



안티랜섬웨어 도움말



NEVER MIND THE SECURITY

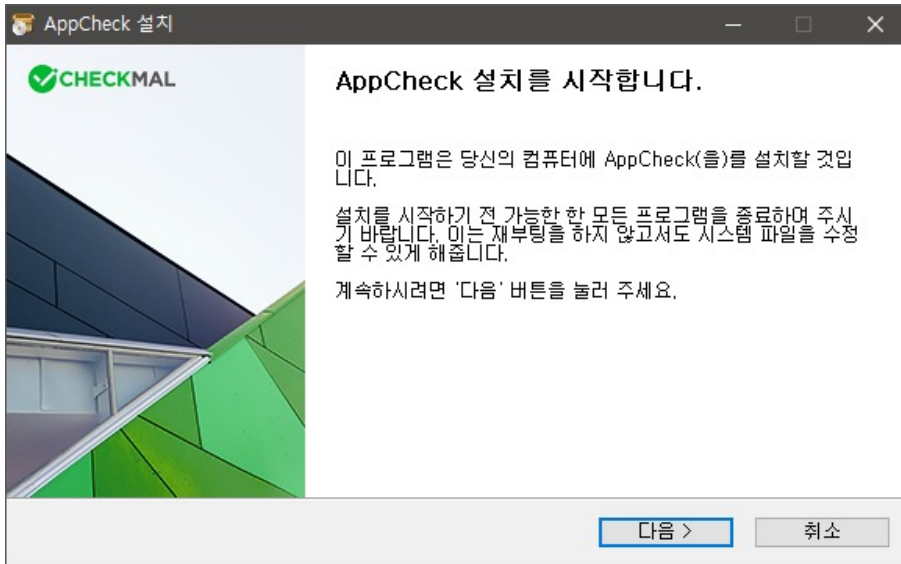
100% Signatureless Anti-Ransomware
Next Generation Anti-Ransomware Solution AppCheck



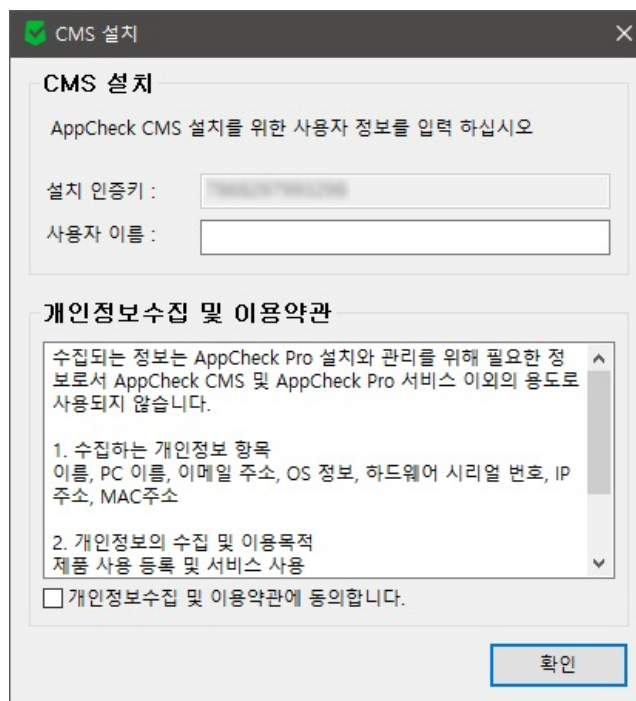
1. 설치하기

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.

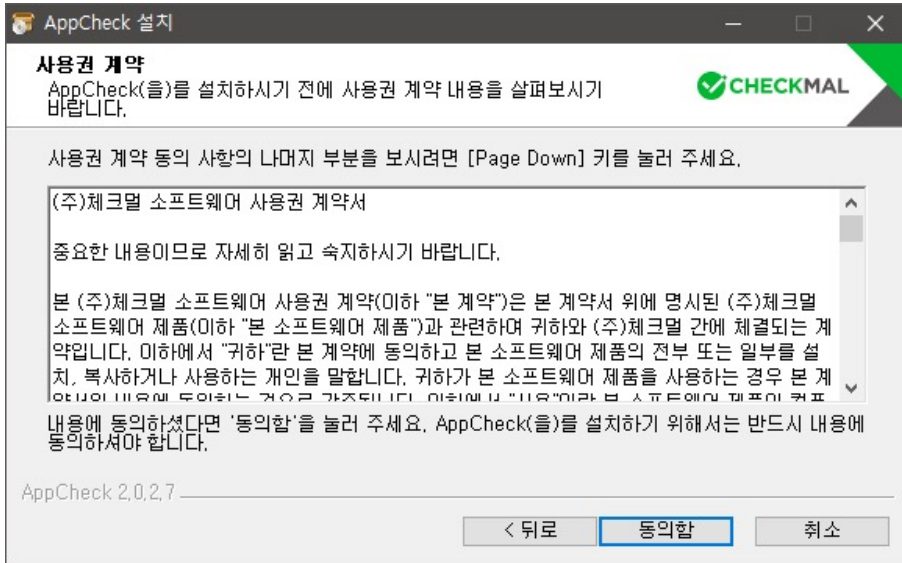


만약 CMS 중앙 관리에서 제공하는 배포 파일을 이용하여 설치 시에는 반드시 CMS 서버와 통신이 가능해야하며 “CMS 설치” 창을 먼저 생성합니다.

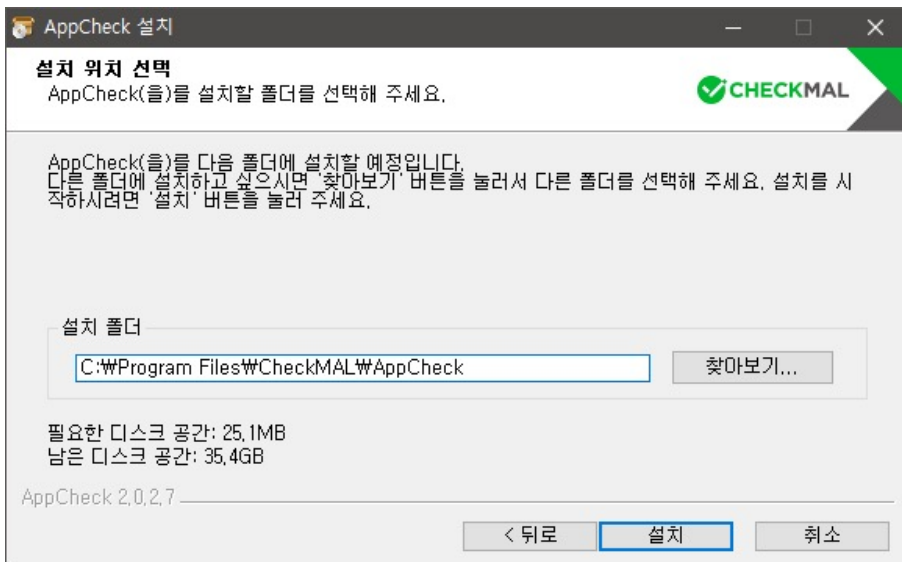


생성된 CMS 설치창에서 사용자 이름은 사내 정책에 따라 등록한 후 “개인정보수집 및 이용약관에 동의합니다.” 박스에 체크 후 확인 버튼을 클릭하시기 바랍니다. 단, 배포 파일명을 임의로 변경할 경우 자동 등록된 “설치 인증키”가 표시되지 않으므로 직접 입력해야 합니다.

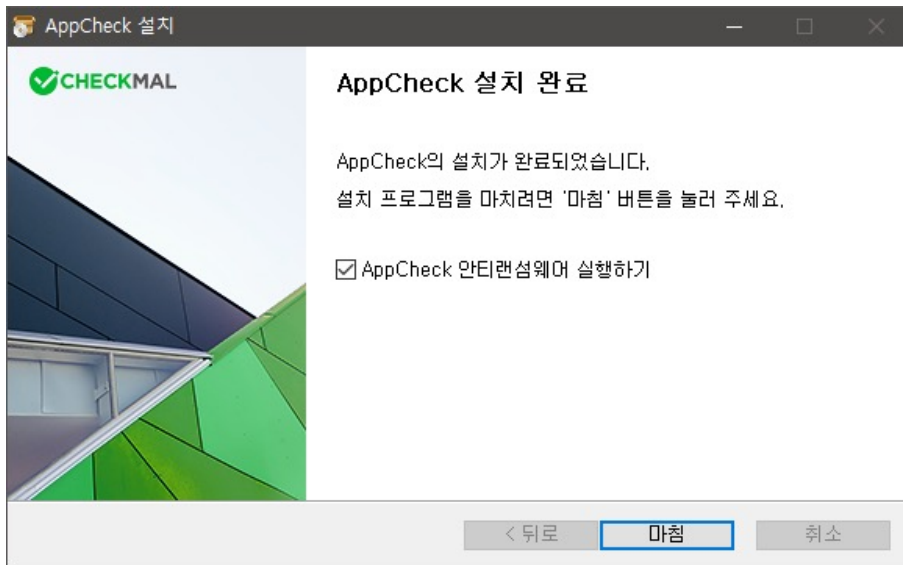
(2) ㈜체크멀 소프트웨어 사용권 계약서 내용에 확인 후 “동의함” 버튼을 클릭하시기 바랍니다.



(3) 앱체크는 “C:\WProgram Files\CheckMAL\WAppCheck” 기본 설치 폴더(32/64bit 공통)에 프로그램을 설치합니다.

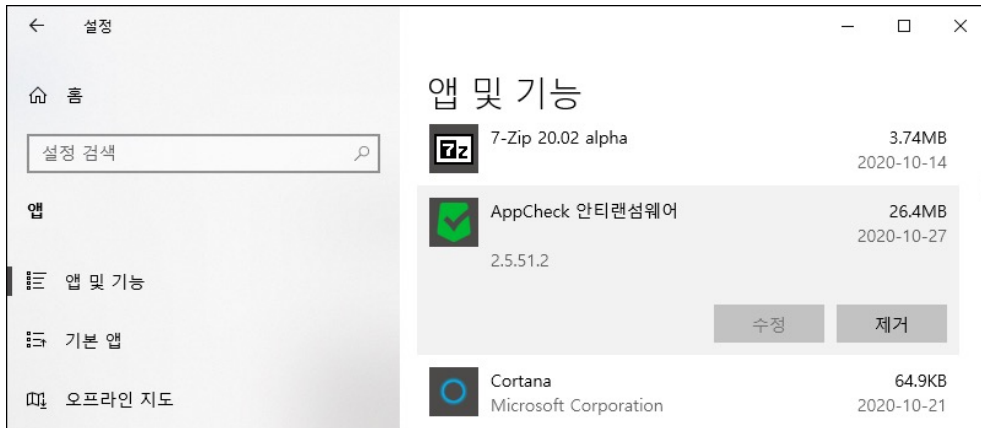


(4) 설치가 완료된 후 “마침” 버튼을 클릭하시면 AppCheck 안티랜섬웨어 프로그램이 자동 실행됩니다.

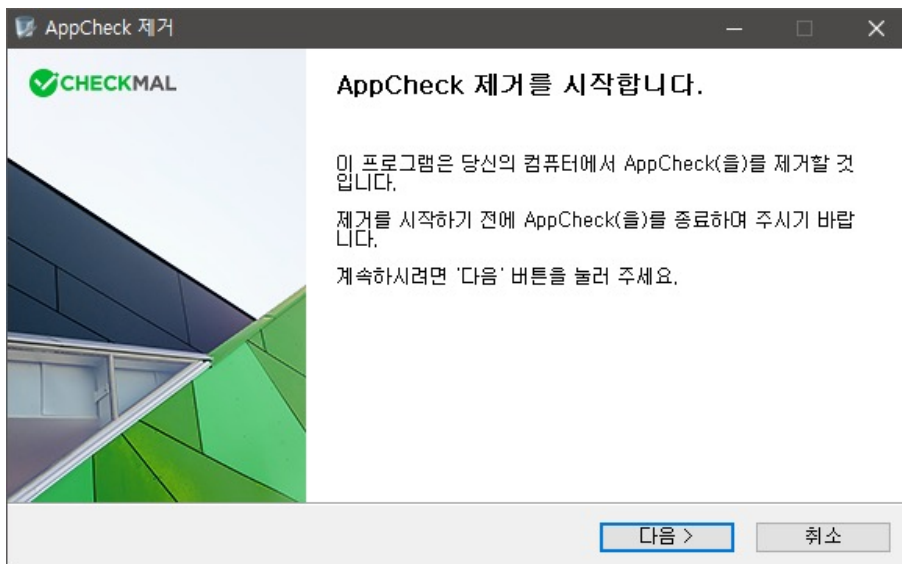


2. 제거하기

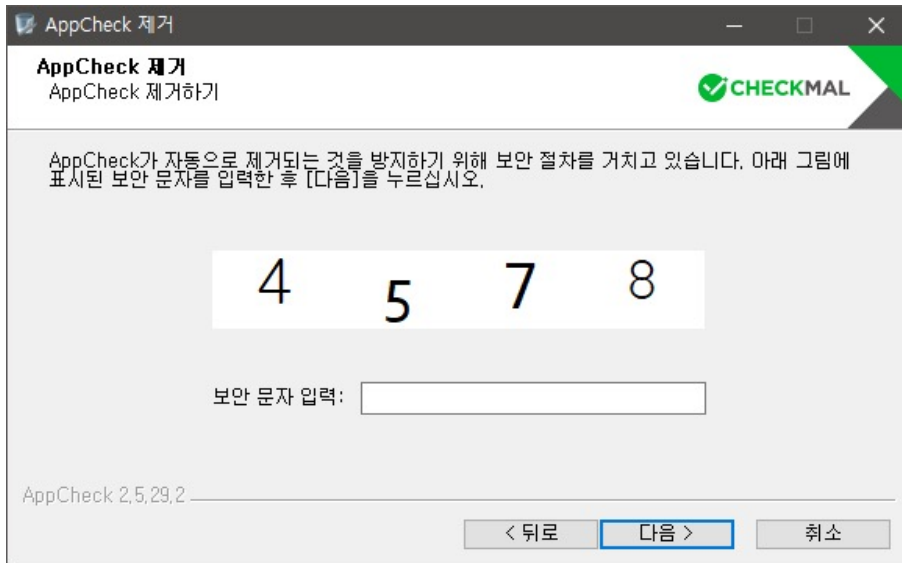
(1) 앱체크를 제거하기 위해서는 제어판의 “프로그램 및 기능” 또는 설정의 “앱 및 기능”에 등록된 “AppCheck 안티랜섬웨어” 항목을 찾아 제거 버튼을 클릭하시기 바랍니다.



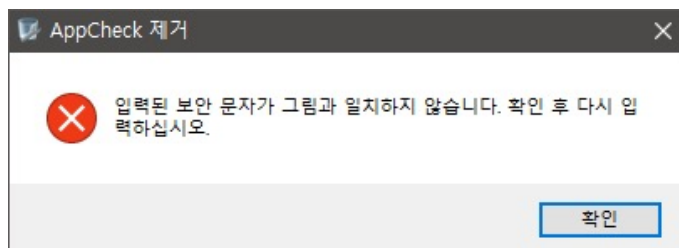
(2) 프로그램 제거를 위한 “AppCheck 제거를 시작합니다.” 화면에서 다음 버튼을 클릭하시기 바랍니다.



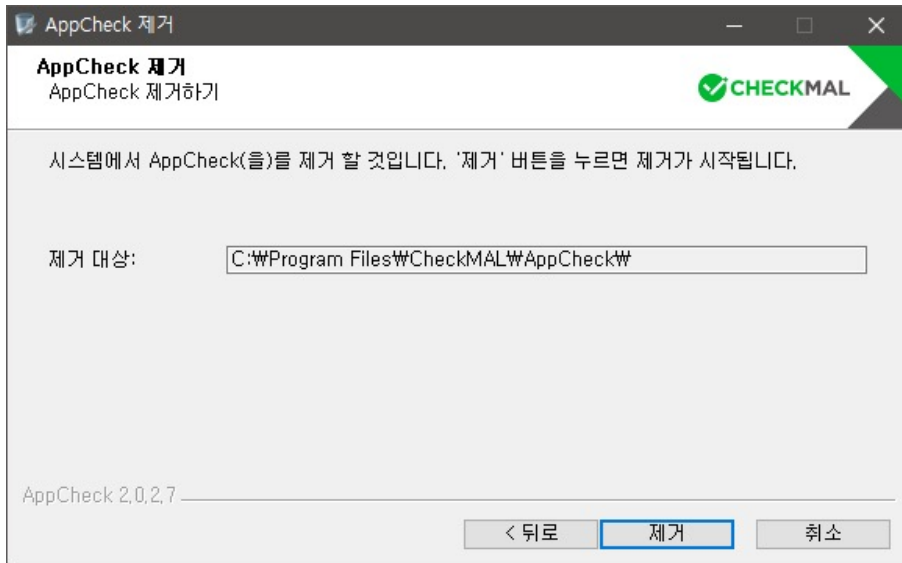
(3) 앱체크가 자동으로 제거되는 것을 방지하기 위한 보안 문자(CAPTCHA)를 확인하여 “보안 문자 입력” 영역에 입력하신 후 “다음” 버튼을 클릭하시기 바랍니다.



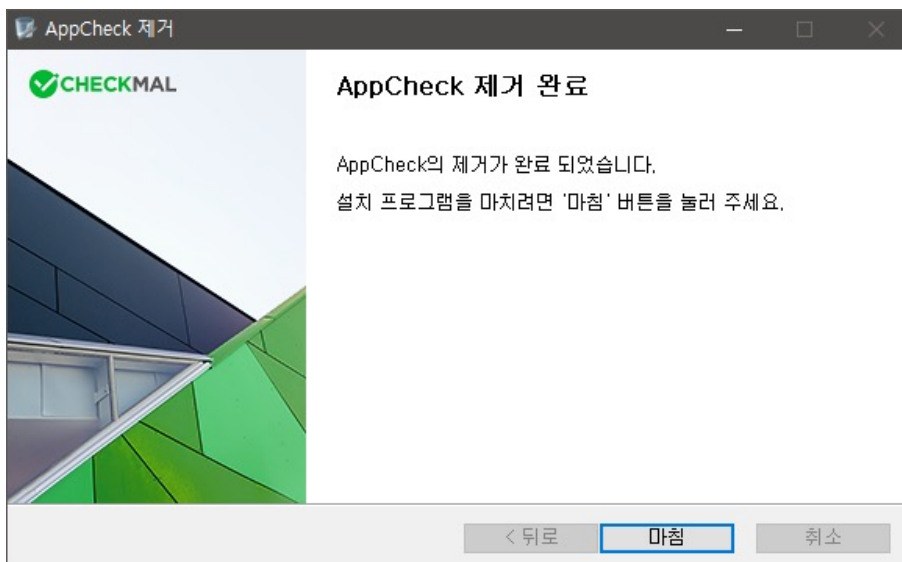
만약 잘못된 보안 문자를 입력할 경우 “입력된 보안 문자가 그림과 일치하지 않습니다. 확인 후 다시 입력하십시오.” 메시지 창이 생성되므로 확인 후 다시 입력하시기 바랍니다.



(4) 시스템에서 앱체크를 제거하기 위해서는 “제거” 버튼을 클릭하시기 바랍니다.

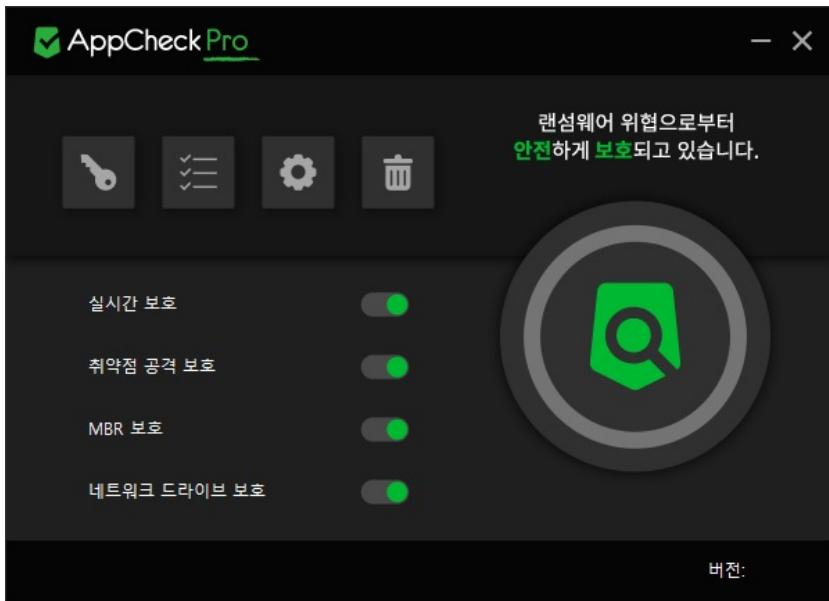


(5) 앱체크 제거가 완료된 후에는 “마침” 버튼을 클릭하시면 프로그램 제거가 종료되며, 시스템 환경에 따라서는 재부팅을 요구할 수 있습니다.



3. 메뉴 구성

① 메인 화면 메뉴 구성



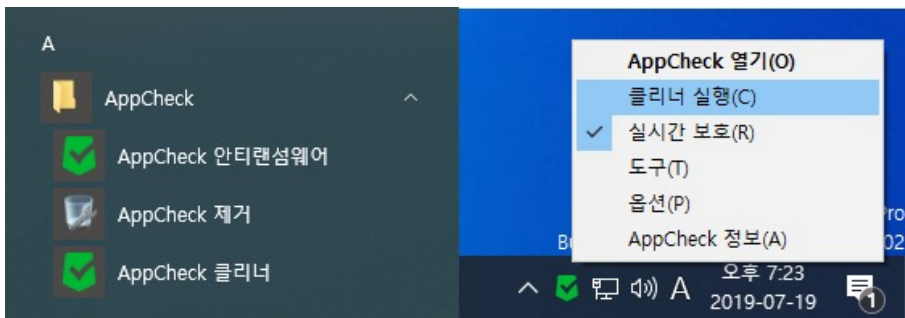
	정품 등록	AppCheck Pro 온라인 정품 등록 메뉴입니다.
	도구	AppCheck 도구(위협 로그, 일반 로그, 검역소) 메뉴입니다.
	옵션	AppCheck 옵션 (일반, 랜섬 가드, 취약점 가드, 대피소, 클리너, 자동 백업, 사용자 신뢰 파일, SMB 허용/차단 목록) 메뉴입니다.
	랜섬웨어 대피소 비우기	랜섬웨어 대피소(AppCheck 옵션 - 대피소 경로 참조) 폴더 삭제 메뉴입니다.

◎ **실시간 보호** : 랜섬웨어 행위 차단, 취약점 공격 보호, MBR 보호, 네트워크 드라이브 보호, 랜섬웨어 대피소 폴더 및 자동 백업(AutoBackup(AppCheck)) 폴더 보호 기능 (비)활성화 메뉴입니다.

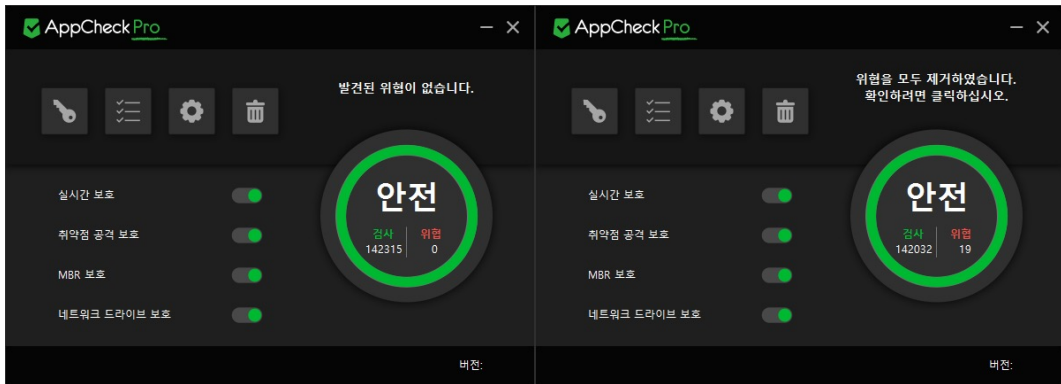
- ◎ **취약점 공격 보호** : 보호할 응용 프로그램(웹 브라우저, 플러그인, 미디어 재생기, 오피스)의 버그(Bug)를 통해 실행되는 취약점 코드를 차단하는 (비)활성화 메뉴입니다.
- ◎ **MBR 보호** : Master Boot Record (MBR)과 GUID Partition Table (GPT) 영역의 변조를 시도하는 파일 실행 차단 (비)활성화 메뉴입니다.
- ◎ **네트워크 드라이브 보호** : 네트워크 드라이브를 통해 연결된 공유 폴더에 존재하는 파일 암호화 시 차단 (비)활성화 메뉴입니다. (AppCheck Pro 전용)
- ◎ **클리너** : 변조된 시스템 검사, 네트워크 환경 검사, 악성 프로그램 제거, 광고 프로그램 제거, 브라우저 확장 프로그램 제거, 바로가기 파일 내 악성 URL 제거, 랜섬웨어 노트 제거, 임시 파일/폴더 제거 기능입니다.

[1-1] 클리너

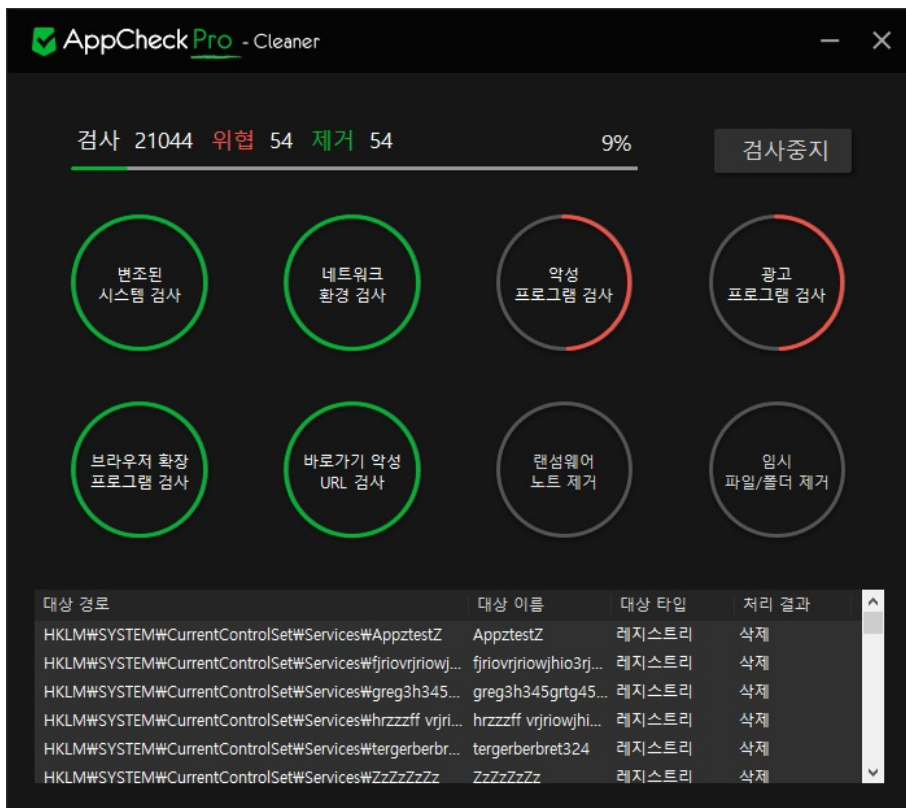
클리너 기능은 변조된 시스템 검사, 네트워크 환경 검사, 악성 프로그램 제거, 광고 프로그램 제거, 브라우저 확장 프로그램 제거, 바로가기 파일 내 악성 URL 제거, 랜섬웨어 노트 제거, 임시 파일/폴더 제거 기능을 통해 시스템에 설치된 악성코드 및 광고 프로그램 제거와 임시 파일/폴더 삭제 기능을 제공합니다.



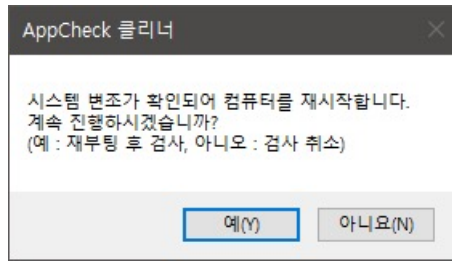
클리너 실행을 위해서는 앱체크 메인 화면의 클리너 버튼, 프로그램 목록의 “AppCheck 클리너” 또는 작업 표시줄 알림 영역의 앱체크 메뉴에서 제공하는 “클리너 실행” 메뉴를 통해 실행할 수 있습니다.



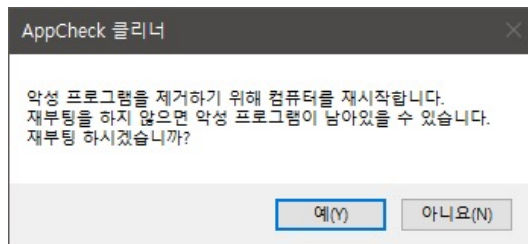
앱체크 메인 화면에서 제공하는 클리너 버튼에서는 검사 완료 시 위협 요소 여부에 따라 “발견된 위협이 없습니다.” 또는 “위협을 모두 제거하였습니다. 확인하려면 클릭하십시오.” 메시지를 표시합니다.



클리너 검사 중 앱체크 메인 화면의 클리너 버튼을 클릭할 경우 클리너 검사창이 추가 생성되어 각 검사 항목 및 세부적인 탐지 내역과 처리 결과를 확인할 수 있습니다.



변조된 시스템 검사 항목에서 탐지가 이루어질 경우에는 “시스템 번조가 확인되어 컴퓨터를 재시작합니다. 계속 진행하시겠습니까? (예 : 재부팅 후 검사, 아니오 : 검사 취소)” 메시지 창을 생성하여 재부팅 후 자동 재검사가 진행됩니다.



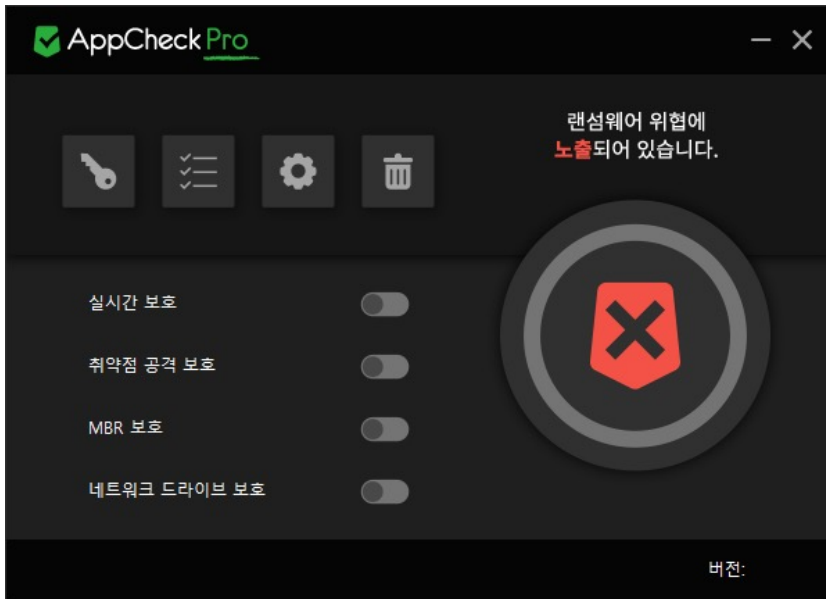
클리너 검사 중 “재부팅 후 삭제” 처리 항목이 존재할 경우에는 검사 완료 단계에서 “악성 프로그램을 제거하기 위해 컴퓨터를 재시작합니다. 재부팅을 하지 않으면 악성 프로그램이 남아있을 수 있습니다. 재부팅 하시겠습니까?” 메시지 창을 생성하여 재부팅을 통해 탐지된 악성 프로그램을 제거할 수 있습니다.



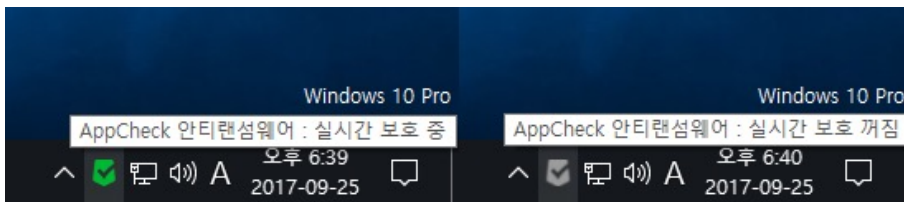
클리너 검사를 통해 탐지 및 제거된 세부적인 정보는 AppCheck 도구의 위협 로그에서 확인할 수 있으며, 제거된 항목 중 복원을 원하는 경우에는 검역소에 백업된 항목을 찾아 복원할 수 있습니다.

[1-2] 실시간 보호

실시간 보호는 랜섬웨어 행위 차단, 취약점 공격 보호, MBR 보호, 네트워크 드라이브 보호, 랜섬웨어 대피소 (C:\ProgramData\CheckMAL\AppCheck\RansomShelter) 폴더 및 자동 백업(AutoBackup(AppCheck)) 폴더 보호 (비) 활성화 기능을 제공합니다.



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

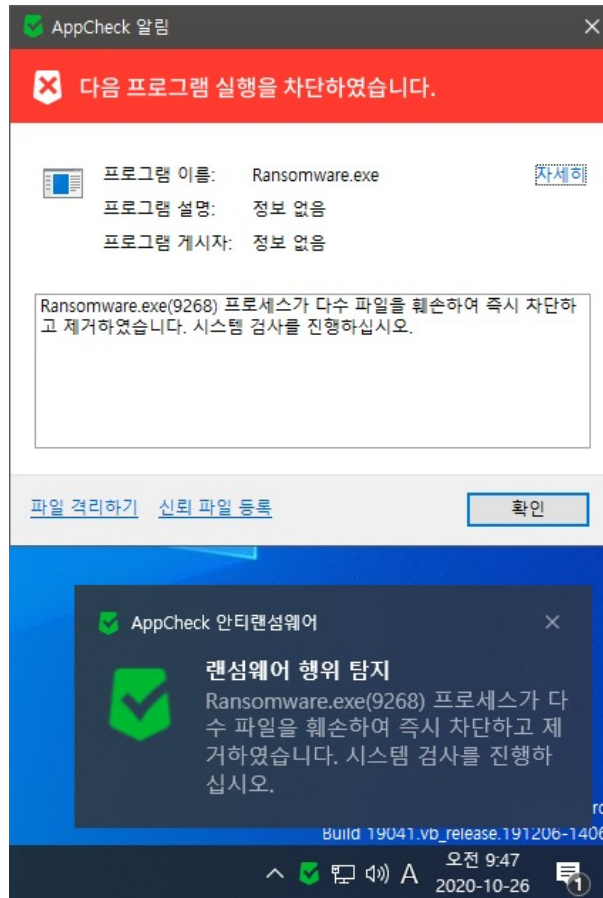


● **녹색 아이콘** : 실시간 보호 중

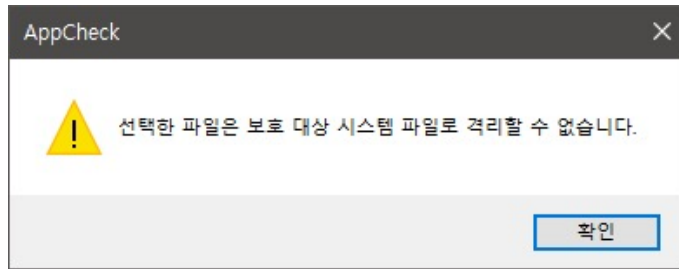
● **회색 아이콘** : 실시간 보호 꺼짐

실시간 보호는 랜섬 가드 또는 취약점 가드 보호 기능을 통해 랜섬웨어(Ransomware) 또는 취약점(Exploit) 코드가 실행될 경우 작업 표시줄 알림 영역에 “랜섬웨어 행위 탐지” 또는 “취약점 공격 탐지” 알림창을 생성합니다.

사용자가 생성된 랜섬웨어 행위 탐지 알림창을 클릭할 경우 “다음 프로그램 실행을 차단하였습니다.” 알림창 생성을 통해 차단된 프로그램 정보 및 세부적인 옵션을 제공합니다.

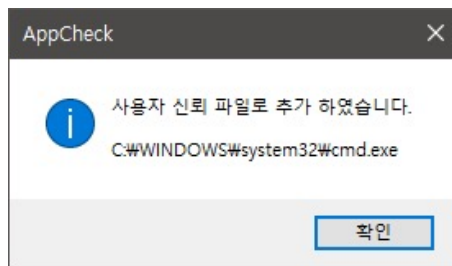


- ◎ **자세히** : AppCheck 도구 메뉴의 위험 로그, 일반 로그, 검역소 정보를 확인할 수 있습니다.
- ◎ **파일 격리하기** : 랜섬웨어 행위 탐지를 통해 차단된 파일을 검역소로 격리(삭제)하여 더 이상 실행되지 않도록 합니다. 단, 시스템 파일과 디지털 서명이 포함된 파일은 차단만 지원합니다.

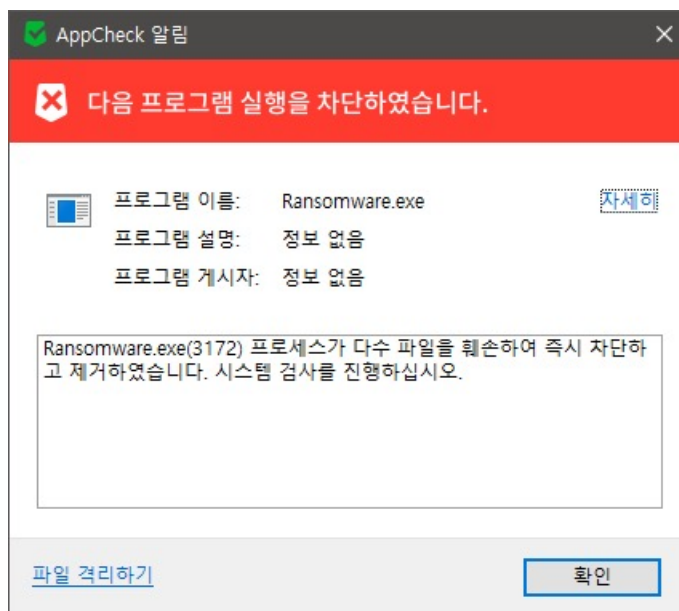


랜섬웨어 행위 탐지를 통해 차단된 파일을 사용자가 “파일 격리하기”를 선택할 경우 보호 대상 시스템 파일인 경우 “선택한 파일은 보호 대상 시스템 파일로 격리할 수 없습니다.” 메시지 창이 생성됩니다.

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



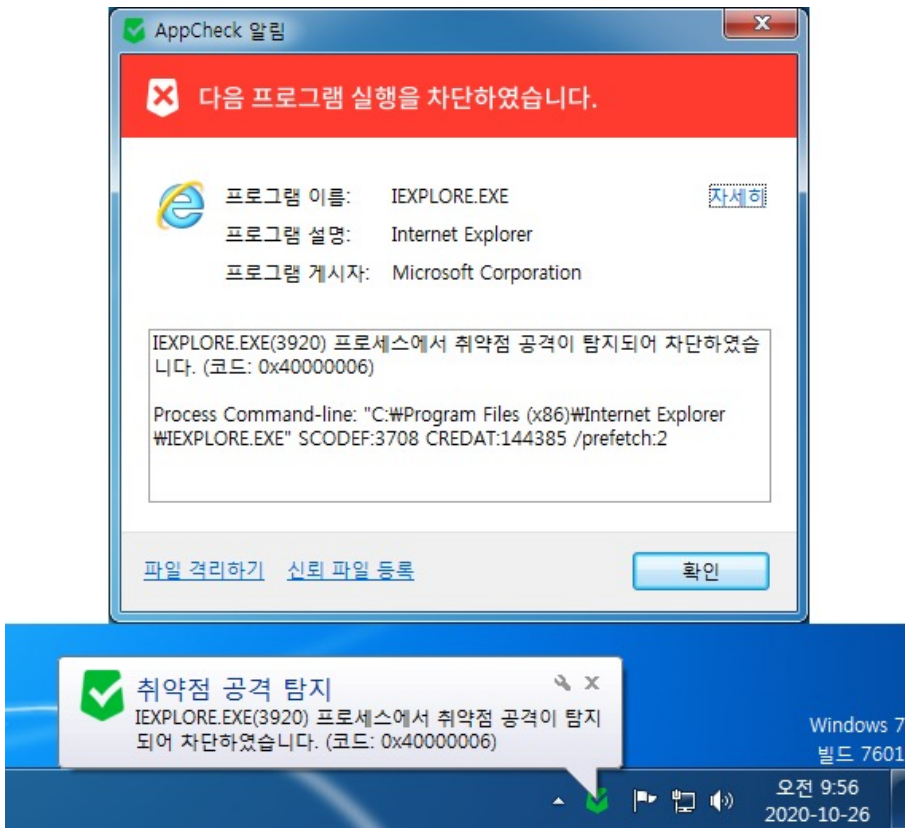
만약 “잠금 설정 사용” 또는 CMS 정책을 통해 “Lock Mode” 환경인 경우에는 랜섬웨어 행위 탐지를 통한 AppCheck 알림창에서 “신뢰 파일 등록” 메뉴가 표시되지 않습니다.



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

[1-3] 취약점 공격 보호

취약점 공격 보호 기능은 취약점 가드를 통해 보호할 응용 프로그램(웹 브라우저, 플러그인, 미디어 재생기, 오피스)의 버그(Bug)를 통해 취약점 코드가 실행되어 악성코드 자동 감염이 발생하는 것을 차단합니다.

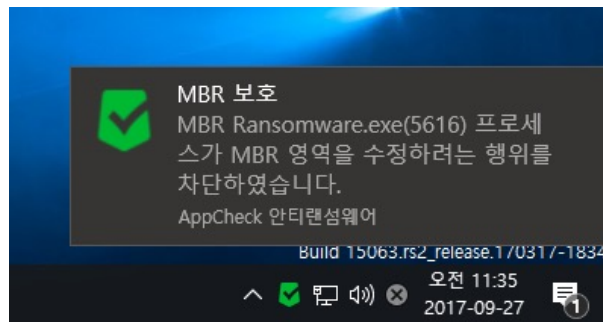


웹 브라우저 사용 중에 발생하는 취약점 공격 탐지가 발생할 경우 알림창을 통해 프로세스 커맨드라인(Process Command-line), 타겟 커맨드라인(Target Command-line), 유포 URL(Distribution URL), 경유 URL(Referrer URL), 취약점 URL(Exploit URL) 정보를 확인할 수 있습니다.

취약점 공격 탐지가 발생한 PC에서는 Windows, 웹 브라우저, 플러그인, 미디어 재생기, 오피스 프로그램에 대한 최신 보안 업데이트를 확인하여 구버전인 경우에는 최신 버전으로 업데이트하시기 바랍니다.

[1-4] MBR 보호

MBR 보호 기능은 Master Boot Record (MBR) 영역을 훼손하여 Windows 부팅을 방해하는 랜섬웨어를 비롯한 악성코드 행위 시 차단을 통해 MBR 영역을 보호할 수 있습니다.



MBR 보호 기능을 통해 차단되는 파일은 삭제하지 않으며 차단만 이루어집니다.

[1-5] 네트워크 드라이브 보호

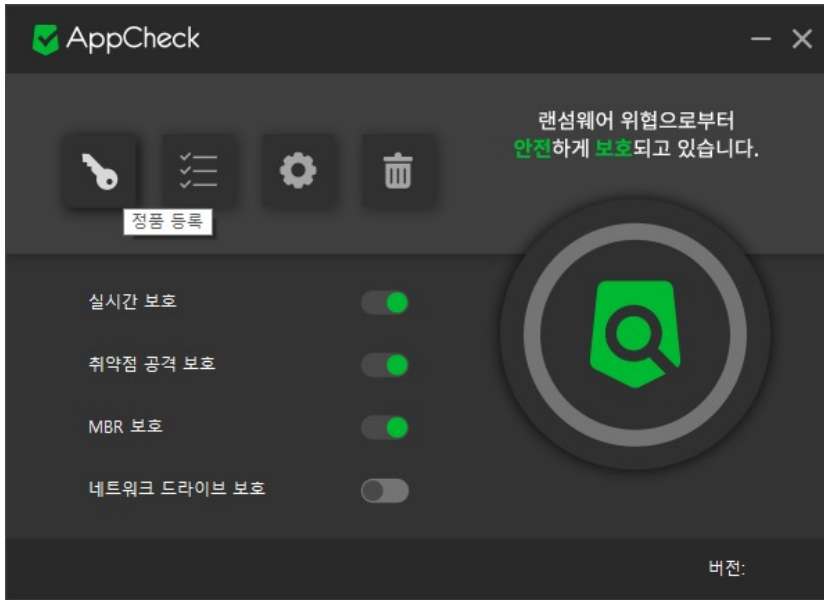
AppCheck Pro 정품 버전에서 제공하는 네트워크 드라이브 보호 기능은 앱체크(AppCheck)가 설치된 PC와 네트워크 드라이브를 통해 연결된 공유 폴더에 존재하는 파일이 앱체크가 설치된 PC에서 실행된 랜섬웨어(Ransomware)에 의해 공유 폴더 내 파일이 암호화 될 경우 “랜섬웨어 행위 탐지” 알림창을 통해 차단(제거) 및 차단 이전에 일부 훼손된 파일을 자동 복원합니다.

네트워크 드라이브 보호 기능은 SMB 서버 보호 기능과 달리 앱체크가 설치된 PC에서 실행된 랜섬웨어(Ransomware)가 네트워크 드라이브(공유 폴더) 영역에 존재하는 파일에 대한 암호화 시 차단하는 기능입니다.

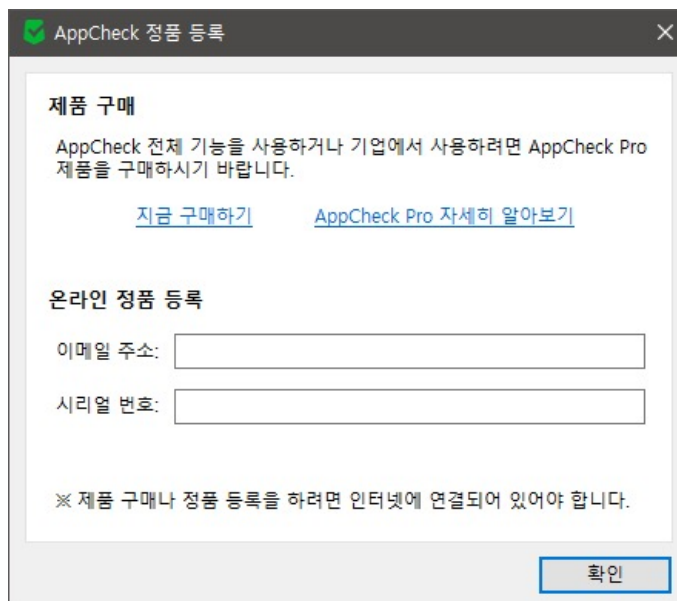
그러므로 네트워크 드라이브 보호 기능을 비활성화한 경우에는 SMB 보호 옵션이 체크되어 있다면 SMB 보호(IP 차단) 기능은 동작합니다.

[1-5] 정품 등록

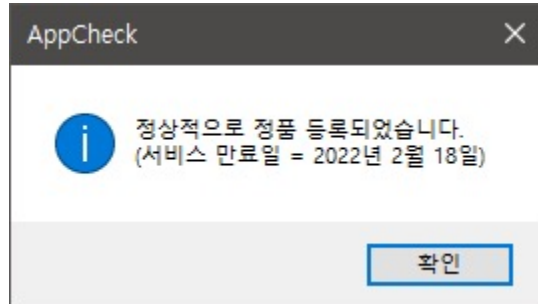
AppCheck 안티랜섬웨어 개인 사용자용 무료 버전은 랜섬가드 기능 일부(AppCheck Pro 확장 기능)와 자동 백업 기능을 사용할 수 없으며, 기업/관공서 및 기능 제한없이 사용을 원하시는 개인 사용자는 AppCheck Pro 정품 버전을 구매해야 합니다.



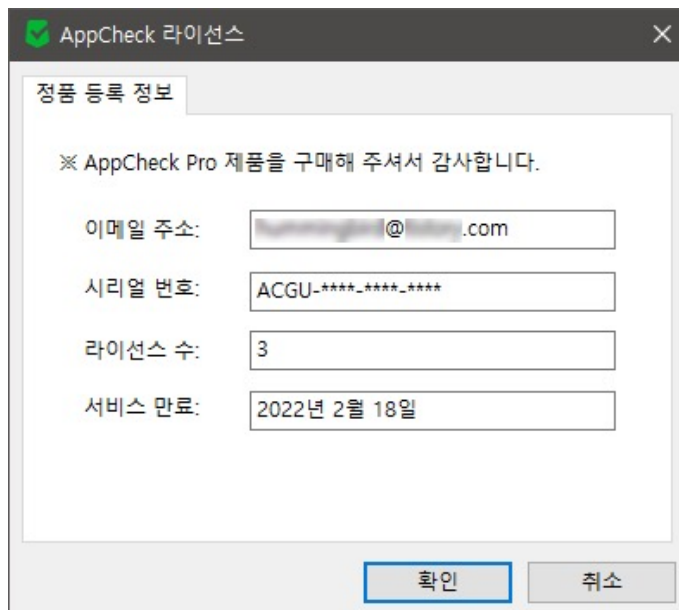
AppCheck Pro 라이선스를 구입하신 후 정품 등록을 위해서는 앱체크 메인 화면의 “정품 등록” 버튼(열쇠 모양 아이콘)을 클릭하여 온라인 정품 등록을 진행하시기 바랍니다.



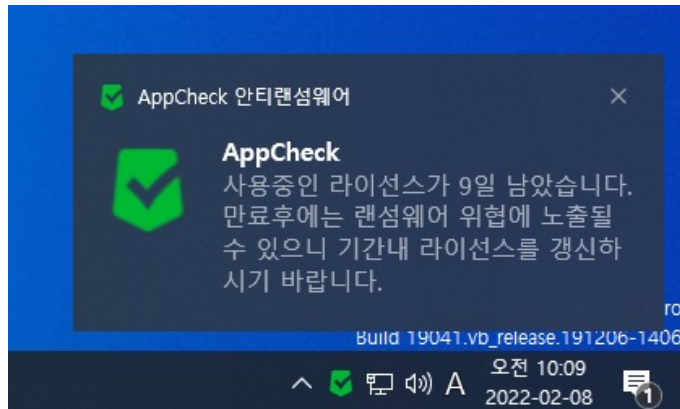
온라인 정품 등록을 위해서는 반드시 인터넷이 연결되어 있어야하며, 라이선스 주문 시 입력한 이메일 주소와 제공받은 시리얼 번호를 입력 후 “확인” 버튼을 클릭하시면 정품 등록이 이루어집니다.



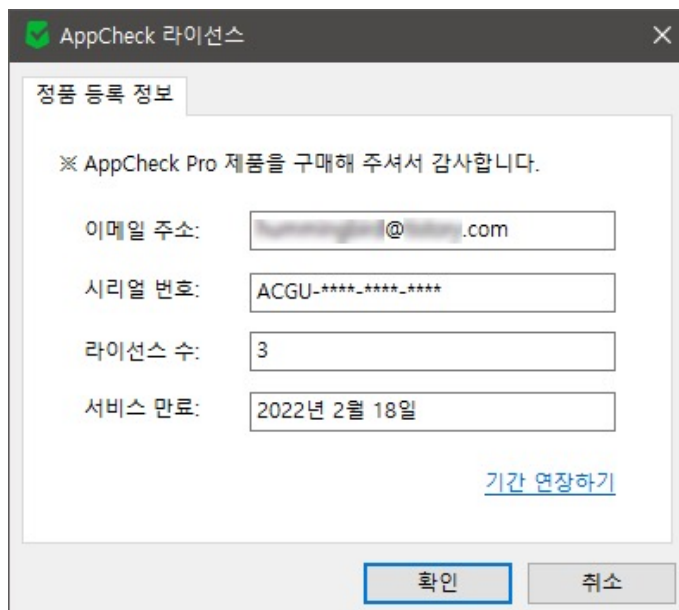
입력한 정보가 유효할 경우 “정상적으로 정품 등록되었습니다.” 메시지를 통해 서비스 만료일을 안내합니다.



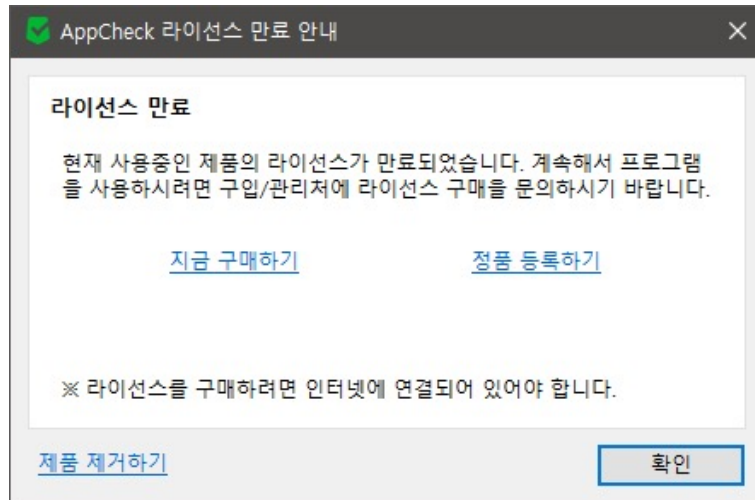
이후 등록된 AppCheck 라이선스 정품 등록 정보(이메일 주소, 시리얼 번호, 라이선스 수, 서비스 만료일)를 표시합니다.



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



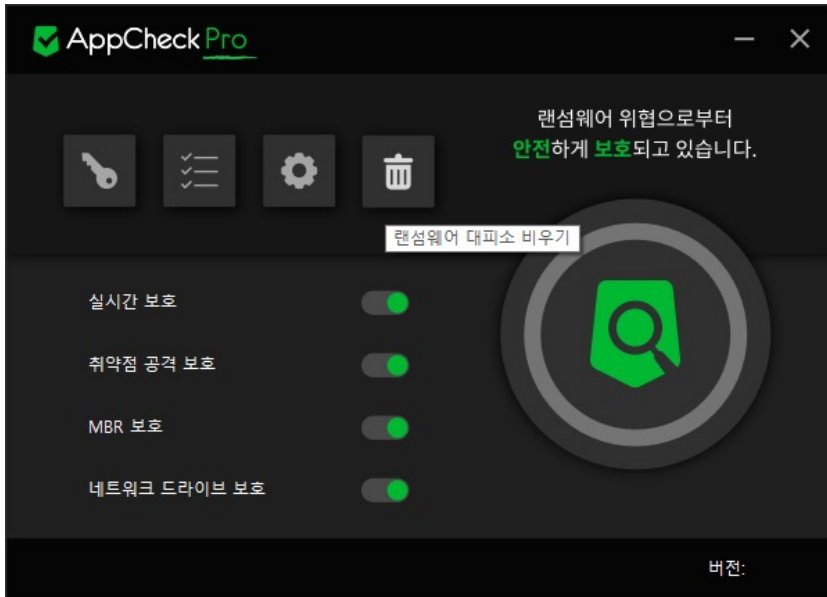
AppCheck 라이선스 만료 이전에 갱신을 위해서는 “기간 연장하기” 버튼을 클릭할 경우 AppCheck Pro 재구매 페이지로 연결되어 할인된 가격으로 라이선스 재구매를 진행할 수 있습니다.



AppCheck 라이선스 기간이 만료된 후에는 모든 기능이 종료되며 제품 클릭 시 "AppCheck 라이선스 만료 안내" 메시지를 통해 프로그램을 계속 사용하기 위한 "지금 구매하기", "정품 등록하기"와 프로그램 삭제를 위한 "제품 제거하기"를 선택할 수 있도록 안내합니다.

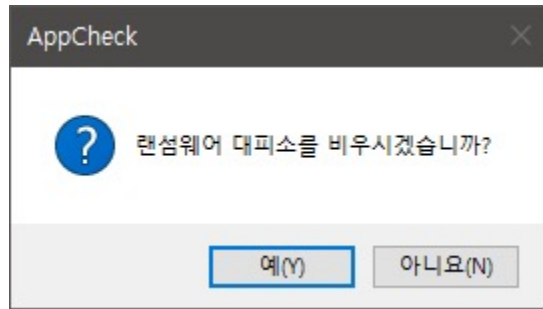
[1-7] 랜섬웨어 대피소 비우기

랜섬웨어 대피소 기능은 보호할 파일 확장명이 특정 조건에 따라 생성/변경/삭제 행위가 발생할 경우 해당 파일이 위치한 드라이브에 랜섬웨어 대피소(C:\ProgramData\CheckMAL\AppCheck\RansomShelter) 폴더를 생성하여 최대 7일 동안 임시 백업된 후 기간 경과 시 자동 삭제됩니다.



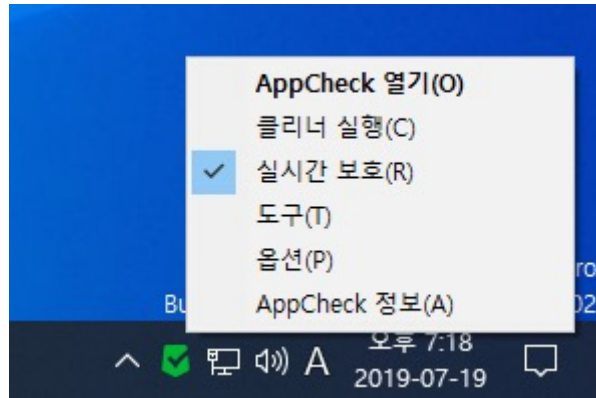
만약 랜섬웨어(Ransomware)에 의해 파일 암호화가 진행될 경우 랜섬웨어 대피소 폴더에 원본 파일이 임시 백업되며 랜섬웨어 행위 탐지와 동시에 롤백(Rollback) 기능을 통해 임시 백업된 원본 파일을 이용하여 일부 훼손된 파일을 자동 복원합니다.

이런 용도로 생성된 랜섬웨어 대피소 폴더는 실시간 보호 기능을 통해 보호되며 사용자가 디스크 용량 등의 이유로 랜섬웨어 대피소 폴더 자체를 삭제하기 위해서는 앱체크 메인 화면에 위치한 “랜섬웨어 대피소 비우기” 버튼(휴지통 아이콘)을 클릭하시면 랜섬웨어 대피소 폴더를 삭제할 수 있습니다.



참고로 삭제된 랜섬웨어 대피소 폴더 및 내부 파일은 휴지통으로 이동되지 않고 완전 삭제가 이루어지며, 만약 권한 문제로 랜섬웨어 대피소 비우기 기능을 통해 삭제되지 않는 경우에는 앱체크 실시간 보호 기능을 비활성화(OFF)하신 후 폴더를 찾아 직접 삭제하시기 바랍니다.

② 작업 표시줄 알림 영역의 앱체크 메뉴 구성



◎ **AppCheck 열기** : 앱체크 메인 화면 실행

◎ **클리너 실행** : 변조된 시스템 검사, 네트워크 환경 검사, 악성 프로그램 제거, 광고 프로그램 제거, 브라우저 확장 프로그램 제거, 바로가기 파일 내 악성 URL 제거, 랜섬웨어 노트 제거, 임시 파일/폴더 제거 기능을 위한 클리너 검사창 실행

◎ **실시간 보호** : 랜섬웨어 행위 차단, 취약점 공격 보호, MBR 보호, 네트워크 드라이브 보호, 랜섬웨어 대피소(C:\ProgramData\CheckMAL\AppCheck\RansomShelter) 폴더 및 자동 백업(AutoBackup(AppCheck)) 폴더 보호 기능 (비)활성화 기능

◎ **도구** : 위협 로그, 일반 로그, 검역소 정보 확인

◎ **옵션** : 일반, 랜섬 가드, 취약점 가드, 대피소, 클리너, 자동 백업, 사용자 신뢰 파일, SMB 허용/차단 목록 설정

◎ **AppCheck 정보** : 앱체크 버전, 수동 업데이트 확인, 저작권 및 라이선스 안내, 정품 등록 정보 표시

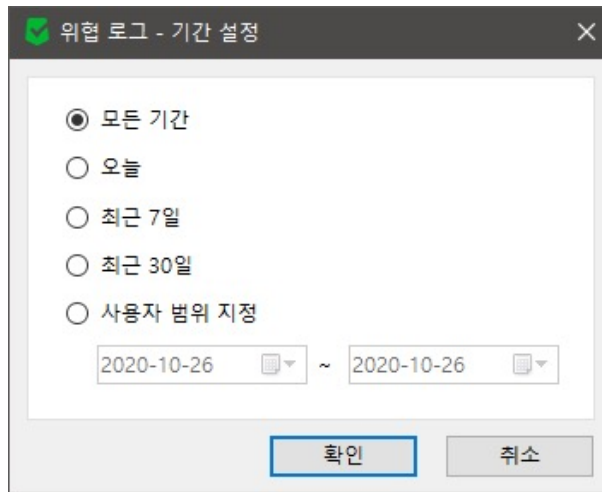
[2-1] 도구

AppCheck 도구는 위험 로그, 일반 로그, 검역소 정보를 세부적으로 제공되며, 기록된 로그의 누적량이 일정 수준 초과할 경우 자동으로 오래된 기록부터 자동 정리됩니다.

AppCheck 도구의 위험 로그, 검역소 칼럼(Column)에서는 MD5값을 추가적으로 확인할 수 있는 항목이 포함되어 있으므로 체크할 경우 Hash값을 확인할 수 있습니다.

◆ AppCheck 도구 : 위험 로그


위험 로그는 랜섬 가드(랜섬웨어 행위 탐지), 취약점 가드(취약점 공격 탐지), 클리너 검사를 통해 처리된 파일에 대한 처리 내역(차단, 제거, 복원, 제거 실패) 정보를 표시합니다.



기간 설정에서는 위험 로그에 기록된 로그를 특정 기간(모든 기간, 오늘, 최근 7일, 최근 30일, 사용자 범위 지정)에 따라 필터링하여 표시할 수 있습니다.

날짜	탐지 주제	위험	종류	대상 경로	처리	MD5
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_1.doc	복원	62e383d87
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_1.doc.[1CC28B51].[paybtcfork...	제거	caf7afa035
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_1.doc	복원	62e383d87
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_2.hwp	복원	c94f8f1a74
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_2.hwp.[1CC28B51].[paybtcfork...	제거	46cf2f84f4
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_2.hwp	복원	c94f8f1a74
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_3.pdf	복원	8c7d7187e
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_3.pdf.[1CC28B51].[paybtcfork...	제거	be06117bc
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_3.pdf	복원	8c7d7187e
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_4.ppt	복원	baa4b2c9d
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_4.ppt.[1CC28B51].[paybtcfork...	제거	cb75d3ebt

- ◎ **차단** : 랜섬웨어 행위 탐지 또는 MBR 차단으로 탐지된 프로세스(파일), 취약점 공격 탐지를 통해 탐지된 프로세스 및 주소(URL) 연결을 차단합니다.
- ◎ **제거** : 랜섬웨어 행위 탐지 파일 및 랜섬웨어에 의해 암호화된 파일 및 생성된 파일, 클리너를 통해 탐지된 파일 및 레지스트리를 자동 삭제합니다.
- ◎ **복원** : 랜섬웨어 대피소에 임시 백업된 원본 파일을 원래 위치로 복원합니다.
- ◎ **제거 실패** : 랜섬웨어 행위 탐지가 발생하여 제거해야 할 파일이 이미 삭제되어 없거나 파일을 특정 조건으로 제거하지 못하고 차단한 경우이며, 일반적으로 Windows 재부팅 시 자동 삭제 처리합니다.

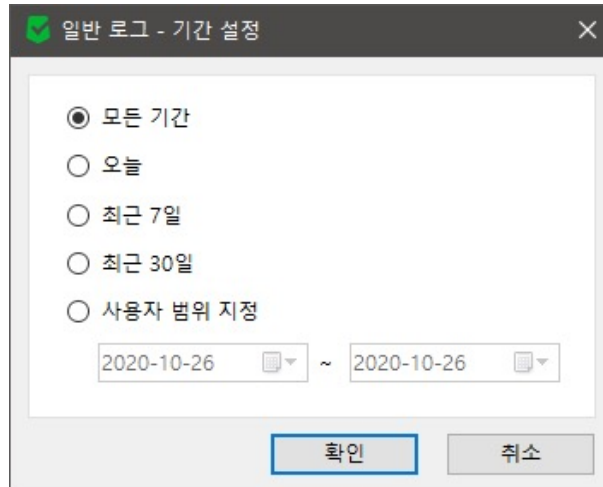


날짜	탐지 주제	위협	종류	대상 경로	처리	MD5
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_1.doc	복원	62e383d8f
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_3.pdf	복원	8c7d7187e
2020-10-27 오전 10:03:14	랜섬 가드	랜섬웨어 파일 생성	파일	D:\원본 폴더\원본 문서_4.ppt	제거	cb75d3ebt

- ◎ **파일 위치 열기** : Windows 탐색기를 이용하여 선택한 파일이 저장된 위치(대상 경로) 열기
- ◎ **복사** : 선택한 항목의 위협 로그 세부 정보 복사하기
- ◎ **모두 선택** : 위협 로그에 표시된 모든 항목 일괄 선택하기
- ◎ **새로 고침** : 위협 로그에 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, 랜섬 가드/취약점 가드 알림 메시지, 클리너 검사 등의 정보를 표시합니다.



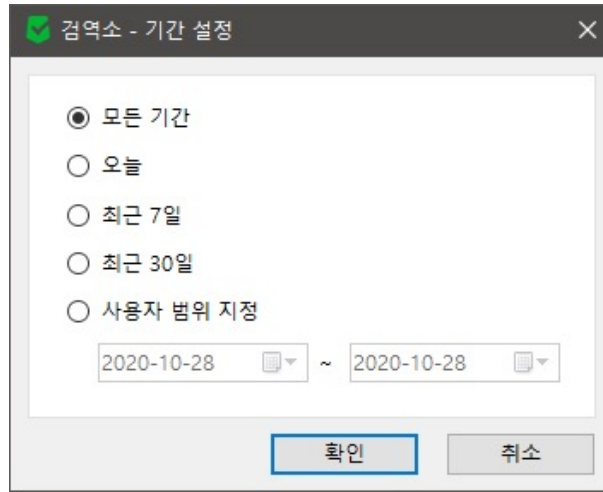
기간 설정에서는 일반 로그에 기록된 로그를 특정 기간(모든 기간, 오늘, 최근 7일, 최근 30일, 사용자 범위 지정)에 따라 필터링하여 표시할 수 있습니다.



- ◎ 복사 : 선택한 항목의 일반 로그 세부 정보 복사하기
- ◎ 모두 선택 : 일반 로그에 표시된 모든 항목 일괄 선택하기
- ◎ 새로 고침 : 일반 로그에 표시된 정보 갱신

◆ AppCheck 도구 : 검역소

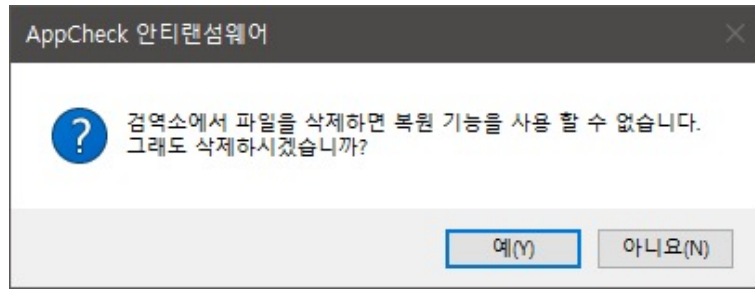
검역소는 랜섬웨어 행위 탐지 및 클리너 검사를 통해 삭제되어 검역소 폴더(C:\ProgramData\CheckMAL\AppCheck\Quarantine)에 백업된 파일 및 레지스트리 정보를 제공하며, 사용자가 필요에 의해 검역소에 백업된 항목에 대하여 복원할 수 있습니다.



기간 설정에서는 검역소에 기록된 로그를 특정 기간(모든 기간, 오늘, 최근 7일, 최근 30일, 사용자 범위 지정)에 따라 필터링하여 표시할 수 있습니다.



- ◎ **원래 위치로 복원** : 검역소에 백업된 선택 파일을 원래 위치(대상 경로)로 복원하기
- ◎ **지정 위치로 내보내기** : 검역소에 백업된 선택 파일을 사용자가 지정한 폴더로 내보내기
- ◎ **삭제** : 검역소에 백업된 파일 삭제하기



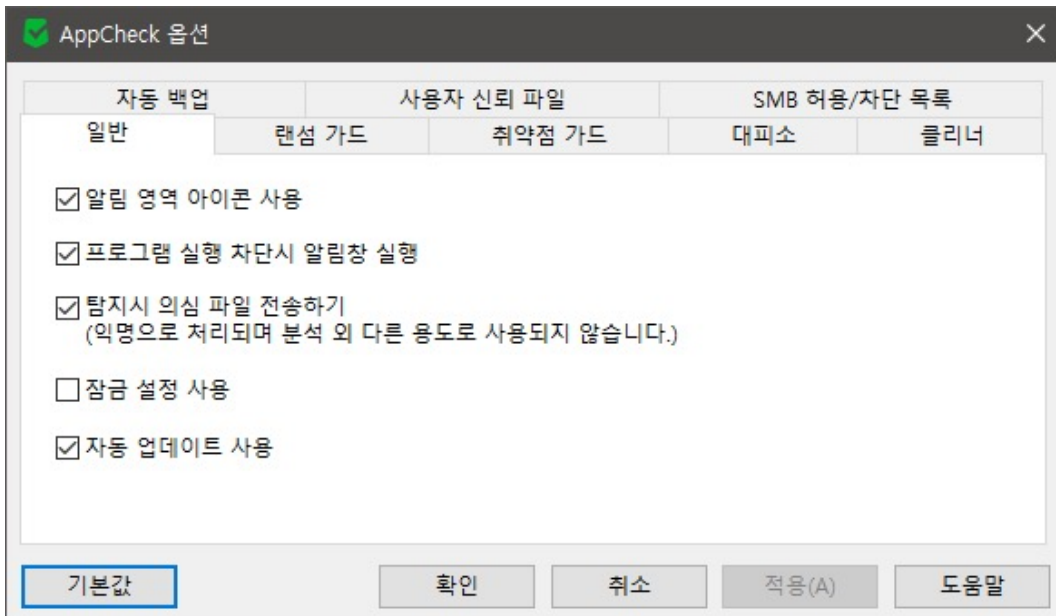
검역소 파일 삭제 시에는 “검역소에서 파일을 삭제하면 복원 기능을 사용 할 수 없습니다. 그래도 삭제하시겠습니까?” 메시지가 생성되며, 삭제된 파일은 휴지통으로 이동하지 않고 완전히 삭제 처리됩니다.

- **파일 위치 열기** : Windows 탐색기를 이용하여 선택한 파일이 존재했던 위치(대상 경로) 열기
- **복사** : 선택한 항목의 검역소 세부 정보 복사하기
- **모두 선택** : 검역소에 표시된 모든 항목 일괄 선택하기
- **새로 고침** : 검역소에 표시된 정보 갱신

[2-2] 옵션

AppCheck 옵션은 일반, 랜섬 가드, 취약점 가드, 대피소, 클리너, 자동 백업 (AppCheck Pro 전용), 사용자 신뢰 파일, SMB 허용/차단 목록(AppCheck Pro 전용) 설정을 제공합니다.

◆ AppCheck 옵션 : 일반



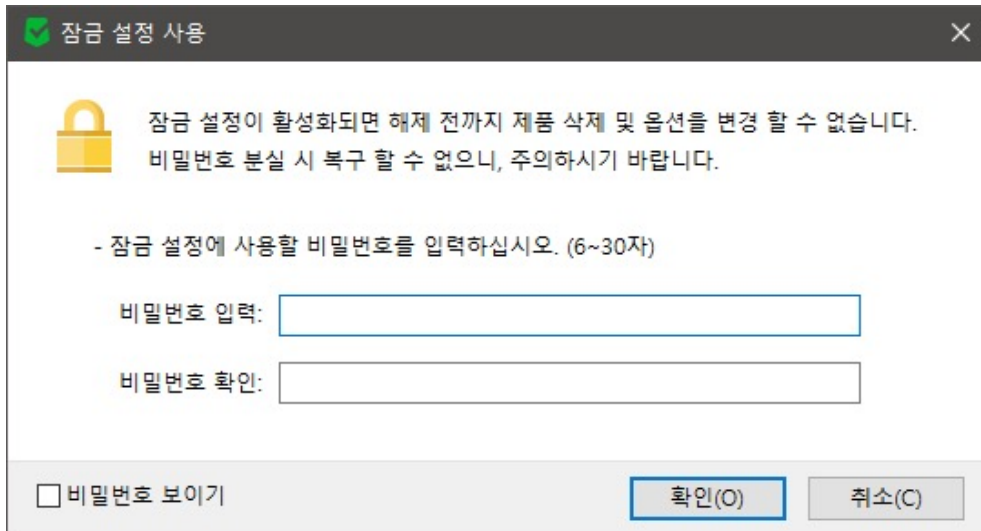
◎ 알림 영역 아이콘 사용 : 작업 표시줄 알림 영역에 앱체크 아이콘 표시

참고로 “알림 영역 아이콘 사용” 옵션이 체크된 경우 알림 영역에 표시된 앱체크 아이콘(AppCheck.exe)이 종료될 경우 최대 2분 이내에 자동으로 재실행합니다.

◎ 프로그램 실행 차단 시 알림창 실행 : 프로그램 실행 차단 시 작업 표시줄 알림 영역에 랜섬웨어 행위 탐지, MBR 보호, 취약점 공격 탐지 알림창 표시

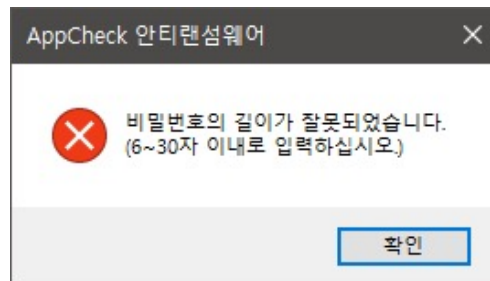
◎ 탐지 시 의심 파일 전송하기 (익명으로 처리되며 분석 외 다른 용도로 사용되지 않습니다.): 앱체크 이용 중 랜섬 가드, 취약점 가드, MBR 보호 기능으로 탐지되는 파일을 익명으로 체크말 서버로 전송

◎ 잠금 설정 사용 : 사용자가 입력한 비밀번호를 통해 앱체크 옵션, 실시간 보호, 앱체크 제거 기능을 변경하지 못하게 설정 (AppCheck Pro 전용, AppCheck CMS 버전은 Lock Mode 대체)

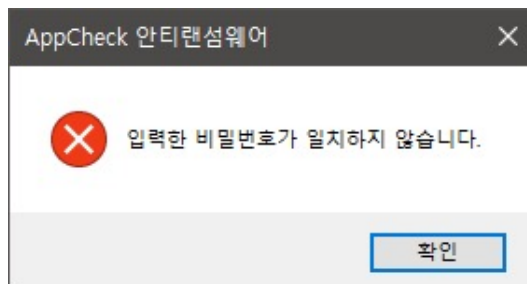


잠금 설정 사용에서는 잠금 설정이 활성화되면 해제 전까지 제품 삭제 및 옵션을 변경할 수 없으며, 비밀번호 분실 시 복구할 수 없다고 안내하고 있습니다.

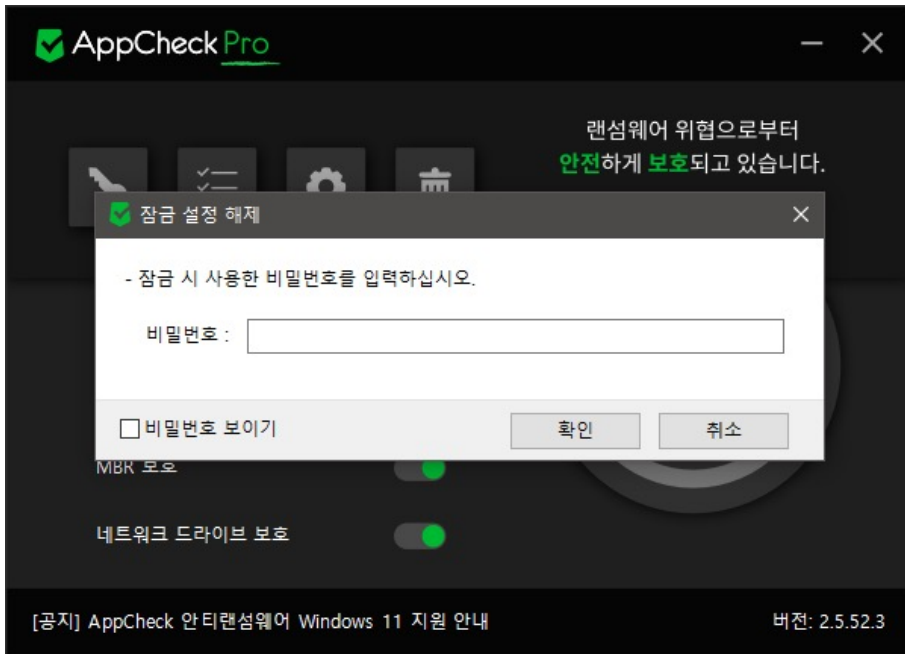
잠금 설정에 사용할 비밀번호는 6~30자 길이로 지정할 수 있으며, “비밀번호 보이기” 박스에 체크할 경우 입력한 비밀번호가 표시됩니다.



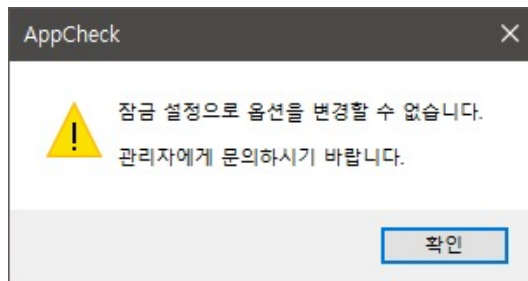
입력한 비밀번호가 조건에 만족하지 않을 경우 “비밀번호의 길이가 잘못되었습니다. (6~30자 이내로 입력하십시오.)” 알림창이 생성됩니다.



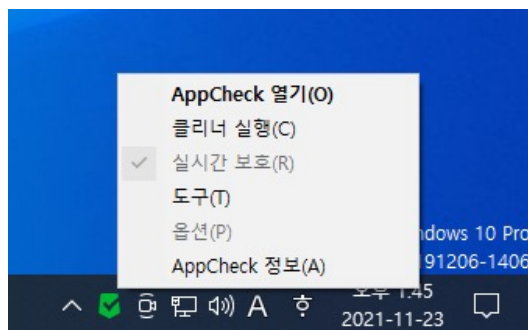
입력한 비밀번호가 틀린 경우 “입력한 비밀번호가 일치하지 않습니다.” 알림창이 생성됩니다.



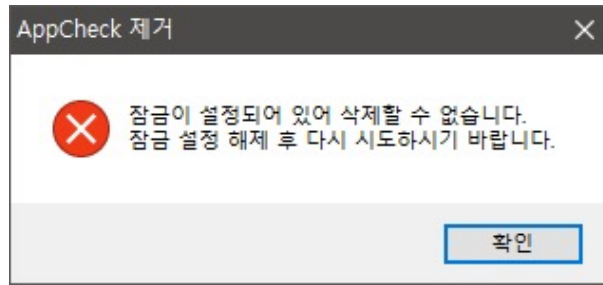
잠금 설정이 적용된 환경에서는 AppCheck 옵션 메뉴 접근 시 “잠금 설정 해제” 창을 생성하여 잠금 시 사용한 비밀번호를 입력해야 합니다.



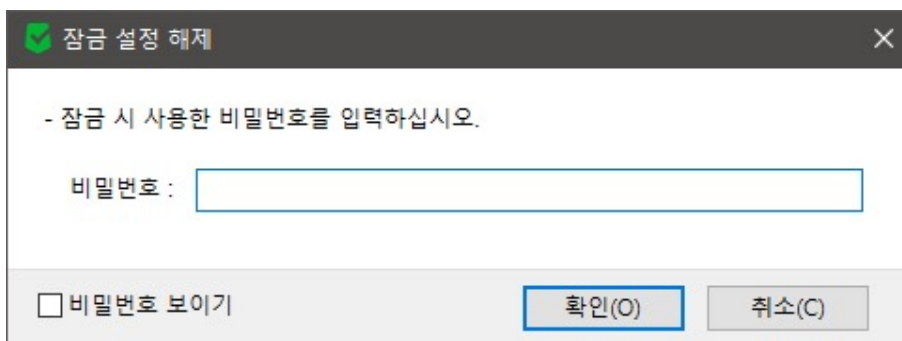
만약 CMS 정책을 통한 Lock Mode가 적용된 환경에서는 AppCheck 옵션 메뉴 접근 시 “잠금 설정으로 옵션을 변경할 수 없습니다. 관리자에게 문의하시기 바랍니다.” 안내창이 생성됩니다.



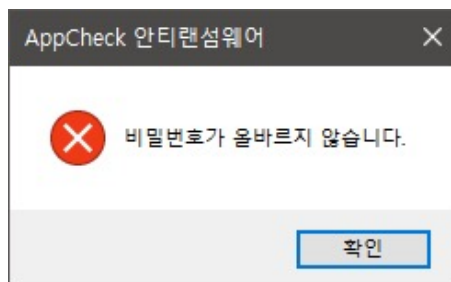
잠금 설정 또는 Lock Mode가 적용된 경우 앱체크 알림 아이콘의 메뉴 중 실시간 보호, 옵션 메뉴는 자동으로 비활성화 처리됩니다.



잠금 설정이 이루어진 환경에서 앱체크 제거를 시도할 경우 “잠금이 설정되어 있어 삭제할 수 없습니다. 잠금 설정 해제 후 다시 시도하시기 바랍니다.” 알림창이 생성됩니다.



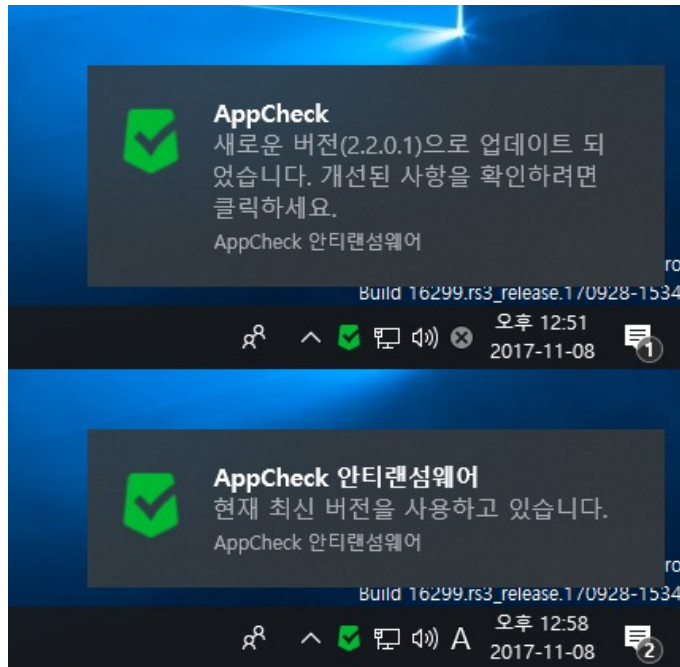
잠금 설정을 해제하기 위해서는 “잠금 설정 사용” 체크 박스를 클릭하여 잠금 설정 해제창에 잠금 시 사용한 비밀번호를 입력하시기 바랍니다.



만약 잠금 설정 해제 시 입력한 비밀번호가 부정확한 경우 “비밀번호가 올바르지 않습니다.” 알림창이 생성됩니다.

◎ **자동 업데이트 사용** : 6~12시간 주기로 앱체크 업데이트 자동 확인 (AppCheck 무료 버전 기준, AppCheck Pro 정품 버전은 3시간 주기)

- **업데이트 에이전트로 사용** : AppCheck 무료 버전에서 활성화되는 하위 메뉴로 P2P 방식으로 AppCheck 업데이트가 동작합니다.



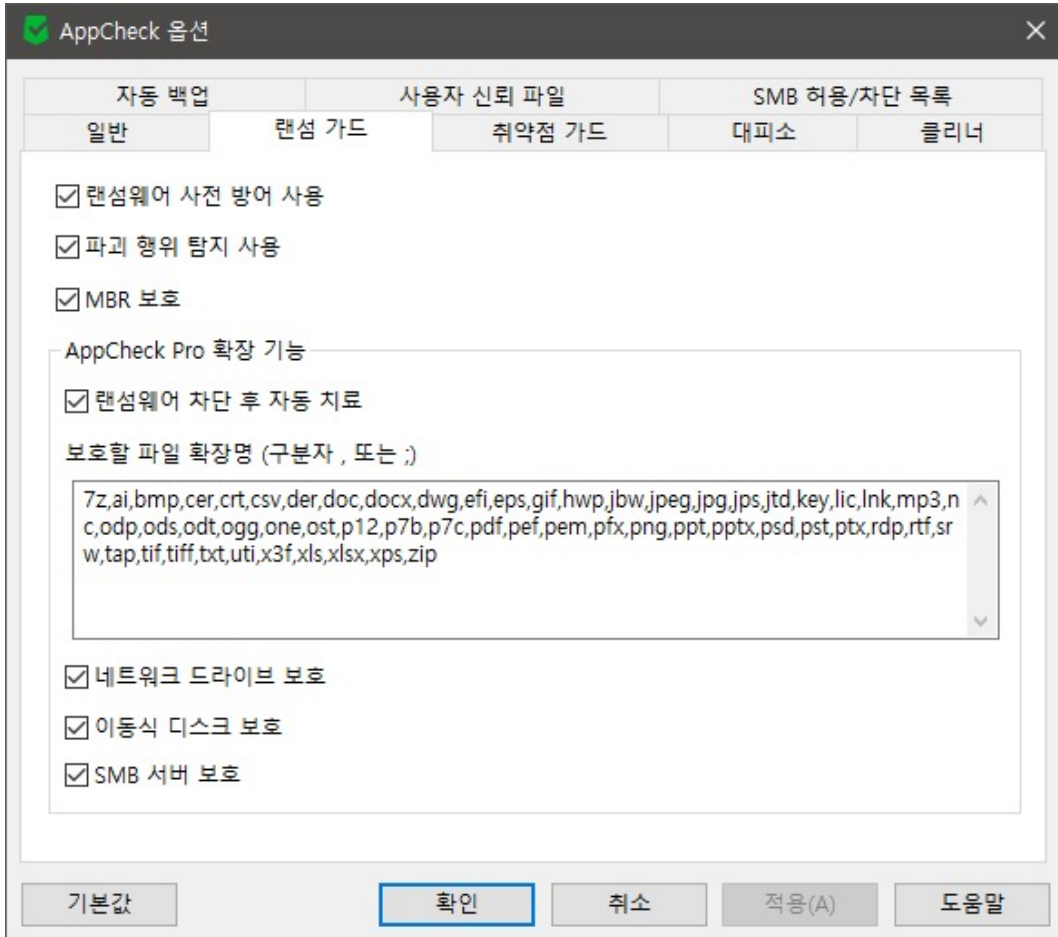
앱체크 개인 사용자용 무료 버전의 자동 업데이트는 6~12시간 주기로 자동 확인이 이루어지며 상위 버전으로 업데이트된 경우 “새로운 버전으로 업데이트되었습니다. 개선된 사항을 확인하려면 클릭하세요.” 알림창이 생성됩니다.

사용자가 업데이트 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.

◎ **기본값** : 일반 옵션 설정을 초기화

◆ AppCheck 옵션 : 랜섬 가드



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

◎ **파괴 행위 탐지 사용** : 원본 파일 삭제없이 다른 데이터로 덮어쓰기 방식으로 훼손하거나 복구 불가능하게 원본 파일을 삭제하는 행위를 탐지하여 차단하는 기능

◎ **MBR 보호** : Master Boot Record (MBR)과 GUID Partition Table (GPT) 영역의 변조를 시도하는 파일 실행 차단

◎ **AppCheck Pro 확장 기능 - 랜섬웨어 차단 후 자동 치료**

랜섬웨어 사전 방어 기능을 통해 탐지된 악성 파일 자동 치료(삭제)

◎ AppCheck Pro 확장 기능 - 보호할 파일 확장명 (구분자 , 또는 ;)

파일 훼손 행위로부터 보호되는 기본 파일 확장명은 총 56종(7z, ai, bmp, cer, crt, csv, der, doc, docx, dwg, efi, eps, gif, hwp, jbw, jpeg, jpg, jps, jtd, key, lic, lnk, mp3, nc, odp, ods, odt, ogg, one, ost, p12, p7b, p7c, pdf, pef, pem, pfx, png, ppt, pptx, psd, pst, ptx, rdp, rtf, srw, tap, tif, tiff, txt, uti, x3f, xls, xlsx, xps, zip)이며, 사용자에게 의한 추가적인 파일 확장명 등록은 AppCheck Pro 정품 버전에서만 제공됩니다.



보호할 파일 확장명에 사용할 수 없는 문자가 포함될 경우 “사용할 수 없는 문자가 포함되어 있습니다.” 알림창 생성을 통해 적용되지 않도록 합니다.

◎ AppCheck Pro 확장 기능 - 네트워크 드라이브 보호

앱체크(AppCheck)가 설치된 PC에서 랜섬웨어(Ransomware)가 실행되어 네트워크 드라이브로 연결된 공유 폴더 내 파일들이 암호화될 경우 차단 및 자동 복원하는 기능입니다.

◎ AppCheck Pro 확장 기능 - 이동식 디스크 보호

앱체크(AppCheck)가 설치된 PC와 USB 포트를 통해 연결된 USB 드라이브 또는 CF 메모리에 저장된 파일이 랜섬웨어(Ransomware)에 의해 암호화될 경우 차단 및 자동 복원하는 기능입니다.

단, USB 포트를 통해 연결된 외장 하드 디스크는 앱체크 기본 랜섬웨어 행위 차단 기능을 통해 보호됩니다.

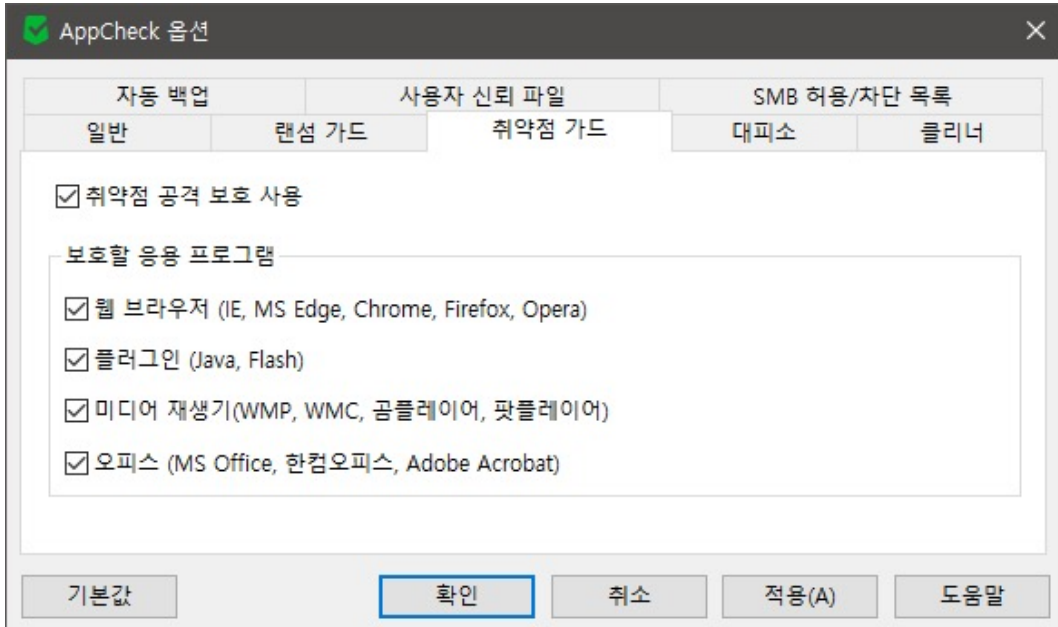
◎ AppCheck Pro 확장 기능 - SMB 서버 보호

앱체크(AppCheck)가 설치되어 있지 않은 원격지 PC에서 랜섬웨어(Ransomware)가 실행되어 네트워크 드라이브를 통해 연결된 공유 폴더(앱체크 설치 PC) 내 파일들이 암호화될 경우 원격지 IP 차단(1시간) 및 자동 복원하는 기능입니다.

차단된 원격지 PC에 대한 액세스는 기본적으로 1시간 경과 시 자동으로 해제되며, 수동으로 해제하기 위해서는 AppCheck 옵션의 “SMB 허용/차단 목록”에 등록된 “차단된 주소 목록”에서 차단된 IP를 선택하여 임시 허용 또는 항상 허용하시거나 앱체크 실시간 보호를 비활성화(OFF)하시면 됩니다.

◎ 기본값 : 랜섬 가드 옵션 설정을 초기화

◆ AppCheck 옵션 : 취약점 가드



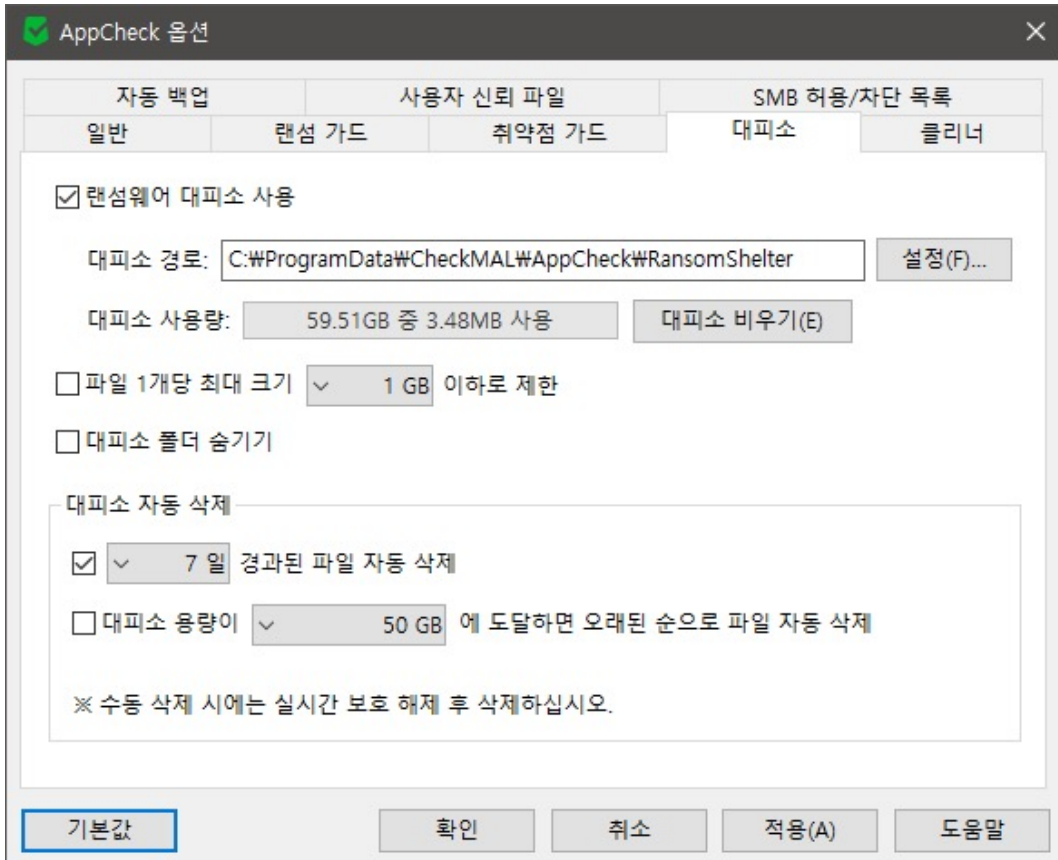
취약점 가드는 보호할 응용 프로그램에 대하여 취약점(Exploit) 코드가 실행될 경우 차단하여 악성코드 자동 감염을 차단하며 “취약점 공격 보호 사용” 박스를 해제할 경우 전체 기능이 중지됩니다. 단, 보호할 응용 프로그램별 체크 박스 선택 여부에 따라 일부 응용 프로그램에 대하여 보호할 수 있습니다.

웹 브라우저	Internet Explorer, Microsoft Edge, Chrome, Firefox, Opera
플러그인	Java, Adobe Flash
미디어 재생기	Windows Media Player, Windows Media Center, 곰플레이어(GomPlayer), 팟플레이어(PotPlayer)
오피스	Microsoft Office, 한컴오피스, Adobe Acrobat

보호할 응용 프로그램 중 오피스(Office)는 AppCheck Pro 정품 버전에서만 활성화할 수 있습니다.

◎ **기본값** : 취약점 가드 옵션 설정을 초기화

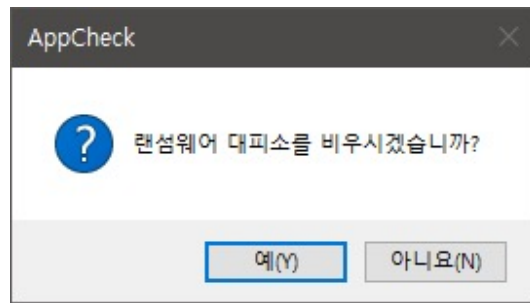
◆ AppCheck 옵션 : 대피소



◎ **랜섬웨어 대피소 사용** : 특정 조건에 맞는 파일 훼손 행위 발생 시 랜섬웨어 대피소 폴더에 원본 파일을 임시 백업하며 랜섬웨어 행위 탐지를 통해 훼손된 파일을 자동 복원해 주는 기능입니다. 참고로 랜섬웨어 대피소 폴더 및 내부 파일을 삭제하기 위해서는 앱체크 메인 화면에서 제공하는 “랜섬웨어 대피소 비우기” 메뉴를 실행하거나 또는 실시간 보호를 임시 중지하시고 사용자가 직접 폴더를 찾아 삭제하시기 바랍니다.

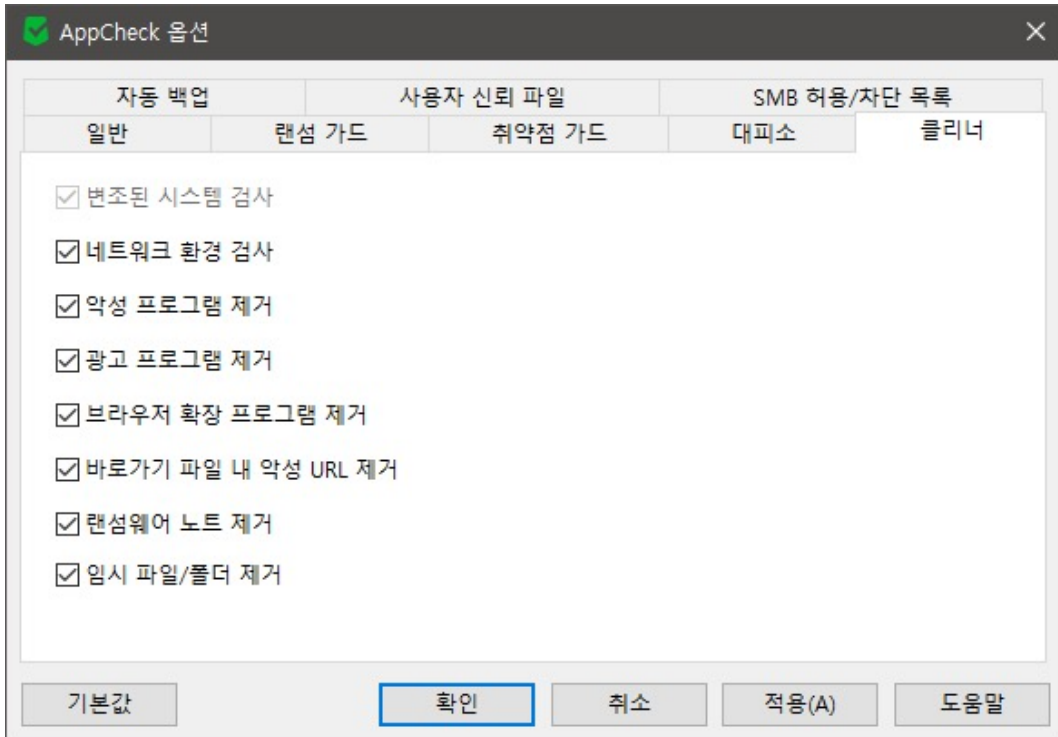
만약 랜섬웨어 대피소 기능 자체를 사용하지 않을 경우 탐지 가능한 랜섬웨어 중 일부가 탐지되지 않을 수 있으므로 반드시 랜섬웨어 대피소 기능을 사용하시기 바랍니다.

- **대피소 경로** : 대피소 경로 기본 위치는 “C:\ProgramData\CheckMAL\AppCheck\RansomShelter” 폴더이며, 설정 버튼을 클릭하여 원하는 폴더로 변경 가능합니다. 단, 대피소 경로를 변경한 경우 기존의 대피소 폴더는 보호 해제됩니다.
- **대피소 사용량** : 지정된 대피소 내 저장된 파일 용량 표시
- **대피소 비우기** : 대피소 폴더 및 내부 파일 일괄 삭제되며, 삭제된 폴더 및 내부 파일은 휴지통으로 이동되지 않고 완전 삭제됩니다.



- ◎ **파일 1개당 최대 크기 제한** : 대피소에 임시 백업되는 파일 용량(100MB, 200MB, 500MB, 1GB, 2GB, 5GB) 제한
- ◎ **대피소 폴더 숨기기** : 대피소 폴더 속성을 숨김(H)으로 변경합니다.
- ◎ **대피소 자동 삭제 - ○일 경과된 파일 자동 삭제** : 대피소 폴더에 임시 백업된 파일을 10분, 20분, 30분, 1시간, 3시간, 6시간, 12시간, 1일, 2일, 3일, 4일, 5일, 6일, 7일 경과 시 자동 삭제 (기본값 : 7일)
- ◎ **대피소 자동 삭제 - 대피소 용량이 ○○에 도달하면 오래된 순으로 파일 자동 삭제** : 대피소 폴더에 임시 백업된 파일 용량이 5GB, 10GB, 20GB, 50GB, 100GB, 디스크의 10%, 디스크의 20%, 디스크의 30%, 디스크의 40%, 디스크의 50%에 도달하면 오래된 파일순으로 자동 삭제 (기본값 : 50GB)
- ◎ **기본값** : 대피소 옵션 설정을 초기화

◆ AppCheck 옵션 : 클리너



- ◎ **변조된 시스템 검사** : Windows 운영 체제 시스템 관련 항목 중 변조된 파일 또는 레지스트리가 존재할 경우 수정하며, 필요에 따라서는 Windows 재부팅을 요구할 수 있습니다. 참고로 해당 검사는 필수 검사 항목입니다.
- ◎ **네트워크 환경 검사** : 시스템의 네트워크 구성 정보를 확인하여 악의적인 설정이 되어 있는 경우 수정
- ◎ **악성 프로그램 제거** : 시스템에 악성 프로그램이 설치되어 있는 경우 제거
- ◎ **광고 프로그램 제거** : 시스템에 사용자에게 불편을 유발할 수 있는 광고 프로그램 제거
- ◎ **브라우저 확장 프로그램 제거** : 웹 브라우저를 통해 동작하는 악성 브라우저 확장 프로그램(BHO) 제거
- ◎ **바로가기 파일 내 악성 URL 제거** : 바탕 화면 또는 즐겨찾기 영역에 바로가기를 생성하여 클릭 시 악성 사이트로 연결이 이루어질 경우 제거
- ◎ **랜섬웨어 노트 제거** : 랜섬웨어(Ransomware) 감염으로 생성되는 결제 안내 파일 제거
- ◎ **임시 파일/폴더 제거** : 임시 폴더(%Temp%) 내에 존재하는 불필요한 파일 및 폴더 제거
- ◎ **기본값** : 클리너 옵션 설정을 초기화

◆ AppCheck 옵션 : 자동 백업

AppCheck 옵션
✕

일반
랜섬 가드
취약점 가드
대피소
클리너

자동 백업
사용자 신뢰 파일
SMB 허용/차단 목록

자동 백업 사용

스케줄 설정(S)

백업할 대상

폴더 목록 [추가](#) [삭제](#)

폴더 경로

지정한 확장명만 백업 (구분자 , 또는 ;)

제외할 대상

폴더 목록 [추가](#) [삭제](#)

폴더 경로

백업시 제외할 파일 확장명 (구분자 , 또는 ;)

백업할 위치

로컬 디스크 ▼ C:\#AutoBackup(AppCheck) 이력 파일 유지 개수 : 3 ▼

네트워크 공유 폴더(SMB/CIFS)

서버 주소 공유 폴더

사용자 ID 비밀번호

※ 수동 삭제시에는 실시간 보호 해제 후 삭제하십시오.

기본값

확인

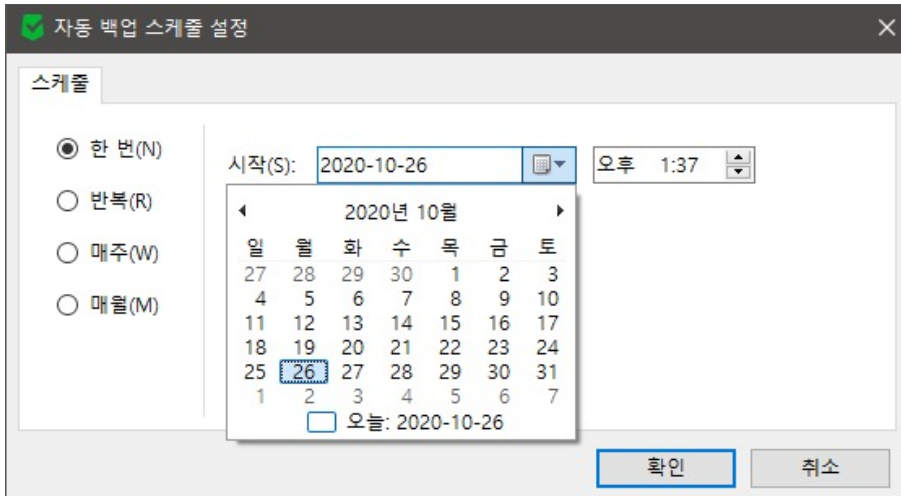
취소

적용(A)

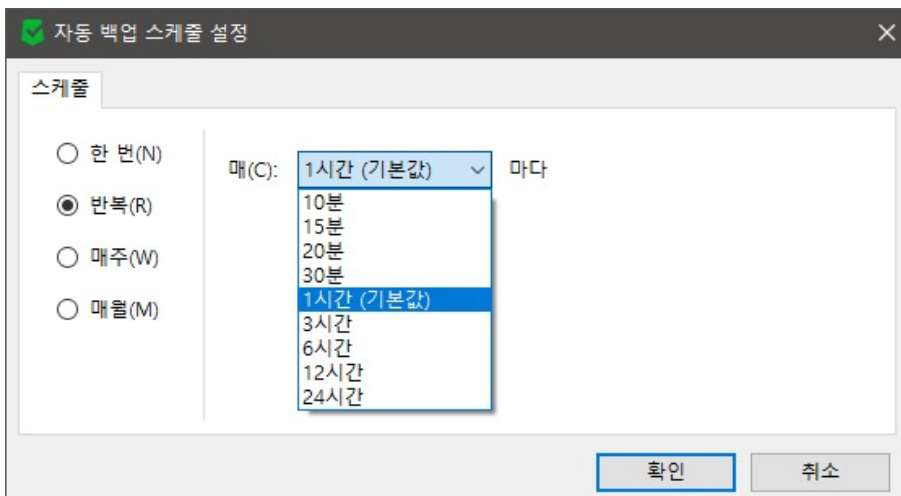
도움말

◎ 스케줄 설정 : 한 번, 반복, 매주, 매월 단위로 자동 백업

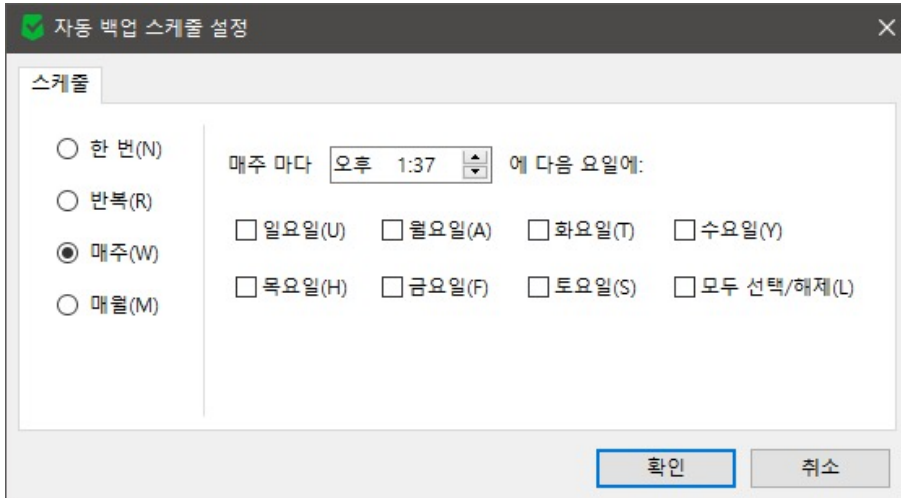
- 한 번 : 지정한 특정일의 특정 시간에 1회 자동 백업하도록 설정합니다.



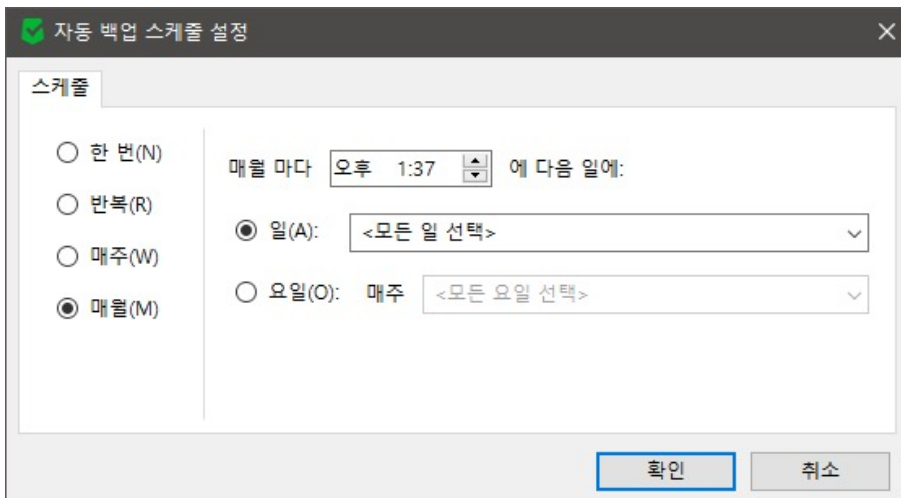
- 반복 : 10분, 15분, 20분, 30분, 1시간(기본값), 3시간, 6시간, 12시간, 24시간 단위로 자동 백업하도록 설정합니다.



- **매주** : 지정한 특정 요일의 특정 시간에 자동 백업하도록 설정합니다.

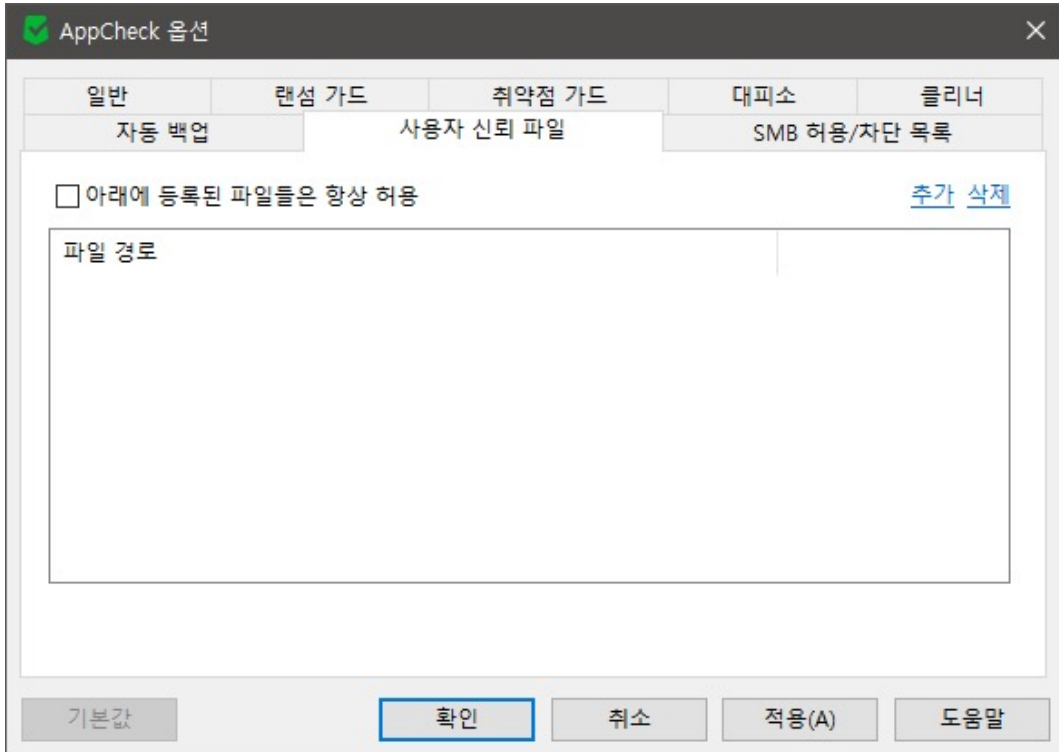


- **매월** : 매월 지정한 특정일 또는 특정 요일의 특정 시간에 자동 백업하도록 설정합니다.



- ◎ **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 또는 네트워크 공유 폴더(SMB/CIFS) 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 지정 가능
- ◎ **이력 파일 유지 개수** : 자동 백업 대상 원본 파일이 수정될 경우 기존의 백업 파일은 이력 파일(.history)로 변경되며, 이력 파일 수는 0~10개로 사용자가 지정할 수 있습니다. (기본값 : 3개)
참고로 이력 파일수가 초과할 경우 가장 오래된 이력 파일부터 자동 삭제합니다.
- ◎ **네트워크 공유 폴더(SMB/CIFS)** : 서버 주소(IP 주소 또는 원격지 PC 이름), 공유 폴더(공유 설정이 이루어진 원격지 드라이브/폴더 이름), 사용자 ID, 비밀번호 입력 필수
안전하게 네트워크 공유 폴더를 사용하기 위해서는 SMB 취약점 관련 최신 보안 업데이트를 지속적으로 하시기 바라며, 공유 폴더 접근을 위한 사용자 계정 비밀번호 관리 및 권한 설정을 하시기 바랍니다.
또한 자동 백업 폴더(AutoBackup(AppCheck)) 및 내부 파일을 삭제하기 위해서는 애플체크 실시간 보호를 임시 중지하시고 삭제하시기 바랍니다.

◆ AppCheck 옵션 : 사용자 신뢰 파일



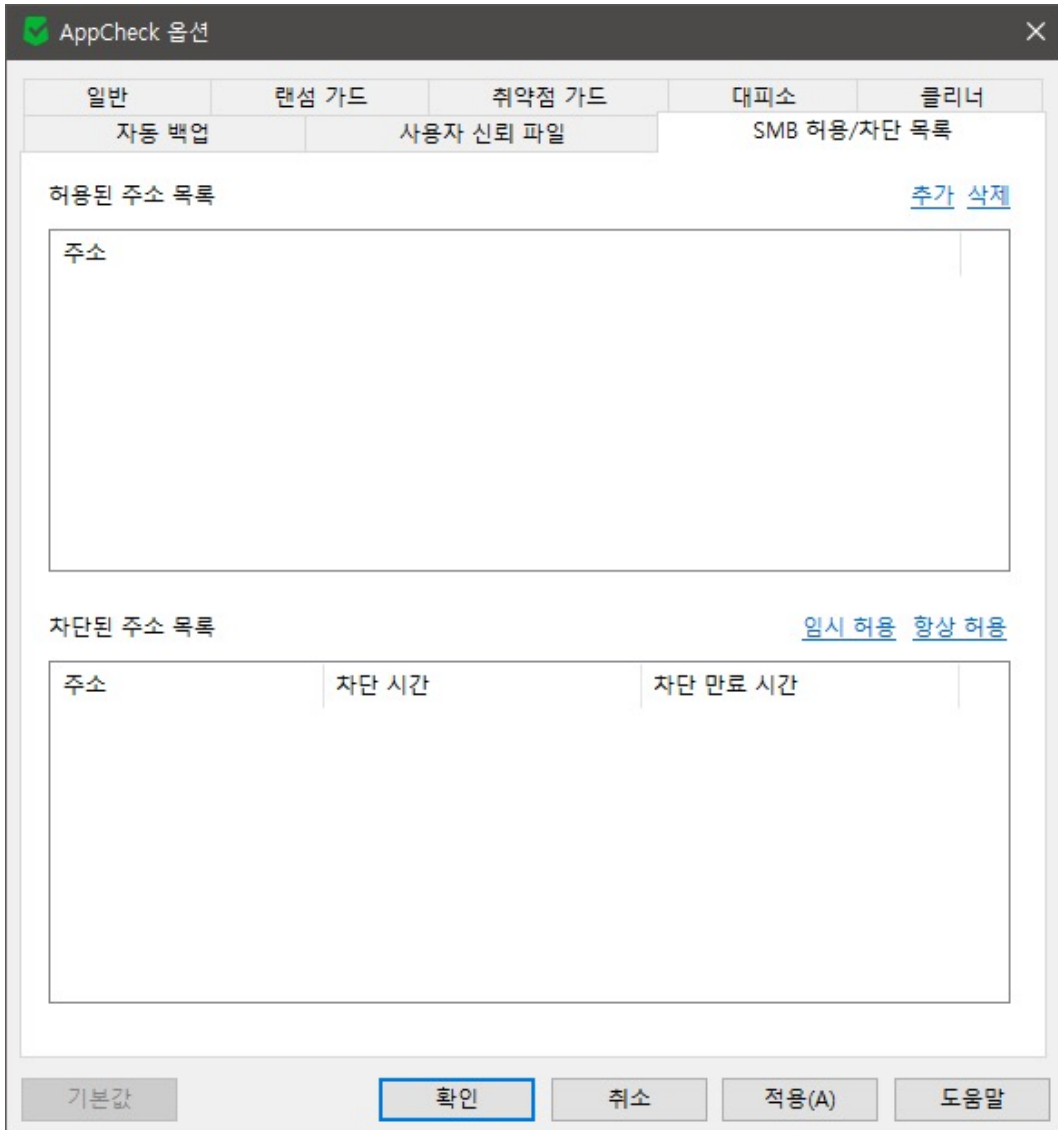
사용자 신뢰 파일은 랜섬웨어 행위 탐지로 차단된 파일 중 과탐으로 확인된 경우 또는 사용자 판단에 따라 진단 제외 처리를 원하는 파일을 추가할 수 있는 기능이며, 사용자 신뢰 파일을 추가한 후에는 반드시 “아래에 등록된 파일들은 항상 허용” 박스에 체크하시기 바랍니다.

기본적으로 사용자 신뢰 파일로 추가된 파일이 다른 파일을 훼손할 경우 훼손되는 파일은 대피소 폴더에 임시 백업 처리되지 않습니다.

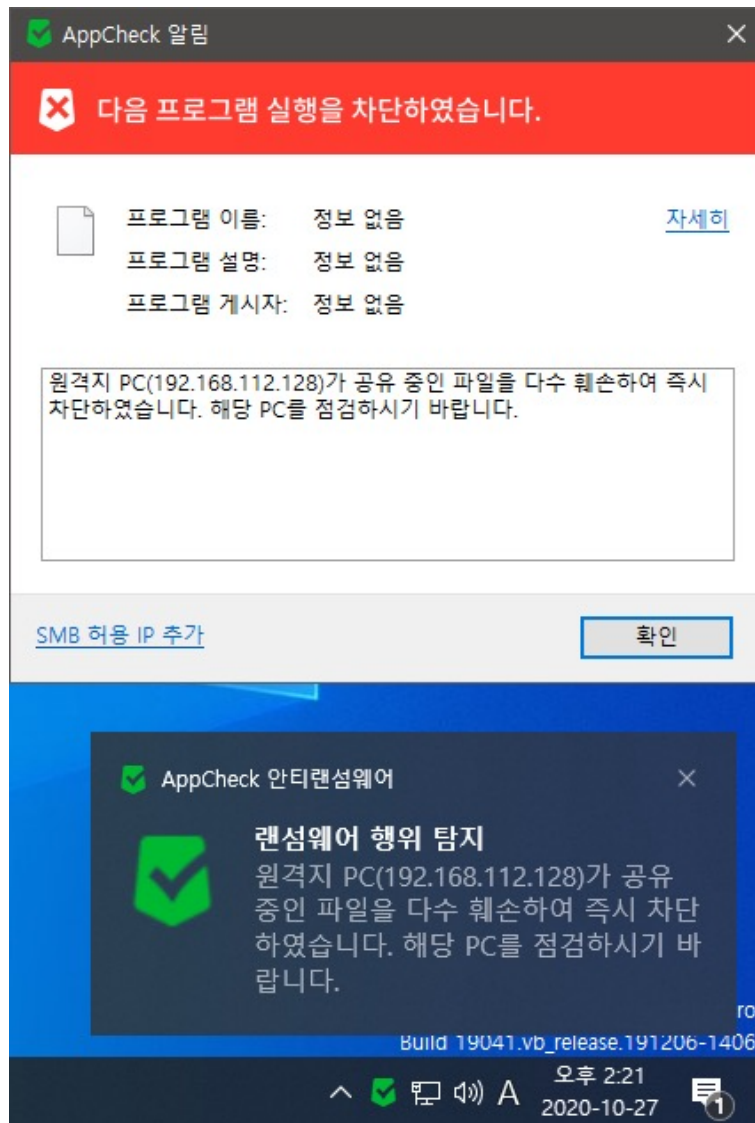
단, 사용자 신뢰 파일로 추가된 파일이 특정 조건에 따라 파일 훼손 행위가 발생할 경우 랜섬웨어 행위 탐지가 이루어질 수 있습니다.

주의할 점은 explorer.exe / svchost.exe 등 Windows 시스템 파일은 랜섬웨어에 의해 악용 소지가 매우 높으므로 신뢰 파일에 추가할 경우 랜섬웨어 탐지에 실패할 수 있습니다.

◆ AppCheck 옵션 : SMB 허용/차단 목록



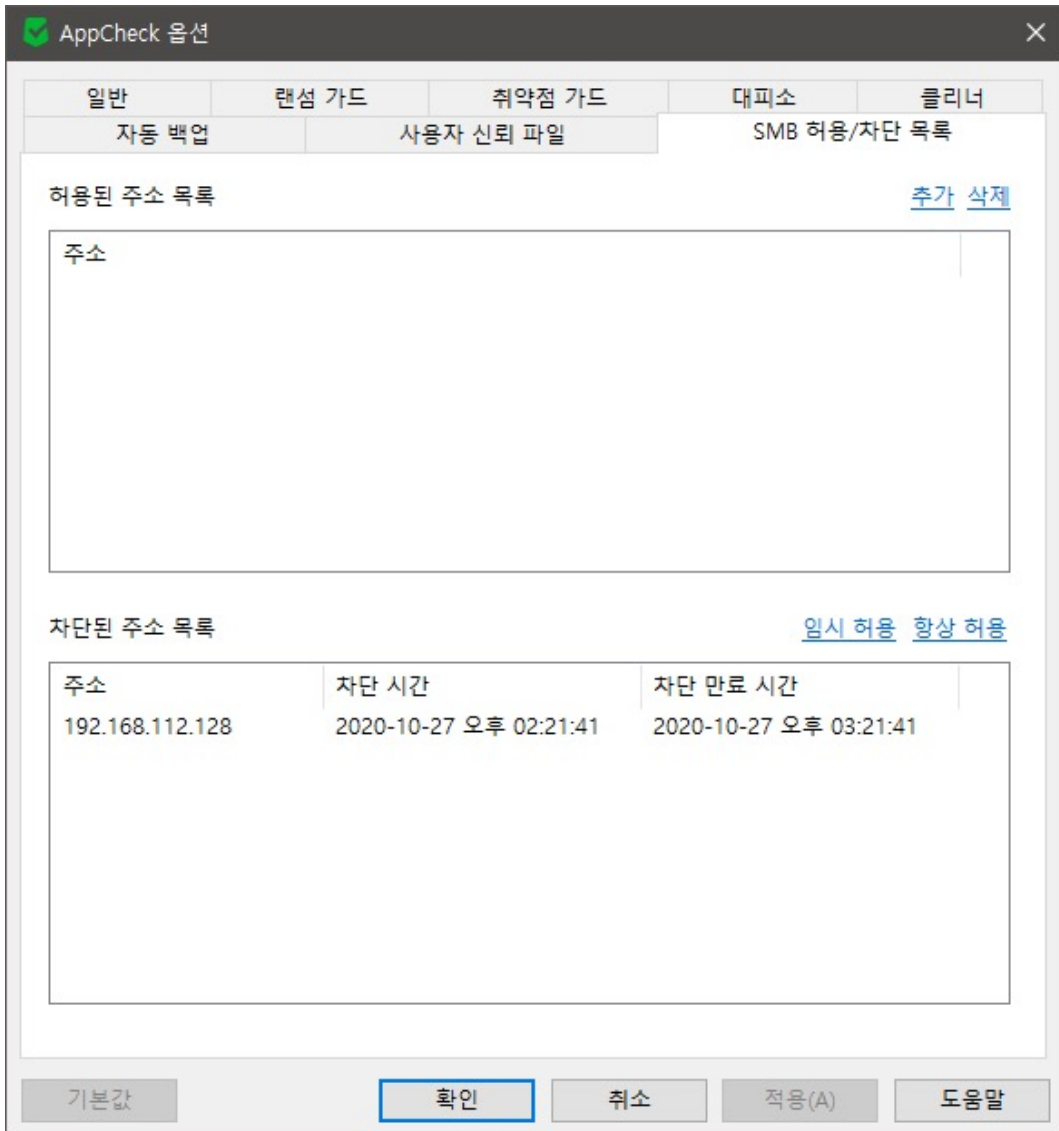
SMB 허용/차단 목록 옵션은 AppCheck Pro 정품 버전에서만 표시되며, 원격지 PC에서 실행된 랜섬웨어가 네트워크 드라이브를 통해 공유 폴더에 접근하여 파일 암호화 행위를 진행할 경우 SMB 서버 보호 기능을 통해 차단되는 IP(IPv4, IPv6) 주소에 대한 허용/차단 여부를 세부적으로 설정할 수 있습니다.



원격지 PC에서 실행된 랜섬웨어에 의해 공유 폴더 내의 파일이 훼손될 경우 IP(IPv4, IPv6) 주소를 차단하는 “랜섬웨어 행위 탐지” 차단 메시지가 생성됩니다.

사용자가 차단 메시지를 클릭할 경우 AppCheck 알림창 생성을 통해 차단 IP 정보가 표시되며, 사용자의 판단에 의해 “SMB 허용 IP 추가” 클릭 시 AppCheck 옵션의 “SMB 허용/차단 목록”에 해당 IP가 “허용된 주소 목록”에 추가되어 접근을 지속적으로 허용합니다.

AppCheck 알림창의 “자세히” 메뉴를 클릭할 경우 AppCheck 옵션의 “SMB 허용/차단 목록”으로 연결되어 “차단된 주소 목록”에 차단된 IP 주소 정보가 표시됩니다.



임시 차단된 IP 주소는 1시간 동안 공유 폴더에 대한 접근이 차단되며, 추가적으로 사용자가 임시 허용 또는 항상 허용을 통해 차단된 IP 주소에 대한 허용 여부를 결정할 수 있습니다.

- **임시 허용** : 차단된 주소 목록에서 선택한 IP 주소 삭제를 통해 공유 폴더에 대한 접근이 가능하며 재탐지 시 IP 차단

- **항상 허용** : 차단된 주소 목록에서 선택한 IP 주소를 “허용된 주소 목록”에 등록하여 공유 폴더에 대한 접근이 항상 허용

임시 차단된 IP 주소는 차단 만료 시간(1시간)이 경과될 경우 자동으로 차단된 주소 목록에서 삭제 처리되며 원격지 PC에서는 재접속이 가능합니다.

SMB 허용 목록 추가
✕

IP 주소(A) :

IP v4

- ※ 개별 : 192.168.1.1
- ※ 순차 : 192.168.1.1-10
(192.168.1.1 ~ 192.168.1.10 까지 허용)
- ※ 전체 : 192.168.1.0/24
(192.168.1.1 ~ 192.168.1.255 까지 허용)

IP v6

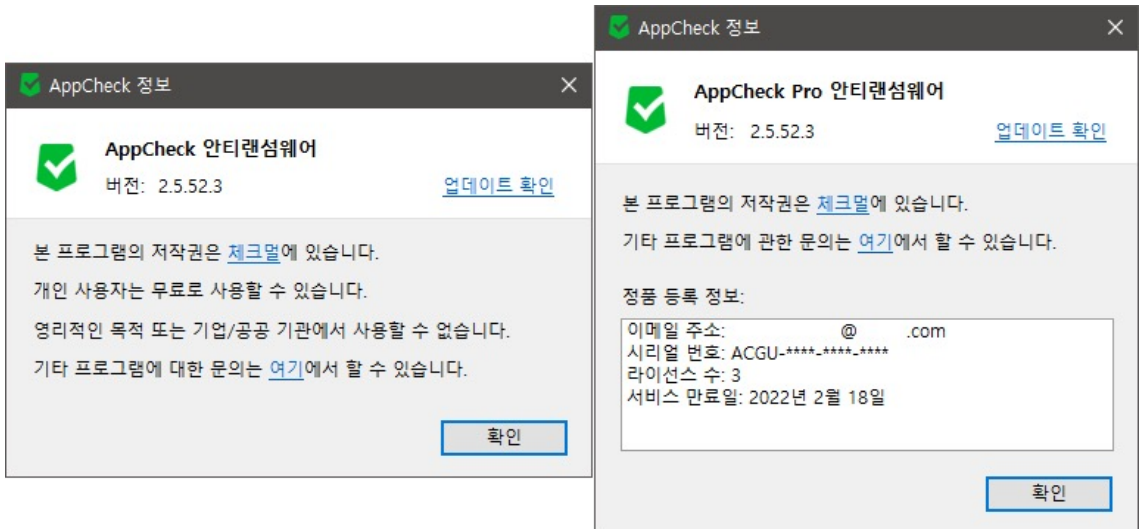
- ※ 개별 : 2001:0DB8:1000:0000:0000:0000:1111:2222
- ※ 순차 : 2001:DB8:1000::1111:2222-3333
(2001:DB8:1000::1111:2222 ~ 2001:DB8:1000::1111:3333 까지 허용)
- ※ 전체 : 2001:DB8::/32
(2001:0DB8:0000:0000:0000:0000:0000:0000 ~ 2001:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 까지 허용)

차단된 주소 목록에 등록된 IP 주소 외에 사용자가 직접 추가를 원하는 경우 “허용된 주소 목록”의 추가 버튼을 통해 등록할 수 있습니다.

SMB 허용 목록 추가에서는 IPv4, IPv6 프로토콜 주소에 대한 개별, 순차, 전체 등록이 가능하며, 각 예제에서 안내하는 패턴을 참고하여 추가할 수 있습니다.

참고로 특정 IP 주소에 대한 SMB 허용 시에는 원격지 PC에 앱체크(AppCheck)가 설치되어 있는 경우 또는 신뢰할 수 있는 기기에 대해서만 추가하시길 권장합니다.

[2-3] AppCheck 정보



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

또한 AppCheck 정보 확인은 앱체크 메인 화면 상단의 앱체크(AppCheck) 로고 영역을 클릭할 경우에도 확인할 수 있습니다.