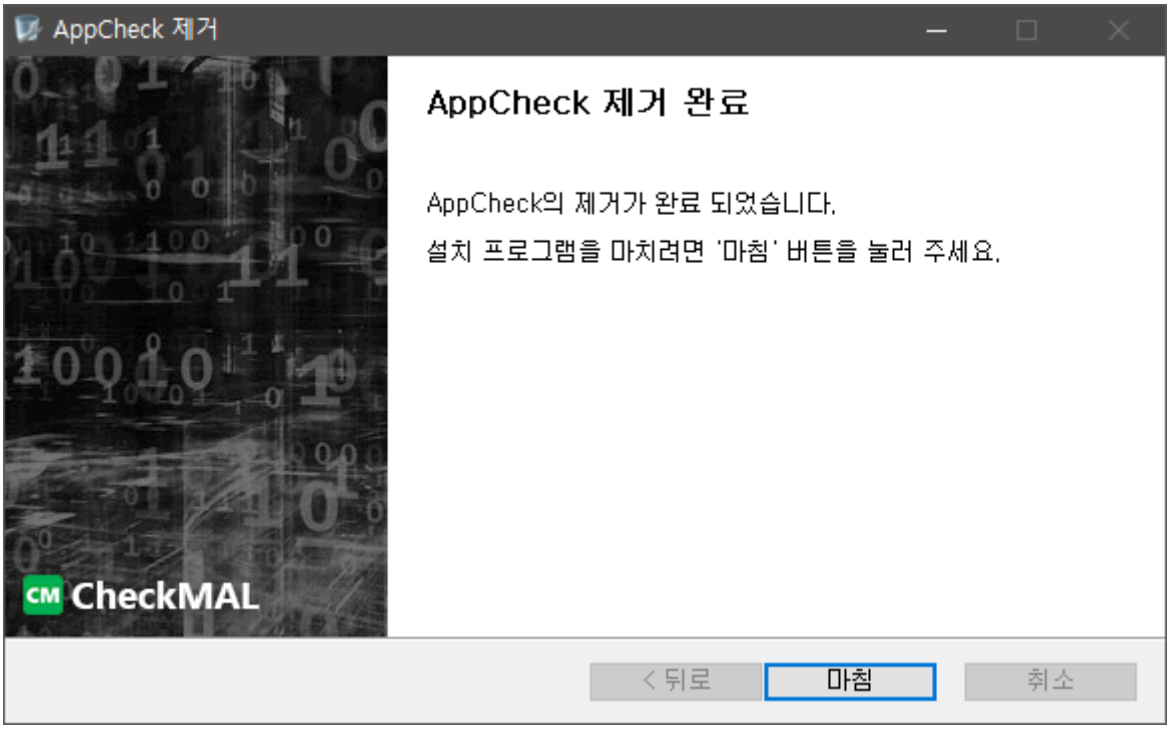
(2) 프로그램 제거를 시작하기 전에 작업 표시줄에 표시된 "AppCheck 안티랜섬웨어" 알림 아이콘 메뉴를 통해 프로그램을 종료하시기 바랍니다.



(3) 시스템에서 앱체크를 제거하기 위해서는 "제거" 버튼을 클릭하시기 바랍니다.



(4) 앱체크 제거가 완료된 후에는 "마침" 버튼을 클릭한 후 각 드라이브에 생성되었을 수 있는 랜섬웨어 대피소 폴더<Backup(AppCheck)>를 찾아 직접 삭제하시기 바랍니다.



앱체크(AppCheck) 안티랜섬웨어 : 메뉴 구성

① 메인 화면 메뉴 구성

⊙ **정품 등록 :** AppCheck Pro 제품 구매 안내 및 온라인 정품 등록

⊙ **도구** : 위협 로그, 검역소, 일반 로그 정보 제공

⊙ **MZK 바로 가기 (AppCheck 무료 전용) :** 바이러스 제로 시즌 2 보안 카페에서 제공하는 Malware Zero Kit (MZK) 보조 악성코드 제거 스크립트 바로 가기

⊙ **옵션 :** 일반, 랜섬가드, 자동 백업, 사용자 신뢰 파일 설정 기능

⊙ **시스템 검사 :** 랜섬웨어 결제 안내 파일 검사 기능

⊙ **실시간 보호 :** 랜섬가드(랜섬웨어 행위 차단, 랜섬웨어 대피소), 랜섬웨어 대피소 <Backup(AppCheck)> 및 자동 백업<AutoBackup(AppCheck)> 폴더 보호 기능 (비)활성화 기능

⊙ **랜섬웨어 행위 차단 (부분 유료) :** 랜섬웨어 사전 방어, 파괴 행위 탐지, 랜섬웨어 차단 후 자동 치료(AppCheck Pro 전용), MBR 보호(AppCheck Pro 전용), 공유된 폴더내 파일 보호(AppCheck

Pro 전용)

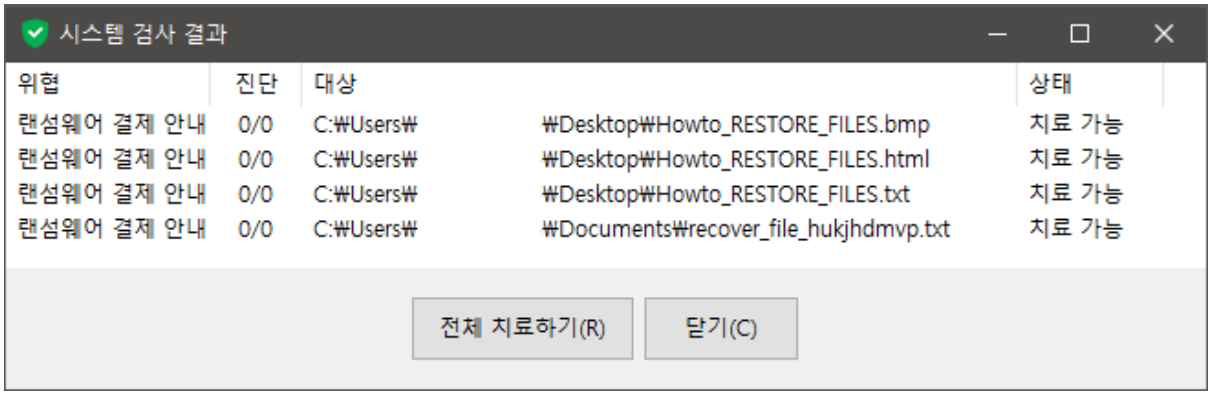
⊙ **랜섬웨어 대피소 :** 다양한 원본 파일 훼손 행위 중 조건에 맞을 경우 랜섬웨어 대피소 폴더 <Backup(AppCheck)>에 원본 파일을 실시간 백업 및 일부 훼손된 파일 자동 복구 기능

⊙ **자동 백업 (AppCheck Pro 전용) :** 자동 백업 폴더<AutoBackup(AppCheck)>에 백업할 폴더를 파일 히스토리(File History) 방식으로 주기적인 자동 백업 기능

[1-1] 시스템 검사

시스템 검사는 랜섬웨어 결제 안내 파일에 대한 수동 검사를 통해 "안전" 또는 "위험"으로 검사 결과를 표시합니다.

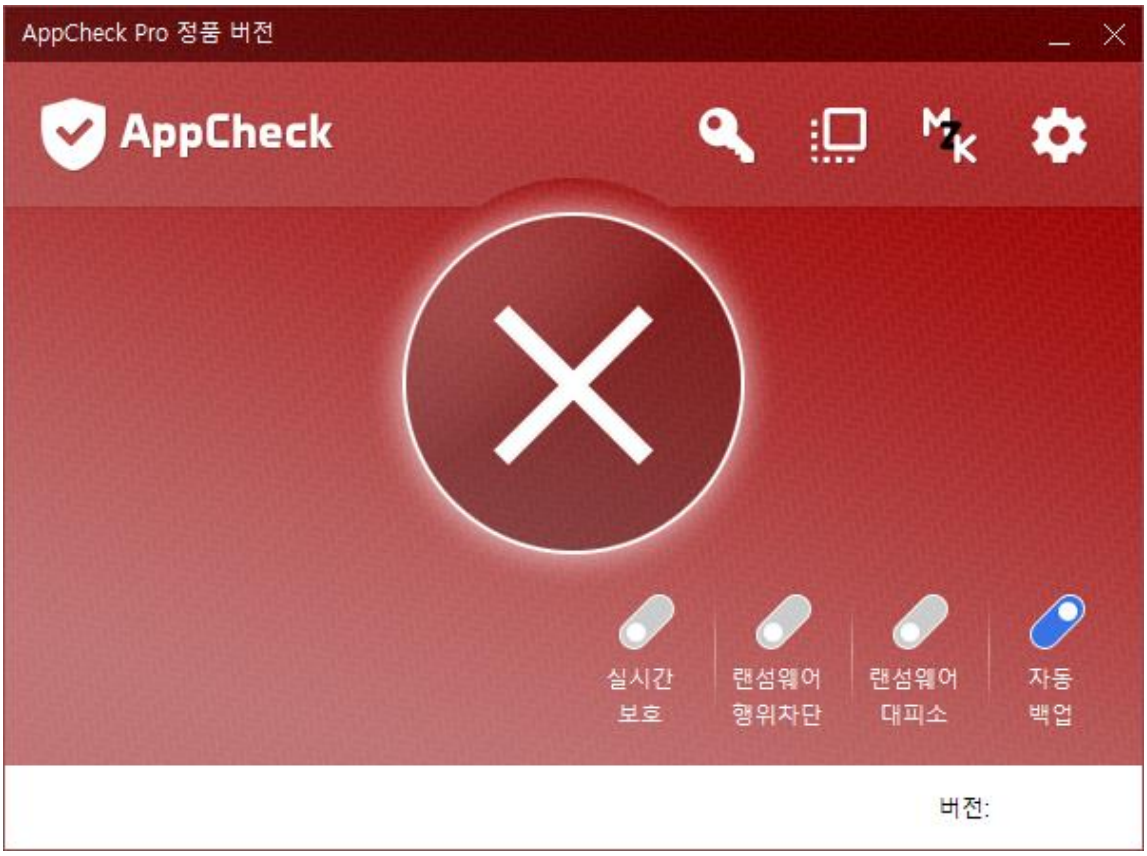
시스템 검사 결과 "위험"으로 진단될 경우 위험 표시를 클릭하시면 세부적인 시스템 검사 결과를 확인할 수 있으며 "전체 치료하기" 버튼을 클릭하면 진단된 파일을 치료(삭제)할 수 있습니다.



시스템 검사를 통해 치료(삭제)된 파일은 검역소에 백업되므로 사용자 필요에 따라 복원할 수 있습니다.

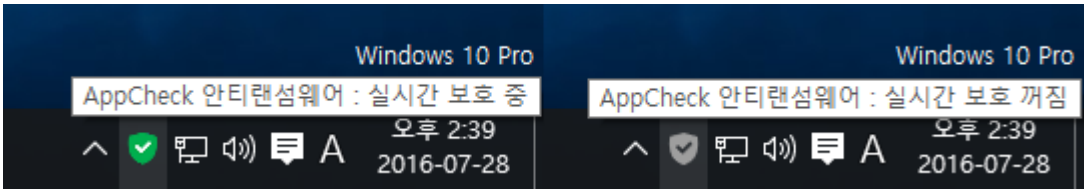
[1-2] 실시간 보호

실시간 보호는 랜섬가드(랜섬웨어 사전 방어, 랜섬웨어 대피소, 파괴 행위 탐지, MBR 보호, 공유된 폴더내 파일 보호), 랜섬웨어 대피소 내에 저장된 파일에 대한 자동 삭제, 랜섬웨어 대피소 <Backup(AppCheck)> 및 자동 백업<AutoBackup(AppCheck)> 폴더 보호 (비)활성화 기능을 제공합니다.



AppCheck Pro 정품 버전의 자동 백업 기능은 실시간 보호의 (비)활성화의 영향을 받지 않지만, 실시간 보호 기능이 비활성화 될 경우 자동 백업 폴더<AutoBackup(AppCheck)> 보호 기능이 해제되어 내부 파일을 보호할 수 없습니다.

앱체크 실시간 보호의 (비)활성화 여부에 따라 작업 표시줄 알림 영역에 표시된 앱체크 아이콘 색상이 변경됩니다.

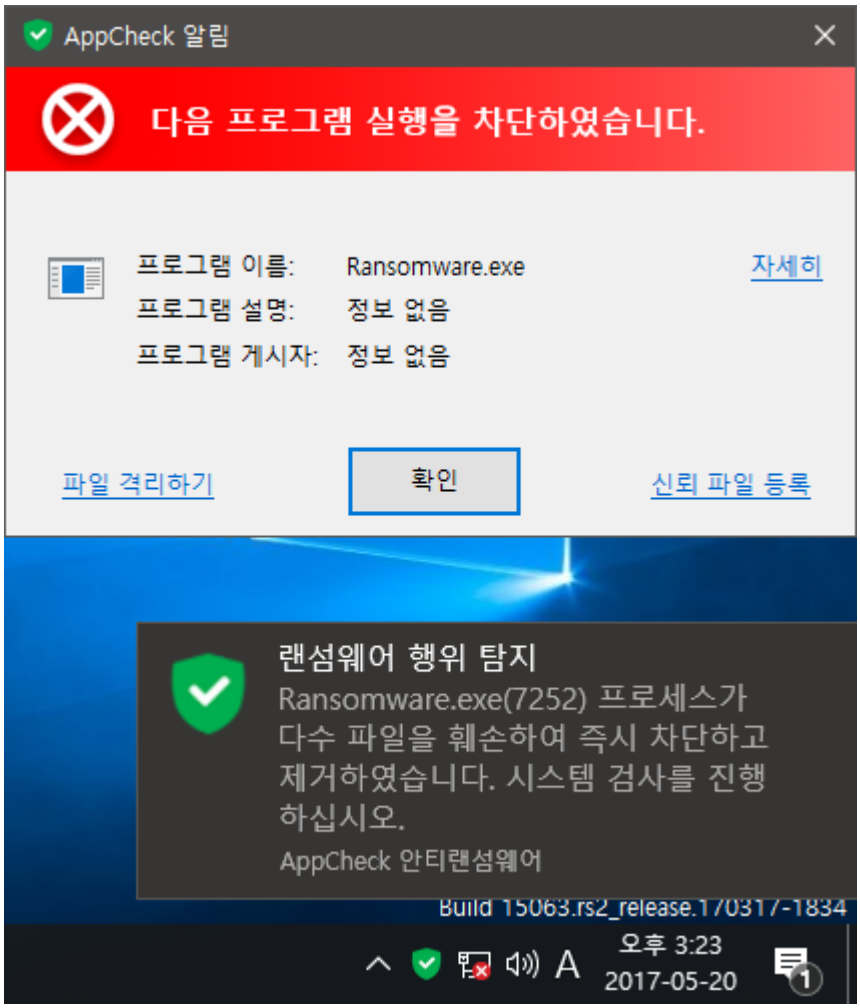


⊙ **녹색 아이콘** : 실시간 보호 중

⊙ **회색 아이콘** : 실시간 보호 꺼짐

[1-3] 랜섬웨어 행위 차단

랜섬가드 기능에 포함된 랜섬웨어 행위 차단은 랜섬웨어(Ransomware) 악성코드 감염으로 파일 암호화 행위가 진행될 경우 "랜섬웨어 행위 탐지" 알림창 생성을 통해 암호화 행위 파일을 차단 및 제거하는 기능입니다.



⊙ **자세히** : AppCheck 도구로 연결되어 위협 로그, 검역소, 일반 로그 정보 확인

⊙ **파일 격리하기 :** 랜섬웨어 행위 차단을 통해 차단된 파일을 검역소로 격리(삭제)하여 더 이상 실행되지 않도록 합니다. 단, 시스템 파일과 디지털 서명이 포함된 파일은 차단만 지원합니다.

⊙ **신뢰 파일 등록 :** 정상적인 프로그램 행위를 과탐한 경우 차단된 파일을 사용자 신뢰 파일로 등록하여 차후 차단되지 않도록 설정합니다.

참고로 앱체크 개인(비상업)용 무료 버전에서는 랜섬웨어 행위 탐지 시 차단만을 지원하며, AppCheck Pro 정품 버전에서는 차단 및 자동 치료(삭제) 기능을 제공합니다.

[1-4] 랜섬웨어 대피소

랜섬가드 기능에 포함된 랜섬웨어 대피소는 랜섬웨어(Ransomware) 악성코드 감염을 통해 파일 암호화 행위 또는 특정 조건에 부합되는 원본 파일 훼손 행위가 발생할 경우 자동으로 랜섬웨어 대피소 폴더<Backup(AppCheck)>에 원본 파일을 백업하는 기능을 제공합니다.

또한 랜섬웨어 행위 탐지 발생 시 랜섬웨어 대피소에 백업된 원본 파일을 이용하여 훼손된 파일은 자동 제거하고 보호 파일 확장명에 한하여 원본 파일로 자동 복원합니다.

랜섬웨어 대피소 폴더<Backup(AppCheck)>는 각 드라이브에 생성되며 백업된 파일 중 7일이 경과된 경우에는 디스크 용량 관리 차원에서 자동 삭제되도록 옵션을 제공합니다.

[1-5] 자동 백업

자동 백업은 AppCheck Pro 정품 버전에서 제공하는 기능으로 사용자가 지정한 백업할 대상 폴더를 자동 백업 폴더<AutoBackup(AppCheck)>에 파일 히스토리(File History) 방식으로 주기적으로 백업하는 기능입니다.

자동 백업 옵션에서는 백업할 대상 폴더 내의 특정 파일 확장명만을 지정하여 백업할 수 있으며, 백업할 대상 폴더 내의 특정 하위 폴더 및 파일 확장명을 지정하여 백업 시 제외 처리를 할 수 있습니다.

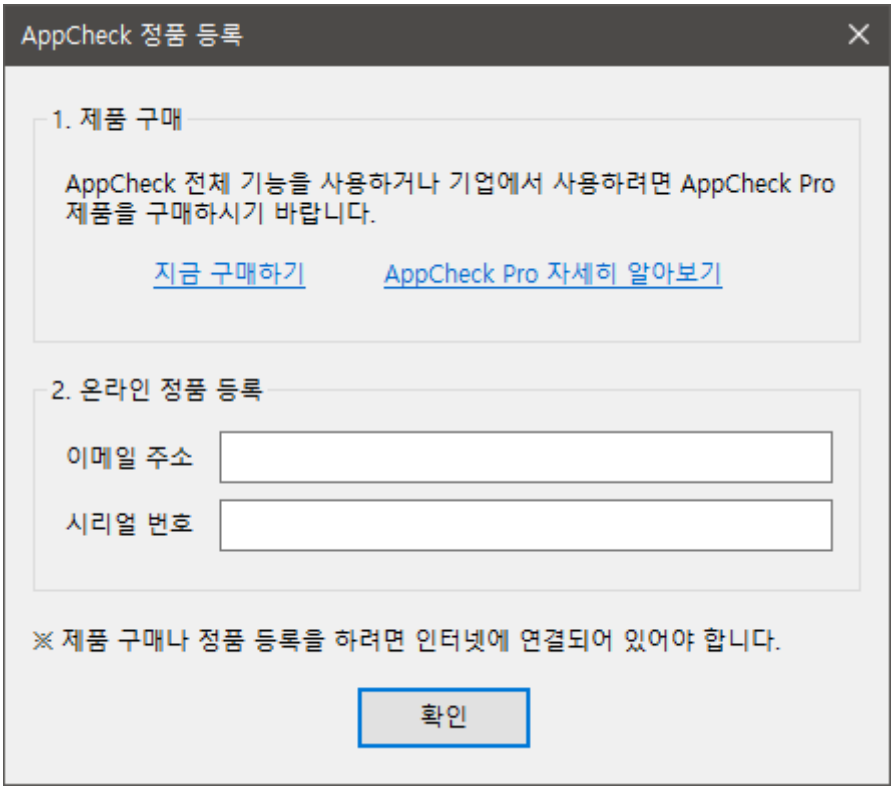
백업할 위치는 로컬 디스크, 네트워크 공유 폴더(SMB/CIFS), 중앙 관리 서버(CMS Enterprise) 방식으로 지정할 수 있습니다.

특히 자동 백업 폴더<AutoBackup(AppCheck)>는 랜섬웨어(Ransomware)를 비롯한 다양한 파일 훼손 행위로부터 백업 파일을 안전하게 보호해줍니다.

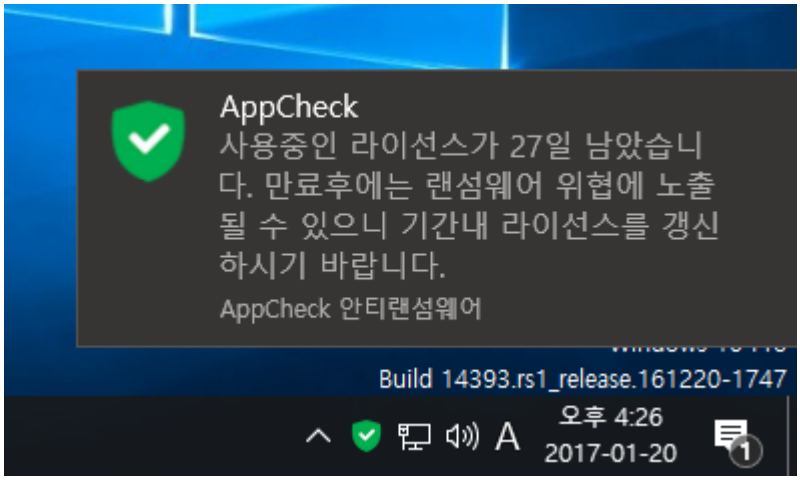
[1-6] 정품 등록

AppCheck 안티랜섬웨어 개인(비상업)용 무료 버전은 랜섬가드 기능 일부와 자동 백업 기능을 사용할 수 없으며, 기업/관공서 및 기능 제한없이 사용을 원하시는 개인 사용자는 AppCheck Pro 정품 버전을 구매해야 합니다.

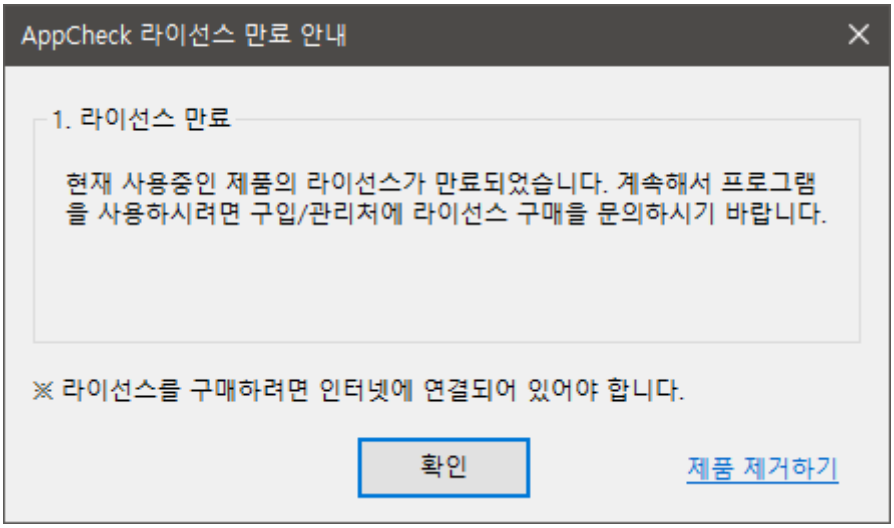
AppCheck Pro 라이선스를 구입하신 후 정품 등록을 위해서는 앱체크 메인 화면 상단의 "정품 등록" 버튼(열쇠 모양 아이콘)을 클릭하여 온라인 정품 등록을 진행하시기 바랍니다.



온라인 정품 등록을 위해서는 반드시 인터넷이 연결되어 있어야하며, 라이선스 주문 시 입력한 이메일 주소와 제공받은 시리얼 번호를 입력 후 "확인" 버튼을 클릭하시면 정품 등록이 이루어집니다.



정품 등록이 이루어진 AppCheck Pro 정품 버전은 라이선스 만료 30일 전부터 "사용중인 라이선스가 ○○일 남았습니다. 만료후에는 랜섬웨어 위협에 노출될 수 있으니 기간내 라이선스를 갱신하시기 바랍니다."라는 라이선스 만료 안내 메시지가 생성됩니다.



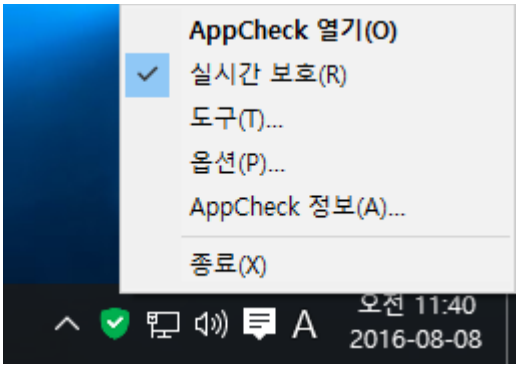
AppCheck 라이선스 기간이 만료된 후에는 모든 기능이 종료되며 제품 클릭 시 "AppCheck 라이선스 만료 안내" 메시지를 통해 프로그램을 계속 사용하기 위한 재구매 또는 제품 제거를 진행할 수 있도록 안내합니다.

[1-7] MZK 바로 가기

MZK 바로 가기 기능은 AppCheck 개인(비상업)용 무료 버전에서만 표시되며, MZK 바로 가기 버튼을 클릭하시면 바이러스 제로 시즌 2 보안 카페에서 제공하는 Malware Zero Kit (MZK) 보조 악성코드 제거 스크립트 페이지로 연결됩니다.

앱체크 사용 중 악성코드 또는 랜섬웨어 행위 탐지가 발생할 경우 시스템에 대한 전반적인 검사를 원하시는 분들은 Malware Zero Kit (MZK) 도구를 이용하여 검사를 진행해보시기 바랍니다.

② 작업 표시줄 알림 영역의 앱체크 메뉴 구성



⊙ **AppCheck 열기 :** 앱체크 메인 화면 실행

⊙ **실시간 보호 :** 랜섬가드(랜섬웨어 행위 차단, 랜섬웨어 대피소, MBR 보호, 공유된 폴더내 파일 보호, 랜섬웨어 대피소 내에 저장된 파일에 대한 자동 삭제), 랜섬웨어 대피소 <Backup(AppCheck)> 및 자동 백업<AutoBackup(AppCheck)> 폴더 보호 기능 (비)활성화 기능

⊙ **도구 :** 위협 로그, 검역소, 일반 로그 정보 확인

⊙ **옵션 :** 일반, 랜섬가드, 자동 백업, 사용자 신뢰 파일 설정

⊙ **AppCheck 정보 :** 앱체크 버전, 수동 업데이트 확인, 저작권 및 라이선스 안내, 도움을 주고 계신 분들, 정품 등록 정보 표시

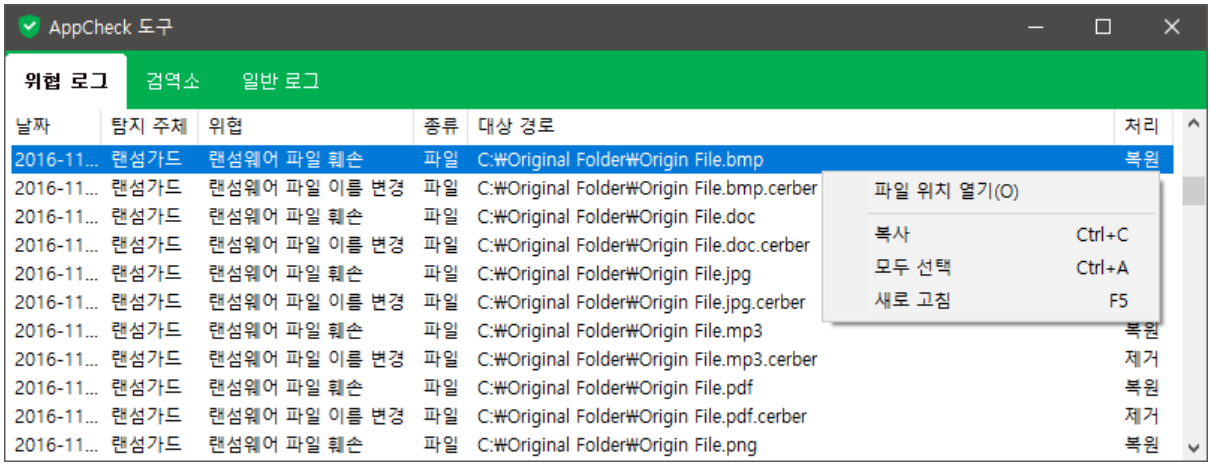
⊙ **종료 :** 앱체크 GUI 화면 종료

[2-1] 도구

AppCheck 도구는 위협 로그, 검역소, 일반 로그 정보를 세부적으로 제공되며, 기록된 로그의 누적량이 일정 수준 초과할 경우 자동으로 정리됩니다.

◆ AppCheck 도구 : 위협 로그

위협 로그는 랜섬웨어 행위 탐지를 통한 자동 치료(차단, 제거, 복원) 정보를 표시합니다.



⊙ **파일 위치 열기 :** 선택한 파일이 저장된 위치(대상 경로)로 파일 탐색기를 통한 연결

⊙ **복사 :** 선택한 파일에 대한 위협 로그에 표시된 세부 정보 복사

⊙ **모두 선택 :** 위협 로그에 표시된 모든 항목 일괄 선택

⊙ **새로 고침 :** 위협 로그에 표시된 정보 갱신

◆ AppCheck 도구 : 검역소

검역소는 랜섬웨어 행위 탐지를 통해 삭제되어 검역소 폴더에 백업된 랜섬웨어 파일, 암호화된 파일, 랜섬웨어 결제 안내 파일 정보를 표시하며, 검역소 폴더 위치는 "C:₩ProgramData₩CheckMAL₩AppCheck₩Quarantine"입니다.

⊙ **원래 위치로 복원 :** 검역소에 백업된 선택 파일을 대상 경로로 복원하기

⊙ **지정 위치로 내보내기 :** 선택한 파일을 사용자가 지정한 폴더로 내보내기

⊙ **삭제 :** 검역소에 백업된 파일 삭제하기

⊙ **파일 위치 열기 :** 선택한 파일이 저장된 위치(대상 경로)로 파일 탐색기를 통한 연결

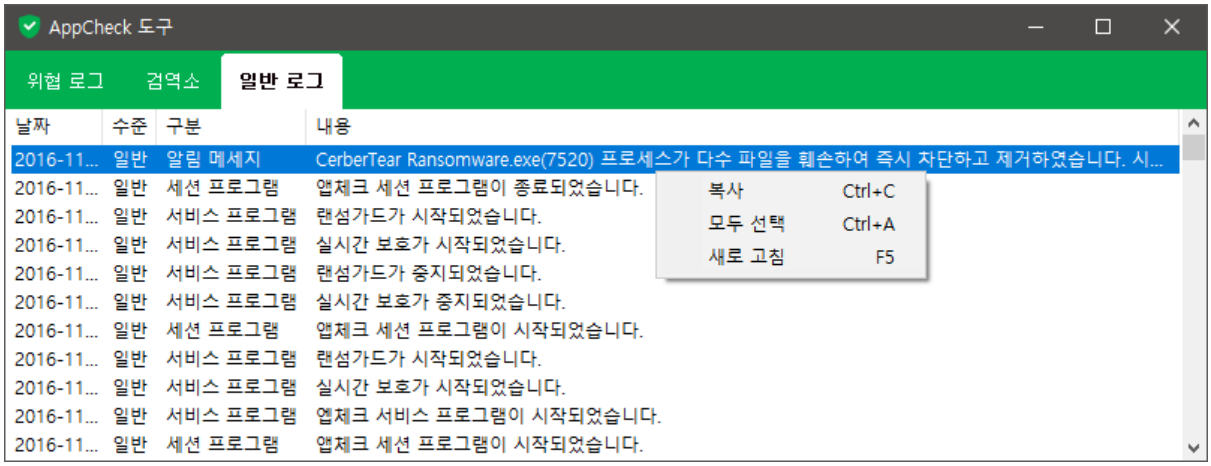
⊙ **복사 :** 선택한 파일에 대한 검역소에 표시된 세부 정보 복사

⊙ **모두 선택 :** 검역소에 표시된 모든 항목 일괄 선택

⊙ **새로 고침 :** 검역소에 표시된 정보 갱신

◆ AppCheck 도구 : 일반 로그

일반 로그는 앱체크 동작 시 발생하는 프로그램 시작/종료, 서비스 시작/종료, 실시간 보호 시작/종료, 랜섬가드 시작/종료, 업데이트, 자동 백업, 옵션 설정, 랜섬가드 알림 메시지 등의 정보를 표시합니다.



⊙ **복사 :** 선택한 파일에 대한 일반 로그에 표시된 세부 정보 복사

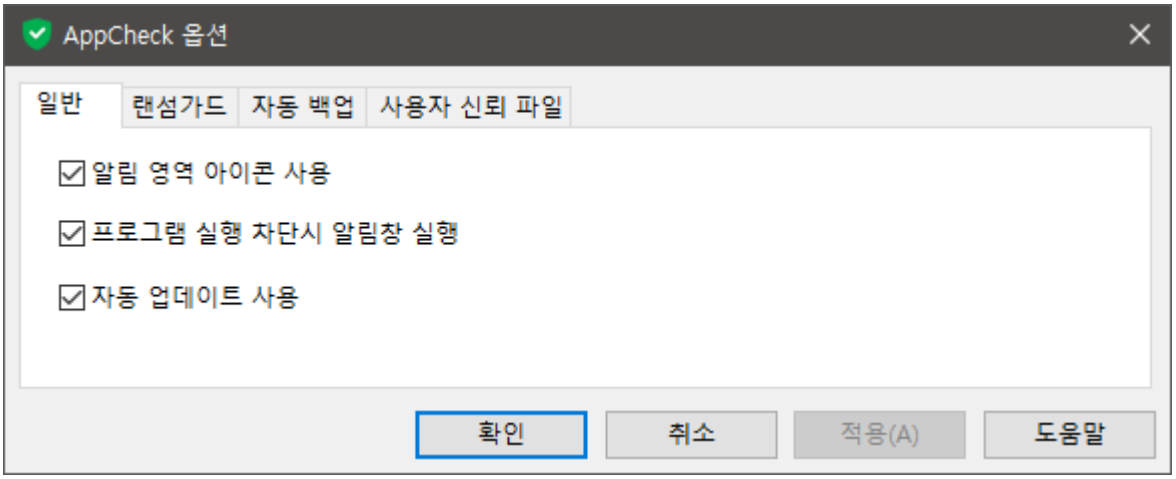
⊙ **모두 선택 :** 일반 로그에 표시된 모든 항목 일괄 선택

⊙ **새로 고침 :** 일반 로그에 표시된 정보 갱신

[2-2] 옵션

AppCheck 옵션은 일반, 랜섬가드, 자동 백업(AppCheck Pro 전용), 사용자 신뢰 파일 설정을 제공합니다.

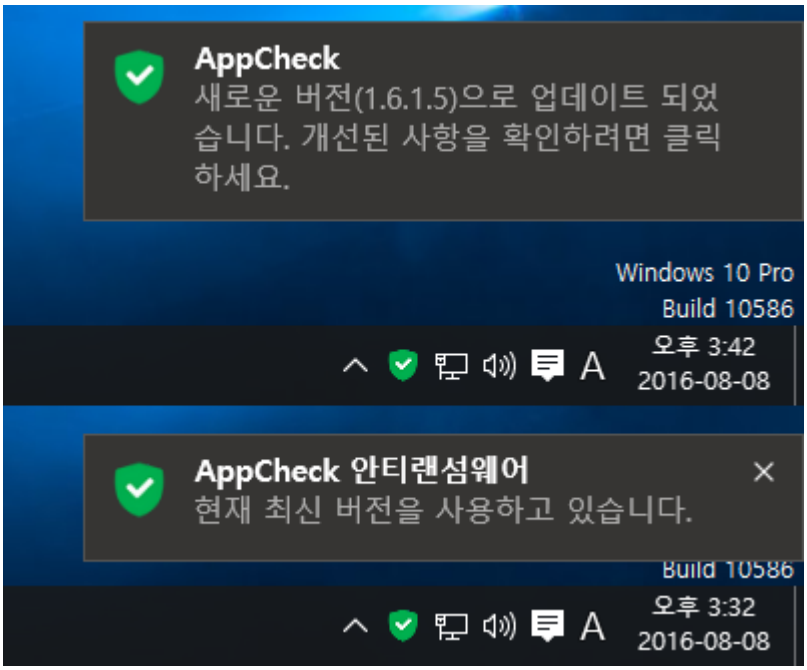
◆ AppCheck 옵션 : 일반



⊙ **알림 영역 아이콘 사용 :** 작업 표시줄 알림 영역에 앱체크 아이콘 표시

⊙ **프로그램 실행 차단시 알림창 실행 :** 랜섬웨어 행위 탐지 시 작업 표시줄 알림 영역에 알림창 표시

⊙ **자동 업데이트 사용 :** 6시간 주기로 앱체크 업데이트 확인(AppCheck 무료 버전 기준)

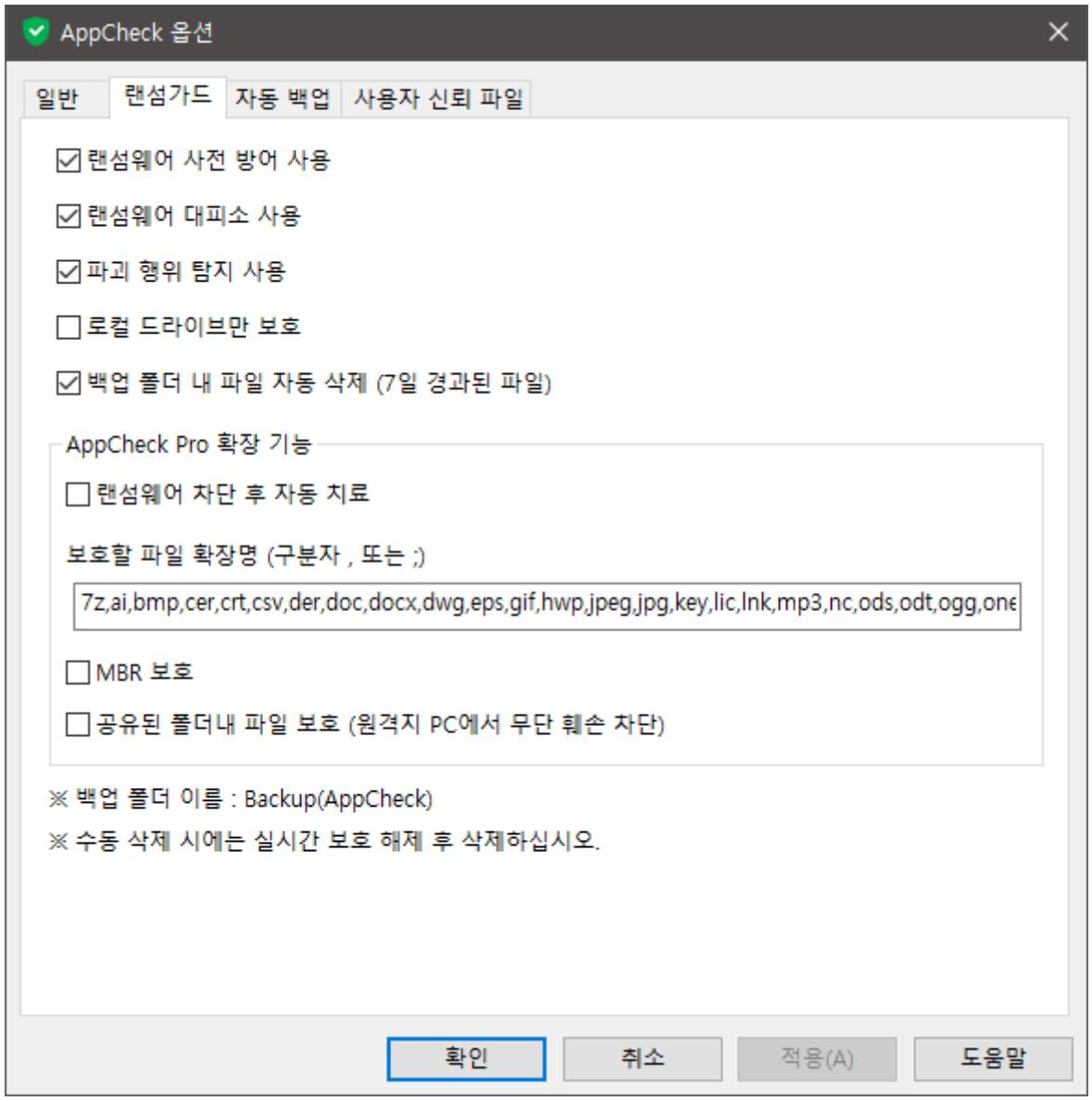


앱체크 자동 업데이트 기능은 6시간 주기로 자동 확인이 이루어지며 상위 버전으로 업데이트된 경우에는 재부팅 이후 "새로운 버전으로 업데이트되었습니다. 개선된 사항을 확인하려면 클릭하세요." 알림창이 생성됩니다.

만약 사용자가 알림창을 클릭할 경우 체크멀(CheckMAL) 공지사항에 게시된 AppCheck 업데이트 내역 게시글로 연결됩니다.

또한 AppCheck 정보의 "업데이트 확인" 메뉴를 사용자가 실행하여 최신 버전인 경우 "현재 최신 버전을 사용하고 있습니다." 알림창이 생성됩니다.

◆ **AppCheck 옵션 : 랜섬가드**



⊙ **랜섬웨어 사전 방어 사용 :** 파일 훼손 행위 발생 시 "랜섬웨어 행위 탐지" 알림창을 생성하여 암호화 행위 프로세스 차단을 통한 랜섬웨어 행위 중지 기능

⊙ **랜섬웨어 대피소 사용 :** 파일 훼손 행위 발생 시 랜섬웨어 대피소<Backup(AppCheck)> 폴더에 원본 파일을 백업하며 랜섬웨어 행위 탐지를 통해 훼손된 파일을 자동 복원해 주는 기능입니다. 참고로 랜섬웨어 대피소 폴더 및 내부 파일을 삭제하기 위해서는 실시간 보호를 임시 중지하시고 삭제하시기 바랍니다.

⊙ **파괴 행위 탐지 사용 :** 원본 파일을 복구 불가능하게 삭제하는 행위를 탐지하여 차단하는 기능

⊙ **로컬 드라이브만 보호 :** 네트워크 드라이브를 제외한 하드 디스크, 외장 하드, USB 저장 매체

보호 기능

⊙ **백업 폴더 내 파일 자동 삭제 (7일 경과된 파일) :** 랜섬웨어 대피소<Backup(AppCheck)> 폴더에 저장된 폴더(파일) 중 7일 경과 시 자동 삭제 기능

⊙ **랜섬웨어 차단 후 자동 치료 (AppCheck Pro 전용) :** 랜섬웨어 행위 탐지 시 악성 파일 자동 치료(삭제)

⊙ **보호할 파일 확장명 (구분자 , 또는 ;) :** 파일 훼손 행위로부터 보호되는 파일 확장명은 총 49종(7z, ai, bmp, cer, crt, csv, der, doc, docx, dwg, eps, gif, hwp, jpeg, jpg, key, lic, lnk, mp3, nc, ods, odt, ogg, one, p12, p7b, p7c, pdf, pef, pem, pfx, png, ppt, pptx, psd, ptx, rdp, rtf, srw, tap, tif, tiff, txt, uti, x3f, xls, xlsx, xps, zip)이며, 추가적인 파일 확장명 등록은 AppCheck Pro 정품 버전에서만 제공됩니다.

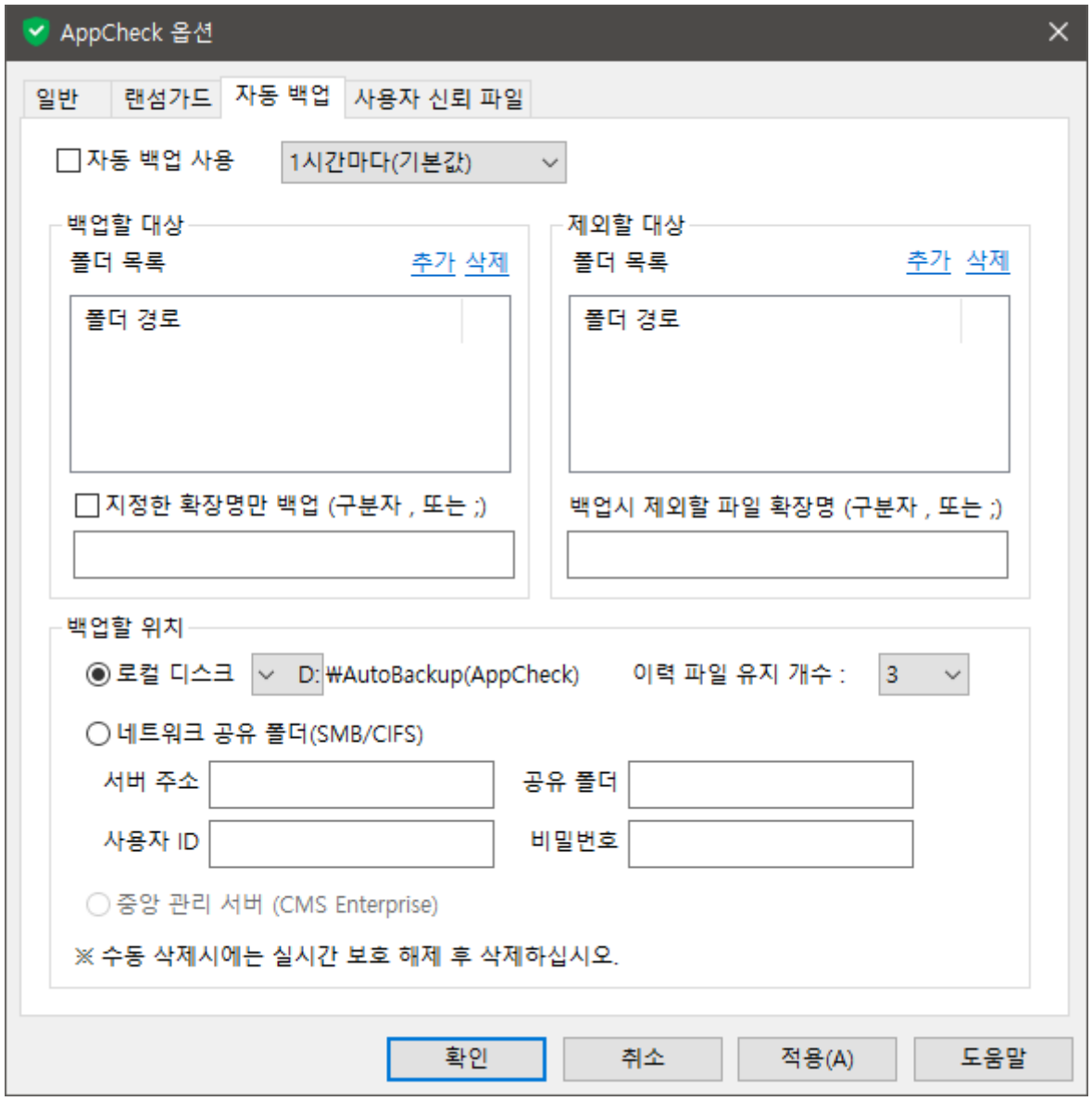
⊙ **MBR 보호 (AppCheck Pro 전용) :** Master Boot Record (MBR) 영역의 변조를 시도하는 파일 실행 차단

⊙ **공유된 폴더내 파일 보호 (원격지 PC에서 무단 훼손 차단) :** 네트워크 드라이브를 통해 앱체크가 설치되어 있지 않은 원격지 PC와 파일 공유가 이루어지는 환경에서 원격지 PC의 랜섬웨어 감염으로 인하여 공유 파일이 암호화되는 행위를 차단 및 자동 복원하는 기능

차단된 공유 폴더에 대한 액세스는 기본적으로 1시간 경과 시 자동으로 해제되며, 수동으로 해제하기 위해서는 앱체크 실시간 보호를 비활성화(OFF)하시면 됩니다.

또한 정상적인 랜섬웨어 차단을 위해서는 공유 폴더를 제공하는 서버(Server)의 네트워크의 "인터넷 프로토콜 버전 6(TCP/IPv6)" 체크를 반드시 해제하시고 사용하시기 바랍니다.

◆ AppCheck 옵션 : 자동 백업



⊙ **자동 백업 주기 :** 10분, 15분, 20분, 30분, 1시간(기본값), 3시간, 6시간, 12시간, 매일 단위로 자동 백업

⊙ **백업할 대상 폴더 목록 :** 사용자 선택에 따라 백업을 원하는 폴더 추가 및 삭제 가능

⊙ **지정한 확장명만 백업 (구분자 , 또는 ;) :** 백업할 대상 폴더 내에 저장된 파일 중 사용자가 지정한 파일 확장명만 백업 가능

⊙ **제외할 대상 폴더 목록 :** 백업할 대상 폴더 목록에 포함된 하위 폴더 중 사용자 선택에 따라 자동 백업 시 제외 처리 추가 및 삭제 가능

⊙ **백업 시 제외할 파일 확장명 (구분자 , 또는 ;) :** 백업할 대상 폴더 내에 저장된 파일 중 사용자가 지정한 파일 확장명은 백업 시 제외 처리 가능

⊙ **백업할 위치 :** 로컬 디스크, 네트워크 공유 폴더(SMB/CIFS), 중앙 관리 서버(CMS Enterprise) 중 선택 가능

⊙ **로컬 디스크 :** PC와 물리적으로 연결된 하드 디스크 중 사용 가능한 디스크 용량이 가장 많은 드라이브가 기본적으로 자동 선택되며, 사용자 선택에 따라 자동 백업 폴더 <AutoBackup(AppCheck)>가 저장될 드라이브 혹은 폴더 지정 가능

⊙ **이력 파일 유지 개수 :** 자동 백업 기능을 통해 생성된 백업 파일이 수정될 경우 생성되는 이력 파일(.history) 수를 0~10개로 사용자가 지정할 수 있으며, 기본값은 3개의 이력 파일로 지정되어 있습니다.

⊙ **네트워크 공유 폴더(SMB/CIFS) :** 서버 주소(IP 주소 또는 원격지 PC 이름), 공유 폴더(공유 설정이 이루어진 원격지 드라이브 이름), 사용자 ID, 비밀번호 입력 필수

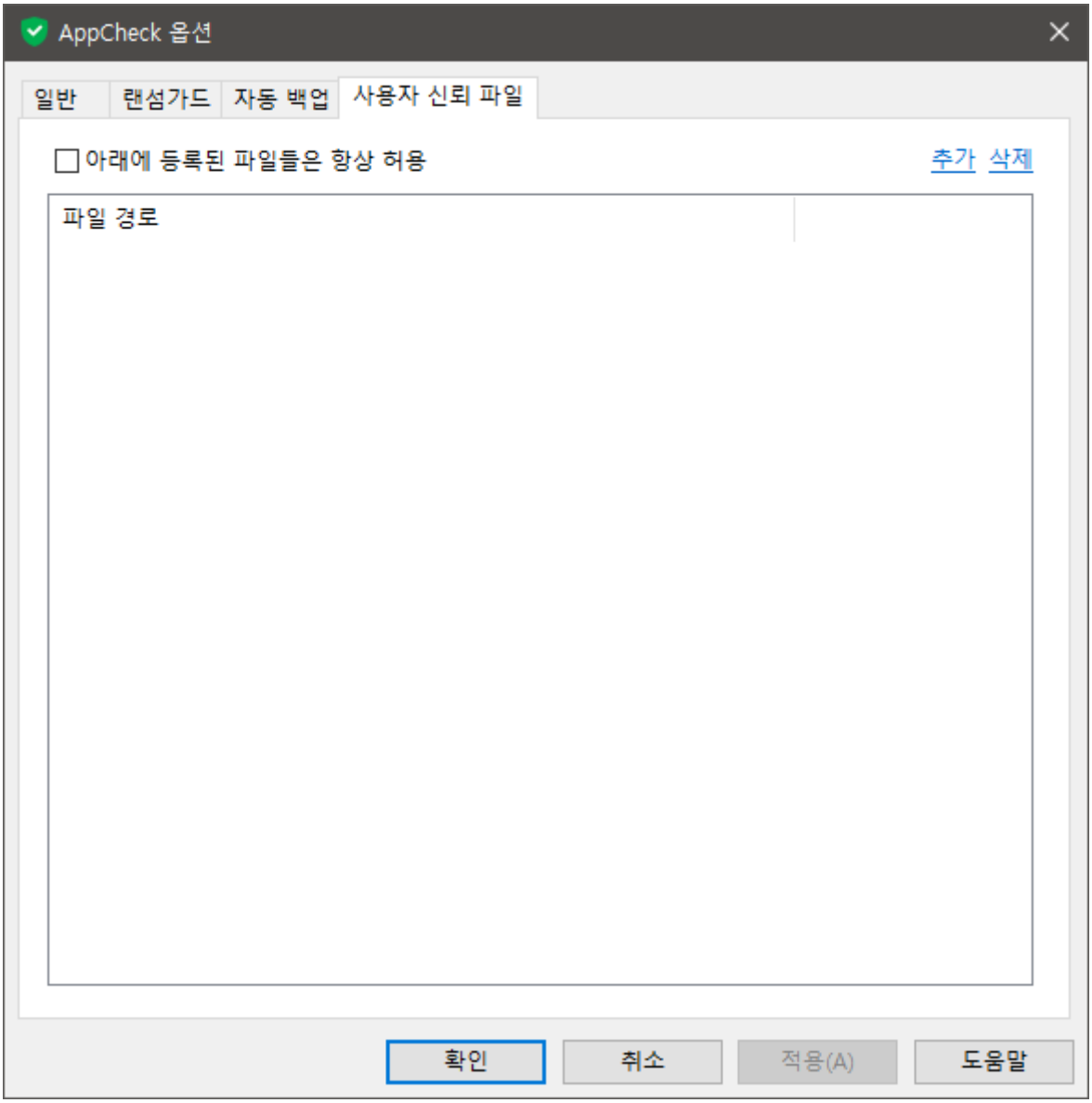
⊙ **중앙 관리 서버(CMS Enterprise) :** 기업 환경에서 중앙 관리 서버를 통해 앱체크 배포, 라이선스 및 전체 에이전트 관리를 할 수 있는 통합 서비스

안전하게 네트워크 공유 폴더를 사용하기 위해서는 별도 계정 생성을 통해 백업용으로 사용하시기 바라며 불필요한 공유 폴더 탐색을 하지 않는 것을 권장합니다.

또한 자동 백업 폴더<AutoBackup(AppCheck)> 및 내부 파일을 삭제하기 위해서는 앱체크 실시간 보호를 임시 중지하시고 삭제하시기 바랍니다.

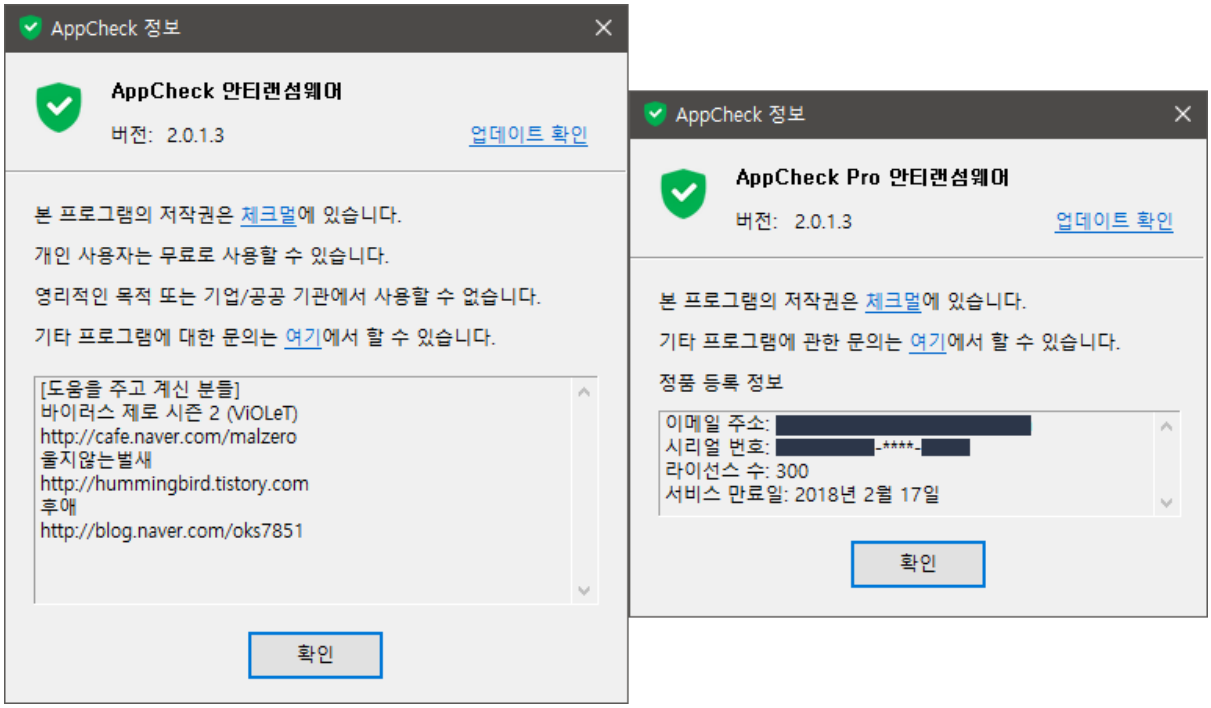
◆ AppCheck 옵션 : 사용자 신뢰 파일

사용자 신뢰 파일은 랜섬가드 기능을 통해 차단될 수 있는 파일 중 사용자 판단에 따라 진단 제외 처리하도록 파일을 추가할 수 있는 기능입니다.



[2-3] AppCheck 정보

AppCheck 정보는 앱체크 버전, 수동 업데이트 확인, 저작권 및 라이선스 안내, 도움을 주고 계신 분들, 정품 등록 정보를 표시합니다.



앱체크(AppCheck) 안티랜섬웨어 : 차단/탐지된 프로그램 처리 방법

앱체크 개인(비상업)용 무료 버전에서는 랜섬가드를 통한 랜섬웨어 행위 탐지 시 차단만 지원하며 자동 치료(삭제) 기능을 제공하지 않습니다.

또한 AppCheck Pro 정품 버전에서는 기본적으로 자동 치료(삭제) 기능을 제공하지만, 악성 파일 중 디지털 서명이 포함된 경우에는 차단 기능만 제공하고 있습니다.

그러므로 앱체크 사용 중 랜섬웨어 행위 탐지로 파일이 차단된 경우에는 다음과 같은 추가적인 조치를 하시기 바랍니다.

(1) 앱체크(AppCheck) 안티랜섬웨어 제품과 함께 사용하시는 백신 프로그램을 이용하여 정밀 검사를 하시기 바랍니다.

(2) 앱체크 메인 화면의 "MZK 바로 가기" 메뉴를 실행하여 바이러스 제로 시즌 2 보안 카페에서 제공하는 Malware Zero Kit (MZK) 보조 악성코드 제거 스크립트를 이용하여 검사하시기 바랍니다.

(3) 앱체크를 통해 차단(탐지)된 악성 프로그램을 삭제할 수 없는 경우에는 보안 업체, 바이러스 제로 시즌 2 보안 카페, 울지않는벌새 보안 블로그에 문의하시기 바랍니다.