TCOSVC

ShieldOS 사용자 매뉴얼

㈜티씨오서비스

개요

본 문서는 Anti-Ransomware Solution 쉴도스(ShieldOS)의 설명과 메뉴 구성 및 동작 과정을 설명하여 사용자 편의를 제공하는데 그 목적이 있습니다.

문서 이력

버전	주요제/개정내용	변경일	작성자
1.0	제정(초안)	2016.08.08	오준식
1.1	개정 (라이선스 관리)	2017.04.10	고호경
1.2	개정(이미지)	2017.04.12	고호경
1.3	개정	2017.04.17	김태욱
1.4	개정	2022.01.26	김경호
1.5	개정(보호 확장자 기능추가)	2022.02.15	김경호
1.6	개정(로고변경)	2022.07.29	김경호

목차

쉴도스란?

랜섬웨어 예방 솔루션

ShieldOS 는 3No(No 탐지, No 치료, No 백업) 컨셉으로 바이러스 및 랜섬웨어에 걸릴 위험이 있는 비정상적인 프로그램이나 허용되지 않은 일체 행위들을 원천적으로 차단하여 사용자의 소중한 데이터가 위조 및 변조되는 것을 근원적으로 막는 전문 랜섬웨어 예방 솔루션입니다.

✓ **안전한 파일보호**

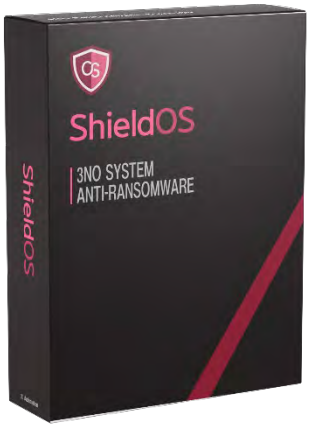
기존 랜섬웨어뿐만 아니라 새로운 랜섬웨어 공격까지 대응

✓ **확실한 차단정책**

인가되지 않은 프로세스는 확실하게 차단하여 데이터 파일을 안전하게 보호

✓ **지속적인 지원서비스**

지속적으로 인가 혹은 비인가 프로세스를 확보하여 패치를 지원



1 ShieldOS Agent 설치

1.1 Agent 설치

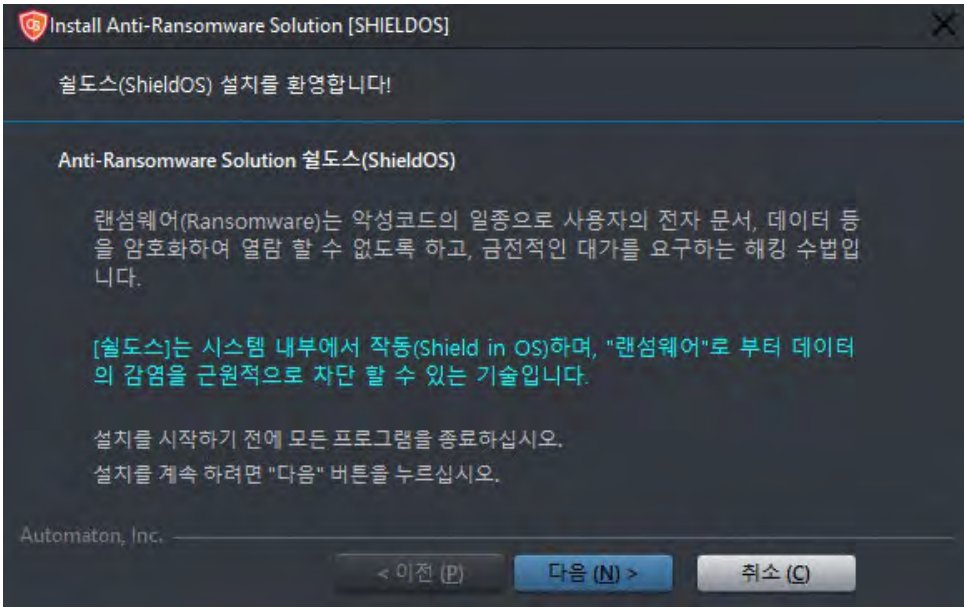
사전에 안내받은 이메일을 통해서 ShieldOS 에이전트를 다운로드 및 설치할 수 있습니다.

■ 설치과정

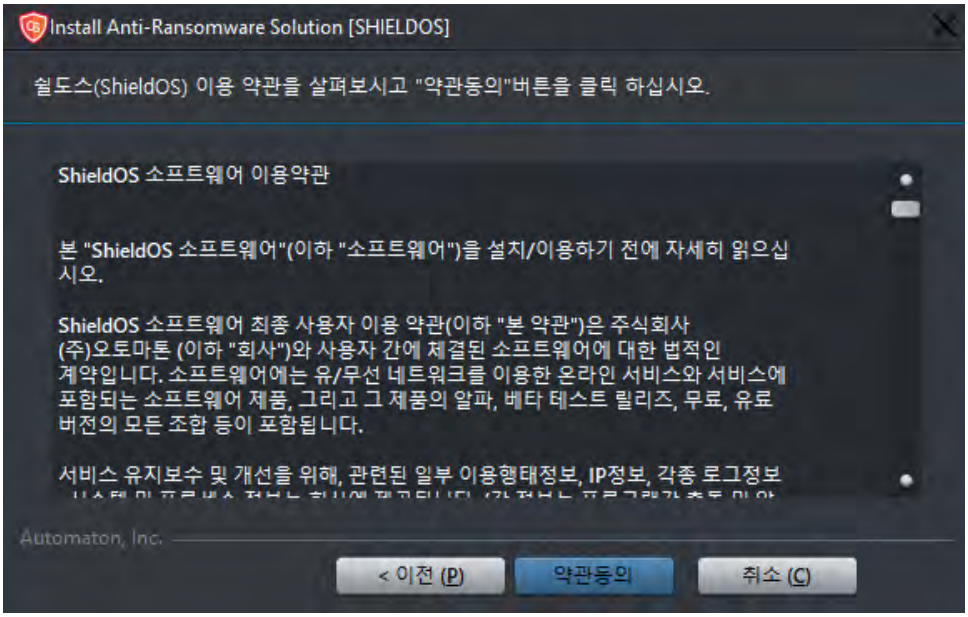
① 메일의 안내대로 ShieldOS 설치파일(ShieldosSetup.exe)을 다운로드 합니다

② 다운받은 파일을 우측 클릭하여 관리자 권한으로 실행합니다.

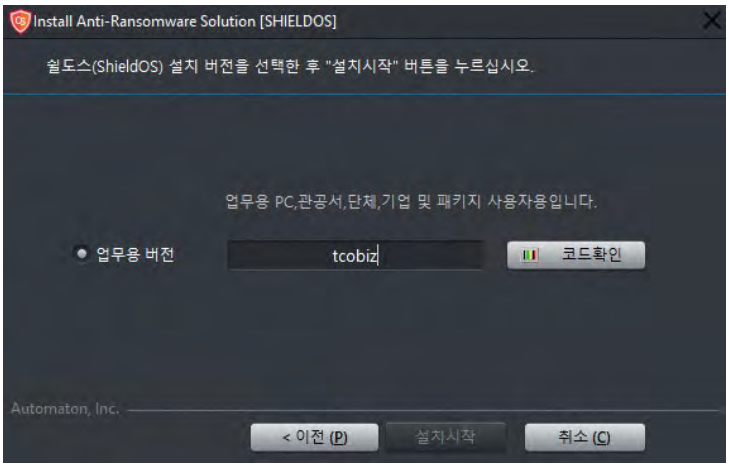
③ 설치화면 안내대로 '다음' 버튼을 클릭합니다.



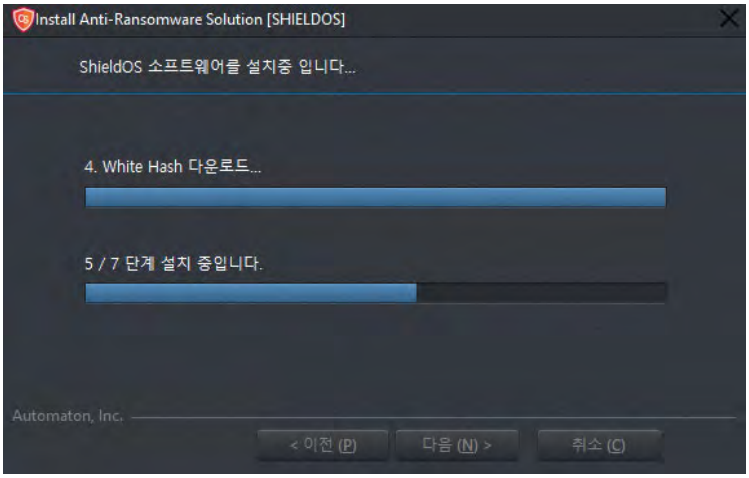
④ 다음과 같이 이용 약관 확인하는 화면이 나타납니다. 내용 확인 후 '약관동의' 버튼을 클릭합니다.
(* 약관 미동의 시 서비스 이용에 제한받을 수 있습니다.)

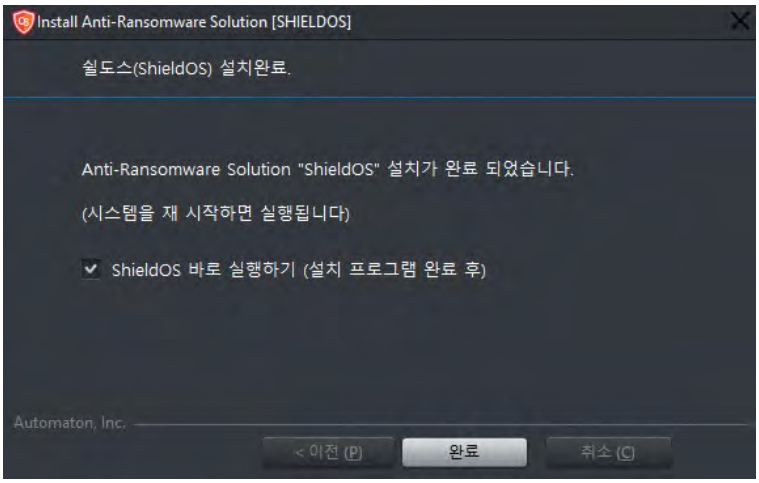


⑤ 업무용 버전을 선택 후 메일에 동봉된 라이선스 코드(* 체험판인 경우 무료코드)를 입력 후 '코드확인' 버튼을 클릭하시면 설치시작 버튼이 활성화됩니다. 활성화된 '설치시작' 버튼을 클릭합니다.



⑥ 설치 진행이 완료되면 ShieldOS 바로 실행하기 버튼을 체크하고 완료 버튼을 클릭합니다. 설치를 모두 마치셨으면 PC 를 재부팅 합니다.

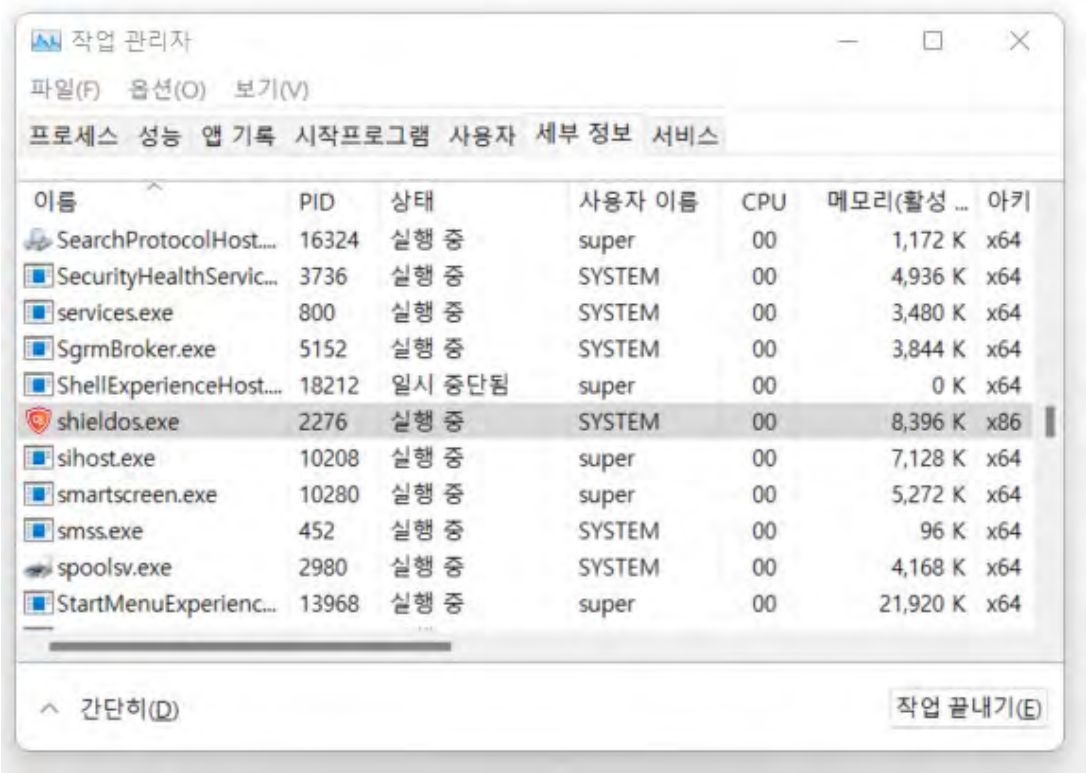




1.2 제품 상태 확인

작업관리자 실행 후 '세부정보' 항목에서 shieldos.exe 실행 상태를 확인할 수 있습니다.

■ 제품 프로세스 (shieldos.exe)



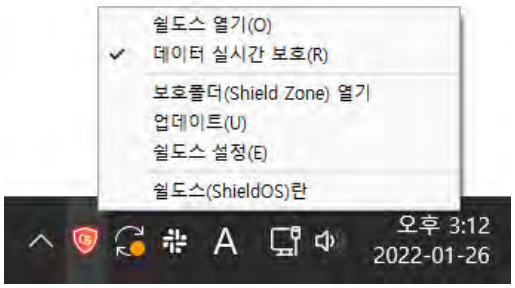
또한 PC 작업표시줄 트레이 아이콘을 통해서도 확인이 가능 합니다.

2 기능 설명

2.1 기본 화면 구성

ShieldOS 화면 구성은 '트레이 아이콘 메뉴'와 '메인화면'으로 나뉩니다.

✓ Tray Icon



① 쉴도스 열기: 쉴도스 메인화면을 실행합니다.
② 데이터 실시간 보호: 데이터 실시간 보호 기능을 켜고 끕니다.
③ 보호폴더(Shield Zone) 열기: Shield Zone(보호존)으로 설정된 폴더를 실행합니다.
④ 업데이트: 수동으로 ShieldOS 업데이트를 진행합니다.
⑤ 쉴도스 설정: 쉴도스 설정화면을 실행합니다.
⑥ 쉴도스(ShieldOS)란: 쉴도스 도움말 화면을 실행합니다.

✓ 메인화면

① 쉴도스 데이터 보호: 실시간 보호기능을 켜고 끕니다.
② 실행 환경 설정: 쉴도스 환경 설정을 사용자에 맞게끔 지정할 수 있습니다.
③ MY 차단, 허용: 차단, 허용 프로세스 목록을 확인할 수 있습니다.
④ 쉴도스 공지! 업데이트 내용에 관한 공지를 확인할 수 있습니다.
⑤ 라이선스: 에이전트에 등록된 라이선스 정보를 확인 및 갱신할 수 있습니다.
⑥ 쉴도스란...: 쉴도스 정보 및 도움말을 확인할 수 있습니다.

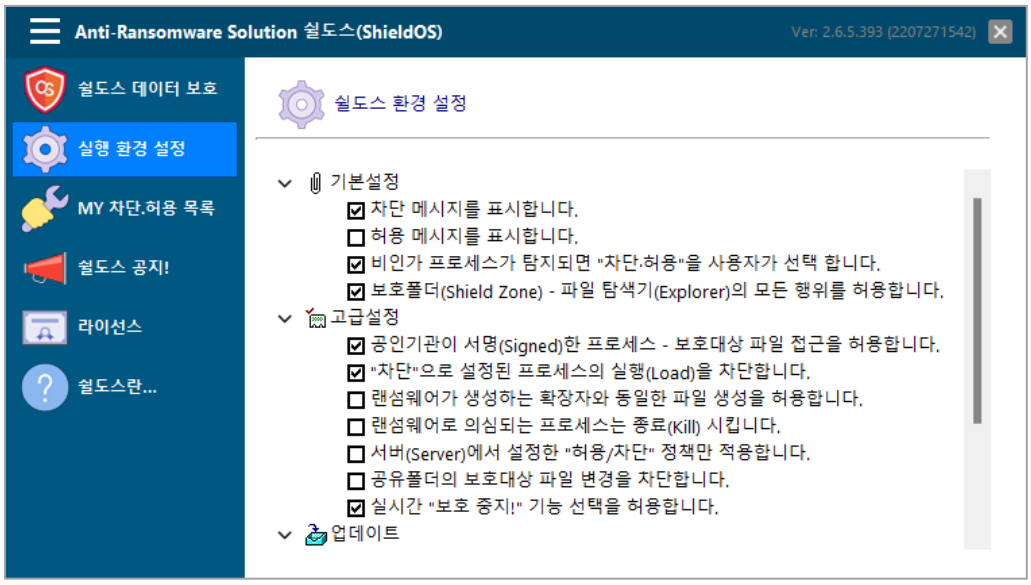
2.2 데이터 실시간 보호

데이터 실시간 보호는 ShieldOS 의 랜섬웨어 감지 동작상태를 의미합니다. 사용자의 필요에 따라 해당 기능을 중지할 수 있습니다. 중지된 상태에서는 ShieldOS 기능이 작동하지 않게 되며, 랜섬웨어로부터 보호받지 못하는 상태가 됩니다.

실시간 보호 기능을 중단하기 위해서는 [환경설정-기능설정-고급설정-실시간 "보호 중지!" 기능 선택을 허용합니다.]에 체크되어 있어야만 가능합니다.

* 혹시 모르는 충돌 및 호환성 문제가 발생하여 사용자 업무 중단이 발생하는 경우 해당 실시간 보호 기능을 끄시기 바랍니다.

✓ 실시간 보호 중지 설정 화면



■ '실시간 보호 중지' 설정 적용 방법은 다음과 같습니다.

① 좌측 메뉴 '실행 환경 설정(톱니바퀴 아이콘)'을 클릭합니다.
② 고급설정 클릭 후 '실시간 보호 중지! 기능선택을 허용합니다'에 체크를 합니다.

✓ 보호 확장자 보기

현재 ShieldOS 에서 보호되고 있는 확장자명들을 확인할 수 있습니다.

2.3 보호 폴더 열기

✓ 보호 폴더 열기

Shield Zone 은 C:₩Shield Zone 폴더로 자동 생성되며 파일 보호를 위한 전용 폴더입니다. 한번의 Write 만 가능하고 rename, 삭제, 수정, Append 등은 차단하나 Read 는 가능 합니다. (하위 폴더 생성은 가능하나 삭제나 변경은 불가능 합니다.)

■ 하위 폴더도 내 파일을 삭제하고자 하는 경우

[환경설정 - 쉴도스 옵션 - 기본설정] - "보호폴더 (C:₩Shield Zone)내 파일 탐색기 (Explorer)의 모든 행위를 허용합니다]에 선택 체크되어 있는 경우에는 파일 탐색기 (Explorer)로 copy, Rename, Delete, 잘라내기 등이 가능 합니다.)

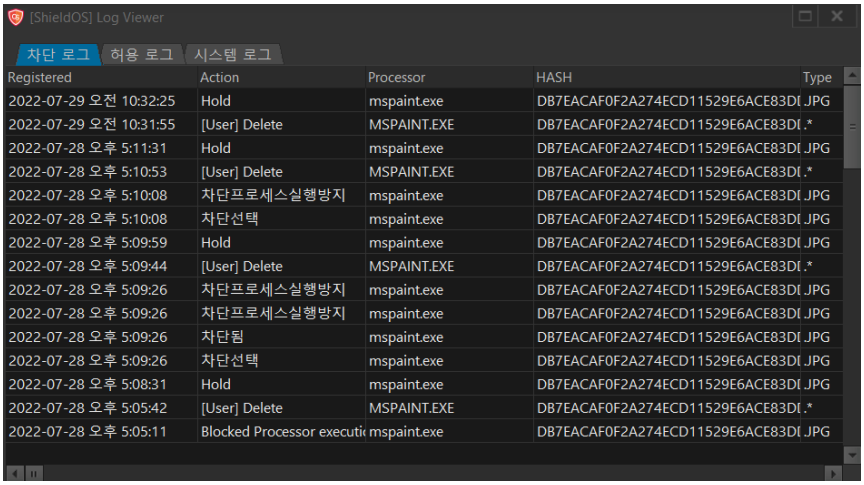
2.4 허용/차단 로그

✓ 허용/차단 로그보기

① 허용 로그: 사용자나 엔진에 의한 허용로그 등을 볼 수 있는 기능 (허용선택, 허용됨, 서명됨) 입니다.

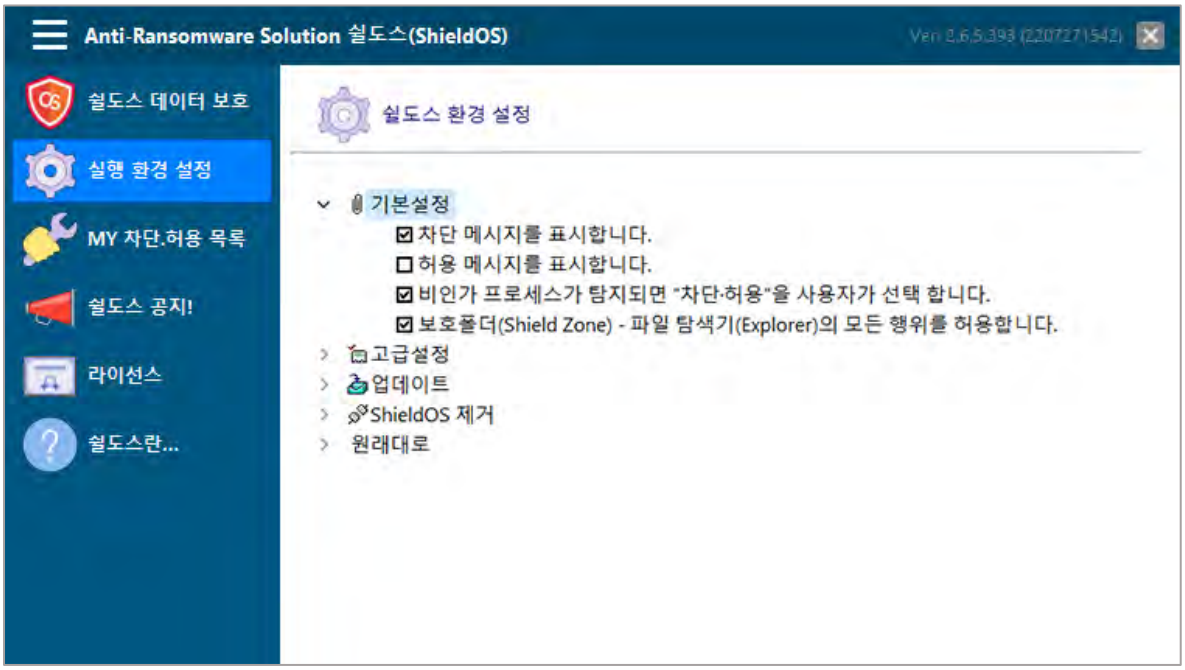
② 차단 로그: 사용자나 엔진에 의한 차단 및 선택보류 로그 등을 볼 수 있는 기능(랜섬파일생성차단, 랜섬웨어 의심됨 Kill, 차단 프로세스 실행 방지, 차단선택, 차단됨, Hold, 선택보류) 입니다.

③ 시스템 로그: 시스템과 커널의 작동 시간을 확인하기 위한 기능입니다. 로그는 10,000 개 이내, 30 일 이내 기준으로 자동 갱신됩니다.



3 실행 환경 설정

3.1 기본설정



① 차단 메시지를 표시합니다.

체크 (기본값)

윈도우창의 우측 하단에 차단되는 경우에는 해당 프로세스 정보와 대상 파일 정보를 표시합니다. 마지막 차단 기준으로 5 초 동안 표시합니다.
랜섬웨어로 의심되는 프로세스에 대하여는 경고 메시지를 추가로 표시합니다. 보호대상파일에 프로세스가 접근하는 경우에만 표시됩니다.

메시지는 랜섬파일생성차단, 랜섬웨어 의심됨 Kill, 차단 프로세스 실행 방지, 차단선택, 차단됨, Hold, 선택보류 등의 타이틀이 붙습니다.
랜섬파일생성차단, 랜섬웨어 의심됨 Kill, 차단 프로세스 실행 방지, 차단선택, 차단됨의 경우에는 빨강색으로 표시되며 동일 프로세스가 접근하는 파일 개수를 표시해 줍니다.

최대 10 까지 표시되며, 한 프로세스내의 행위 표시는 100 개까지 지원합니다. 프로세스의 행위는 메시지의 우측 하단에 상세보기를 선택하면 됩니다.

체크해제

차단 메시지를 표시하지 않습니다.

② 허용 메시지를 표시합니다.

체크

윈도우창의 우측 하단에 허용되는 경우에는 해당 프로세스 정보와 대상 파일 정보를 표시합니다. 마지막 허용 기준으로 5 초 동안 표시합니다.

보호대상파일에 프로세스가 접근하는 경우에만 표시됩니다. 메시지는 '허용선택, 허용됨, 서명됨' 총 3 가지 종류의 타이틀이 붙습니다.

체크해제 (기본값)

허용 메시지를 표시하지 않습니다.

③ 비인가 프로세스가 탐지되면 차단·허용 선택창을 표시합니다.

* 비인가 프로세스의 기준은 운영자 정책에 의한 White&Black List 와 사용자가 선택(등록)한 White&Bl ack List 를 제외한 모든 프로세스를 말합니다.
* 설정에 따라서는 Signed 프로세스도 포함될 수 있음 (고급 설정 참조)

체크 (기본값)

비인가 프로세스가 탐지되면 윈도우창의 중앙에 [차단·허용 선택창]을 띄우며 사용자의 선택을 기다 립니다. 탐지의 기준은 비인가 프로세스가 [보호대상 파일]에 대하여 수정, 삭제, 이름변경 등 시도하는 경우입니다.

설정에 따라서는 단순 파일 접근도 차단함(고급 설정 참조) 차단을 먼저 진행하고 선택창을 출력합니다.

'차단', '허용', '자세히' 선택하지 않고 창닫기 등이 가능합니다. (6 번 '차단·허용' 선택창 참조) 'Hold' 차단 메시지가 표시됩니다.

체크해제

[차단·허용 선택창]이 뜨지 않고 내부적으로 차단만 진행합니다.

사용자에 의한 차단 혹은 허용을 추가 기능이 없어집니다. "Hold" 차단 메시지가 빨강색으로 표시됩니다.

④ 보호폴더에서 파일 탐색기의 모든 행위를 허용합니다.

* 보호폴더는 ShieldOS 설치와 함께 자동으로 생성되는 폴더입니다.
* 2 차적인 백업 폴더로 사용자에 의해 백업된 데이터에 대하여 모든 프로세스로부터 위·변조 행위를 차단하여 보호합니다.
* 보호 대상 포맷에 제한되지 않습니다. (4 번 보호폴더 열기(Shield Zone) 참조)

체크 (기본값)

허용 프로세스(White List)를 포함한 모든 프로세의 수정 및 삭제 등 접근은 근본적으로 차단합니다.

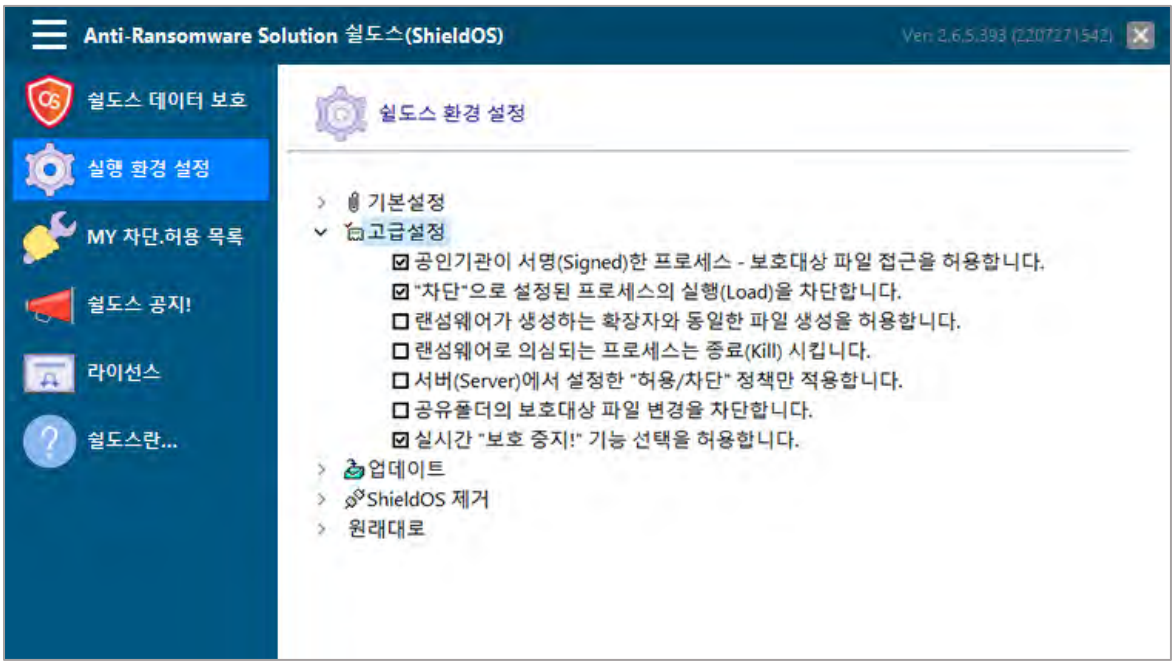
단, 보호폴더(C:₩Shield Zone)내 파일 탐색기(Explorer)만 모든 접근을 허용하므로 삭제도 가능합니다.

체크해제

파일 탐색기(Explorer)를 포함한 모든 프로세스의 수정 및 삭제 등 위·변조 행위를 차단합니다.

보안 강화를 위해서는 미 선택을 권장합니다.

3.2 고급설정



① 공인기관이 서명(Signed)한 프로세스 -보호대상 파일 접근을 허용합니다.

인가된 프로세스인 White List 외에도 인정 서명된 경우에는 White List 와 동일하게 허용하는 기능입니다. MS 나 기타 보안 프로그램은 보안 서명이 되어 있습니다. (보안 서명이 되어 있지 않다고 하여 모 두 악성코드는 아닙니다.

체크 (기본값)

보안 서명된 프로세스는 자동으로 White List 로 인정되어 인가된 프로세스가 됩니다.

"서명됨" 허용 메시지가 표시됩니다.

체크해제

보안 서명된 프로세스도 White List 에 등록되어 있지 않으면 비인가 프로세스로 판단 합니 다.
비인가 프로세스는 설정에 따라 [차단 · 허용 선택창]이 뜨게 됩니다.
보안강화를 위해서는 미선택을 권장하나 [차단 · 허용 선택창]이 많이 뜨게 됩니다. "Hold" 차단 메시지가 표시됩니다.

- "차단"을 선택하면 보호대상파일에 접근을 차단합니다.
- "허용"을 선택하면 보호대상 파일에 접근을 허용합니다.

② "차단"으로 설정된 프로세스의 실행(Load)을 차단합니다.
Black List 로 등록된 프로세스를 실행하지 못하게 하는 기능입니다.

체크 (기본값)

Black List 로 등록된 프로세스의 실행을 차단합니다. (실패하는 경우에는 [보호대상파일] 접근 시 프로세스를 강제종료(Kill) 시킵니다)
Black List 로 등록된 프로세스는 설치(저장)을 차단하여 실행이 불가능하게 합니다

"차단프로세스실행방지" 차단 메시지가 빨강색으로 표시됩니다.

체크해제

Black List 로 등록된 프로세스의 실행을 차단하지는 않으나 [보호대상파일]에 대한 접근은 차단합니다.
사용자 실수로 등록된 프로세스의 강제 종료로 인한 업무 지장을 최소화하고자 하는 기능입니다

"차단됨" 차단 메시지가 빨강색으로 표시됩니다.

③ 랜섬웨어가 생성하는 확장자와 동일한 파일 생성을 허용합니다.
차단 확장자로 등록된 파일을 생성을 허용하는 기능입니다. 기본적으로 랜섬웨어 의심 프로세스의 행 위에 대한 엔진의 분석에 따라 차단하도록 구현되어 있습니다.

체크

확장자 생성은 허용합니다.

체크해제 (기본값)

랜섬웨어 의심 프로세스를 강제 종료 (Kill) 시킵니다.

④ 랜섬웨어로 의심되는 프로세스는 강제종료 (Kill) 시킵니다.
엔진 분석 알고리즘에 의한 랜섬웨어 행위로 판단되는 프로세스를 종료시키는 기능입니다.

체크
랜섬웨어로 의심되면 해당 프로세스를 종료(Kill) 시킵니다.
비인가 프로세스이므로 [보호대상 파일]에 대한 접근을 차단합니다.
"랜섬의심됨 Kill" 차단 메시지가 빨강색으로 표시됩니다 (권장)

체크해제 (기본값)
프로세스를 종료시키지는 않으나 비인가 프로세스이므로 [차단·허용 선택창]을 뜨게 됩니다.
엔진 알고리즘이나 정책 설정에 대한 오류 발생 가능성에 대한 보완 기능입니다. "Hold" 차단 메시지가 표시됩니다.

⑤ 서버(Server)에서 설정한 "허용/차단" 정책만 적용합니다.
쉴도스 서버에 설정되어 있는 허용 및 차단 목록만 허용합니다. 목록은 좌측 (쉴도스란? -> ShieldOS 도움말 바로가기)에서 확인하실 수 있습니다.

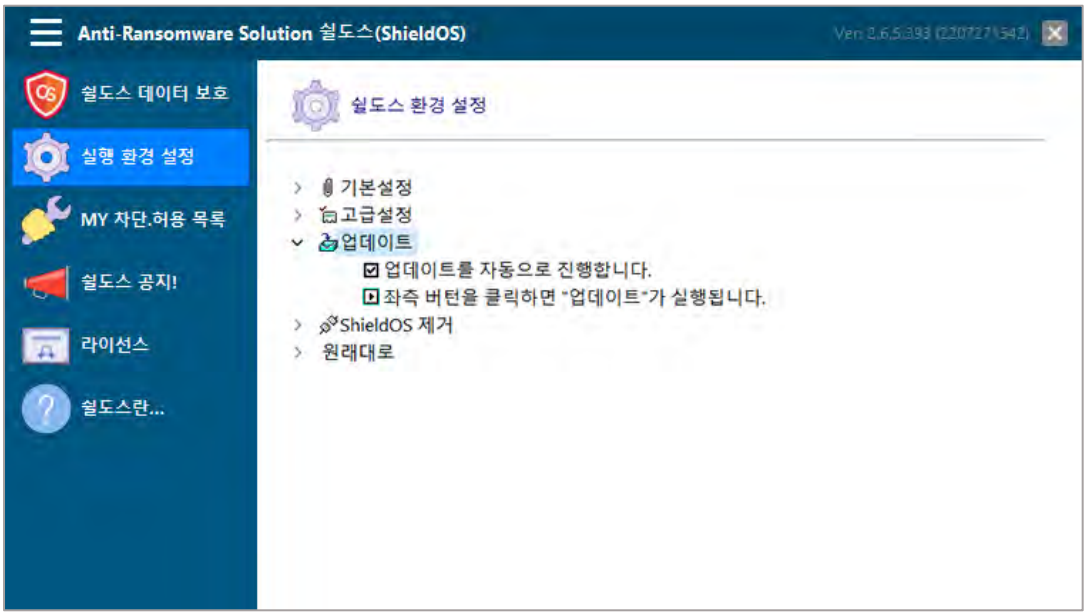
⑥ 공유폴더의 보호대상 파일 변경을 차단합니다.
공유폴더 내에 보호대상 파일(문서, 압축파일 등)에 대한 삭제, 수정을 하지 못하도록 차단하는 기능입니다.
보호대상 파일에 대한 목록은 ShieldOS 도움말 바로가기에서 볼 수 있습니다.

⑦ 실시간 "보호 중지!" 기능 선택을 허용합니다.
체크
[실시간 보호!]에서 [보호 중지!]로 엔진을 Off 시킬 수 있습니다.
Tray 메뉴에서 [실시간 보호!]를 클릭하면 되며, 엔진을 수동으로 On 시킬 수 있습니다.

체크해제 (기본값)
[실시간 보호!]에서 [보호 중지!]로 엔진을 Off 시킬 수 없습니다.
사용자에 의한 실수를 예방하기 위한 기능입니다.

3.3 업데이트

쉴도스 Agent 자동업데이트를 허용합니다.



① 아이콘을 클릭하면 업데이트가 실행됩니다.

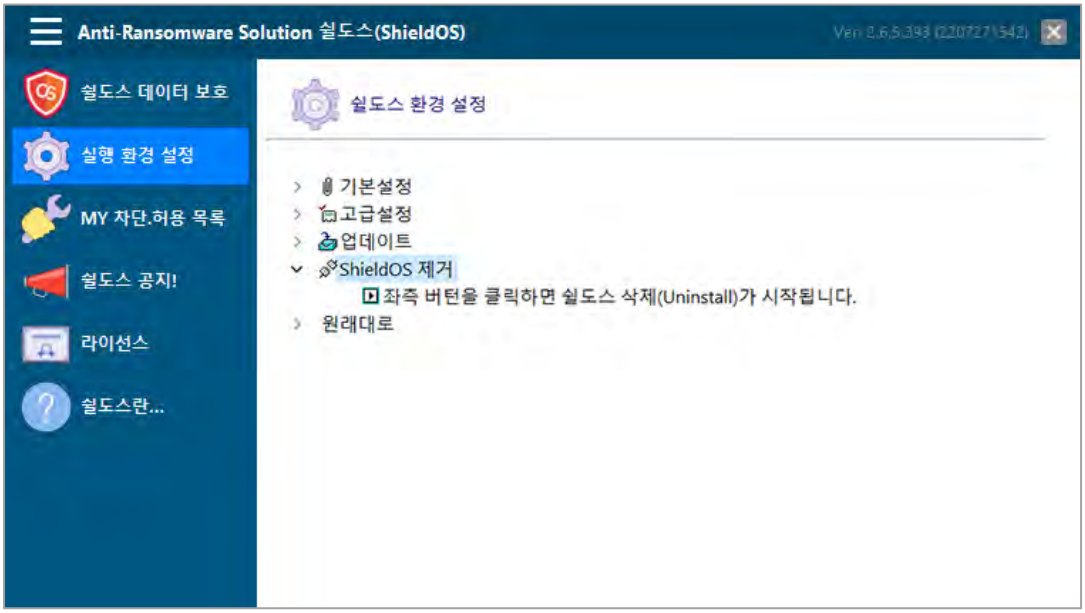
체크 (기본값)

자동으로 업데이트를 주기적으로 진행합니다.

체크해제

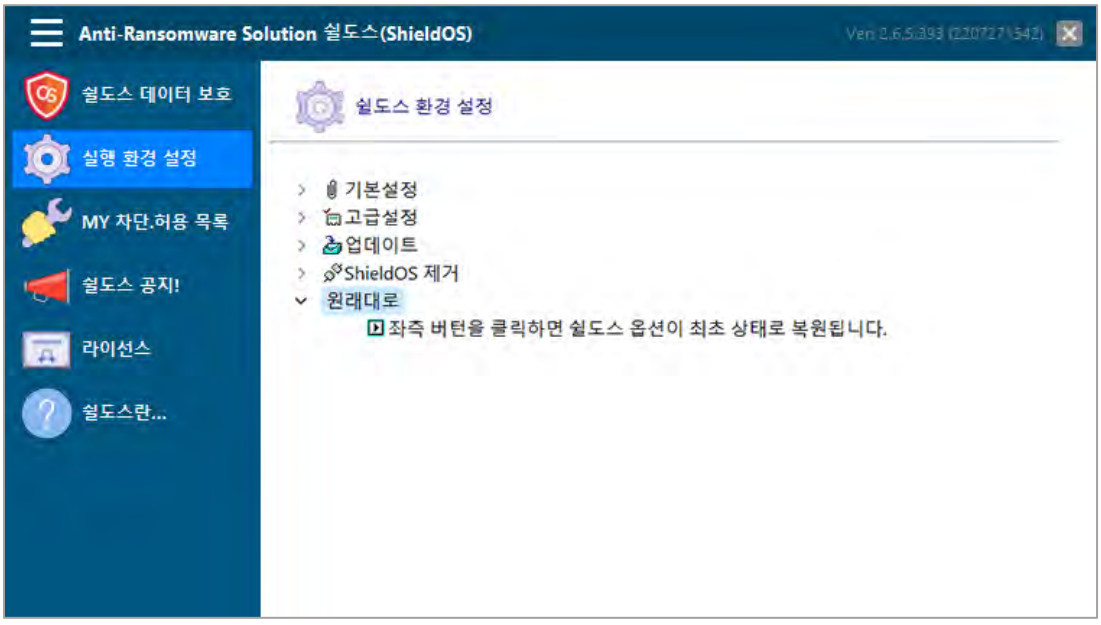
사용자 선택시에만 업데이트를 진행합니다.
아이콘을 클릭하면 업데이트가 실행됩니다.

3.4 쉴도스 제거



① 아이콘을 클릭하면 쉴도스 삭제가 시작됩니다.
좌측 버튼 아이콘을 클릭하면 쉴도스 삭제 진행을 위한 프로그램이 실행됩니다. 삭제 프로그램에서 진행 여부를 결정할 수 있습니다.
필요에 따라서는 원격으로 삭제를 할 수 있습니다. (라이센스 정책에 따라 불법적인 사용의 경우임)

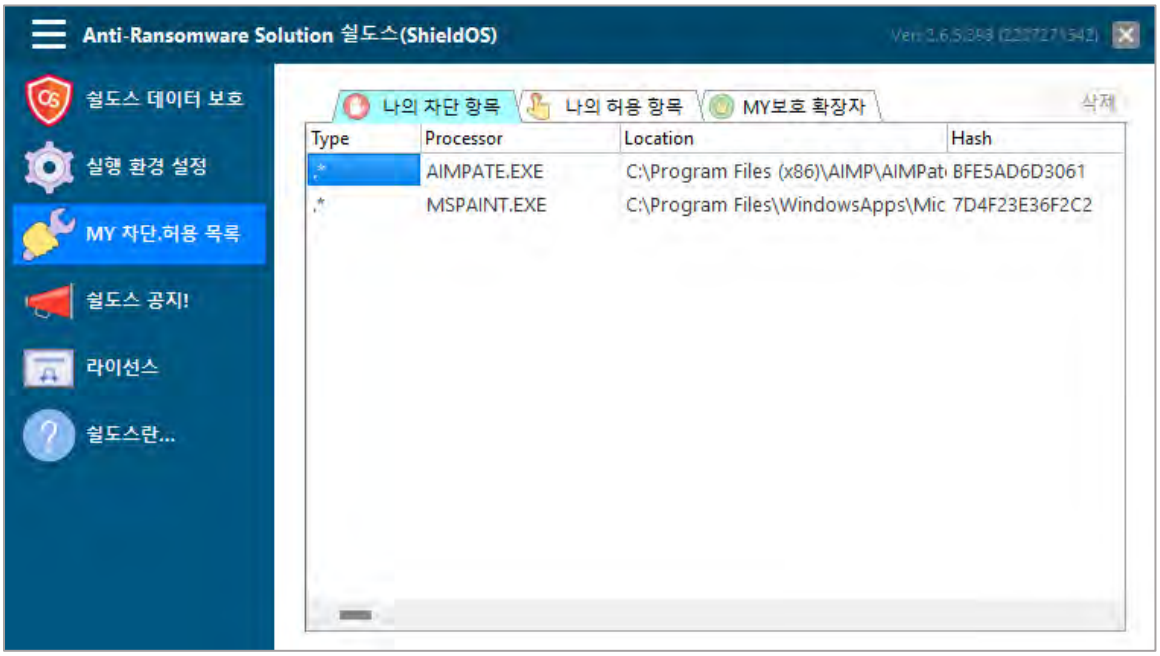
3.5 원래대로



① 아이콘을 클릭하면 쉴도스 기능설정이 초기화 됩니다.
좌측 버튼 아이콘을 클릭하면 설치 시 default 로 설정되어 있는 설정 값으로 변경이 되어 적용됩니다.

4 차단 및 허용항목 확인

4.1 나의 차단 항목



① 사용자에 의한 "차단"의 경우에 자동으로 등록됩니다. (실시간 등록)
차단·허용 선택창이 출력된 상태에서 사용자에 의해 "차단"을 선택하는 경우 등록됩니다.

② 사용자 정의 Black List 로 사용됩니다.
Black List 로 등록 후에는 해당 프로세스는 차단됩니다.

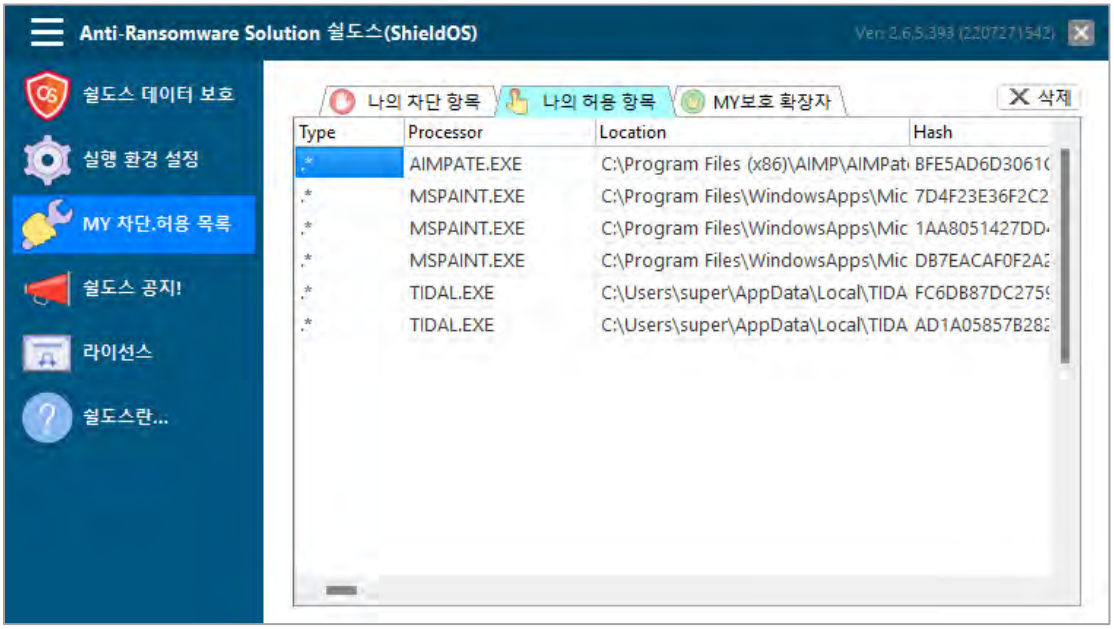
③ 고급설정에 따라 실행 자체를 차단하거나 보호대상파일에 접근할 경우 프로세스를 종료시킵니다.

④ 운영자에 의한 Black List 도 동일하게 작동합니다. (사용자는 List 확인이 불가능함)

⑤ 사용자 정의 Black List 는 사용자에 의해 삭제가 가능합니다.

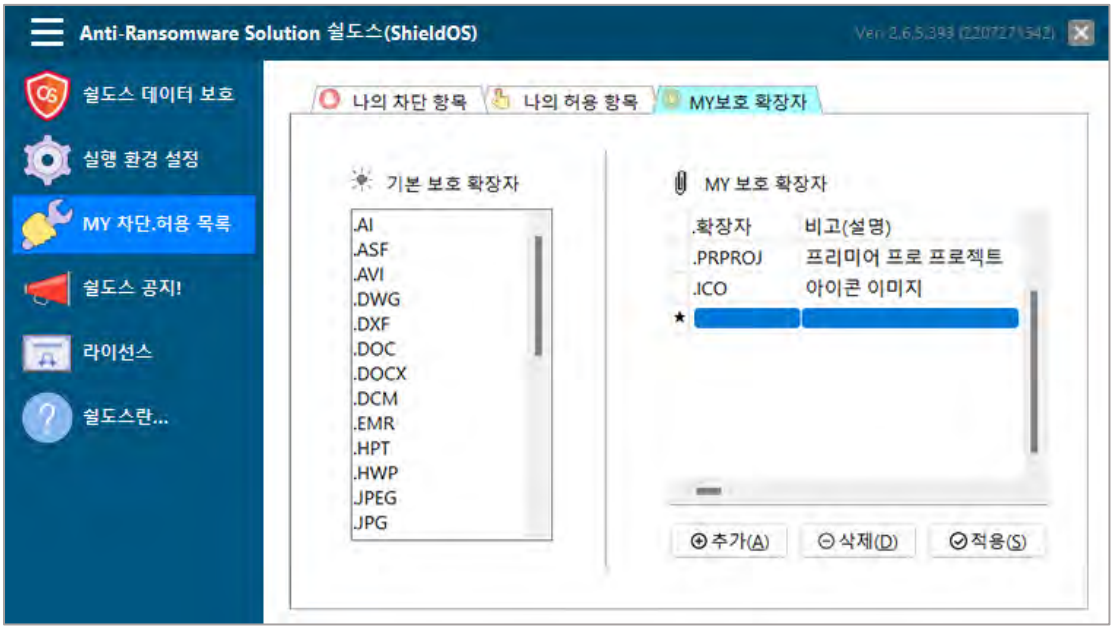
⑥ 삭제를 원하는 프로세스를 선택 후 상단 우측에 있는 삭제 버튼 클릭하면 삭제됩니다.

4.2 나의 허용 항목



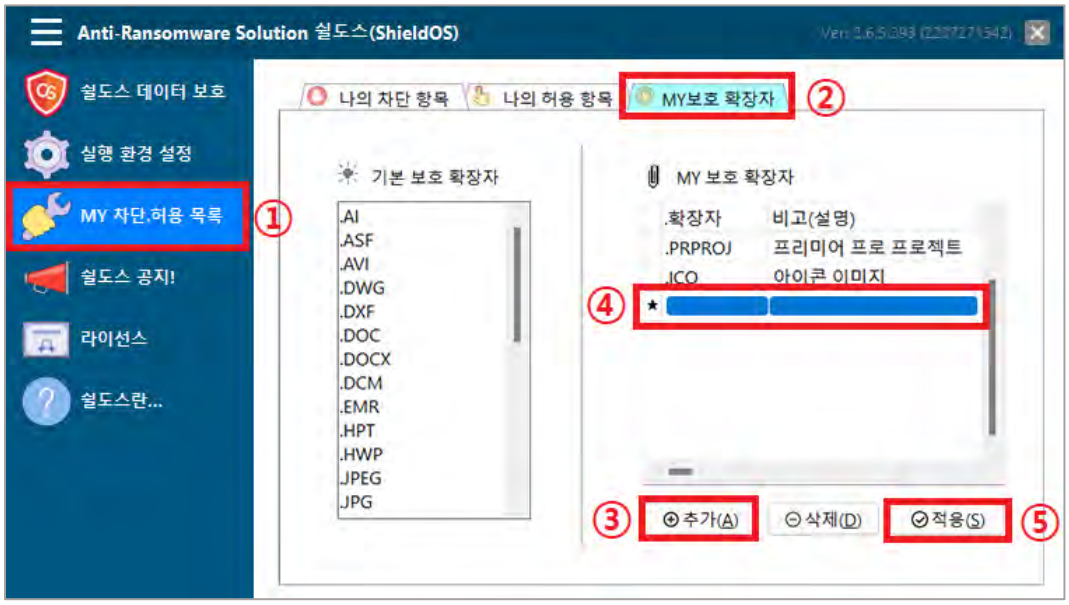
① 사용자에 의한 "허용"의 경우에 자동으로 등록됩니다. (실시간 등록)
② 차단, 허용 선택창이 출력된 상태에서 사용자에 의해 "허용"을 선택하는 경우 등록됩니다.
③ 사용자 정의 White List 로 사용됩니다
④ White List 로 등록 후에는 해당 프로세스는 허용됩니다.
⑤ 운영자에 의한 White List 도 동일하게 작동합니다. (사용자는 List 확인이 불가능함)
⑥ 사용자 정의 White List 는 사용자에 의해 삭제가 가능 합니다.
⑦ 삭제를 원하는 프로세스를 선택 후 상단 우측에 있는 삭제 버튼 클릭하면 삭제됩니다.

4.3 MY 보호 확장자



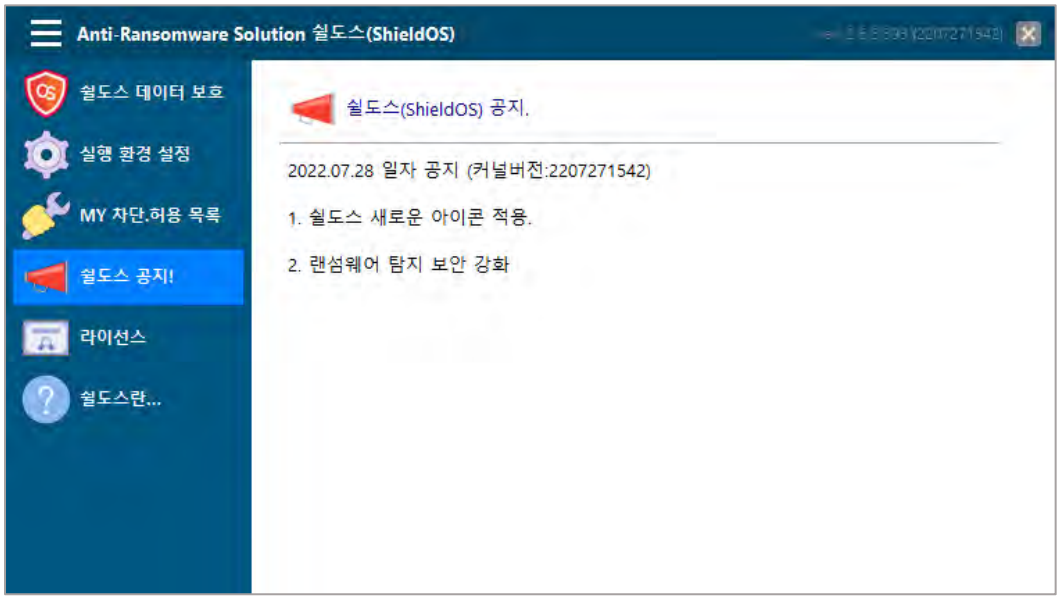
사용자가 직접 보호 확장자를 등록할 수 있습니다.

확장자 등록하는 방법



① MY 차단, 허용 목록 선택
② MY 보호 확장자 탭으로 이동
③ 추가 클릭
④ 추가할 확장자명과 비고란 입력 (확장자명 대소문자 구분 X)
⑤ 적용 클릭

5 쉴도스 공지



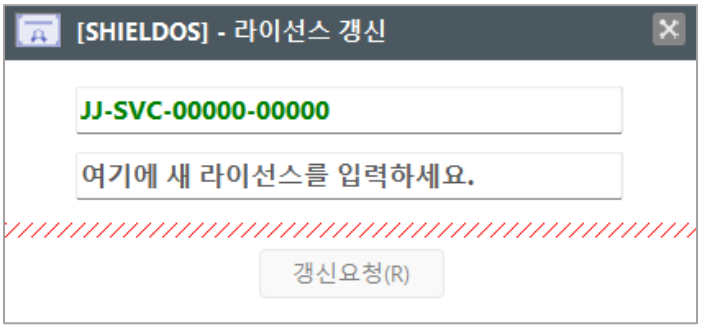
쉴도스 주요 공지사항을 확인할 수 있습니다. (전체공지 바로가기 클릭 시, 웹 페이지로 전체공지 확인이 가능합니다.)

6 라이선스

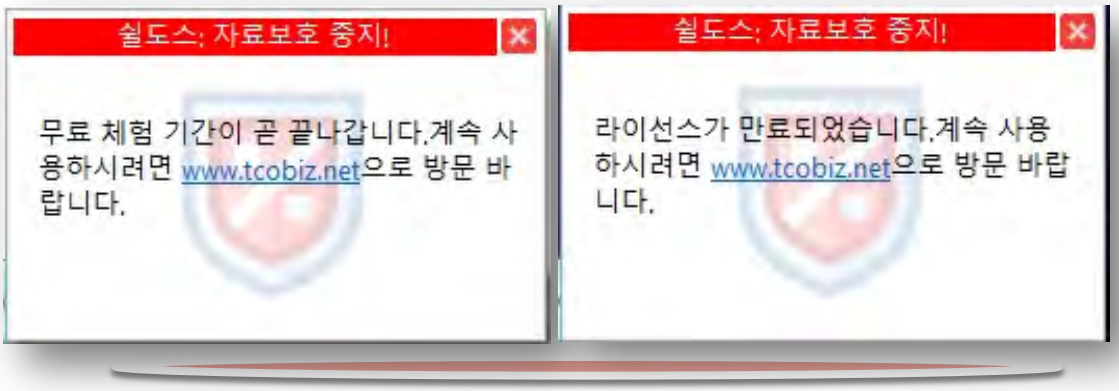
PC 에 설치된 에이전트의 라이선스를 확인 및 갱신할 수 있습니다.
(우측 하단 쉴도스 아이콘 더블클릭 -> 라이선스)

6.1 라이선스 갱신

라이선스 갱신 버튼을 누르면 아래와 같은 화면이 나타나며 갱신할 라이선스를 입력할 수 있습니다.



6.2 라이선스 이전 및 만료 시

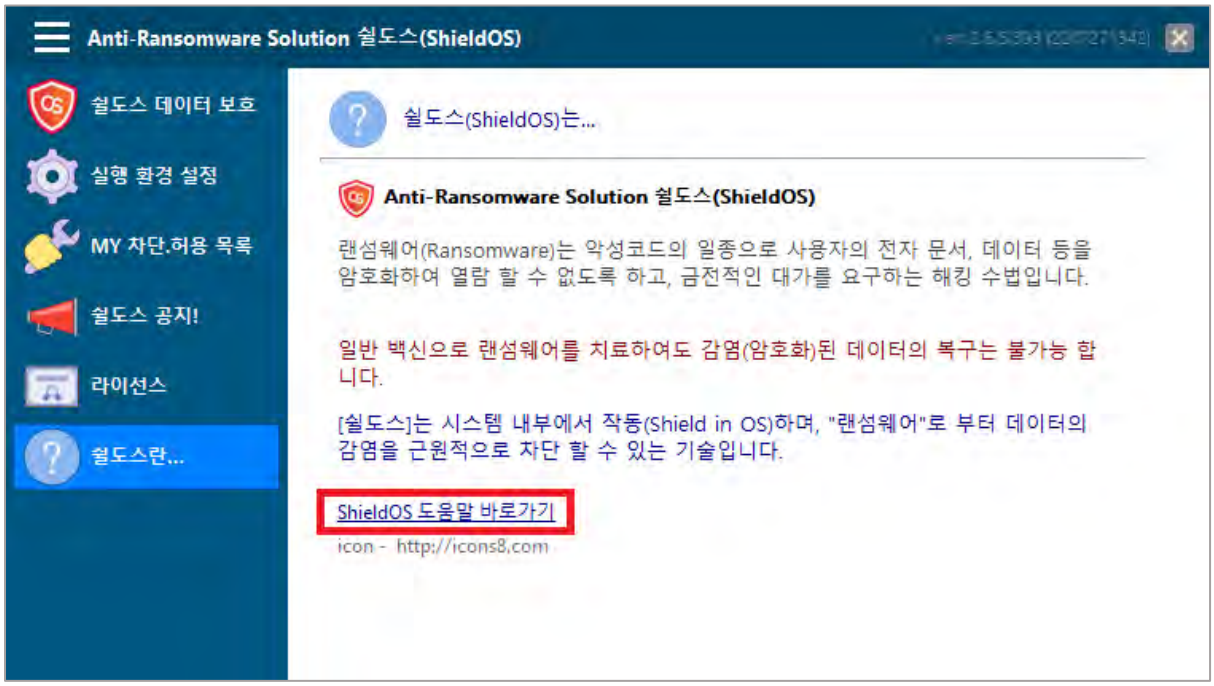


라이선스 만료되기 전 또는 라이선스가 만료되면 아래와 같은 메시지가 팝업 됩니다. 그리고 라이선스를 갱신하지 않아 만료되면 쉴도스의 데이터 보호기능이 일괄 중지됩니다.

7 ShieldOS 란

쉴도스에 대한 설명과 도움말 웹페이지를 제공합니다.

✓ Anti-Ransomware Solution 쉴도스(ShieldOS)는 랜섬웨어에 대한 감염을 근원적으로 차단할 수 있는 솔루션입니다. 랜섬웨어는 악성코드의 일종으로, 사용자의 전자문서, 데이터 등을 암호화하여 열람할 수 없도록 하고, 금전적인 대가를 요구하는 해킹 수법입니다.



① 쉴도스란 탭으로 이동하면 ShieldOS 도움말 바로가기라는 항목이 있습니다.
② 페이지의 가장 하단으로 이동합니다.
③ ShieldOS 의 보호 대상 포맷이라는 항목으로 정의되어 있습니다.