TACHYON

TACHYON

Internet Security 5.0

사용자 설명서

INCA I.n.t.e.r.n.e.t

목차

1장

제품 소개

1. 제품 소개

1. 제품 소개

TACHYON Internet Security 5.0은 강력한 엔드포인트 보안 기술로 고도화된 악성코드, 스파이웨어, 랜섬웨어를 비롯한 각종 사이버 위협을 안전하게 차단합니다. 더욱 향상된 실시간 감시와 보호 기능으로 사용자 시스템과 중요 정보를 안전하게 지켜 드립니다.

자체 엔진과 비트디펜더 엔진을 기반으로 높은 악성코드 탐지 및 진단율

TACHYON Internet Security 5.0은 잉카인터넷의 TACHYON 기반의 엔진과 비트디펜더의 엔진을 동시에 사용함으로써 높은 악성코드 탐지 및 진단율을 가지고 있습니다. 이를 통해 국내외 악성코드에 대해 발빠르게 대응하여 안심하게 PC를 이용할 수 있습니다.

≫ 기능

안티 멀웨어

- 바이러스, 스파이웨어, 랜섬웨어를 비롯한 악성코드 실시간, 정밀 검사
- 다양한 파일 포맷 분석과 멀티 진단
- MS워드, 엑셀, 파워포인트의 매크로 바이러스 탐지
- 한글, PDF 문서의 익스플로잇 악성코드 삭제

행위기반 탐지

- 기존 안티바이러스 엔진으로 탐지가 어려운 신변종 악성코드 진단
- APT 공격 사전방지

랜섬웨어 차단

- 랜섬웨어로 의심되는 프로그램 탐지 및 차단
- 파일 암호화 및 훼손 행위 방지

MBR 보호

- MBR 영역 해킹 차단
- PC 부팅 불능 및 데이터 손상 방지

방화벽

- 네트워크 실시간 보호로 해킹 방지
- 비정상적인 트래픽 유입 차단
- 공유폴더 감시 및 접근 관리
- 외부 통신 프로그램 실행 감지 및 알림
- IP/Port 불법적 접근 탐지 및 차단

무결성 검증

- 제품 내 모듈 위·변조 해킹 여부 확인

자체 보호

- 제품 자체 레지스트리, 파일, 프로세스 보호

검역소

- 검역소에 저장된 악성코드 백업 및 복원

PC 관리

- PC에 설치된 설치 프로그램, ActiveX, 시작 프로그램, 툴바 관리

PC 최적화

- 네트워크 속도, 메모리 사용량, 시스템 설정 등 최적화

파일 삭제

- 파일 및 폴더 완전 삭제 기능 지원
- 파일 삭제 알고리즘 4종류 지원, 원하는 알고리즘으로 파일 삭제 가능
- 삭제된 데이터 공간에 반복적으로 데이터를 덮어씀으로써 파일 복구를 방지

업데이트

- 실시간 정기 및 긴급 패턴/제품 업데이트 기능
- 예약 설정을 통한 주기적인 패턴/제품 업데이트 기능
- 자동/수동 업데이트 기능

로그

- 제품의 동작 및 악성코드 진단/치료 등의 로그

※ 체험판 사용 기간 이후에는 다수 기능이 해제되므로, 결제 후 모든 기능을 사용하실 수 있습니다.

2장

제품 설치

1. 설치 환경

2. 설치하기

3. 삭제하기

1. 설치 환경

TACHYON Internet Security 5.0을 설치하기 위해서는 다음의 하드웨어 및 소프트웨어 환경을 만족해야 합니다. 시스템 사양을 확인하신 후에 설치하여 주시기 바랍니다.

구분		내용
하드웨어 사양	CPU	Intel Pentium 4 3.8GHz 이상
	RAM	2GB 이상
	Hard Disk	20GB 이상
운영 체제		Microsoft Windows XP SP3 (32bit) Microsoft Windows Vista SP2 (32bit, 64bit) Microsoft Windows 7 SP1 (32bit, 64bit) Microsoft Windows 8.0 (32bit, 64bit) Microsoft Windows 8.1 (32bit, 64bit) Microsoft Windows 10 (32bit, 64bit) Microsoft Windows 11 (64bit)
지원 언어		한국어, 영어

※ TACHYON 제품이 지원하는 운영체제의 일반 사항이며, 상세 버전은 별도 문의 제공

2. 설치하기

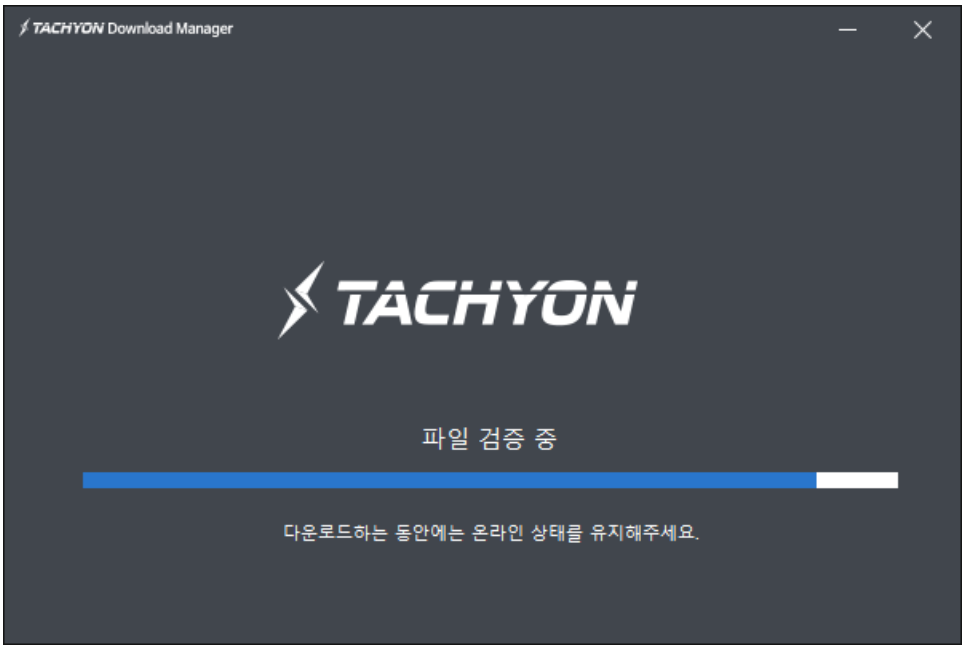
TACHYON Internet Security 5.0은 설치파일을 통해 PC에 설치 할 수 있습니다.

※ TACHYON Internet Security 5.0을 설치하기 전에 이전에 설치한 안티바이러스 및 타사 안티바이러스가 설치되어 있다면 삭제 후 설치를 진행하여 주시기 바랍니다.

1. 다운로드 받은 TIS_Trial.exe 파일을 실행합니다.

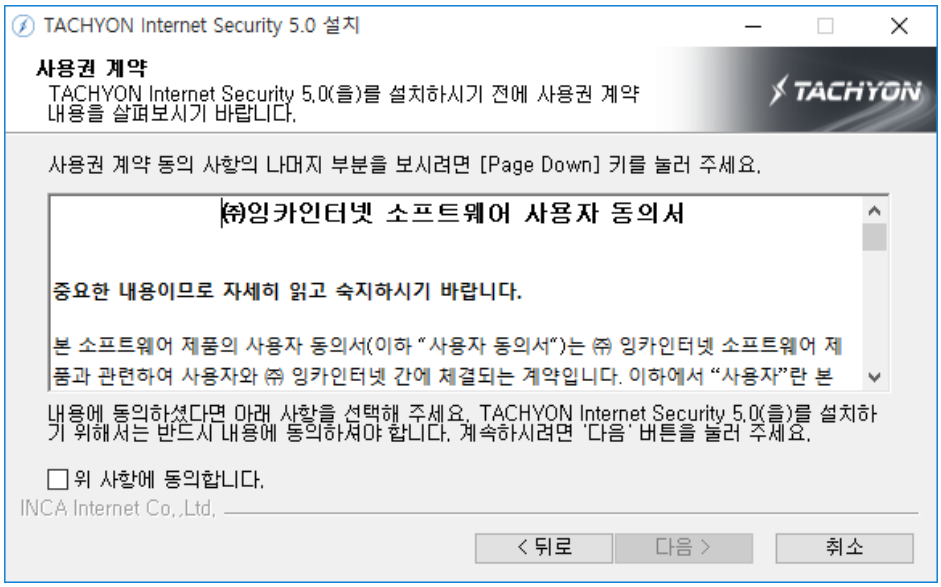
2. TACHYON Internet Security 5.0 설치 파일을 다운로드 받습니다.

3. 다운로드 받은 파일에 대한 검증을 합니다.

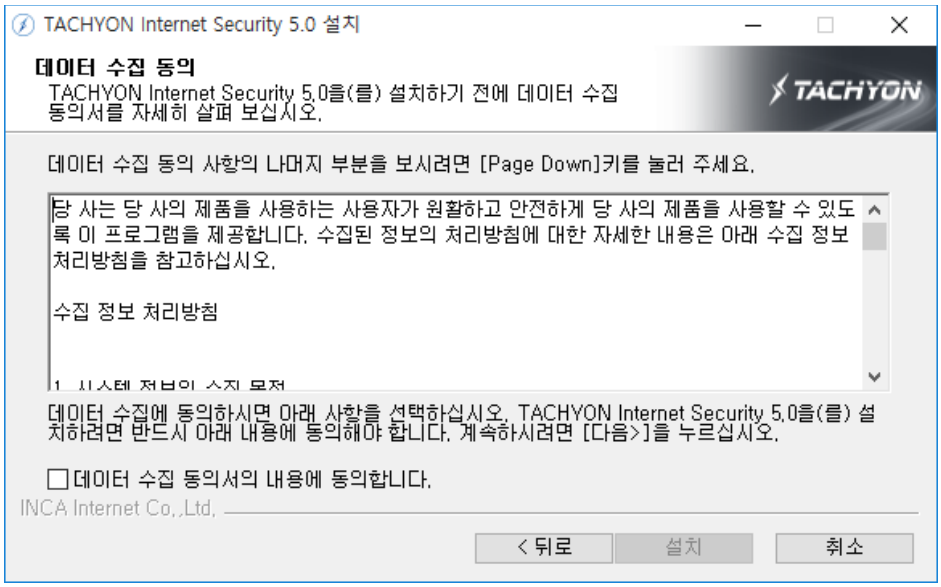


4. 검증이 완료되고, 설치 시작 첫 화면이 나타나면 [다음]을 누릅니다.

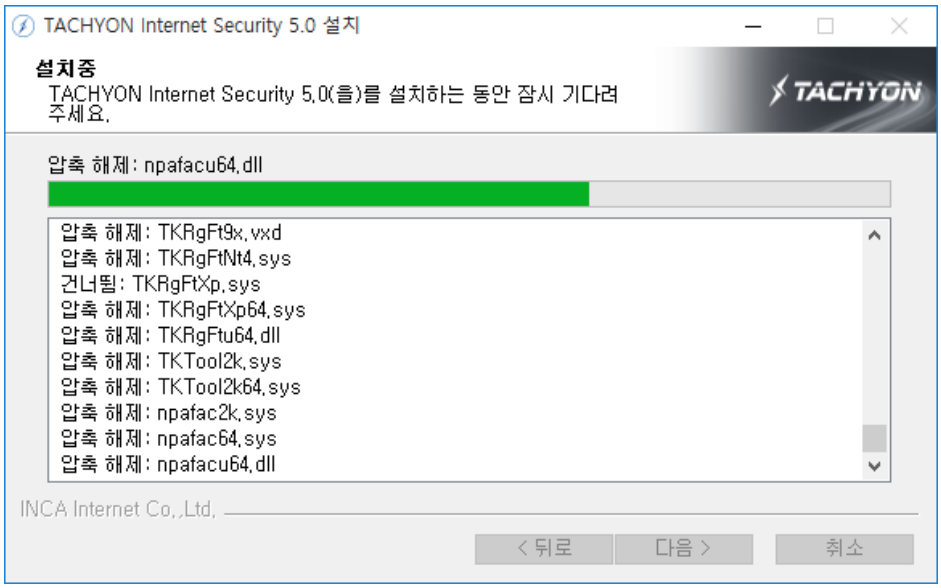
5. [사용권 계약] 화면은 ㈜잉카인터넷 소프트웨어 사용권 계약서의 내용입니다. 사용권 계약서 내용을 잘 읽은 후 내용에 동의하면 “위 사항에 동의합니다.” 선택 후 [다음]을 누릅니다.



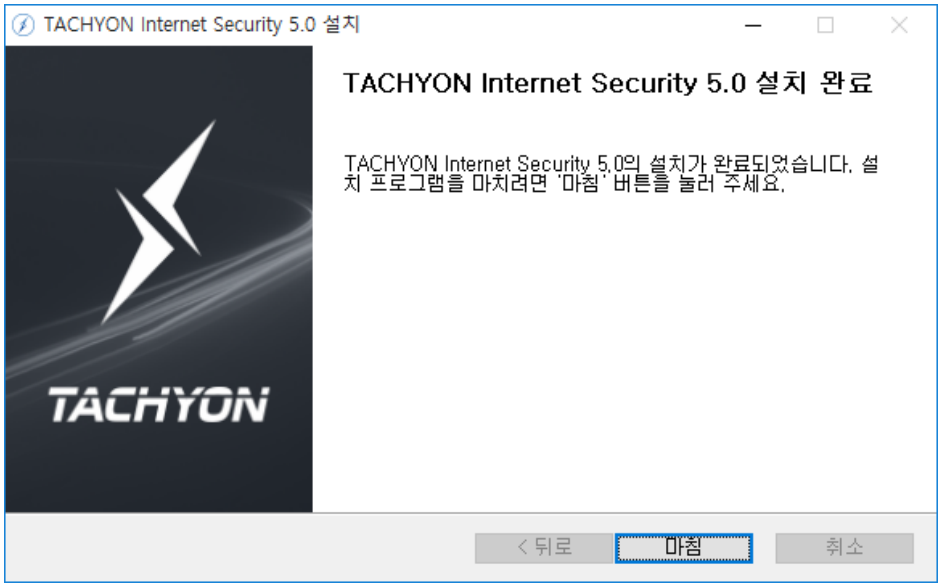
6. [데이터 수집 동의] 화면은, ㈜잉카인터넷 데이터 수집 동의 내용입니다. 데이터 수집 동의 내용을 잘 읽은 후 내용에 동의하면 “데이터 수집 동의서의 내용에 동의합니다.”를 선택 후 [다음]을 누릅니다.



7. 설치 작업을 진행합니다. 설치가 완료될 때까지 기다려 주십시오.



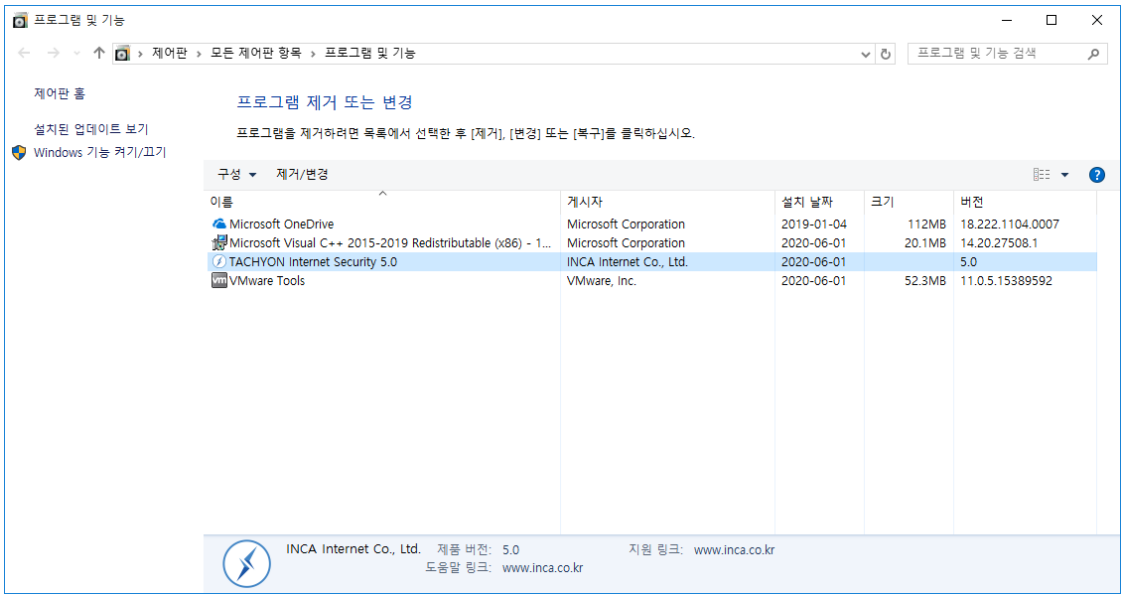
8. 설치 작업이 완료가 되면 [마침]을 클릭하여 설치를 최종적으로 완료합니다.



3. 삭제하기

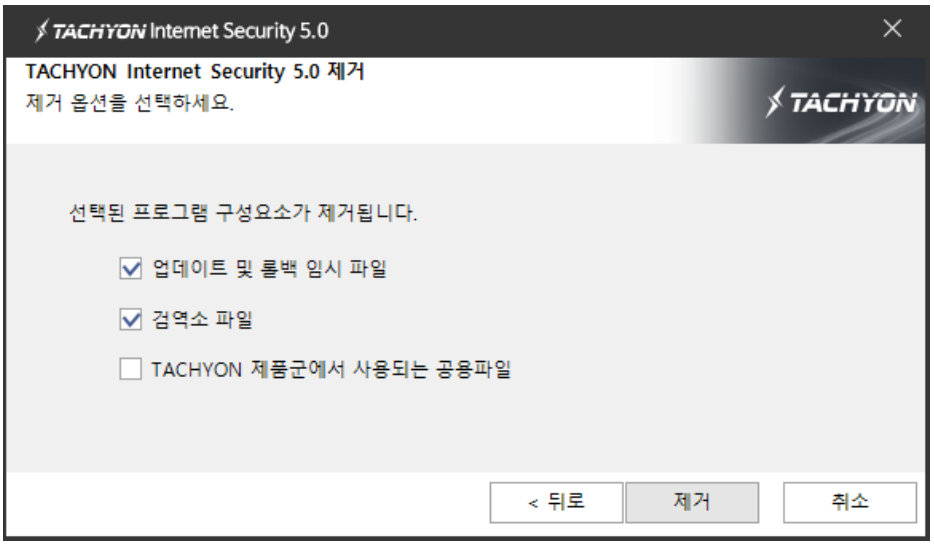
TACHYON Internet Security 5.0은 아래와 같은 방식으로 삭제할 수 있습니다.

1. 시작 > 제어판 > 프로그램 추가/제거에서 “TACHYON Internet Security 5.0” 선택 후 [제거/변경]을 클릭하여 삭제를 시작합니다.

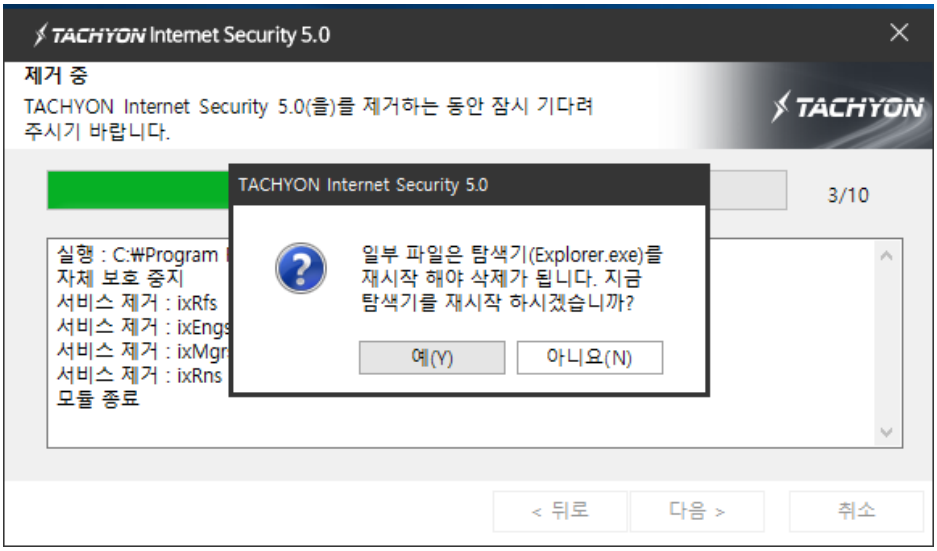


2. TACHYON Internet Security 5.0 제거 화면에서 [다음]을 누릅니다.

3. 제거할 항목을 선택 후 [제거]를 선택하면 삭제가 시작됩니다.



4. 삭제가 진행 중 “일부 파일은 탐색기(Explorer.exe)를 재시작해야 삭제가 됩니다. 지금 탐색기를 재시작 하시겠습니까?” 메시지가 나타날 수 있습니다. 제거를 완료하기 위해 [예(Y)]를 선택하여 주십시오.



5. 탐색기 재시작 여부 메시지에서 [얘(Y)]를 클릭하면 TACHYON Internet Security 5.0 의 삭제가 완료되며 [마침]을 클릭하여 제거를 최종적으로 완료합니다.

3장

둘러보기

1. 실행하기

2. 업데이트

3. 트레이

1. 실행하기

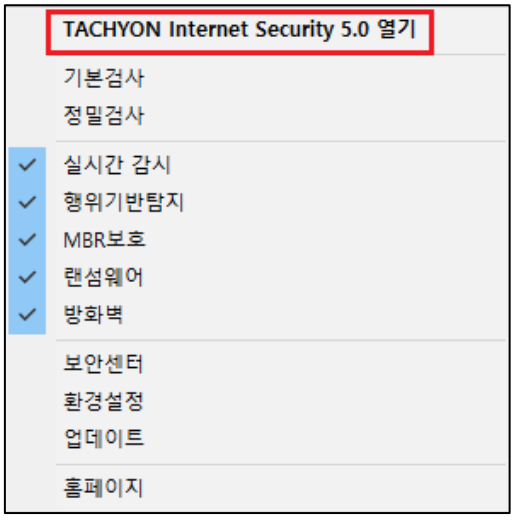
TACHYON Internet Security 5.0은 다양한 방법으로 실행할 수 있습니다.

바탕화면 아이콘을 이용한 실행

바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘을 더블 클릭합니다.

작업표시줄 트레이 아이콘을 이용한 실행

TACHYON Internet Security 5.0 트레이 아이콘 ( )에서 마우스 우클릭한 후, “TACHYON Internet Security 5.0 열기” 메뉴를 선택합니다.



2. 업데이트

업데이트는 TACHYON Internet Security 5.0 사용을 위한 가장 중요한 기능 중 하나입니다.

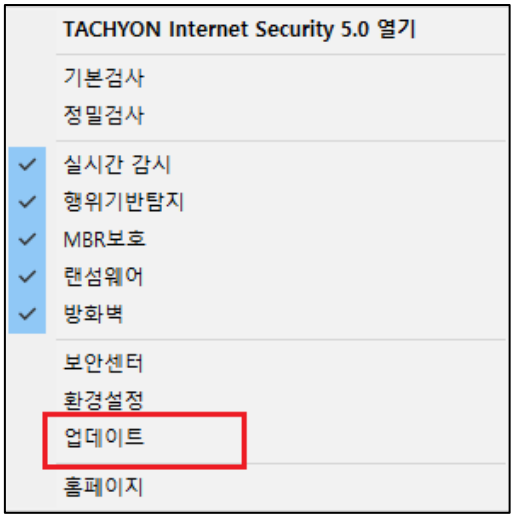
백신 프로그램은 최신 엔진의 업데이트를 적용한 후에 악성코드를 검사해야 새로 발견된 악성코드까지 검사 및 치료할 수 있습니다.

업데이트를 클릭하면 TACHYON 업데이트 서버에 접속하여 최신 엔진 파일로 업데이트합니다.

실행 방법

■ 트레이 아이콘에서 실행하기

TACHYON Internet Security 5.0 트레이 아이콘( )에서 마우스 우클릭한 후, “업데이트”를 선택하면 실행할 수 있습니다.

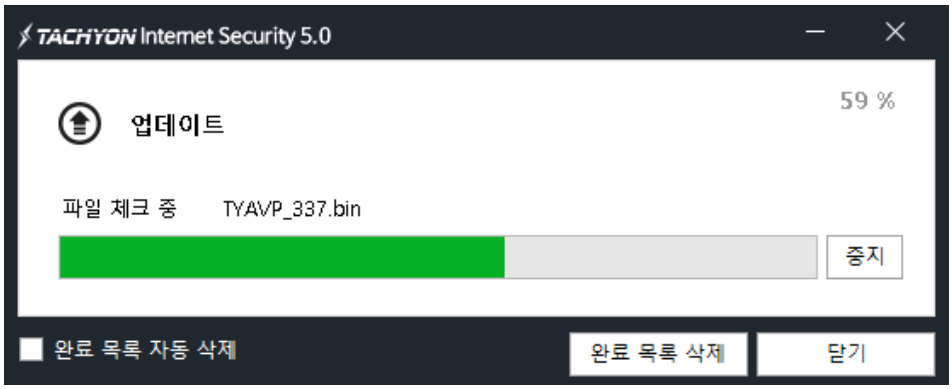


■ 메인 화면에서 실행하기

TACHYON Internet Security 5.0 실행 후 메인 화면에서 [업데이트]를 클릭하여 실행할 수 있습니다.

업데이트 진행 상태

업데이트를 실행하면 진행 상태를 확인할 수 있습니다.



■ 진행 비율 : 업데이트 진행 비율을 표시합니다.

업데이트 진행 메시지

업데이트를 실행하면 진행 단계별로 다음과 같은 메시지가 화면에 나타납니다.

- 준비 중 : 업데이트를 실행한 후 처음 나타나는 메시지로 업데이트를 위한 준비 과정입니다.
- 분석 중 : 업데이트를 위해 PC를 분석하고 있는 과정입니다.
- 파일 체크 중 : 업데이트 대상 파일을 검색하는 과정입니다.
- 다운로드 중 : 업데이트 서버에서 대상 파일을 다운로드 하는 과정입니다.
- 적용 중 : 업데이트 대상 파일을 PC에 복사하는 과정입니다.
- 서비스 중지 중 : 업데이트를 하기 위해 TACHYON Internet Security 5.0 프로세스를 중지하는 과정입니다.
- 서비스 시작 중 : 업데이트를 하기 위해 중지했던 TACHYON Internet Security 5.0 프로세스를 다시 시작하는 과정입니다.
- 패턴 언로드 중 : 업데이트를 하기 위해 TACHYON Internet Security 5.0 패턴을 언로드 하는 과정입니다.
- 패턴 로드 중 : 업데이트를 하기 언로드했던 TACHYON Internet Security 5.0 패턴을 다시 로드 하는 과정입니다.
- 완료 : 업데이트 파일을 다운로드하여 적용을 마친 경우입니다.

3. 트레이

TACHYON Internet Security 5.0을 설치하면 작업 표시줄 우측에 트레이 아이콘( )이 등록됩니다.

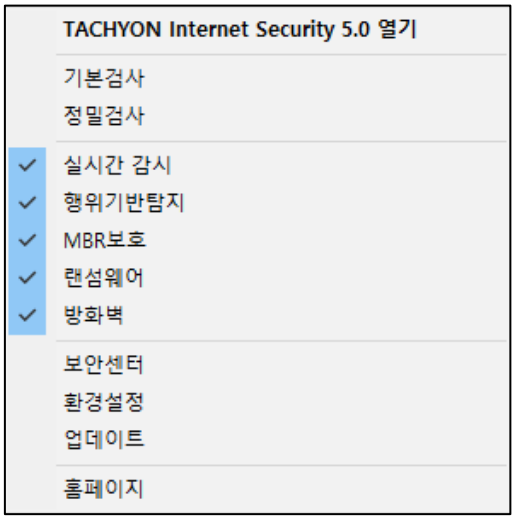
TACHYON Internet Security 5.0의 트레이 아이콘은 실시간 감시 동작 여부에 따라 아이콘 모양이 변경됩니다.

트레이 아이콘

- : TACHYON Internet Security 5.0의 실시간 감시가 실행 중인 경우입니다.
- : TACHYON Internet Security 5.0의 실시간 감시가 중지된 경우입니다.

트레이 아이콘 메뉴

TACHYON Internet Security 5.0의 트레이 아이콘에서 마우스 오른쪽 버튼을 클릭하면 TACHYON Internet Security 5.0의 주요 기능을 실행할 수 있습니다.



- TACHYON Internet Security 5.0 열기 : TACHYON Internet Security 5.0 프로그램의 메인 화면을 보여줍니다.
- 기본검사 : 악성코드의 감염 위험이 높은 중요 폴더와 파일을 검사하는 기본검사를 실행합니다.

기본검사를 실행하면, 기본검사 진행화면이 나타납니다.

- 정밀검사 : 사용자가 지정한 폴더를 검사하는 정밀검사를 실행합니다.
- 실시간 검사 : 사용자 PC에서 발생하는 파일의 복사, 이동, 실행 등의 행위를 검사하는 기능입니다. 실시간 검사를 실행하거나 실행을 중지할 수 있습니다.
- 행위기반탐지 : 악성코드의 행위를 탐지하여 차단하는 기능입니다. 행위기반탐지를 실행하거나 실행을 중지할 수 있습니다.
- MBR보호 : 다른 프로그램이 MBR(Master Boot Record) 영역에 접근하는 것을 차단하는 기능입니다. MBR보호를 실행하거나 실행을 중지할 수 있습니다.
- 랜섬웨어 : 랜섬웨어 악성코드를 탐지하여 차단하는 기능입니다. 랜섬웨어 차단을 실행하거나 실행을 중지할 수 있습니다.
- 방화벽 : 정보보안을 위해 외부에서 내부, 내부에서 외부로의 접근을 허용하거나 차단하는 기능입니다. 방화벽을 실행하거나 실행을 중지할 수 있습니다. 세부기능으로는 침입차단, 침입방지, 프로그램 인증, 파일/프린터 공유 차단, 사이트 차단 기능이 있습니다.
- 보안센터 : 실시간 보호(실시간 감시, 행위기반탐지, MBR보호, 랜섬웨어 차단), 업데이트, 위협요소 보안상태 정보를 이용하여 사용자 시스템의 보안상 문제점을 확인할 수 있습니다.
- 환경설정 : 제품에서 사용할 수 있는 다양한 옵션에 대해 사용자가 직접 선택하여 사용할 수 있는 기능입니다.
- 업데이트 : 업데이트를 즉시 실행합니다.
- 홈페이지 : 인터넷 웹브라우저를 실행하여 잉카인터넷의 홈페이지를 연결합니다.

4장

화면 구성

1. 화면 구성

1. 화면 구성

TACHYON Internet Security 5.0을 실행하면 첫 화면으로 메인 화면이 보이며, 제품의 보안 상태와 엔진 버전, 모듈 버전 등이 보이며, 제품의 검사, 업데이트 등을 실행할 수 있습니다.

A 영역

- ? : TACHYON Internet Security 5.0의 도움말을 실행합니다.
- — : TACHYON Internet Security 5.0 화면을 최소화합니다.
- ✕ : TACHYON Internet Security 5.0 화면을 닫습니다.

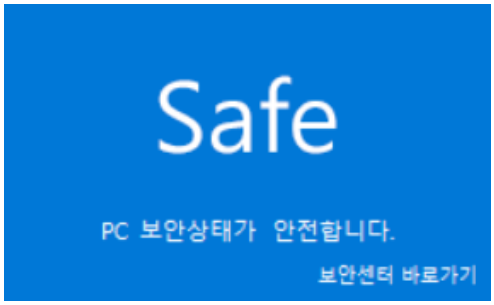
B 영역

- HOME : TACHYON Internet Security 5.0의 메인 화면으로 이동 합니다.
- PC 최적화 : PC 최적화를 실행합니다. PC 최적화는 네트워크 속도, 메모리 사용량, 시스템 설정을 변경하여 최적의 PC 환경과 인터넷 속도를 즐길 수 있습니다.
- 검역소 : 검역소를 실행합니다. 악성코드 치료 전 백업된 파일을 확인 및 복원할 수 있습니다.
- 로그 : 진단된 위협 요소 및 사용자 또는 제품 동작에 대한 로그를 확인 할 수 있습니다.
- 환경설정 : TACHYON Internet Security 5.0에서 제공하는 기능에 대한 ON/OFF 및 옵션을 설정할 수 있습니다.

C 영역

TACHYON Internet Security 5.0의 실시간보호(실시간감시, 방화벽, MBR보호, 행위기반탐지 등), 업데이트 사용 여부에 따른 보안상태를 색깔별로 표시합니다.

- Safe(파란색 표시) : 실시간 감시/행위기반탐지/MBR보호/랜섬웨어 차단 기능이 정상 동작 중이며, 업데이트 항목 및 위협요소가 존재하지 않을 경우 “PC 보안 상태가 안전합니다.”로 표시합니다.

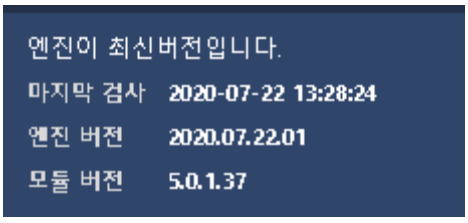


■ Warning(노란색 표시) : 실시간 감시/행위기반탐지/MBR보호/랜섬웨어 차단 기능이 정상 동작 중이나, 최신 업데이트 항목 및 위협요소가 존재할 경우 “PC의 점검이 필요합니다.”로 표시합니다.

■ Danger(빨강색 표시) : 실시간 감시/행위기반탐지/MBR보호/랜섬웨어 차단 기능 중 하나라도 중지된 경우 “PC가 위험한 상태입니다.”로 표시합니다.

D 영역

TACHYON Internet Security 5.0의 모듈 및 엔진의 업데이트 상태 및 마지막 검사 시간을 표시합니다.



■ 엔진이 최신버전입니다. : TACHYON Internet Security 5.0의 모듈 및 엔진의 업데이트 상태가 최신인 상태입니다.

■ 엔진이 최신버전이 아닙니다 : TACHYON Internet Seucrity 5.0의 모듈 및 엔진의 업데이트 상태

가 최신이 아닌 상태입니다.

- 마지막 검사 : 기본, 정밀검사를 통해 마지막으로 악성코드 검사를 실행한 시간을 표시합니다.
- 엔진 버전 : 현재 TACHYON Internet Security 5.0의 엔진 버전을 표시합니다.
- 모듈 버전 : 현재 TACHYON Internet Security 5.0의 모듈 버전을 표시합니다.

E 영역

- 업데이트 : 모듈 및 패턴 업데이트를 실행합니다. 사용자가 수동으로 업데이트 할 수 있습니다.
- 신고하기 : 신고하기는 악성코드로 의심되거나 치료가 실패한 파일을 잉카인터넷으로 보낼 수 있는 기능입니다.

F 영역

- 기본검사 : 악성코드 기본 검사를 실행합니다. 주요 시스템 경로 및 현재 실행중인 프로세스를 검사합니다.
- 정밀검사 : 악성코드 정밀 검사를 실행 합니다.
- 방화벽 : 방화벽 기능의 ON/OFF 할 수 있는 설정화면으로 이동합니다.
- PC관리 : 프로그램, ActiveX, 시작 프로그램, 툴바 관리를 할 수 있습니다.
- 파일 완전 삭제 : 파일 및 폴더를 복구 프로그램으로 복구되지 않도록 완전 삭제할 수 있는 기능입니다.

G 영역

- 실시간 감시 : 악성코드 실시간 감시 기능 ON/OFF 및 실시간 상태를 확인할 수 있습니다.
- 행위기반탐지 : 행위기반탐지 기능 ON/OFF 설정이 가능합니다.

- MBR 보호 : MBR 보호 기능 ON/OFF 설정이 가능합니다.
- 랜섬웨어차단 : 랜섬웨어차단 기능 ON/OFF 설정이 가능합니다.

5장

보안센터

1. 보안센터

1. 보안센터

TACHYON Internet Security 5.0 메인 화면에서 보안상태를 클릭하면 실시간 보호 기능의 실행 상태를 한 화면에서 확인 할 수 있습니다.

이 실시간 보호 기능의 ON/OFF 상태에 따라 메인 화면의 보안상태 색상이 변경됩니다.

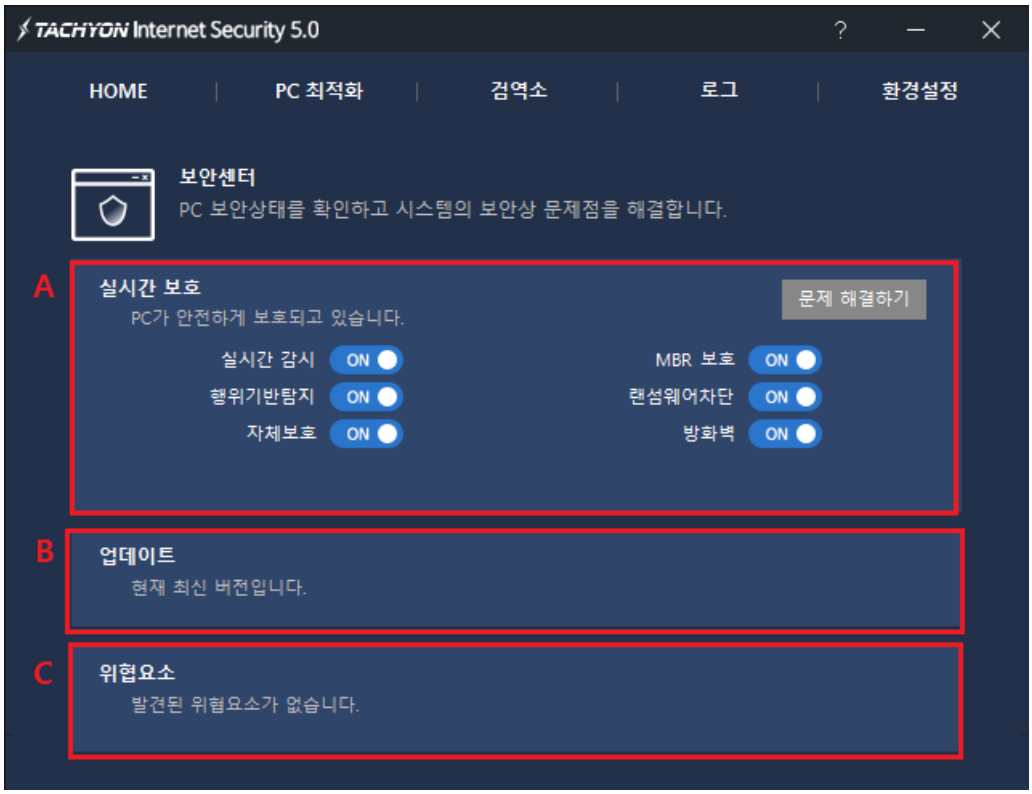
실시간 보호 기능이 모두 ON, 업데이트 최신 버전, 위협요소가 없는 경우 안전(파란색), 업데이트가 최신이 아닌 경우 주의(노란색), 실시간 보호 일부 기능이 OFF 및 위협요소가 있는 경우 위험(빨강색)으로 표시하여 보안 상태 정보를 보여줍니다.

보안센터 실행하기

1. 바탕화면의 TACHYON Internet Security 5.0 아이콘을 더블 클릭합니다.

2. TACHYON Internet Security 5.0 메인 화면에서 [보안센터]를 클릭합니다.

3. 보안센터 화면이 나타납니다.



A 영역

PC 보안 기능의 사용 여부를 ON/OFF 할 수 있습니다.

- 실시간 감시 : 실시간 감시 기능의 사용여부를 ON/OFF 표시하며, 기능을 ON/OFF 할 수 있습니다.
- 행위기반탐지 : 행위기반탐지 기능의 사용여부를 ON/OFF 표시하며, 기능을 ON/OFF 할 수 있습니다.
- 자체보호 : 자체보호 기능의 사용여부를 ON/OFF 표시하며, 기능을 ON/OFF 할 수 있습니다.
- MBR 보호 : MBR 보호 기능의 사용여부를 ON/OFF 표시하며, 기능을 ON/OFF 할 수 있습니다.
- 랜섬웨어차단 : 랜섬웨어차단 기능의 사용여부를 ON/OFF 표시하며, 기능을 ON/OFF 할 수 있습니다.
- 방화벽 : 방화벽 기능의 사용여부를 ON/OFF 표시하며, 기능을 ON/OFF 할 수 있습니다.

B 영역

- 업데이트 : 엔진 파일이 최신 상태가 아닐 경우 [문제 해결하기]가 활성화 됩니다. 버튼을 클릭하여 제품 업데이트를 진행 할 수 있습니다.

C 영역

- 위협요소 : 검사를 통해 발견된 위협 요소 중 검출된 위협 요소 개수가 표시됩니다.

6장

검사/치료

1. 실시간 검사
2. 기본 검사
3. 정밀 검사
4. 탐색기 검사
5. 치료하기

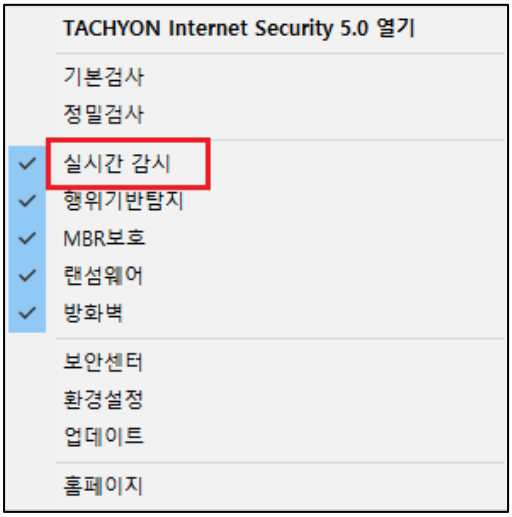
1. 실시간 검사

PC에서 발생되는 파일 접근 (파일의 실행, 저장, 이동, 삭제 등) 및 인터넷에서 파일 다운로드 등의 일련의 행위가 발생될 때 이를 탐지하여 악성코드에 감염된 파일이 있는 경우 차단/치료할 수 있습니다.

실시간 검사 실행 방법

■ 트레이 아이콘에서 실행하기

TACHYON Internet Security 5.0 트레이 아이콘( )에서 마우스 우클릭한 후, “실시간 검사”를 선택하면 실행할 수 있습니다.



■ 메인 화면에서 실행하기

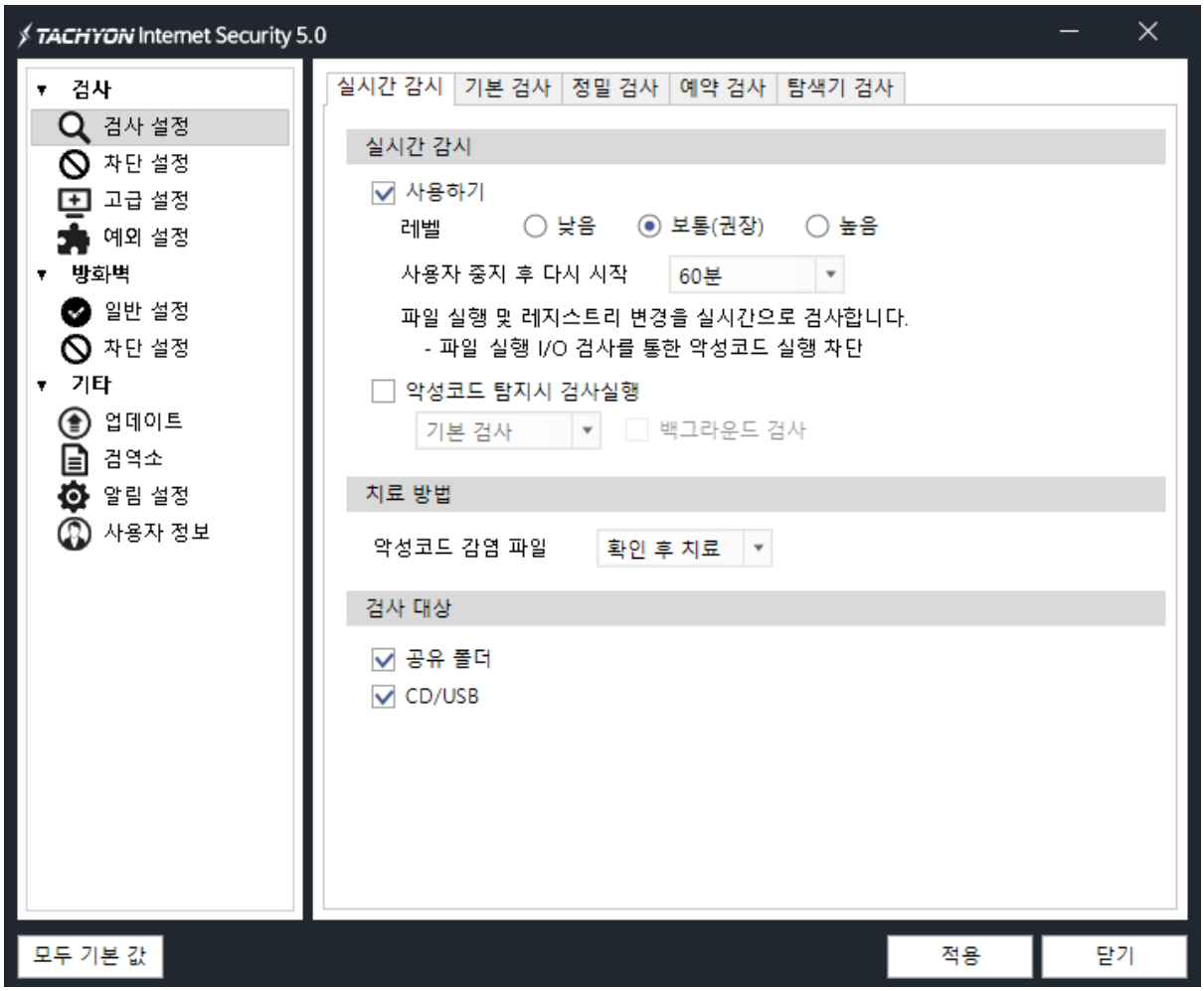
TACHYON Internet Security 5.0 실행 후 메인 화면에서 실시간 감시 슬라이드 버튼을 ON 으로 하여 실행할 수 있습니다.

■ 보안센터에서 실행하기

TACHYON Internet Security 5.0 실행 후 메인 화면에서 [보안센터]를 클릭하여 실시간 보호 설정에서 실시간 감시 슬라이드 버튼을 ON으로 하여 실행할 수 있습니다.

■ 환경설정에서 실행하기

환경설정 실행 후 검사 > 검사 설정 > 실시간 감시 탭을 선택하여 실시간 감시 옵션을 선택할 수 있습니다.



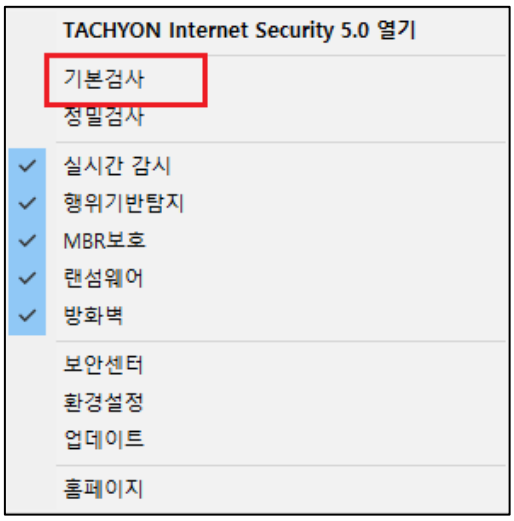
2. 기본 검사

기본 검사는 프로세스, 메모리, 부트, 시스템 중요 폴더를 검사하는 기능입니다. 트레이 아이콘 및 메인 화면에서 기본 검사를 실행할 수 있습니다.

기본 검사 실행 방법

- 트레이 아이콘에서 실행하기

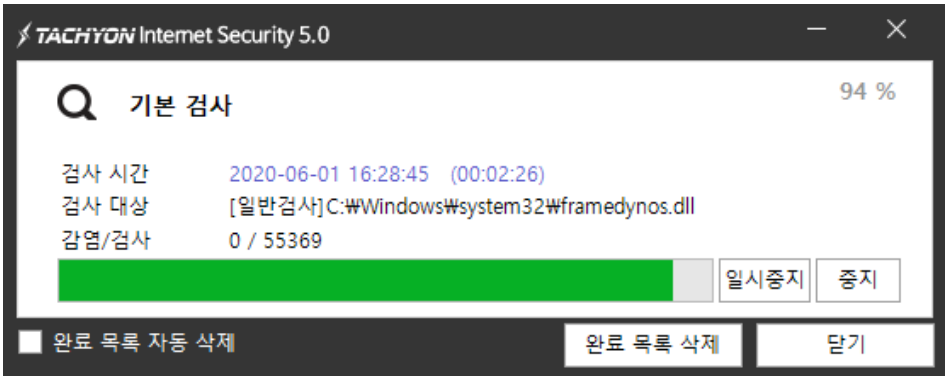
TACHYON Internet Security 5.0 트레이 아이콘( )에서 마우스 우클릭한 후, “기본검사”를 선택하면 실행할 수 있습니다.



■ 메인 화면에서 실행하기

TACHYON Internet Security 5.0 메인 화면에서 [기본검사]를 클릭합니다.

기본 검사 진행 화면



■ 검사 시간 : 검사 실행 후 경과한 시간을 표시합니다.

■ 검사 대상 : 검사가 진행 중인 대상을 표시합니다.

■ 감염/검사

- 감염 : 검사 진행 중 발견된 악성코드 개수를 표시합니다.
- 검사 : 검사한 전체 파일 수를 표시합니다.

■ 일시중지 : 검사가 진행 중인 화면 우측의 [일시중지]를 클릭하면 검사가 일시중지 됩니다. [계속검사]를 통해 검사 진행이 가능합니다.

■ 계속검사 : [일시중지]를 클릭하면 [일시중지]의 이름이 [계속검사]로 변경됩니다. 검사를 다시 시작할 수 있습니다.

■ 중지 : 검사가 진행 중인 화면 우측의 [중지]를 클릭하면 사용자 질의를 통해 중지 여부를 선택할 수 있습니다.

- 중지 : 진행 중인 검사를 중지합니다.
- 계속 : 검사 진행 화면으로 돌아가 검사를 계속합니다.

■ 완료 목록 자동 삭제 : 체크 여부에 따라 작업 진행이 완료된 화면은 목록에서 지워집니다.

■ 완료 목록 삭제 : 작업 진행이 완료된 화면을 지울 수 있습니다.

■ 닫기 : 작업관리자 전체 화면을 종료합니다.

기본 검사 완료 화면

- 검사 시간 : 검사가 완료된 시간을 표시합니다.
- 검사 개수 : 검사한 파일의 개수를 표시합니다.
- 감염 개수 : 감염된 파일의 개수를 표시합니다.
- 치료 개수 : 감염된 파일 중 치료한 파일의 개수를 표시합니다.
- 완료 목록 자동 삭제 : 체크 여부에 따라 작업 진행이 완료된 화면은 목록에서 지워집니다.
- 완료 목록 삭제 : 작업 진행이 완료된 화면을 지울 수 있습니다.
- 닫기 : 작업관리자의 전체 화면을 종료합니다.

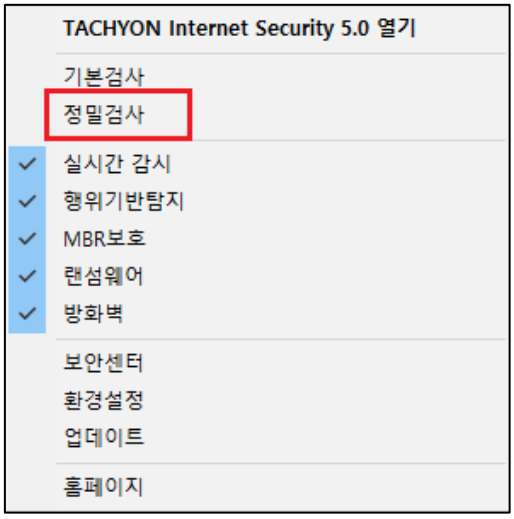
3. 정밀 검사

정밀 검사는 사용자가 선택한 폴더를 검사하는 기능입니다. 트레이 아이콘 및 메인 화면에서 정밀 검사를 진행할 수 있습니다.

정밀 검사 실행 방법

- 트레이 아이콘에서 실행하기

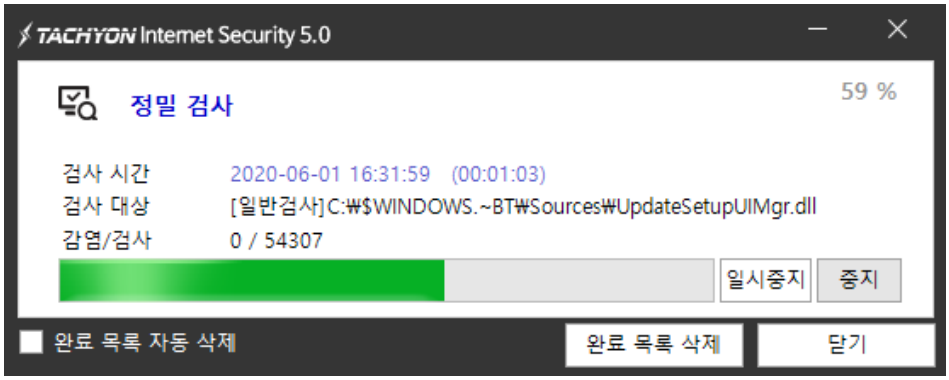
TACHYON Internet Security 5.0 트레이 아이콘( )에서 마우스 우클릭한 후, “정밀검사”를 선택하면 실행할 수 있습니다.



■ 메인 화면에서 실행하기

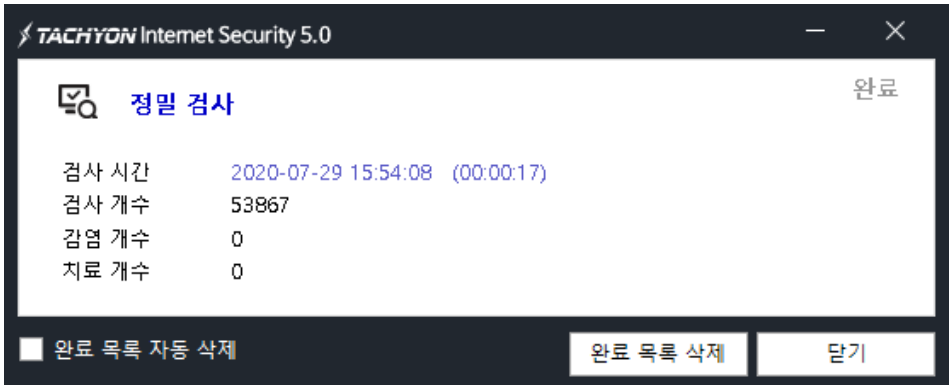
TACHYON Internet Security 5.0 메인 화면에서 [정밀 검사]를 클릭합니다.

정밀 검사 실행 화면



- 검사 시간 : 검사 실행 후 경과한 시간을 표시합니다.
- 검사 대상 : 검사가 진행 중인 대상을 표시합니다.
- 감염/검사
  - 감염 : 검사 진행 중 발견된 악성코드 개수를 표시합니다.
  - 검사 : 검사한 전체 파일 수를 표시합니다.
- 일시중지 : 검사가 진행 중인 화면 우측의 [일시중지]를 클릭하면 검사가 일시중지 됩니다. [계속검사]를 통해 검사 진행이 가능합니다.
- 계속검사 : [일시중지]를 클릭하면 [일시중지]의 이름이 [계속검사]로 변경됩니다. 검사를 다시 시작할 수 있습니다.
- 중지 : 검사가 진행 중인 화면 우측의 [중지]를 클릭하면 사용자 질의를 통해 중지 여부를 선택할 수 있습니다.
  - 중지 : 진행 중인 검사를 중지합니다.
  - 계속 : 검사 진행 화면으로 돌아가 검사를 계속합니다.
- 완료 목록 자동 삭제 : 체크 여부에 따라 작업 진행이 완료된 화면은 목록에서 지워집니다.
- 완료 목록 삭제 : 작업 진행이 완료된 화면을 지울 수 있습니다.
- 닫기 : 작업관리자 전체 화면을 종료합니다.

정밀 검사 완료 화면

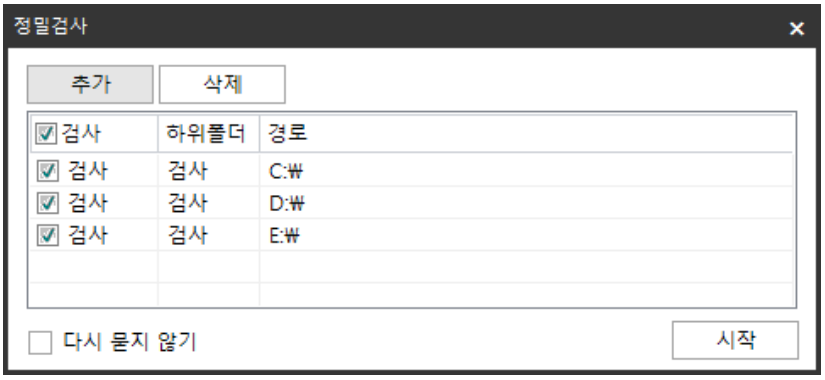


- 검사 시간 : 검사가 완료된 시간을 표시합니다.
- 검사 개수 : 검사한 파일의 개수를 표시합니다.
- 감염 개수 : 감염된 파일의 개수를 표시합니다.
- 치료 개수 : 감염된 파일 중 치료한 파일의 개수를 표시합니다.
- 완료 목록 자동 삭제 : 체크 여부에 따라 작업 진행이 완료된 화면은 목록에서 지워집니다.
- 완료 목록 삭제 : 작업 진행이 완료된 화면을 지울 수 있습니다.
- 닫기 : 작업관리자의 전체 화면을 종료합니다.

검사 폴더 선택 화면

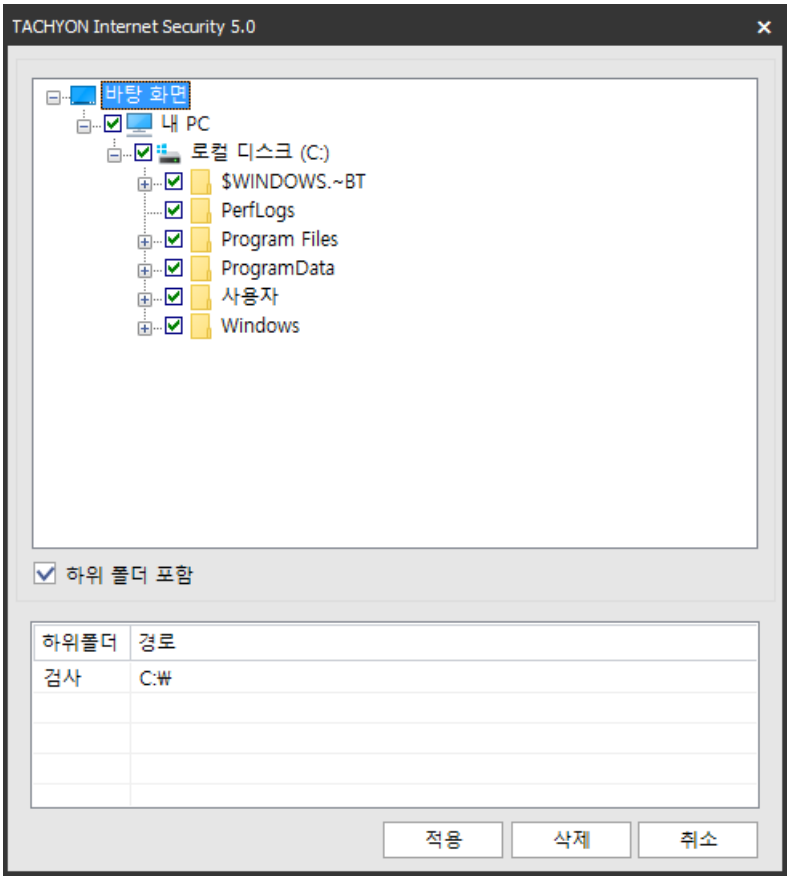
■ 메인 화면

정밀 검사를 실행하면 검사 위치를 설정할 수 있는 창이 나타납니다.

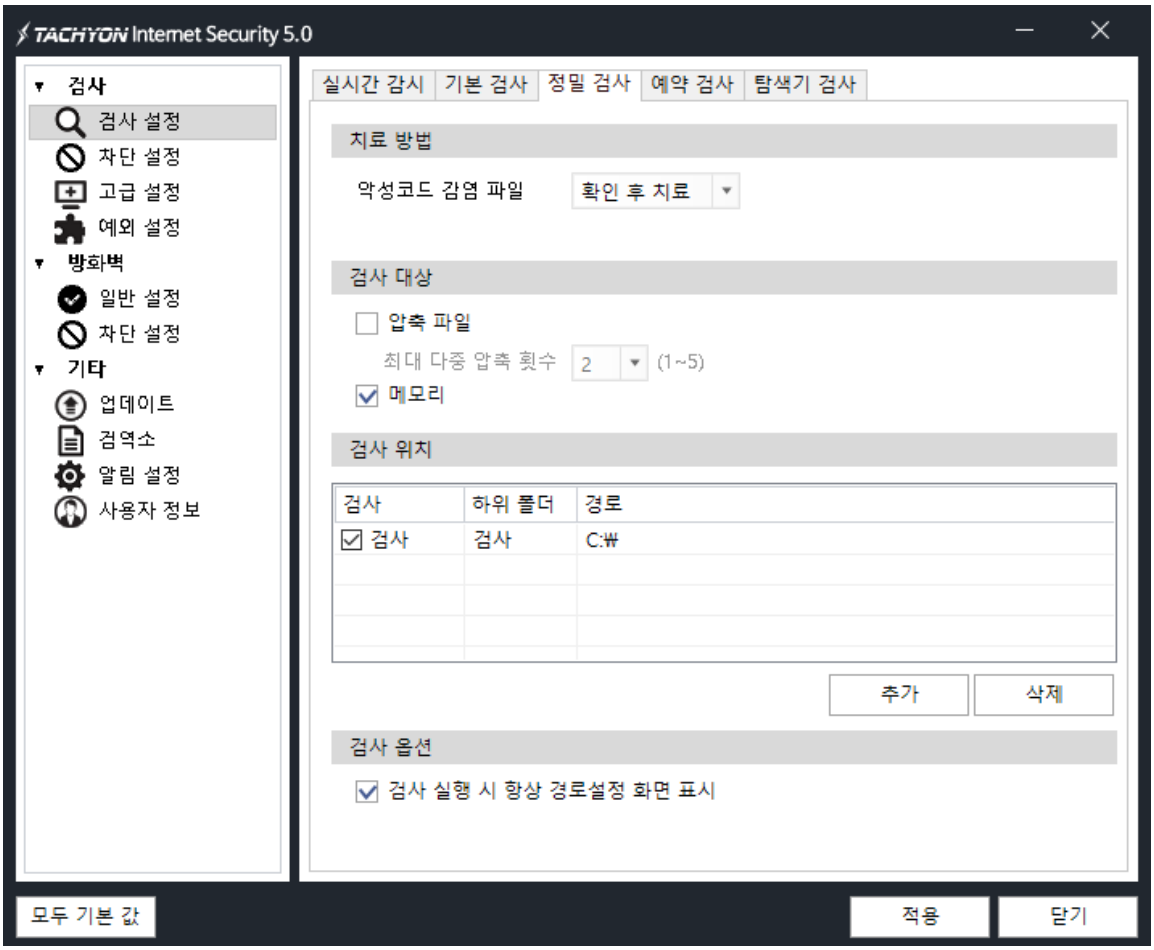


※ 경로 설정 창은 환경 설정에 따라 나타나지 않을 수 있습니다.

[추가]를 클릭하면 검사 위치를 지정할 수 있는 폴더 탐색기 창이 나타납니다.



■ 환경설정



환경설정을 실행한 후, “검사 > 검사 설정 > 정밀 검사 > 검사 위치”에서 [추가]를 클릭해서 검사 위치를 설정할 수 있습니다. 이는 메인 화면에서 정밀 검사를 실행하여 추가하는 것과 동일합니다.

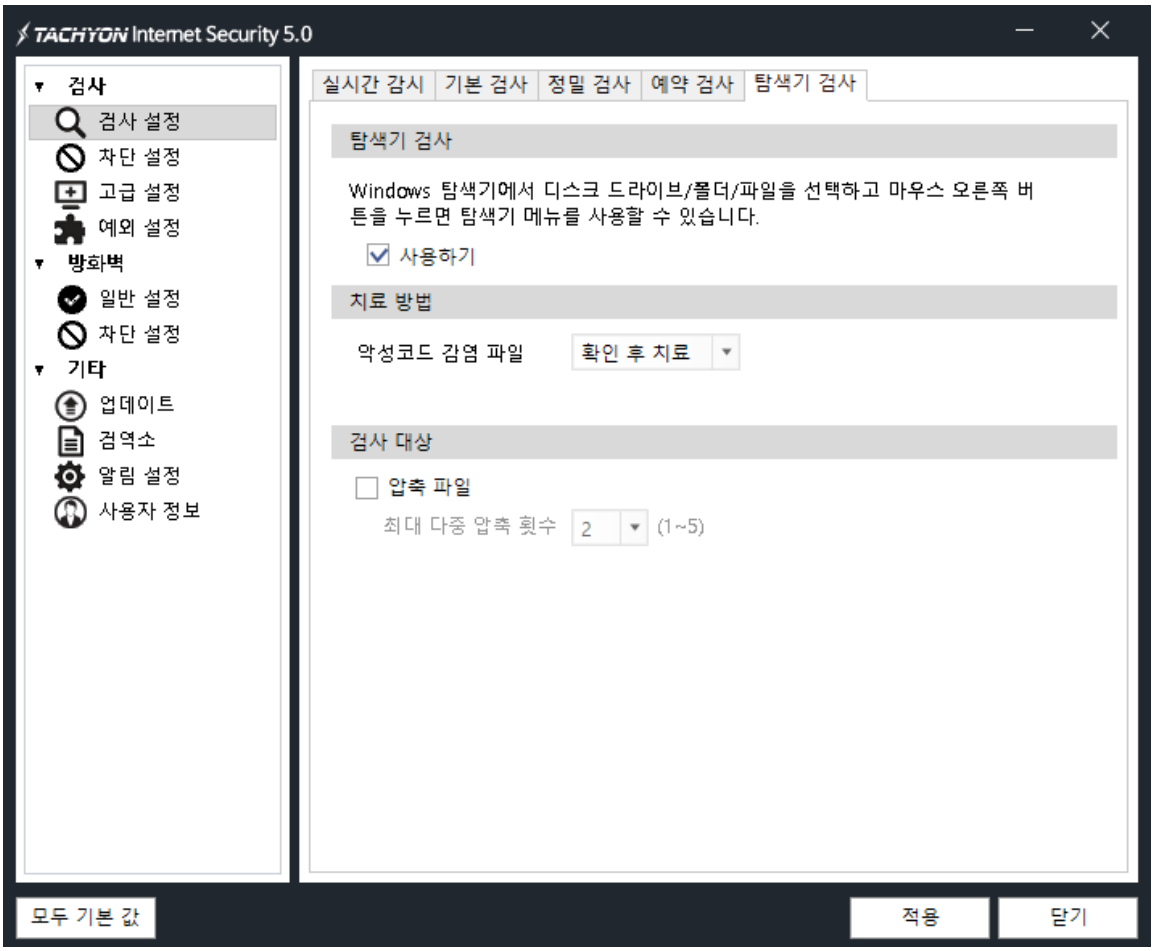
4. 탐색기 검사

탐색기 검사는 Windows 탐색기에서 사용자가 선택한 파일 또는 폴더를 검사하는 기능입니다. 탐색기 검사를 사용하기 위해서는 환경설정에서 탐색기 검사 사용하기를 선택해야 합니다.

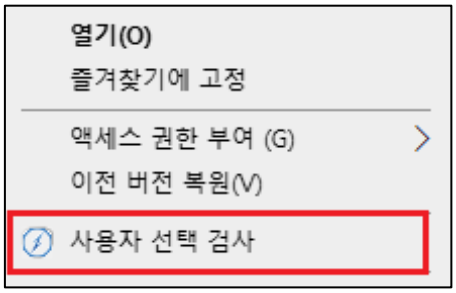
실행 방법

1. 바탕화면의 TACHYON Endpoint Security 5.0 바로가기 아이콘 또는 TACHYON Endpoint Security 5.0 트레이 아이콘( )을 더블 클릭합니다.

2. 환경설정을 클릭한 후, 검사 > 검사 설정 > 탐색기 검사 탭으로 이동하여 “사용하기”에 체크를 하면 탐색기 검사를 실행할 수 있습니다.

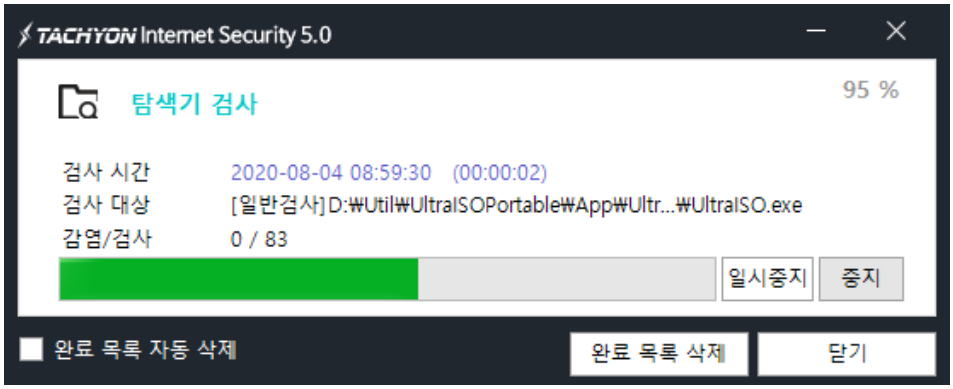


3. 바탕 화면이나 Windows 탐색기에서 폴더나 파일을 선택하고 마우스 오른쪽을 눌러 “사용자 선택 검사”를 선택합니다.



4. 탐색기 검사의 검사 진행 화면이 나타납니다.

탐색기 검사 진행 화면



- 검사 시간 : 검사 실행 후 경과한 시간을 표시합니다.
- 검사 대상 : 검사가 진행 중인 대상을 표시합니다.
- 감염/검사
  - 감염 : 검사 진행 중 발견된 악성코드 개수를 표시합니다.
  - 검사 : 검사한 전체 파일 수를 표시합니다.
- 일시중지 : 검사가 진행 중인 화면 우측의 [일시중지]를 클릭하면 검사가 일시중지 됩니다. [계속검사]를 통해 검사 진행이 가능합니다.
- 계속검사 : [일시중지]를 클릭하면 [일시중지]의 이름이 [계속검사]로 변경됩니다. 검사를 다시 시작할 수 있습니다.
- 중지 : 검사가 진행 중인 화면 우측의 [중지]를 클릭하면 사용자 질의를 통해 중지 여부를 선택할 수 있습니다.
  - 중지 : 진행 중인 검사를 중지합니다.
  - 계속 : 검사 진행 화면으로 돌아가 검사를 계속합니다.
- 완료 목록 자동 삭제 : 체크 여부에 따라 작업 진행이 완료된 화면은 목록에서 지워집니다.
- 완료 목록 삭제 : 작업 진행이 완료된 화면을 지울 수 있습니다.
- 닫기 : 작업관리자 전체 화면을 종료합니다.

탐색기 검사 완료 화면

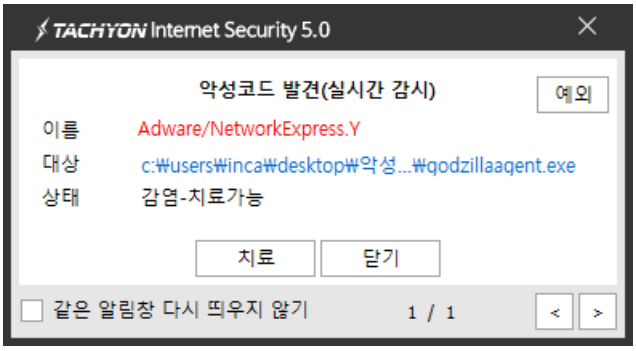
- 검사 시간 : 검사가 완료된 시간을 표시합니다.
- 검사 개수 : 검사한 파일의 개수를 표시합니다.
- 감염 개수 : 감염된 파일의 개수를 표시합니다.
- 치료 개수 : 감염된 파일 중 치료한 파일의 개수를 표시합니다.
- 완료 목록 자동 삭제 : 체크 여부에 따라 작업 진행이 완료된 화면은 목록에서 지워집니다.
- 완료 목록 삭제 : 작업 진행이 완료된 화면을 지울 수 있습니다.
- 닫기 : 작업관리자의 전체 화면을 종료합니다.

5. 치료하기

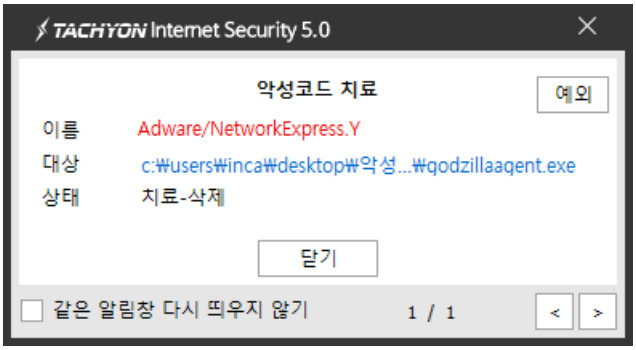
악성코드 검사가 완료되면 검출된 악성코드를 보여주며 이를 치료할 수 있는 화면이 나타납니다.

실시간 검사를 통한 악성코드 진단 및 치료

■ 악성코드 진단 알림창



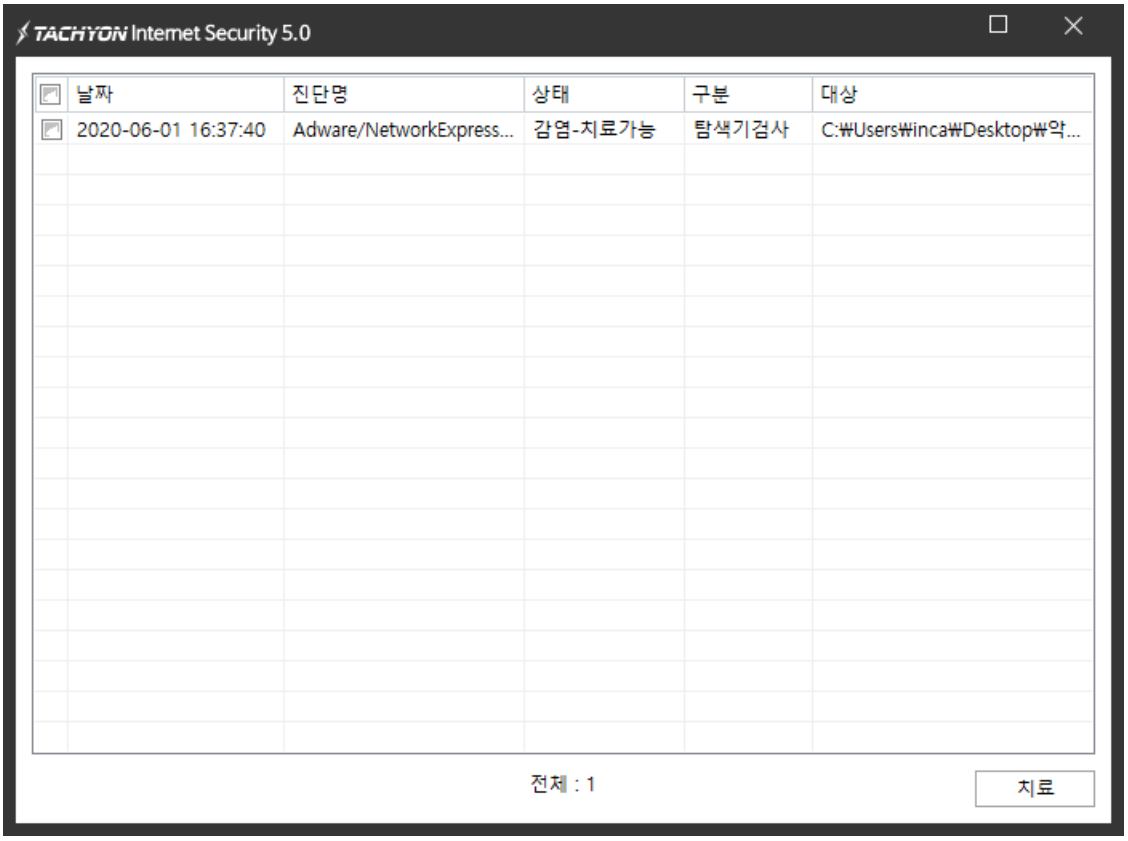
■ 악성코드 치료 알림창



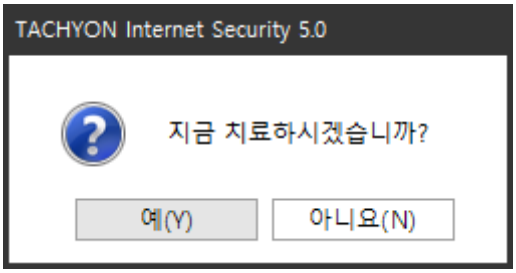
기본 검사, 정밀 검사, 예약 검사, 탐색기 검사를 통한 악성코드 진단 및 치료

■ 악성코드 진단 및 치료창

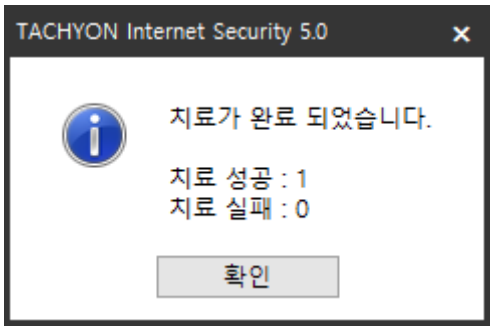
기본 검사, 정밀 검사, 예약 검사, 탐색기 검사를 통해 악성코드가 진단되면 알림창이 나타납니다.



치료하고자 하는 악성코드를 선택한 후, 우측 하단에 [치료]를 클릭하면 사용자 질의창이 나타납니다.



[예(Y)]를 클릭하면 치료가 시작되고 완료되면 결과창이 나타납니다.



7장

검역소

1. 검역소

1. 검역소

검역소는 TACHYON Internet Security 5.0을 이용하여 치료 및 삭제하기 전에 감염된 원본 파일을 백업하는 기능입니다.

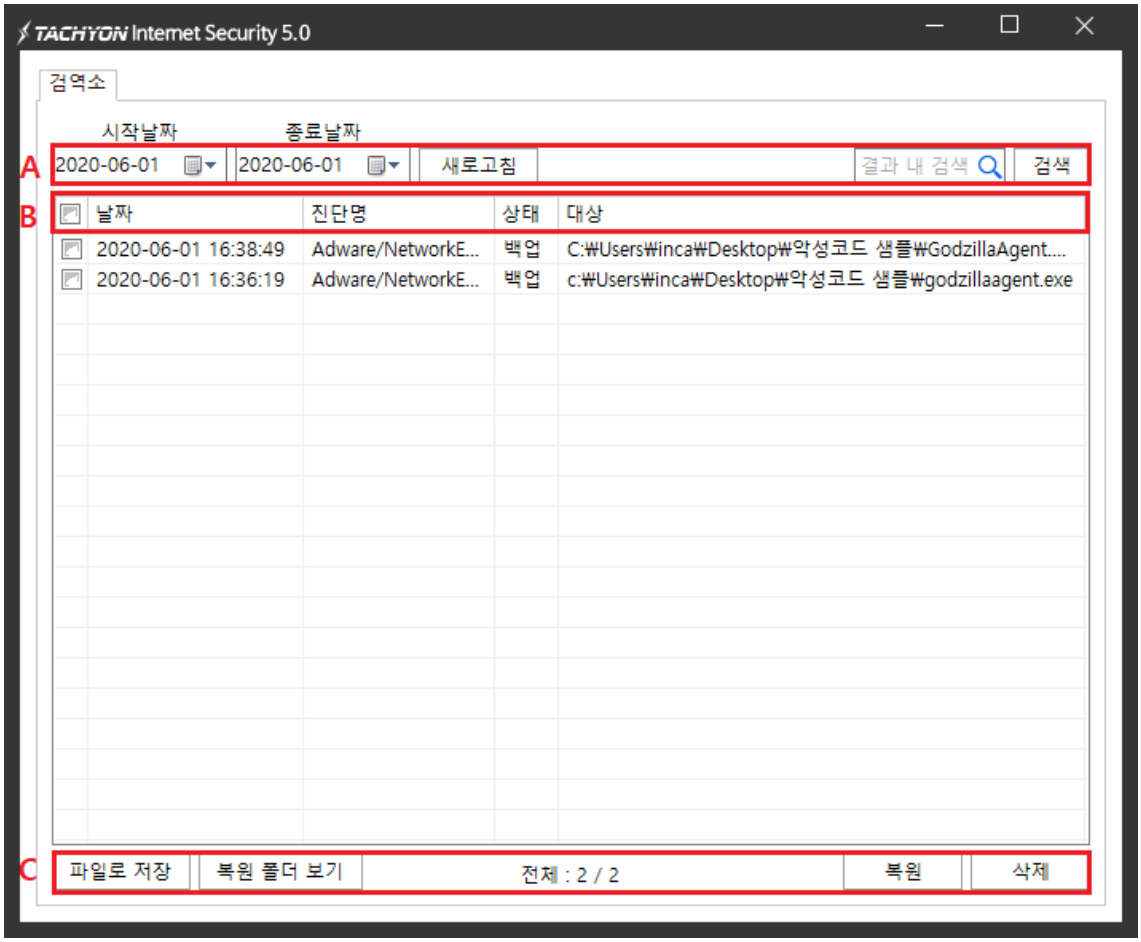
악성코드 치료 후 프로그램이 정상적으로 실행되지 않을 경우를 대비하여 치료 전 원본 파일을 보관하는 용도로 활용할 수 있습니다.

실행 방법

1. 바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘 또는 TACHYON Internet Security 5.0 트레이 아이콘()을 더블 클릭합니다.

2. TACHYON Internet Security 5.0 메인 화면의 상단 메뉴에서 “검역소”를 클릭합니다.

3. TACHYON Internet Security 5.0 검역소가 표시됩니다.



A 영역

검역소에 백업한 날짜를 선택할 수 있습니다.

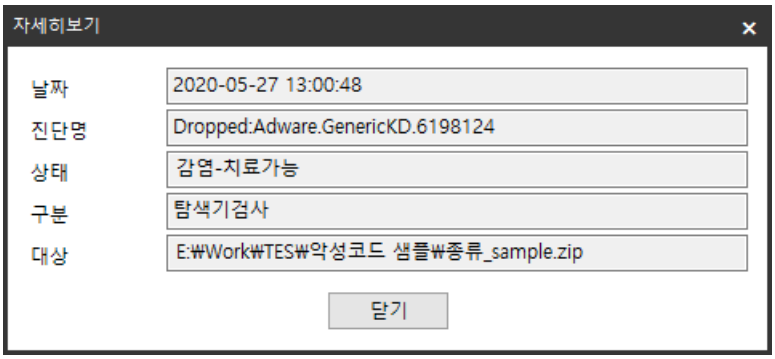
- 날짜 지정 : 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 검역소의 내용을 검색하여 화면에 표시합니다.
- 새로고침 : 검역소의 내용을 최신 정보로 고칩니다.

B 영역

화면 상단에서 지정한 조건에 따라 검역 되어 있는 항목들을 표시합니다.

- 날짜 : 검역소에 백업한 날짜와 시간을 표시합니다.
- 진단명 : 검역소에 백업된 파일이 감염된 악성코드의 이름을 표시합니다.
- 상태 : 파일의 현재 상태를 표시합니다.
- 대상 : 악성코드에 감염된 파일의 원본 위치를 표시합니다.

선택한 백업 파일 리스트를 더블 클릭하면 [자세히보기] 창이 열립니다.



- 날짜 : 검역소에 백업한 날짜와 시간을 표시합니다.
- 진단명 : 검역소에 백업된 파일이 감염된 악성코드의 이름을 표시합니다.
- 상태 : 파일의 현재 상태를 표시합니다.
- 구분 : 악성코드가 진단된 검사의 종류를 표시합니다.
- 대상 : 악성코드에 감염된 파일의 원본 위치를 표시합니다.

C 영역

- 파일로 저장 : 현재 화면에 출력되어 있는 검역 항목들을 엑셀 호환문서(CSV) 형식의 파일로 저장할 수 있습니다.

- 복원 폴더 보기 : 파일을 복원하게 되면 “환경설정 > 기타 > 검역소 설정 > 복원 폴더 지정”에서 지정한 경로에 검역 되기 전의 원본 파일로 복원됩니다.

이 때, 사용자가 폴더를 지정하지 않을 경우 본 제품의 기본 폴더는 다음과 같습니다.

32bit : C:\Program Files\Common Files\TACHYON\T5\Quarantine\Restore

64bit : C:\Program Files (x86)\Common Files\TACHYON\T5\Quarantine\Restore

- 전체 : 현재 화면에 출력되어 있는 개수를 표시합니다.

- 복원 : 검역소에 백업된 파일을 복원할 수 있는 기능입니다. 출력된 항목들 중 체크 박스를 이용하여 선택한 감염 파일을 [복원]을 클릭하여 이전의 원본 파일로 되돌릴 수 있습니다.

- 삭제 : 검역소에 검역 되어 보관 중인 격리 또는 백업 파일에 대해서 삭제할 수 있는 기능입니다. 체크 박스를 이용하여 선택한 검역 파일을 [삭제]를 클릭하면 해당 항목은 검역 항목에서 제거됩니다.

8장

방화벽

1. 방화벽

1. 방화벽

TACHYON Internet Security 5.0의 방화벽을 사용하면 네트워크 규칙과 프로그램 규칙에 따라 허가하지 않은 인터넷 연결을 차단하여 PC를 안전하게 유지할 수 있습니다.

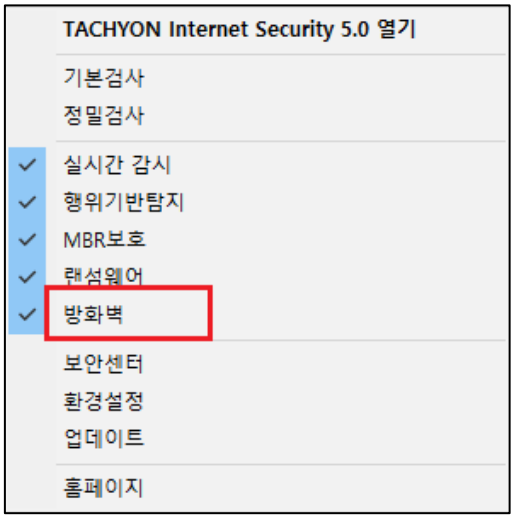
TACHYON Internet Security 5.0의 방화벽은 다른 PC에서 사용자의 PC로 들어오는 데이터와 사용자의 PC에서 다른 PC로 나가는 데이터를 제한합니다.

허가없이 PC에 접근하여 악성코드를 유포하는 공격자의 침입이나 내 PC의 정보가 외부로 유출되는 것을 예방할 수 있습니다.

실행 방법

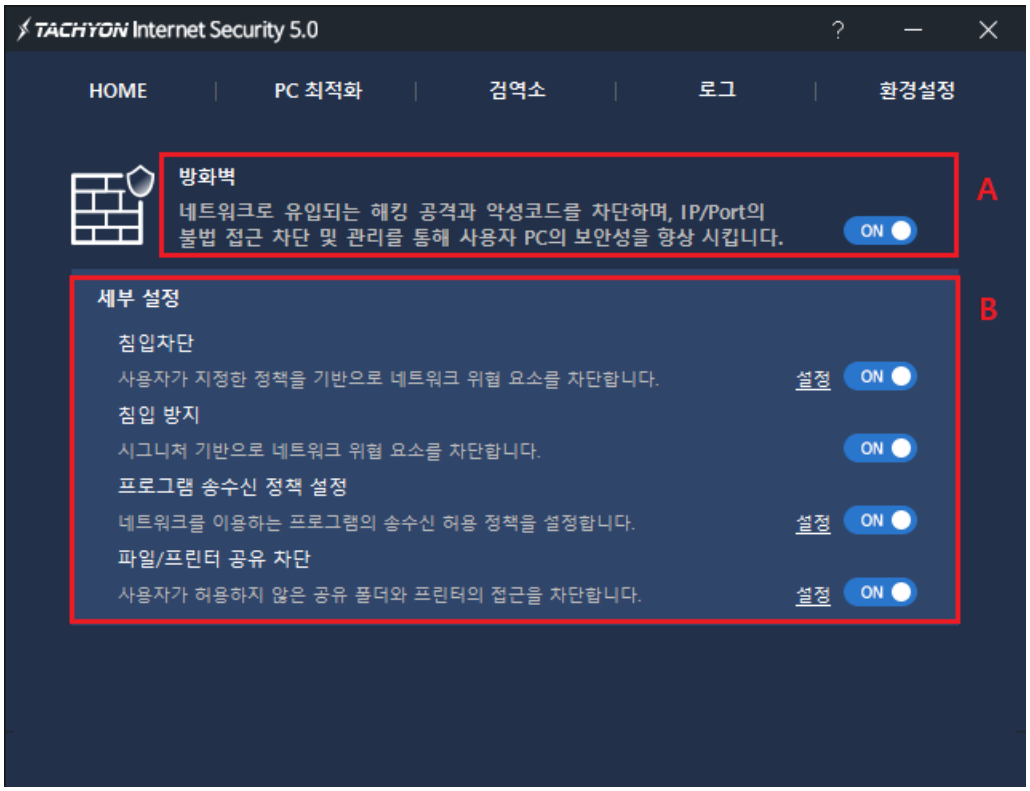
■ 트레이 아이콘에서 실행

TACHYON Internet Security 5.0 트레이 아이콘( )에서 마우스 오른쪽 버튼을 클릭한 후, “방화벽”을 선택하면 실행할 수 있습니다.



■ 메인 화면에서 실행

TACHYON Internet Security 5.0 메인 화면에서 [방화벽]을 클릭합니다.



A 영역

- ON/OFF : 방화벽 기능을 전체 ON/OFF 할 수 있습니다.

B 영역

- 침입차단 : IP, Port 기반으로 사용자가 등록한 IP 또는 Port에 대해 네트워크 연결을 차단하는 기능입니다.
- 침입방지 : 알려진 웜이나 백도어 등의 공격을 Signature 기반으로 차단하는 기능입니다.
- 프로그램 송수신 정책 설정 : 프로그램 송수신 정책에 따라 허가되지 않은 인터넷 연결을 차단하는 기능입니다.
- 파일/프린터 차단 설정 : 파일/프린터 차단 정책에 따라 허가되지 않은 IP에 대해 네트워크 공유 연결을 차단하는 기능입니다.

※ 세부 설정의 각 항목의 ON/OFF 옆에 있는 [설정]을 클릭하면 해당 기능의 환경 설정 화면이 열립니다.

9장

로그

1. 로그

2. 위협요소

3. 방화벽

4. 이벤트

1. 로그

로그는 TACHYON Internet Security 5.0 각 기능이 실행된 기록을 보여줍니다.

악성코드 검사, 방화벽 등을 실행한 기록을 확인할 수 있습니다.

실행 방법

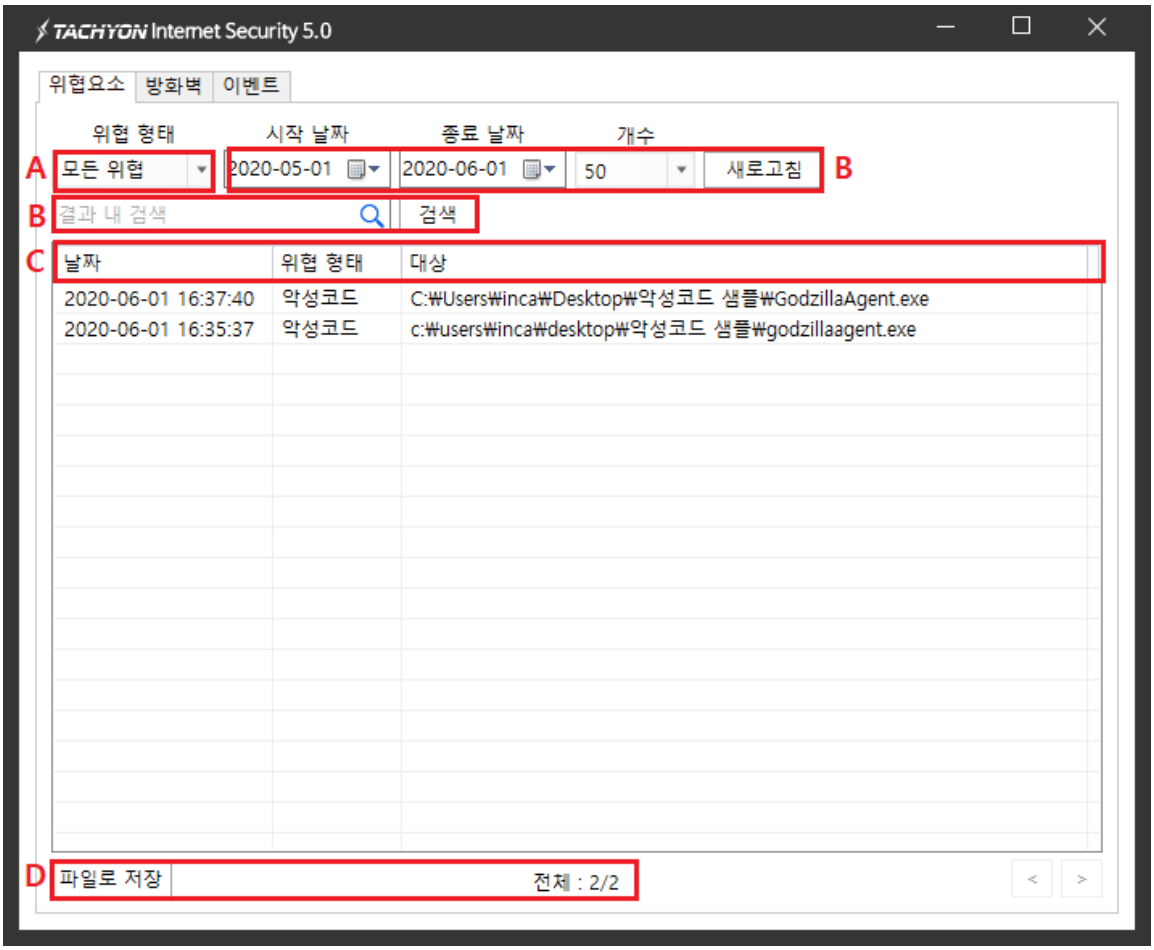
1. 바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘 또는 TACHYON Internet Security 5.0 트레이 아이콘()을 더블 클릭합니다.

2. TACHYON Internet Security 5.0 메인 화면의 상단 메뉴에서 “로그”를 클릭합니다.

3. TACHYON Internet Security 5.0 로그가 표시됩니다.

2. 위협요소

PC에서 진단된 악성코드나 차단된 랜섬웨어 차단에 대한 진단 날짜와 처리 상태를 확인 할 수 있습니다.



A 영역

위협요소 로그의 종류를 선택할 수 있습니다.

- 모든 위협 : 악성코드, 행위기반탐지, MBR보호, 자체보호, 랜섬웨어와 같은 진단 및 치료(삭제,차단)시 기록된 로그를 보여줍니다.
- 악성코드 : 실시간검사, 기본검사, 정밀검사, 예약검사 와 같은 검사를 통해 발견된 악성코드를 진단 및 치료(삭제)시 기록된 로그를 보여줍니다.
- 행위기반탐지 : 행위기반탐지 기능을 통해 발견된 악성코드를 진단 및 치료(삭제, 차단)시 기록

된 로그를 보여줍니다.

- MBR보호 : MBR보호 기능을 통해 발견된 악성코드를 진단 및 치료(삭제, 차단)시 기록된 로그를 보여줍니다.
- 자체보호 : 안정적인 서비스를 위해 자가보호중인 프로세스의 불법적인 접근이 발생시 기록된 로그를 보여줍니다.
- 랜섬웨어 : 랜섬웨어 차단 기능을 통해 발견된 악성코드를 진단 및 치료(차단)시 기록된 로그를 보여줍니다.

B 영역

위협요소 로그의 종류를 선택할 수 있습니다.

- 날짜 지정 : 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 로그를 검색하여 화면에 표시합니다.
- 상태 : 위협 형태가 악성코드일 경우 감염/치료/실패/모두로 구분하여 로그를 출력할 수 있습니다.
- 개수 : 화면에 출력되는 개수를 지정할 수 있습니다.(50/100/200/300/500 중 선택)
- 새로고침 : 로그의 내용을 최신 정보로 고칩니다.

C 영역

모든 위협

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 위협형태 : 해당 로그의 위협형태를 표시합니다.

(악성코드/행위기반탐지/MBR보호/자체보호/랜섬웨어)

- 대상 : 위협요소로 진단된 파일의 전체 경로를 표시합니다.

악성코드

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 진단명 : 감염된 악성코드의 이름이나 발견한 위협의 이름을 보여줍니다.
- 상태 : 악성코드에 감염된 파일의 치료 상태를 표시합니다.
- 구분 : 악성코드로 진단한 검사 종류를 표시합니다.

(실시간 검사/기본검사/정밀검사/탐색기검사/예약검사/자체검사)

- 대상 : 위협요소로 진단된 파일의 전체 경로를 표시합니다.

행위기반탐지

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 차단 : 차단 항목인지 허용된 항목인지 표시합니다.
- 프로세스 : 악성코드로 의심되는 파일을 실행한 프로세스를 표시합니다.
- 실행파일 : 악성코드로 의심되는 행위를 한 파일을 표시합니다.

MBR보호

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 유형 : MBR 영역과 볼륨 영역을 구분하여 표시합니다.

- 볼륨 : 보호된 볼륨 및 MBR을 표시합니다.
- 차단프로세스 : MBR 및 볼륨에 접근한 프로세스를 표시합니다.

자체보호

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 타입 : 자체 보호에 의해 보호된 유형을 표시합니다.
- 차단프로세스 : 보호되고 있는 파일에 접근한 프로세스의 전체 경로를 표시합니다.
- 보호파일 : 보호되고 있는 파일의 전체 경로를 표시합니다.

랜섬웨어

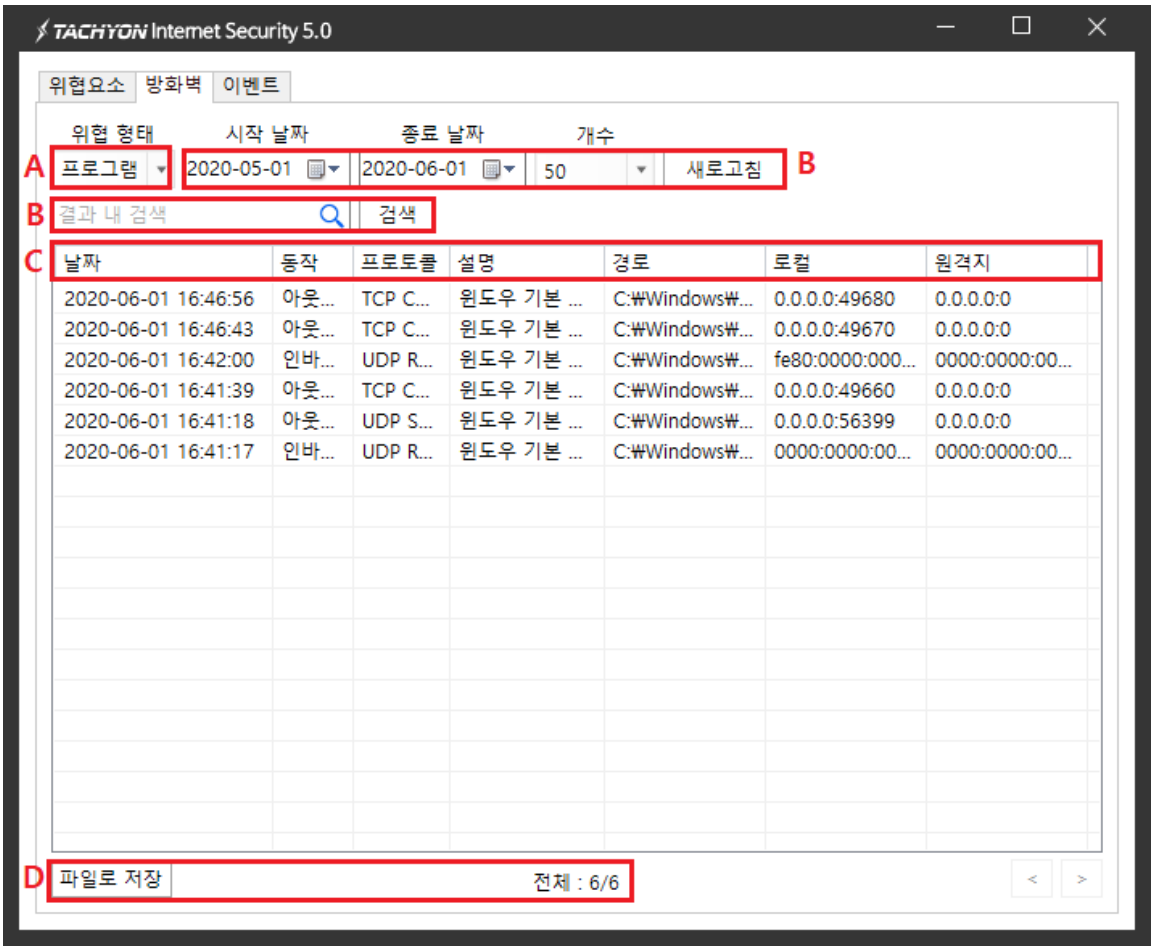
- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 차단프로세스 : 보호되고 있는 파일에 접근한 프로세스의 전체 경로를 표시합니다.

D 영역

- 파일로 저장 : 현재 화면에 출력되어 있는 로그 항목들을 엑셀 호환문서(CSV)형식의 파일로 저장할 수 있습니다.
- 전체 : 현재 화면에 출력되어 있는 로그 개수를 표시합니다.

3. 방화벽

침입차단, 침입방지, 프로그램, 공유 차단, 사이트 차단 기능에 의해 차단된 목록들을 확인할 수 있습니다.



A 영역

방화벽 로그의 종류를 선택할 수 있습니다.

- 침입차단 : 사용자가 등록한 IP 또는 Port에 대해 네트워크 연결 차단에 대해 기록된 로그를 보여줍니다.
- 침입방지 : 알려진 웜이나 백도어 등의 공격에 대해 기록된 로그를 보여줍니다.
- 프로그램 : 허가되지 않은 인터넷 연결 차단에 대해 기록된 로그를 보여줍니다.
- 공유차단 : 허가되지 않은 IP의 네트워크 공유 연결에 대해 기록된 로그를 보여줍니다.

B 영역

- 날짜 지정 : 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- 개수 : 화면에 출력되는 개수를 지정할 수 있습니다.(50/100/200/300/500 중 선택)
- 새로고침 : 로그의 내용을 최신 정보로 고칩니다.
- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 로그를 검색하여 화면에 표시합니다.

C 영역

침입차단

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 이름 : 침입차단 정책의 이름을 표시합니다.
- 동작 : 차단된 항목을 표시합니다.
- 방향 : 트래픽 방향을 표시합니다.(IN: Inbound, OUT: Outbound, IN/OUT)
- 프로토콜 : 차단된 프로토콜 종류를 표시합니다.(TCP, UDP, TCP/UDP)
- 로컬 : 로컬 IP 주소를 표시합니다.
- 원격지 : 로컬 PC에 접근한 원격지 IP를 표시합니다.

침입 방지

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)

- 이름 : 침입방지 정책 이름을 표시합니다.
- 동작 : 차단된 항목을 표시합니다.
- 방향 : 트래픽 방향을 표시합니다.(IN: Inbound, OUT: Outbound, IN/OUT)
- 프로토콜 : 차단된 프로토콜 종류를 표시합니다.(TCP, UDP, TCP/UDP)
- 로컬 : 로컬 IP 주소를 표시합니다.
- 원격지 : 로컬 PC에 접근한 원격지 IP를 표시합니다.
- 설명 : 침입방지된 로그에 대한 설명을 표시합니다.

프로그램

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 동작 : 어떤 주체에 의해 실행되었는지 표시합니다.(CLIENT/SERVER)
- 프로토콜 : 실행된 프로그램의 프로토콜 종류를 표시합니다.(TCP, UDP, TCP/UDP 등)
- 설명 : 프로그램 인증을 시도한 프로그램의 종류를 표시합니다.
- 경로 : 프로그램 인증 알림 창에 표시된 프로그램의 경로를 표시합니다.
- 로컬 : 로컬 IP 주소를 표시합니다.
- 원격지 : 로컬 PC에 접근한 원격지 IP를 표시합니다.

공유차단

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 이름 : 차단 항목의 이름을 표시합니다.
- 동작 : 차단 항목인지 허용된 항목인지 표시합니다.

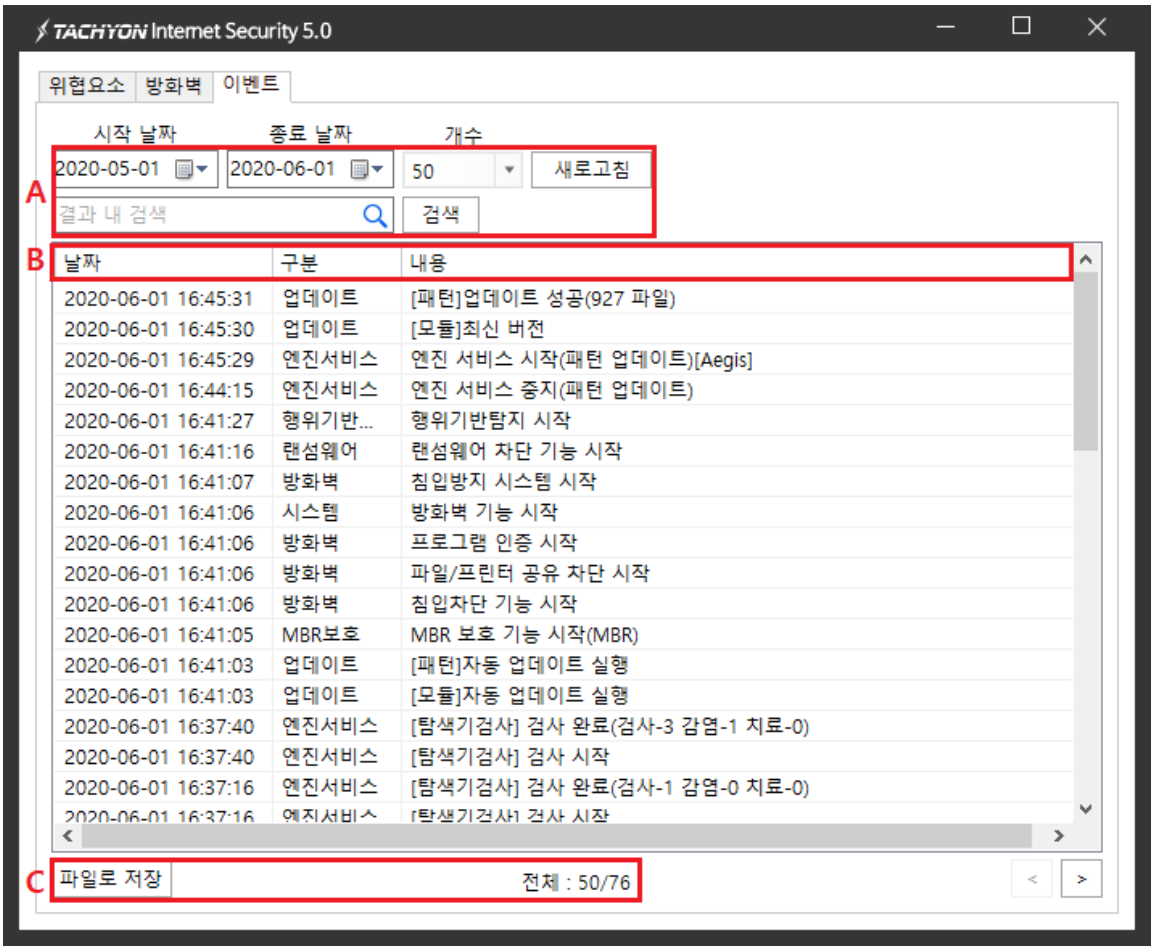
- 방향 : 트래픽 방향을 표시합니다.(IN: Inbound, OUT: Outbound, IN/OUT)
- 프로토콜 : 접근한 프로토콜 종류를 표시합니다.(TCP, UDP, TCP/UDP 등)
- 로컬 : 로컬 IP 주소를 표시합니다.
- 원격지 : 로컬 PC에 접근한 원격지 IP를 표시합니다.

D 영역

- 파일로 저장 : 현재 화면에 출력되어 있는 로그 항목들을 엑셀 호환문서(CSV)형식의 파일로 저장할 수 있습니다.
- 전체 : 현재 화면에 출력되어 있는 로그 개수를 표시합니다.

4. 이벤트

시스템, 업데이트, 서비스 로그를 관리합니다.



A 영역

- 날짜 지정 : 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- 개수 : 화면에 출력되는 개수를 지정할 수 있습니다.(50/100/200/300/500 중 선택)
- 새로고침 : 로그의 내용을 최신 정보로 고칩니다.
- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 로그를 검색하여 화면에 표시합니다.

B 영역

- 날짜 : 해당 로그가 발생한 날짜와 시간을 표시합니다.(연-월-일 시:분:초)
- 구분 : 이벤트 로그에 기록되는 내용의 작업을 진행하는 주체입니다.
- 내용 : 이벤트 로그에 기록되는 구체적인 내용입니다.

C 영역

- 파일로 저장 : 현재 화면에 출력되어 있는 로그 항목들을 엑셀 호환문서(CSV)형식의 파일로 저장할 수 있습니다.
- 전체 : 현재 화면에 출력되어 있는 로그 개수를 표시합니다.

10장

PC 최적화

1. PC 최적화

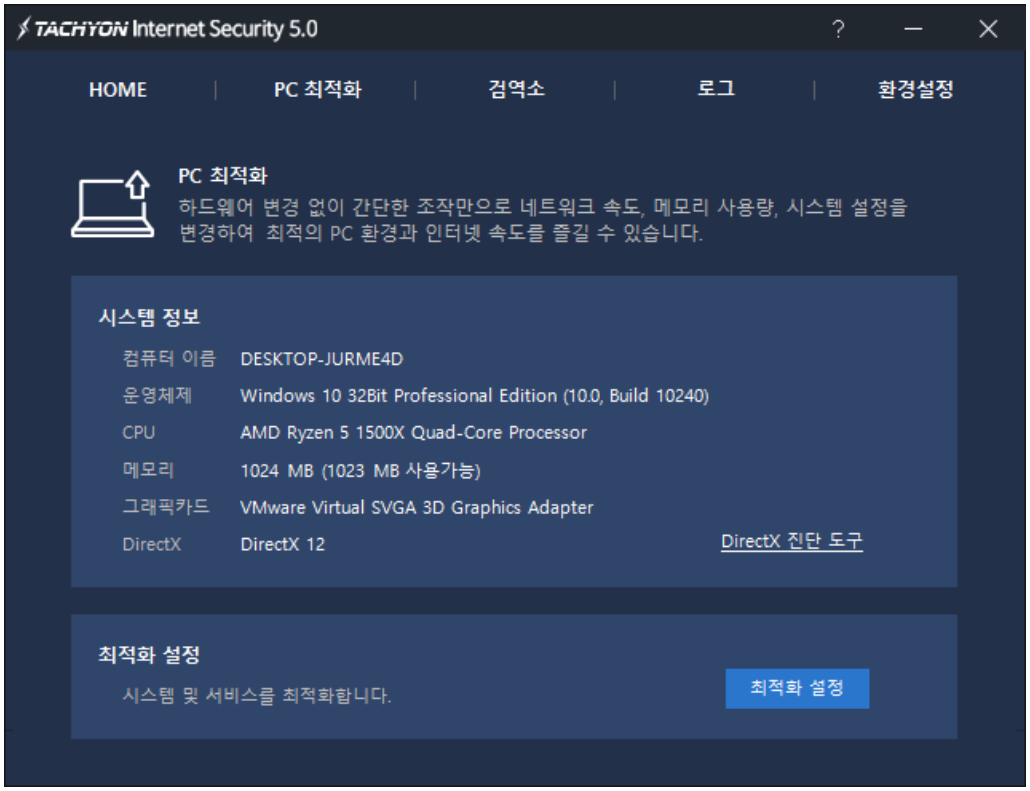
1. PC 최적화

하드웨어 변경 없이 시스템 설정 변경을 통하여 최적의 PC 환경을 만들어 주기 위한 기능입니다. 간단한 조작만으로 한층 업그레이드 된 PC 성능 및 인터넷 속도를 즐길 수 있습니다.

실행 방법

1. 바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘 또는 TACHYON Internet Security 5.0 트레이 아이콘( )을 더블 클릭합니다.

2. TACHYON Internet Security 5.0 메인 화면의 상단 메뉴에서 “PC최적화”를 클릭합니다.



A 영역

PC의 컴퓨터 이름, 운영체제, CPU, 메모리, 그래픽카드 등 하드웨어 정보를 상세히 알려줍니다. DirectX 진단 도구를 클릭하면, 현재 사용자의 PC에 설치되어 있는 DirectX의 버전을 알 수 있으며 정상 동작 여부 등을 확인할 수 있습니다.

시스템 정보

- 컴퓨터 이름 : 사용자 PC의 컴퓨터 이름을 표시합니다.
- 운영체제 : 사용자 PC의 운영체제를 표시합니다.
- CPU : 사용자 PC의 CPU 정보를 표시합니다.
- 메모리 : 사용자 PC의 메모리 용량을 표시합니다.
- 그래픽카드 : 사용자 PC의 그래픽카드 정보를 표시합니다.
- DirectX : 사용자 PC의 DirectX 버전을 표시합니다.
- DirectX 진단 도구 : Windows에 기본적으로 설치되어 있는 DirectX 진단 도구를 실행시켜 줍니다.

B 영역

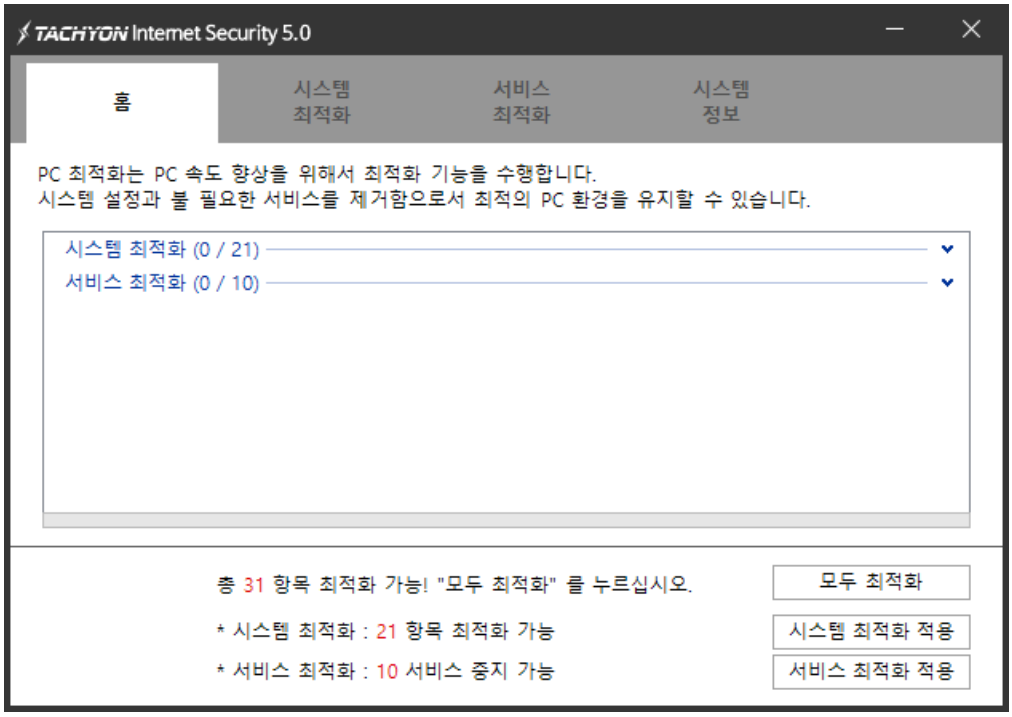
시스템 및 서비스를 최적화 합니다.

화면 우측의 [최적화 설정]을 클릭하면 최적화 설정 창이 실행됩니다.

홈

PC 최적화는 PC 속도 향상을 위해서 최적화 기능을 수행합니다.

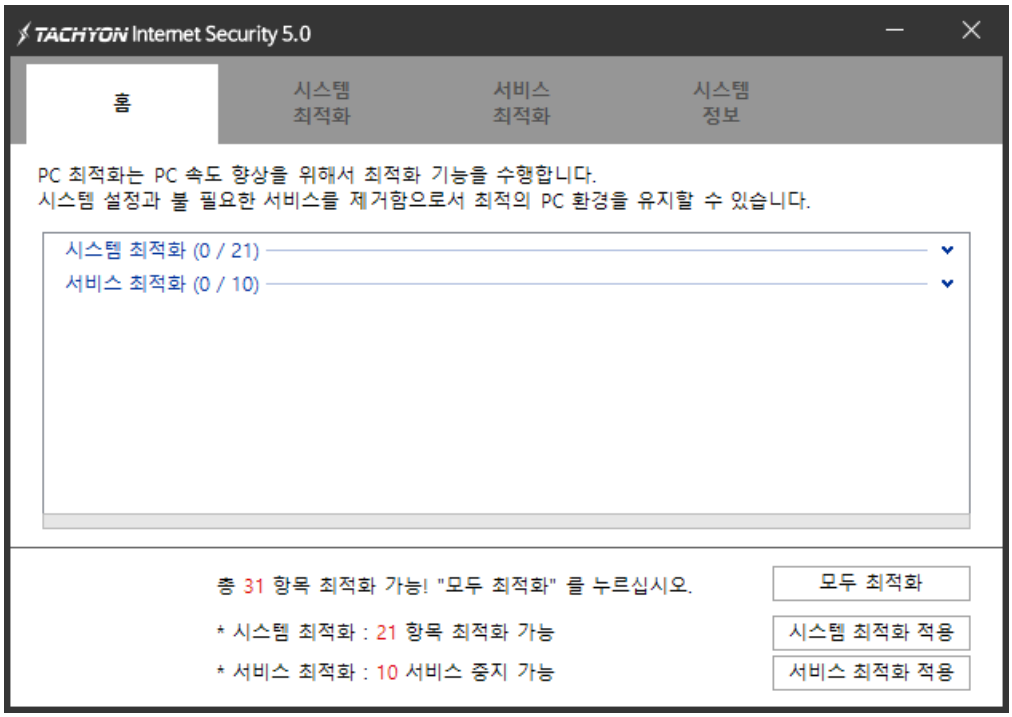
시스템 설정과 불필요한 서비스를 제거함으로서 최적의 PC 환경을 유지할 수 있습니다.



- 모두 최적화 : 사용자 PC의 시스템과 서비스에 대한 최적화를 모두 진행합니다.
- 시스템 최적화 적용 : 사용자 PC의 시스템에 대한 21개 항목의 최적화를 모두 진행합니다.
- 서비스 최적화 적용 : 사용자 PC의 서비스에 대한 10개 항목의 최적화를 모두 진행합니다.

시스템 최적화

사용자 PC의 성능을 향상하기 위해 선택된 항목들을 최적화 합니다.



- 전체선택 : 시스템 최적화를 위한 21개 항목을 모두 선택합니다.
- 전체해제 : 시스템 최적화를 위한 21개 항목을 모두 해제합니다.
- 최적화 적용 : 사용자 PC의 시스템에 대한 21개 항목의 최적화를 모두 진행합니다.
- 최적화 해제 : 사용자 PC의 시스템에 대한 21개 항목의 최적화를 모두 해제합니다.

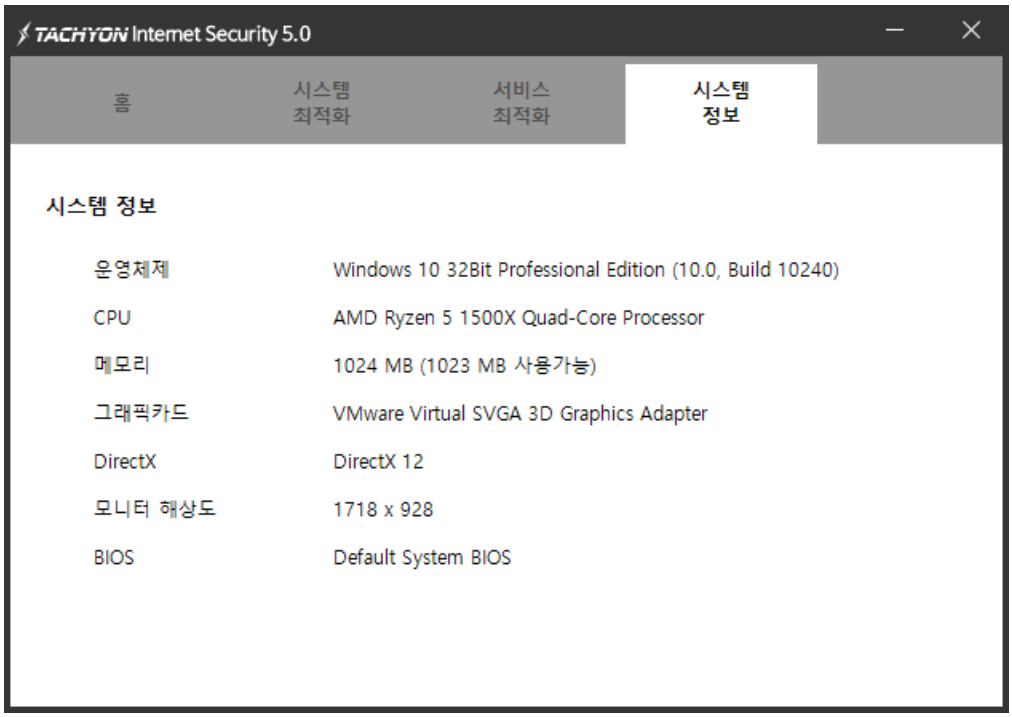
서비스 최적화

사용자 PC의 성능을 향상하기 위해 불필요한 서비스를 종료합니다.

- 전체선택 : 서비스 최적화를 위한 10개 항목을 모두 선택합니다.
- 전체해제 : 서비스 최적화를 위한 10개 항목을 모두 해제합니다.
- 최적화 적용 : 사용자 PC의 서비스에 대한 10개 항목의 최적화를 모두 진행합니다.
- 최적화 해제 : 사용자 PC의 서비스에 대한 10개 항목의 최적화를 모두 해제합니다.

시스템 정보

PC의 운영체제, CPU, 메모리, 그래픽카드 등 하드웨어 정보를 상세히 알려줍니다.



- 운영체제 : 사용자 PC의 운영체제를 표시합니다.
- CPU : 사용자 PC의 CPU 정보를 표시합니다.
- 메모리 : 사용자 PC의 메모리 용량을 표시합니다.
- 그래픽카드 : 사용자 PC의 그래픽카드 정보를 표시합니다.
- DirectX : 사용자 PC의 DirectX 버전을 표시합니다.
- 모니터 해상도 : 사용자 PC의 모니터 해상도를 표시합니다.
- BIOS : 사용자 PC의 BIOS 정보를 표시합니다.

11장

PC 관리

1. PC 관리

2. 시스템 청소

3. 서비스

4. 프로세스

5. 설치 프로그램

6. 시작 프로그램

7. ActiveX

8. 툴바

1. PC 관리

TACHYON Internet Security 5.0의 PC관리를 통해 시스템 청소, 실행 중인 서비스 및 프로세스, 설치된 프로그램 관리, 시작 프로그램 관리, ActiveX 관리, 툴바 관리를 할 수 있습니다.

실행 방법

1. 바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘 또는 TACHYON Internet Security 5.0 트레이 아이콘( )을 더블 클릭합니다.

2. TACHYON Internet Security 5.0 메인 화면의 [PC관리]를 클릭합니다.

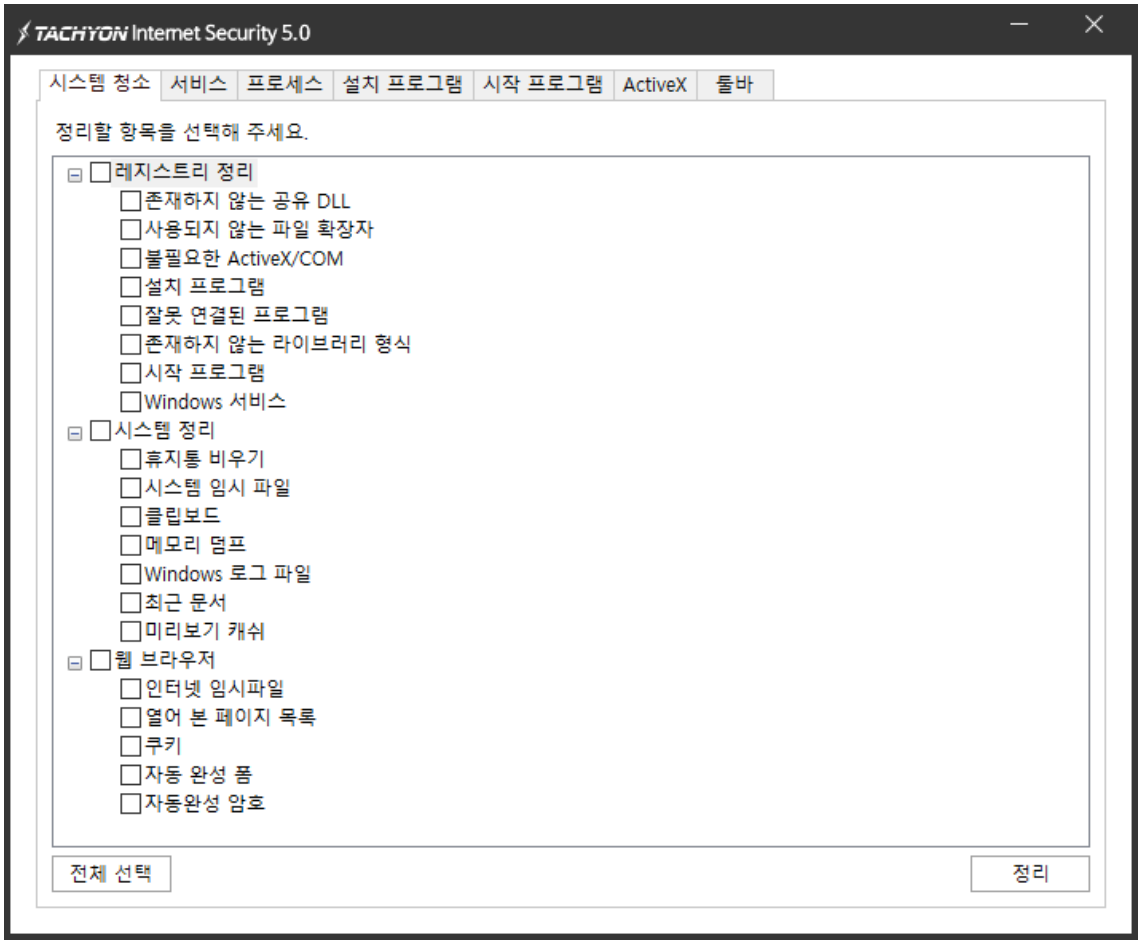
3. TACHYON Internet Security 5.0 PC 관리가 표시됩니다.

2. 시스템 청소

시스템 청소에서는 사용자 PC 내의 사용하지 않는 시스템 정보를 제거하여 시스템을 최적화 시킬 수 있습니다.

이러한 데이터들은 경우에 따라 다시 사용할 수도 있지만 대부분의 경우 삭제해도 PC 운영에 문제가 되지 않는 경우가 많습니다.

디스크 사용을 효율적으로 개선하고 PC 사용 속도와 메모리 사용을 개선하려면 시스템 청소를 실행하여 불필요한 공간 낭비를 최소화하는 것이 좋습니다.



A 영역

레지스트리 정리

- 존재하지 않는 공유 DLL : 레지스트리에 공유 DLL의 경로가 잘못 저장되어 있을 경우 잘못된 정보로 인해 PC에 문제가 발생할 수 있습니다.

  존재하지 않는 공유 DLL을 시스템 청소 대상으로 선택하면 해당 공유 DLL의 레지스트리 정보를 삭제하여 PC 오류를 줄일 수 있습니다.

- 사용되지 않는 파일 확장자 : 레지스트리에 등록된 확장자 정보를 제외한 빈 값으로 설정되어 있는 확장자 키 값을 모두 삭제합니다.

- 불필요한 ActiveX/COM : ActiveX 레지스트리 정보 중 잘못되어 있거나 손상된 정보를 삭제합니다.

- 설치 프로그램 : 프로그램 설치 시 만들어진 레지스트리 키 값으로 해당 키 값에 정의된 디렉토리가 존재하지 않을 경우 키 값을 삭제합니다.

- 잘못 연결된 프로그램 : 레지스트리에 등록된 실행 파일의 경로가 유효하지 않을 경우 해당 키를 삭제합니다.

- 존재하지 않는 라이브러리 형식 : 레지스트리의 타입 라이브러리 키 값이 존재하지 않을 경우 해당 키를 삭제합니다.

- 시작 프로그램 : Windows의 시작 프로그램으로 등록되어 있지만 실제로 시작 프로그램으로 사용하지 않거나 설치되지 않은 프로그램에 대한 키 값을 삭제합니다.

- Windows 서비스 : Windows 서비스와 관련된 레지스트리 키 값 중 사용하지 않는 키 값을 삭제합니다.

시스템 정리

- 휴지통 비우기 : 휴지통에 있는 모든 파일을 삭제합니다.
- 시스템 임시 파일 : PC 사용 중 생성된 임시 파일을 삭제합니다.
- 클립보드 : 클립보드 영역의 정보를 삭제합니다.
- 메모리 덤프 : 메모리 덤프 정보를 삭제합니다.
- Windows 로그 파일 : Windows 사용 중 기록된 로그를 삭제합니다.
- 최근 문서 : 시작 메뉴에 표시되는 최근 사용한 파일 목록을 삭제합니다.
- 미리보기 캐쉬 : 미리보기 캐쉬 데이터를 삭제합니다.

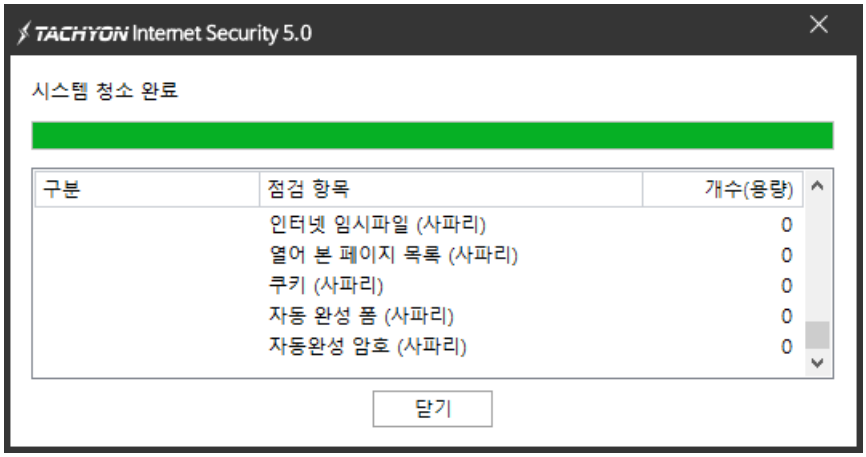
웹 브라우저

- 인터넷 임시파일 : 인터넷 임시 파일을 삭제합니다. 인터넷 임시 파일을 사용하면 접속했던 웹페이지 및 미디어에 다시 접속할 때 속도는 빨라지지만 하드 디스크 공간을 많이 차지할 수 있습니다.
- 열어 본 페이지 목록 : 접속했던 웹페이지의 목록을 삭제합니다.
- 쿠키 : 쿠키를 삭제합니다. 쿠키는 사용자가 웹사이트를 이용한 내역을 저장한 정보입니다.
- 자동 완성 폼 : 자동 완성 기능에서 사용할 입력 값 정보를 삭제합니다. 자동 완성 기능을 사용하면 웹페이지의 입력 란에 기록했던 정보를 모두 저장합니다.
- 자동완성 암호 : 로그인할 때 저장한 암호를 삭제합니다. 저장된 암호를 사용하면 다음 로그인에는 암호를 입력하지 않아도 자동으로 로그인할 수 있지만 보안상 위험할 수 있습니다.

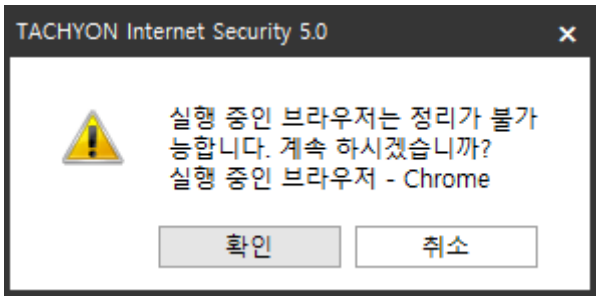
B 영역

- 전체 선택 : 시스템 청소를 진행할 항목을 전체 선택 합니다.
- 전체 해제 : 전체 선택된 항목을 전체 해제 합니다.
- 정리 : 선택한 내용에 따라 시스템 청소를 시작합니다.

  [정리]를 클릭하면 시스템 청소 작업이 진행됩니다.



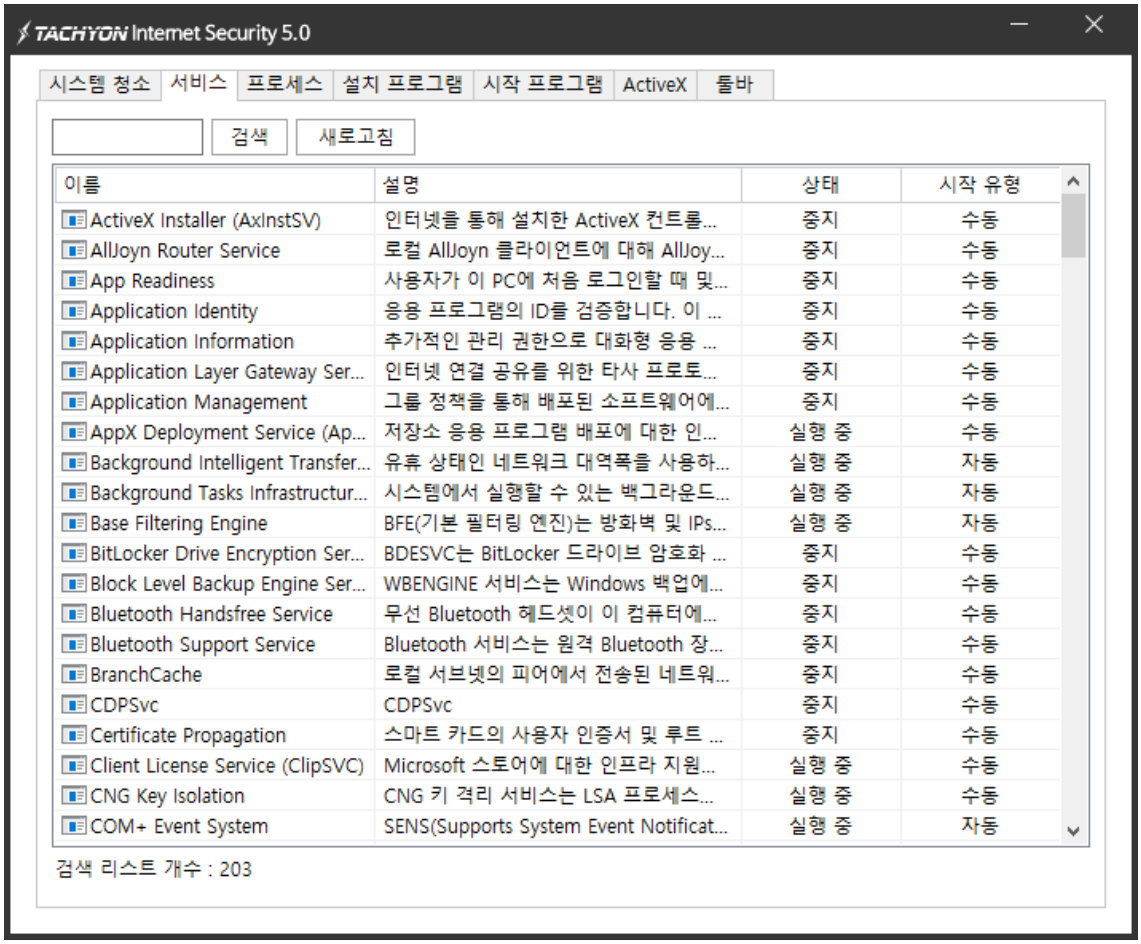
만약 웹브라우저가 실행되고 있다면 아래와 같은 알림창이 나타납니다.



3. 서비스

서비스가 설치되면 서비스를 시작하여야 해당 서비스를 이용할 수 있습니다.

서비스에서는 설치되어 있는 서비스에 대해 시작/중지 및 시작 유형을 변경할 수 있습니다.



A 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 설치되어 있는 서비스를 검색하여 화면에 표시합니다
- 새로고침 : 설치되어 있는 서비스의 항목을 최신 정보로 고칩니다

B 영역

- 이름 : 설치되어 있는 서비스의 이름을 표시합니다.
- 설명 : 설치되어 있는 서비스에 대한 설명을 표시합니다.
- 상태 : 설치되어 있는 서비스의 상태를 표시합니다.(실행 중/중지)
- 시작 유형 : 설치되어 있는 서비스의 시작 유형을 표시합니다.(자동/수동/사용 안함)

C 영역

- 검색 리스트 개수 : 설치되어 있는 서비스의 개수를 표시합니다.

서비스 상태 변경 방법

1. 실행 또는 중지하고자 하는 서비스 항목을 선택합니다.

2. 선택한 서비스에서 마우스 우클릭한 후 “서비스 상태 > 시작/중지”를 선택하면 됩니다.

서비스 시작 유형 변경 방법

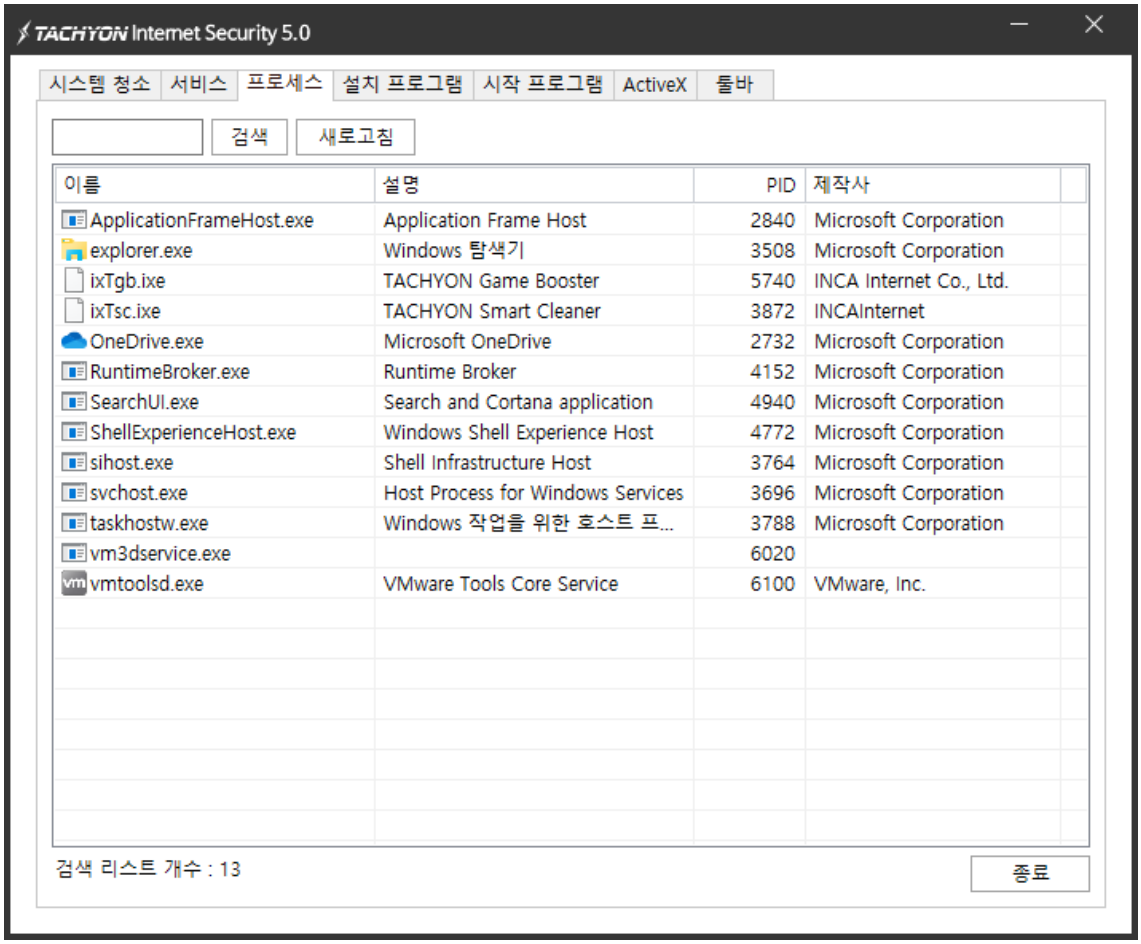
1. 시작 유형을 변경하고 하는 서비스 항목을 선택합니다.

2. 선택한 서비스에서 마우스 우클릭한 후 “시작 유형 > 자동/수동/사용 안함”을 선택하면 됩니다.

4. 프로세스

프로그램이 설치 후 해당 프로그램이 동작하기 위해서는 프로세스가 시작됩니다.

프로세스에서는 실행되어 있는 프로세스 확인 및 불필요한 프로세스를 종료할 수 있습니다.



A 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 실행 중인 프로세스를 검색하여 화면에 표시합니다
- 새로고침 : 실행 중인 프로세스의 항목을 최신 정보로 고칩니다

B 영역

- 이름 : 실행 중인 프로세스의 이름을 표시합니다.
- 설명 : 실행 중인 프로세스에 대한 설명을 표시합니다.
- PID : 실행 중인 프로세스의 PID 를 표시합니다.
- 제작사 : 실행 중인 프로세스의 제작사를 표시합니다.

C 영역

- 검색 리스트 개수 : 실행 중인 프로세스의 개수를 표시합니다.
- 종료 : 실행 중인 프로세스를 종료합니다.

프로세스 종료 방법

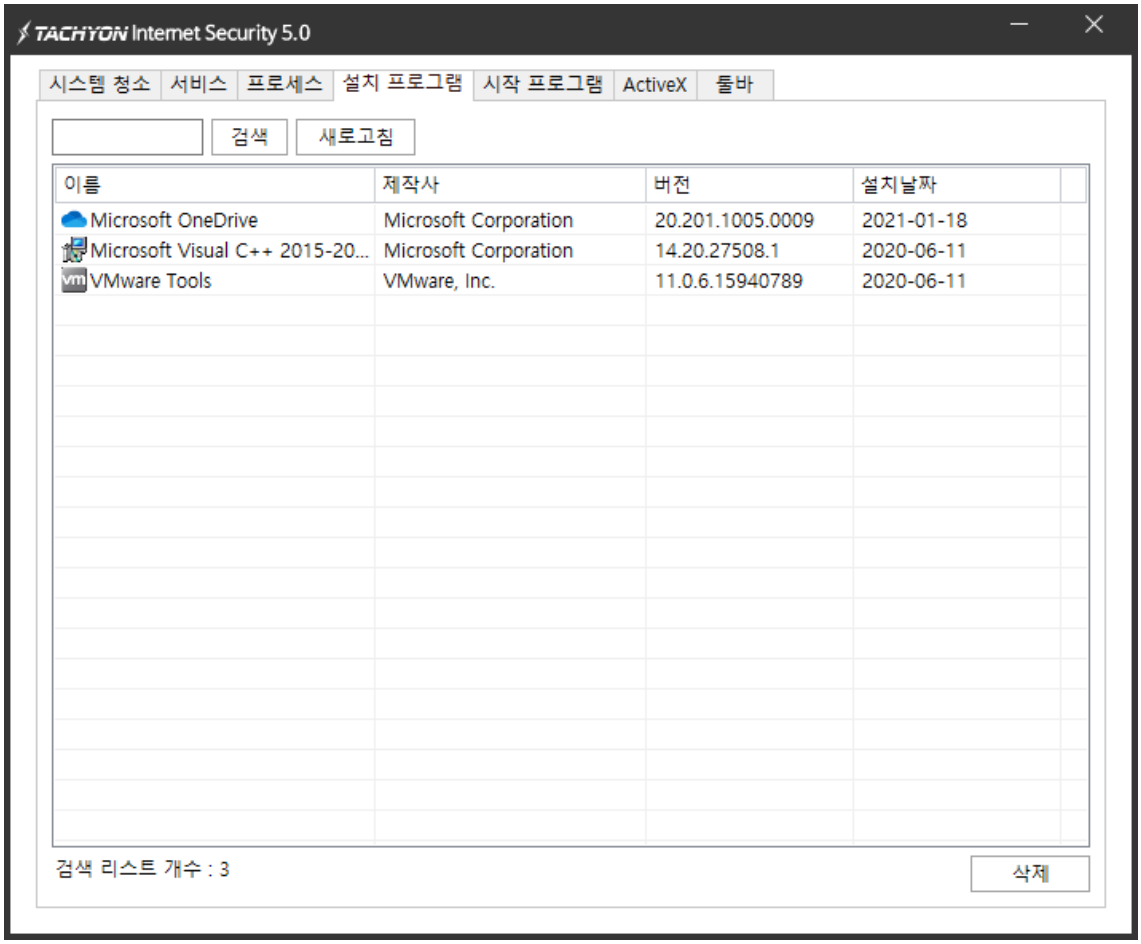
1. 종료하고자 하는 프로세스를 선택합니다.

2. 화면 우측 하단의 [종료] 버튼을 클릭하면 선택된 프로세스가 종료됩니다.

※ 윈도우 프로세스를 잘못 종료할 경우 윈도우가 비정상적으로 종료될 수 있으니 주의하여 주십시오.

5. 설치 프로그램

설치 프로그램 관리에서는 PC 에 설치된 프로그램 목록을 보여주고 사용자가 더 이상 사용되지 않거나 불필요한 프로그램을 삭제할 수 있습니다.



A 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 설치되어 있는 프로그램을 검색하여 화면에 표시합니다.
- 새로고침 : 설치되어 있는 프로그램의 항목을 최신 정보로 고칩니다.

B 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 이름 : 설치되어 있는 프로그램의 이름을 표시합니다.
- 제작사 :설치되어 있는 프로그램의 제작사를 표시합니다.
- 버전 : 설치되어 있는 프로그램의 버전을 표시합니다.
- 설치날짜 : 설치되어 있는 프로그램의 설치 날짜를 표시합니다.

C 영역

- 검색 리스트 개수 : 실행되어 있는 프로그램의 개수를 표시합니다.
- 삭제 : 설치되어 있는 프로그램을 삭제합니다.

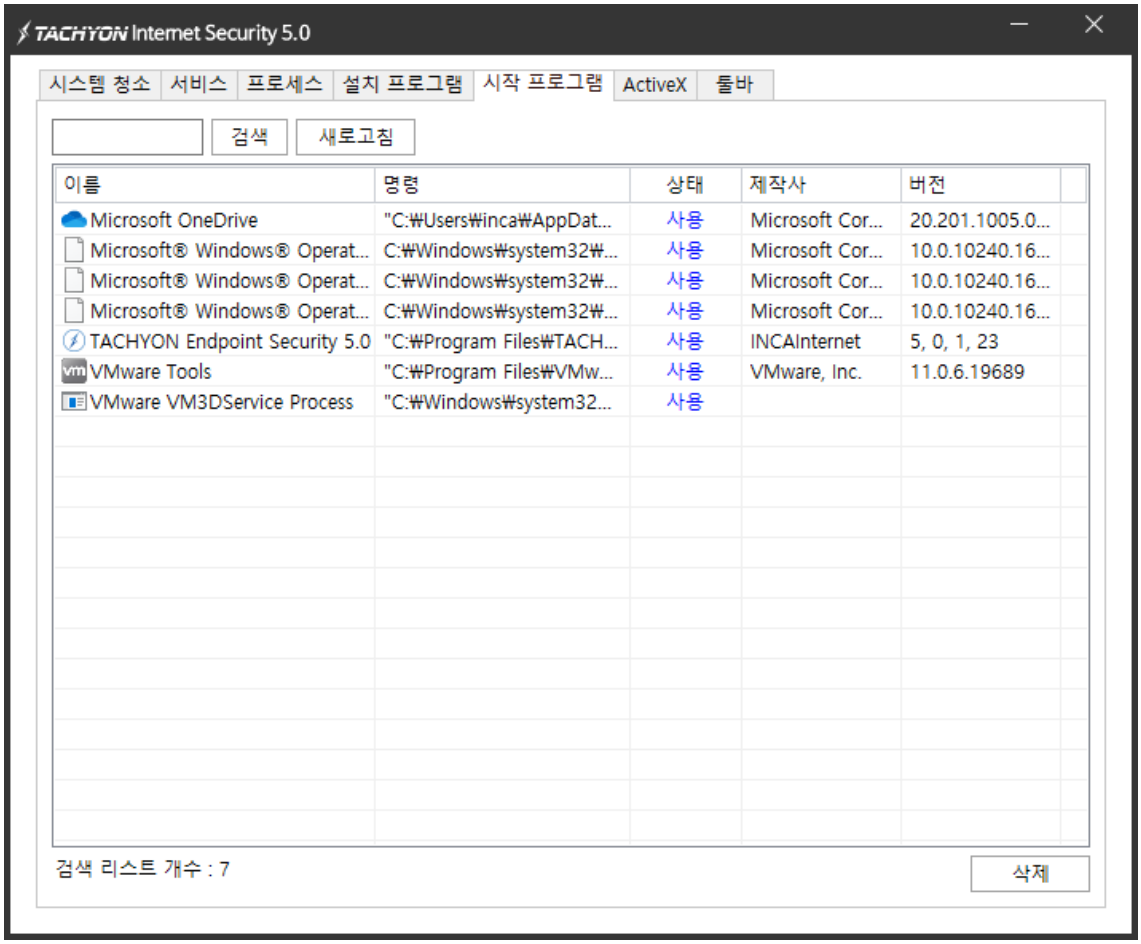
설치 프로그램 삭제 방법

1. 삭제하고자 하는 프로그램을 선택합니다.

2. 화면 우측 하단의 [삭제]를 클릭하면 설치 프로그램을 삭제합니다.

6. 시작 프로그램

시작 프로그램에서는 사용자 PC 의 프로그램 중 윈도우 시작 시에 자동으로 실행되는 프로그램 목록을 확인하고, 원하는 목록을 삭제할 수 있습니다.



A 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 등록되어 있는 시작 프로그램을 검색하여 화면에 표시합니다.
- 새로고침 : 등록되어 있는 시작 프로그램의 항목을 최신 정보로 고칩니다.

B 영역

- 이름 : 등록되어 있는 시작 프로그램의 이름을 표시합니다.
- 명령 : 윈도우 시작 시에 실행될 수 있는 Command 명령어를 표시합니다.
- 상태 : 등록되어 있는 시작 프로그램의 상태를 표시합니다(사용/사용 안함).
- 제작사 : 등록되어 있는 시작 프로그램의 제작사를 표시합니다.
- 버전 : 등록되어 있는 시작 프로그램의 버전을 표시합니다.

C 영역

- 검색 리스트 개수 : 등록되어 있는 시작 프로그램의 개수를 표시합니다.
- 삭제 : 등록되어 있는 시작 프로그램을 삭제합니다.

시작 프로그램 상태 변경 방법

1. 상태를 변경하고 하는 프로그램 목록을 선택합니다.

2. 선택한 프로그램에서 마우스 우클릭한 후 상태를 “사용/사용 안함”으로 변경할 수 있습니다.

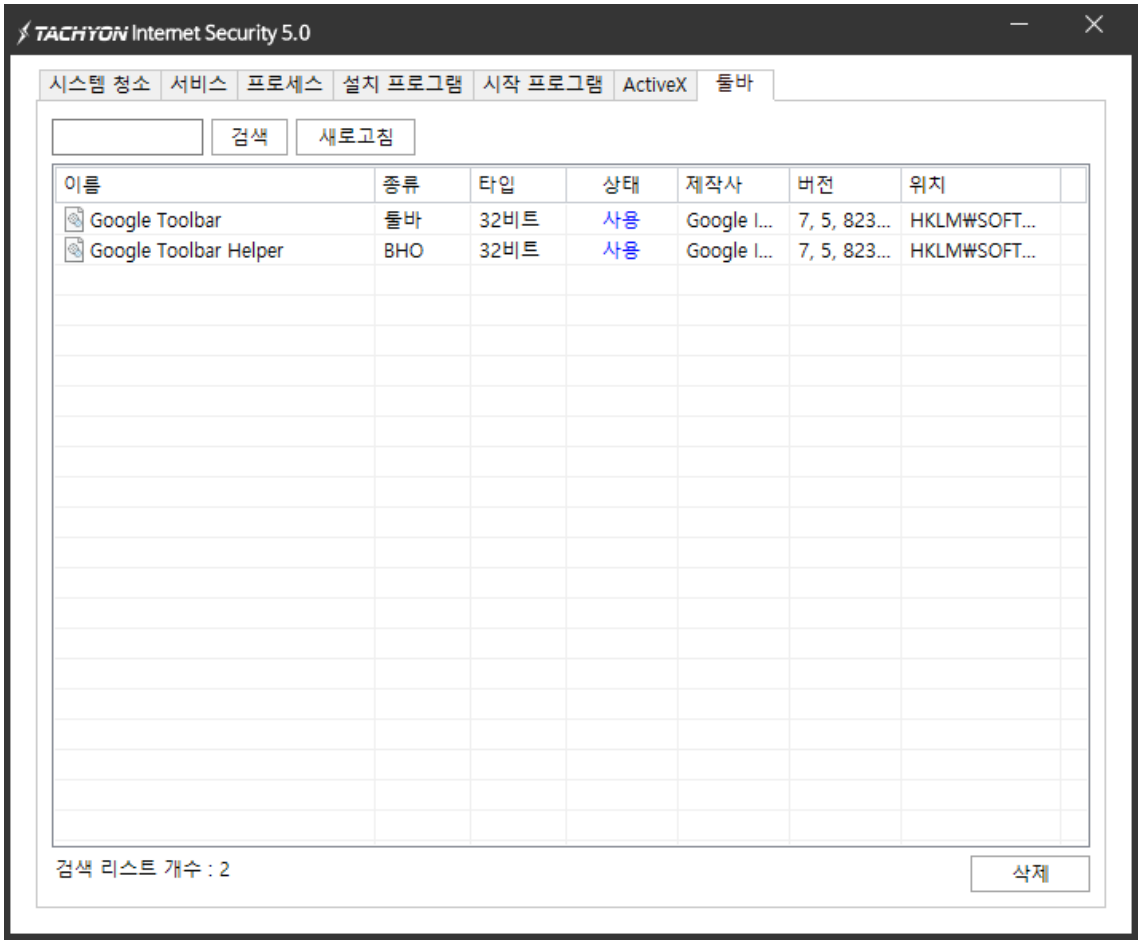
시작 프로그램 삭제 방법

1. 삭제 하고자 하는 프로그램 목록을 선택합니다.

2. 화면 우측 하단의 [삭제]를 클릭하면 시작 프로그램 목록에서 삭제됩니다.

7. ActiveX

ActiveX 관리에서는 사용자 PC 에 설치된 ActiveX 컨트롤러 정보를 확인하고, 원하는 ActiveX 컨트롤러를 삭제할 수 있습니다.



A 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 설치되어 있는 ActiveX 를 검색하여 화면에 표시합니다.
- 새로고침 : 설치되어 있는 ActiveX 의 항목을 최신 정보로 고칩니다.

B 영역

- 이름 : 설치되어 있는 ActiveX 의 이름을 표시합니다.
- 상태 : 설치되어 있는 ActiveX 의 상태를 표시합니다(사용/사용 안함).
- 제작사 : 설치되어 있는 ActiveX 의 제작사를 표시합니다.
- URL : 설치되어 있는 ActiveX 의 URL 을 표시합니다.

C 영역

- 검색 리스트 개수 : 설치되어 있는 ActiveX 의 개수를 표시합니다.
- 삭제 : 설치되어 있는 ActiveX 를 삭제합니다.

ActiveX 상태 변경 방법

1. 상태를 변경하고자 하는 ActiveX 를 선택합니다.

2. 선택한 ActiveX 에서 마우스 우클릭한 후 상태를 “사용/사용 안함”으로 변경할 수 있습니다.

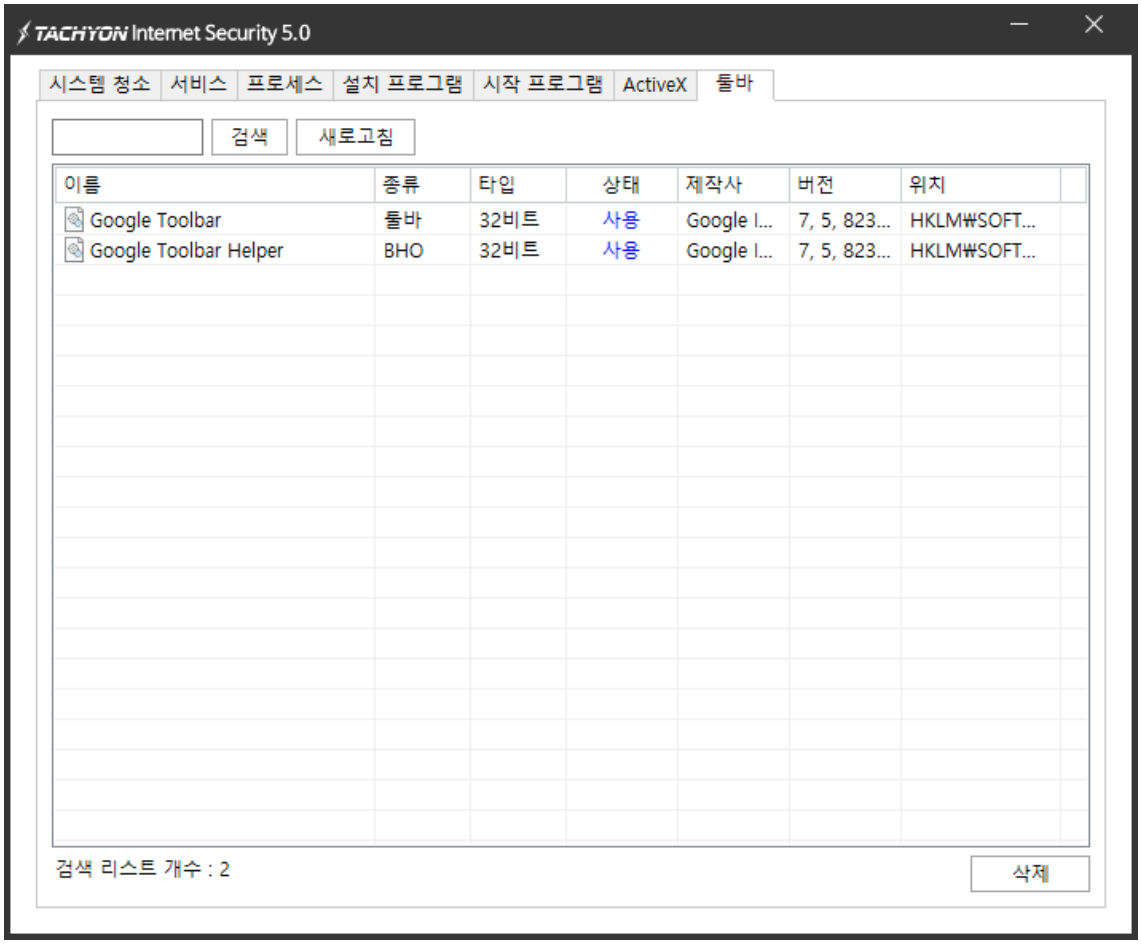
ActiveX 삭제 방법

1. 삭제 하고자 하는 ActiveX 를 선택합니다.

2. 화면 우측 하단의 [삭제]를 클릭하면 ActiveX 를 삭제할 수 있습니다

8. 툴바

툴바에서는 웹 브라우저 Internet Explorer 와 연동되어 동작하는 프로그램 정보를 확인하고, 원하는 프로그램을 삭제할 수 있습니다.



A 영역

- 검색어 입력란 : 검색어를 입력할 수 있습니다.
- 검색 : 설치되어 있는 툴바를 검색하여 화면에 표시합니다.
- 새로고침 : 설치되어 있는 툴바의 항목을 최신 정보로 고칩니다.

B 영역

- 이름 : 설치되어 있는 툴바의 이름을 표시합니다.
- 종류 : 설치되어 있는 툴바의 종류를 표시합니다(툴바/BHO).
- 타입 : 설치되어 있는 툴바의 타입을 표시합니다(32 비트/64 비트).
- 상태 : 설치되어 있는 툴바의 상태를 표시합니다(사용/사용 안함).
- 제작사 : 설치되어 있는 툴바의 제작사를 표시합니다.
- 버전 : 설치되어 있는 툴바의 버전을 표시합니다.
- 위치 : 설치되어 있는 툴바의 위치를 표시합니다.

C 영역

- 검색 리스트 개수 : 설치되어 있는 툴바의 개수를 표시합니다..
- 삭제 : 설치되어 있는 툴바를 삭제합니다.

툴바 상태 변경 방법

1. 상태를 변경하고자 하는 툴바를 선택합니다.

2. 선택한 툴바에서 마우스 우클릭한 후 상태를 “사용/사용 안함”으로 변경할 수 있습니다.

툴바 삭제 방법

1. 삭제 하고자 하는 툴바를 선택합니다.

2. 화면 우측 하단의 [삭제]를 클릭하면 툴바를 삭제할 수 있습니다.

12장

파일완전삭제

1. 파일 완전 삭제

1. 파일 완전 삭제

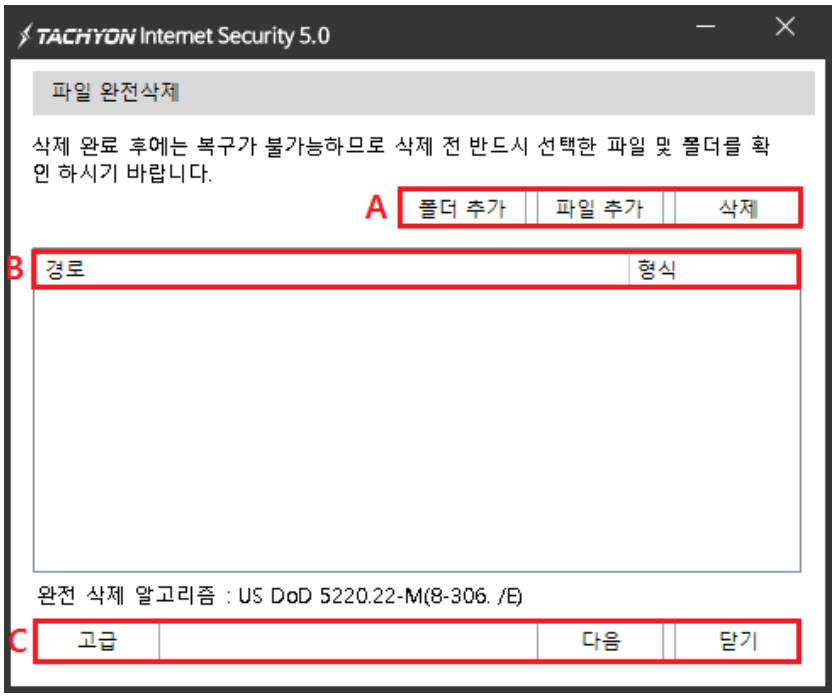
파일 완전 삭제는 사용자가 선택한 파일이나 폴더를 하드 디스크에서 완전히 삭제하여 데이터 복구 프로그램 등으로 인해 파일 내용 및 개인 정보가 유출되지 않도록 보호할 수 있는 기능입니다.

실행 방법

1. 바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘 또는 트레이 아이콘( )을 더블 클릭합니다.

2. TACHYON Internet Security 5.0 메인 화면에서 [파일 완전 삭제]를 클릭합니다.

3. 파일 완전 삭제가 실행됩니다.



A 영역

- 폴더 추가 : 완전 삭제할 폴더를 추가합니다.
- 파일 추가 : 완전 삭제할 파일을 추가합니다.
- 삭제 : 완전 삭제 대상 리스트에서 선택된 항목을 삭제합니다. 완전 삭제 대상 리스트에서 삭제된 항목은 완전 삭제 되지 않습니다.

B 영역

- 경로 : 완전 삭제 대상 폴더나 파일의 경로를 표시합니다.
- 형식 : 완전 삭제 대상의 형식을 표시합니다.(폴더, 파일)

C 영역

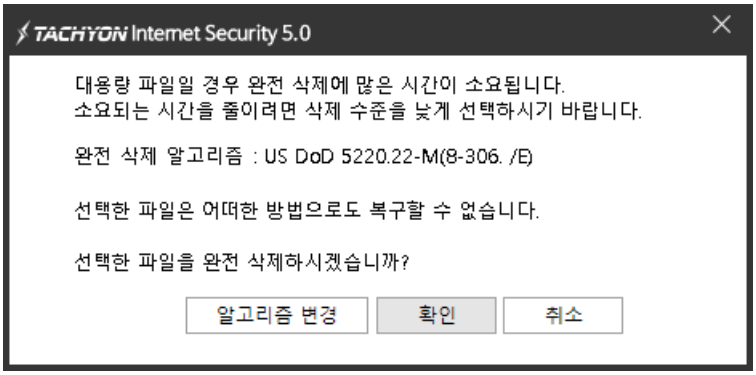
■ 고급 : 완전 삭제 알고리즘을 선택할 수 있습니다.

완전 삭제 수준은 아주 높음, 높음, 보통, 아주 낮음을 선택할 수 있으며 기본값은 보통입니다.

완전 삭제 수준에 따라 삭제 속도가 결정됩니다.

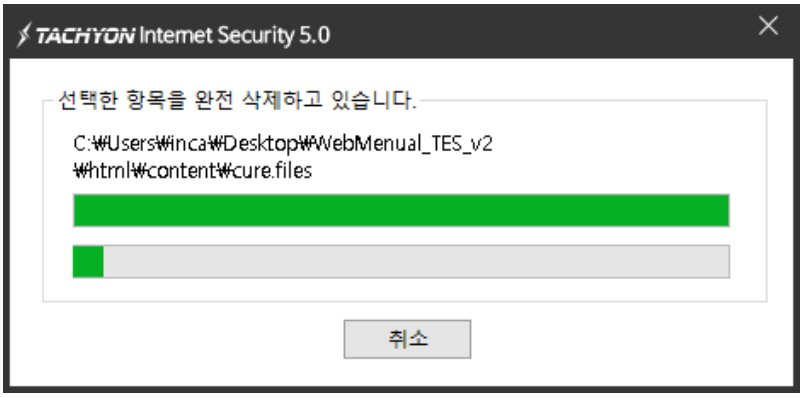
아주 높음인 경우의 삭제 속도는 아주 느림, 높음인 경우의 삭제 속도는 느림, 보통인 경우의 삭제 속도는 보통, 아주 낮음인 경우의 삭제 속도는 아주 빠름입니다.

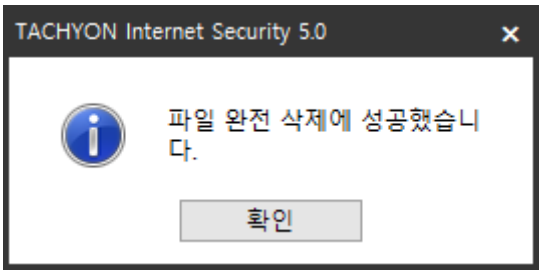
■ 다음 : 완전 삭제 대상 리스트에 있는 폴더나 파일을 완전 삭제합니다.



■ 알고리즘 변경 : 완전 삭제 알고리즘을 변경합니다.

■ 확인 : 폴더나 파일을 완전 삭제합니다.





- 취소 : 폴더나 파일의 완전 삭제를 취소합니다.
- 닫기 : 파일 완전 삭제 창을 종료합니다.

13장

환경설정

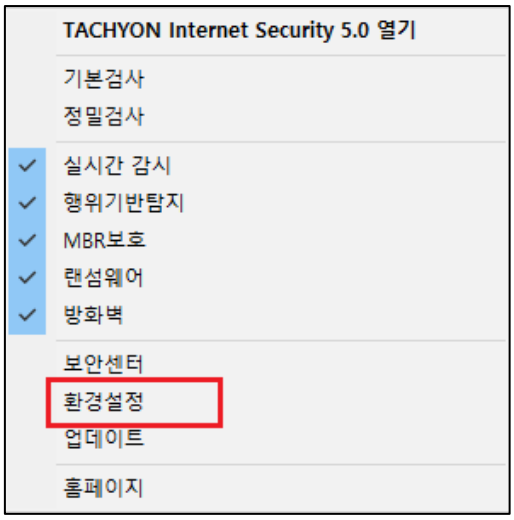
1. 환경설정

환경설정은 TACHYON Internet Security 5.0에서 사용할 수 있는 다양한 옵션에 대해 사용자가 직접 선택하여 사용할 수 있는 기능입니다.

실행 방법

■ 트레이 아이콘에서 실행하기

TACHYON Internet Security 5.0 트레이 아이콘( )에서 마우스 우클릭한 후, “환경설정”을 선택하면 실행할 수 있습니다.



■ 메인화면에서 실행하기

바탕화면의 TACHYON Internet Security 5.0 바로가기 아이콘을 더블 클릭하여 실행한 후 메인 화면 상단 메뉴의 “환경설정”을 클릭하면 실행할 수 있습니다.

환경설정의 공통 버튼

- 모두 기본 값 : 환경설정의 모든 옵션을 TACHYON Internet Security 5.0 에서 권장하는 기본값으로 변경합니다.

  [모두 기본 값]을 클릭하면, 사용자가 설정한 개별 옵션 값은 모두 지워지고 TACHYON Internet Security 5.0 에서 설정한 기본값으로 모두 변경 적용됩니다.

- 적용 : 각 화면에서 사용자가 원하는 설정을 한 후 [적용]을 클릭하면 바로 해당 기능은 사용자가 설정한 상태로 적용됩니다.

- 닫기 : 환경설정 창을 종료합니다.

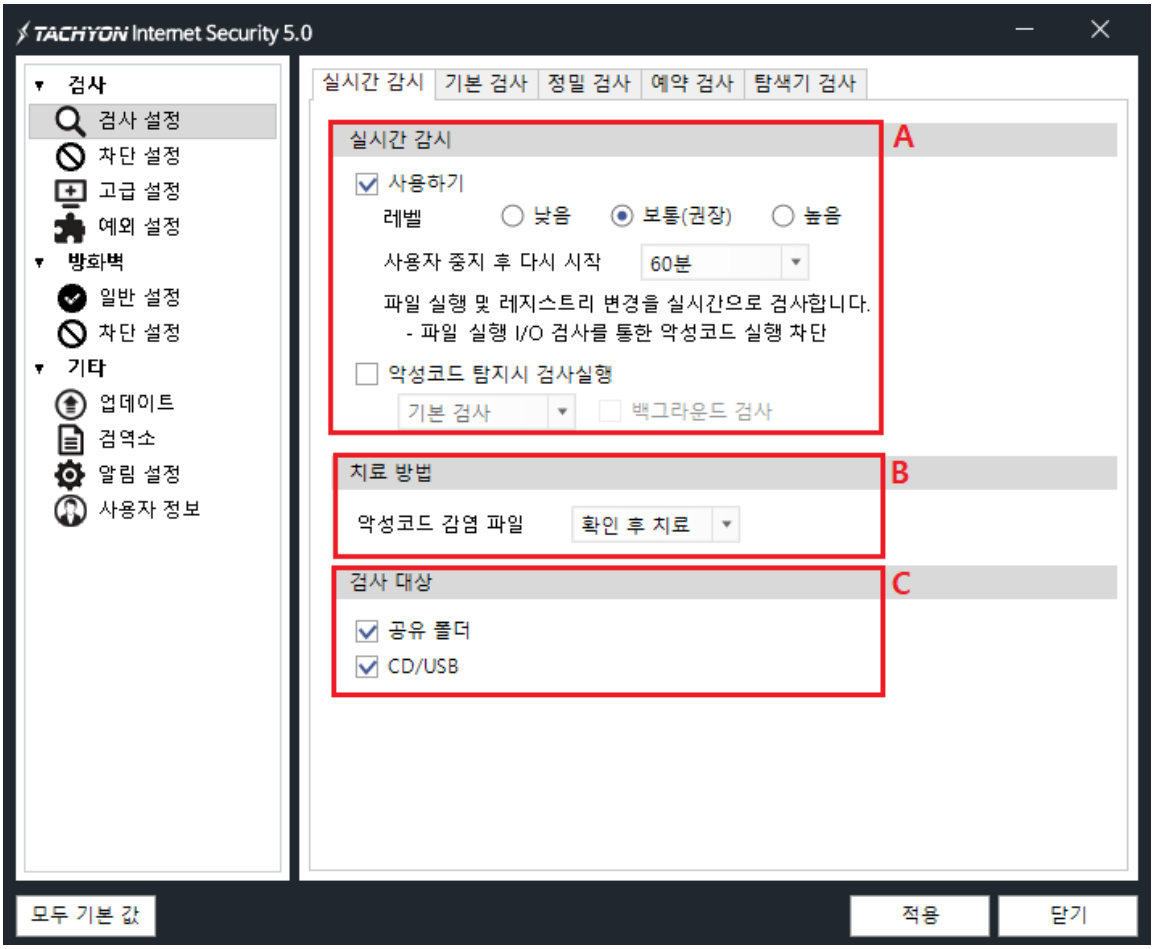
2. 실시간 검사

실시간 검사는 알려지거나 알려지지 않은 악성코드를 지속적으로 탐지하여 차단합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 실시간 감시 탭을 선택합니다.



A 영역

- 사용하기 : 실시간 감시 사용 여부를 선택합니다. 실시간 감시를 사용하려면 이 옵션을 선택해야 합니다. 실시간 감시를 선택하면 실시간 감시가 항상 작동하여 사용자 PC 에서 발생하는 파일의 저장, 이동, 삭제, 실행 등의 일련의 행위를 탐지하여 감염된 악성코드가 있는 경우 치료 방법에 따라 처리합니다.
- 레벨 : 레벨 : 검사 레벨을 지정하여 시스템 성능에 맞게 실시간 검사를 진행할 수 있습니다.
  - 낮음 : 프로세스의 실행/종료만 감지하여 실시간 검사를 진행합니다.
  - 보통(권장) : 파일의 Close I/O, 프로세스의 실행/종료만 감지하여 실시간 검사를 진행합니다.
  - 높음 : 모든 I/O 를 감시하여 실시간 검사를 진행합니다.
- 사용자 중지 후 다시 시작 : 실시간 감시를 종료했을 경우 자동으로 다시 시작할 시간을 설정합니다. 자동으로 다시 시작할 주기는 10 분, 30 분, 60 분, 재부팅 시를 선택할 수 있으며, 선택한 시간이 지난 후에 실시간 감시를 다시 시작합니다. 사용 안함을 선택하면, 실시간 감시를 종료한 후 자동으로 다시 시작하지 않습니다.
- 악성코드 탐지시 검사실행 : 실시간 감시를 통해 악성코드가 탐지될 경우 실행할 검사(기본 검사/정밀 검사)를 설정할 수 있습니다.

B 영역

실시간 감시에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

- 자동 치료 : 악성코드 감염 파일을 발견과 동시에 치료를 진행합니다.
- 확인 후 치료 : 악성코드 감염 파일 발견 시 사용자에게 알린 후 악성코드를 치료하지 않습니다.

C 영역

실시간 감시에서 검사할 대상으로 공유 폴더와 CD/USB 를 선택할 수 있습니다.

- 공유 폴더 : 공유 폴더에서 발생하는 I/O 에 대해 실시간 검사 사용 유무를 설정합니다.
- CD/USB : CD/USB 에서 발생하는 I/O 에 대해 실시간 검사 사용 유무를 설정합니다.

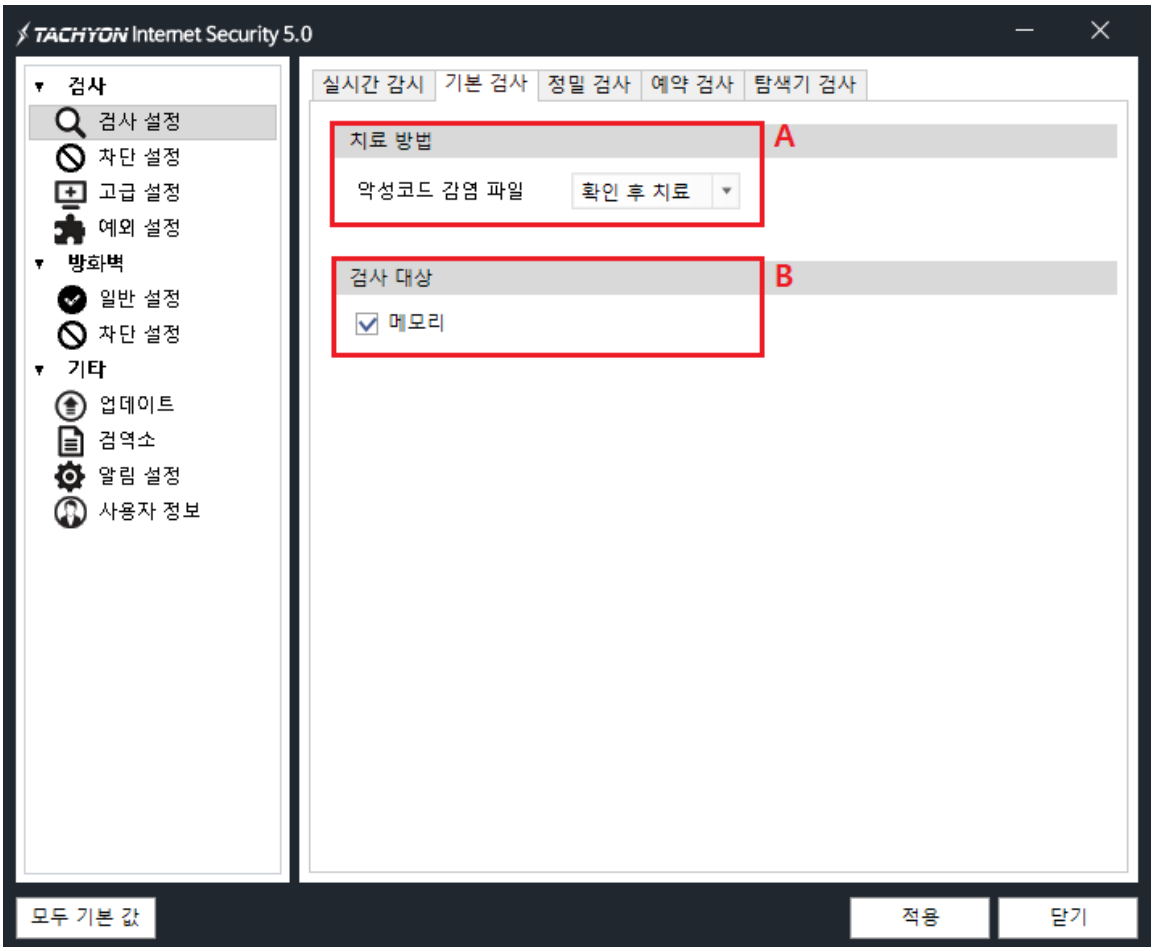
3. 기본 검사

기본 검사에서는 일반 검사 기능에 대한 옵션 설정이 가능합니다. 악성코드 감염 파일 치료 방법, 일반 검사 대상 설정이 가능합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 기본 감사 탭을 선택합니다.



A 영역

기본 검사에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

- 자동 치료 : 악성코드 감염 파일을 발견과 동시에 치료를 진행합니다.
- 확인 후 치료 : 악성코드 감염 파일 발견 시 사용자에게 알린 후 악성코드를 치료하지 않습니다.

B 영역

기본 검사에서 검사할 대상으로 메모리에 실행중인 악성코드를 선택할 수 있습니다.

- 메모리 : 메모리에 실행중인 악성코드를 진단하고 치료합니다.

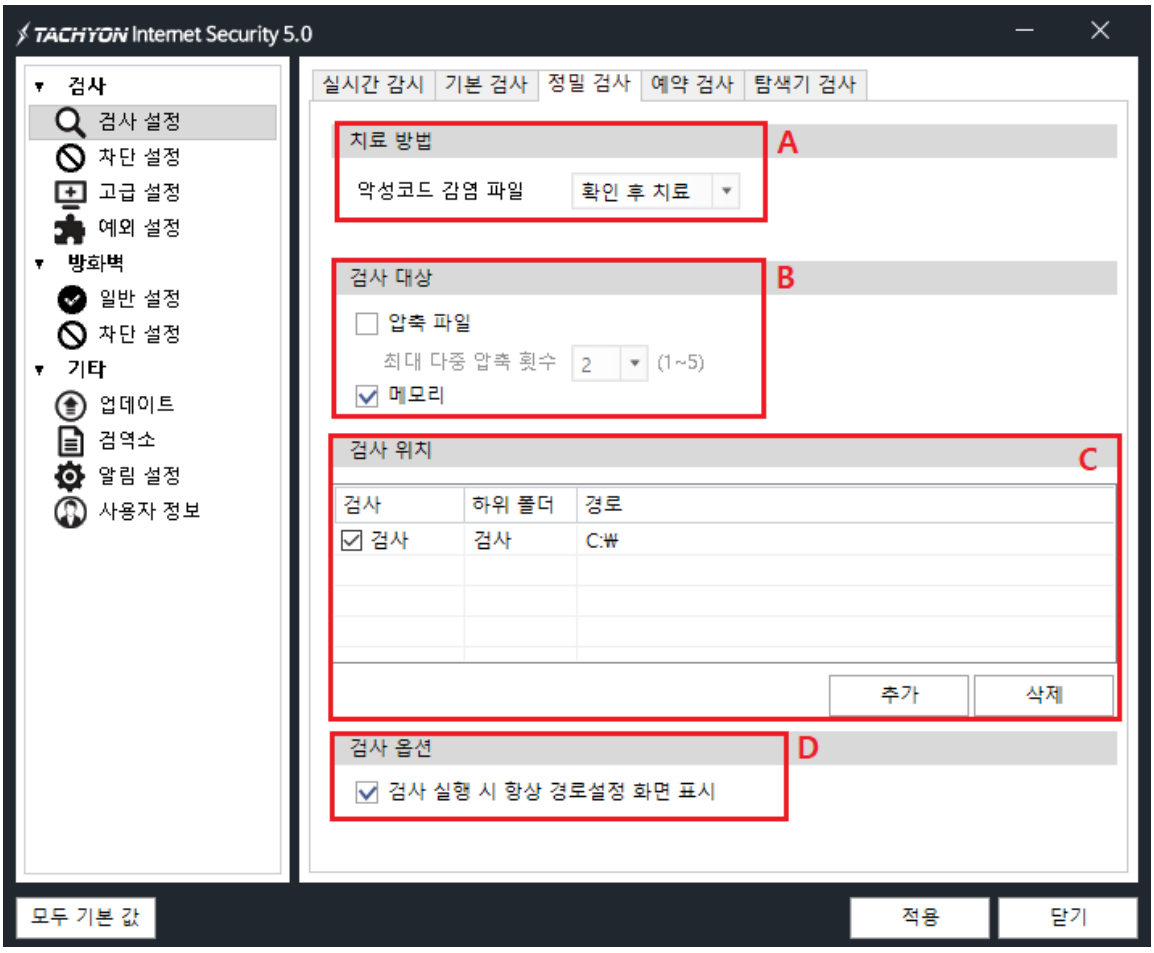
4. 정밀 검사

정밀 검사 기능에 대한 옵션 설정이 가능합니다. 악성코드 감염 파일 치료 방법, 검사 대상, 검사 위치 설정이 가능합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 정밀 검사 탭을 선택합니다.



A 영역

정밀 검사에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

- 자동 치료 : 악성코드 감염 파일을 발견과 동시에 치료를 진행합니다.
- 확인 후 치료 : 악성코드 감염 파일 발견 시 사용자에게 알린 후 악성코드를 치료하지 않습니다.

B 영역

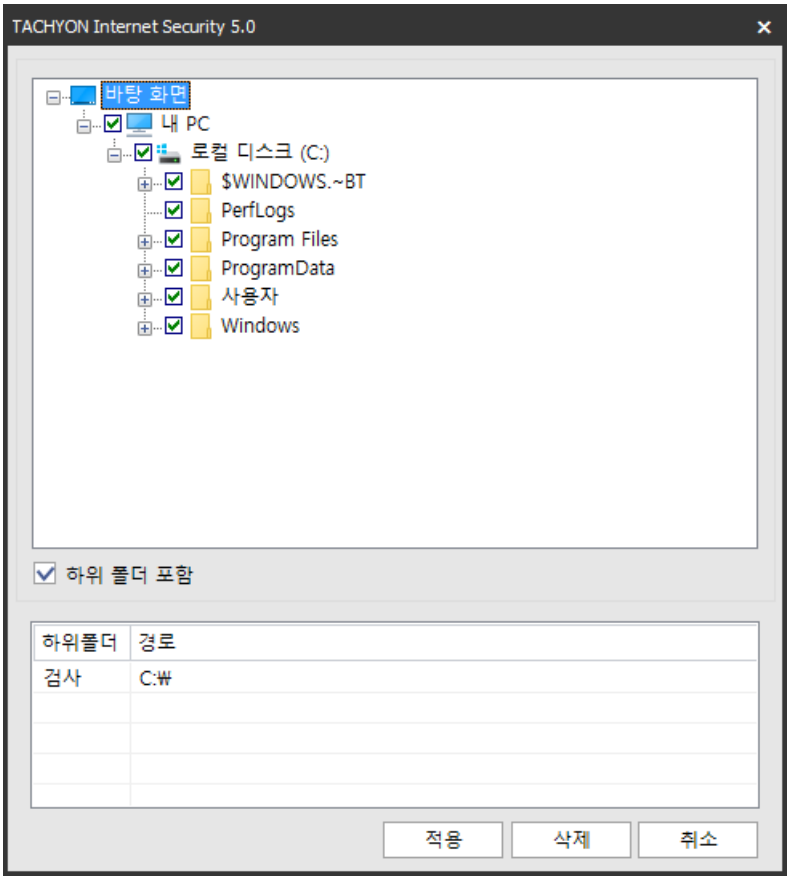
정밀 검사에서 검사할 대상으로 압축 파일과 메모리에 실행중인 악성코드를 선택할 수 있습니다.

- 압축 파일 : 일반 압축 파일을 검사합니다. ZIP, CAB, TAR, JAR, RAR, LZH, TGZ 등 다양한 압축 파일을 지원하며 최대 5 회까지 다중 압축된 파일도 검사 가능합니다.
- 메모리 : 메모리에 실행 중인 악성코드를 진단하고 치료합니다.

C 영역

정밀 검사 기능의 검사 위치를 지정할 수 있습니다. 검사 항목의 체크박스를 이용하여 현재 리스트의 항목 중 검사할 항목을 선택할 수 있습니다.

- 검사 : 해당 리스트의 검사 여부를 설정할 수 있습니다.
- 하위 폴더 : 검사 위치의 하위 폴더 검사 여부를 지정합니다.
- 경로 : 정밀 검사에서 검사할 대상 경로입니다.
- 추가 : 폴더 탐색기 창에서 정밀 검사의 위치를 지정할 수 있습니다.



- 하위 폴더 포함 : 선택한 폴더의 하위 폴더 검사 여부를 지정합니다.
- 적용 : 추가한 폴더를 검사 위치에 적용합니다.
- 삭제 : 리스트에서 선택한 항목을 삭제합니다.
- 취소 : 지금까지 한 모든 작업을 취소하고 폴더 탐색기 창을 종료합니다.
- 삭제 : 검사 위치 리스트에서 선택된 항목을 삭제할 수 있습니다.

D 영역

“검사 실행 시 항상 경로설정 화면 표시” 체크 여부에 따라 정밀 검사 실행 시 검사 위치 설정 화면을 출력할 것인지 선택할 수 있습니다. 선택하지 않으면 현재 설정되어 있는 검사 위치로 검사를 진행합니다.

5. 예약 검사

예약 검사는 사용자가 원하는 시간에 선택한 영역을 자동으로 검사하는 기능입니다.

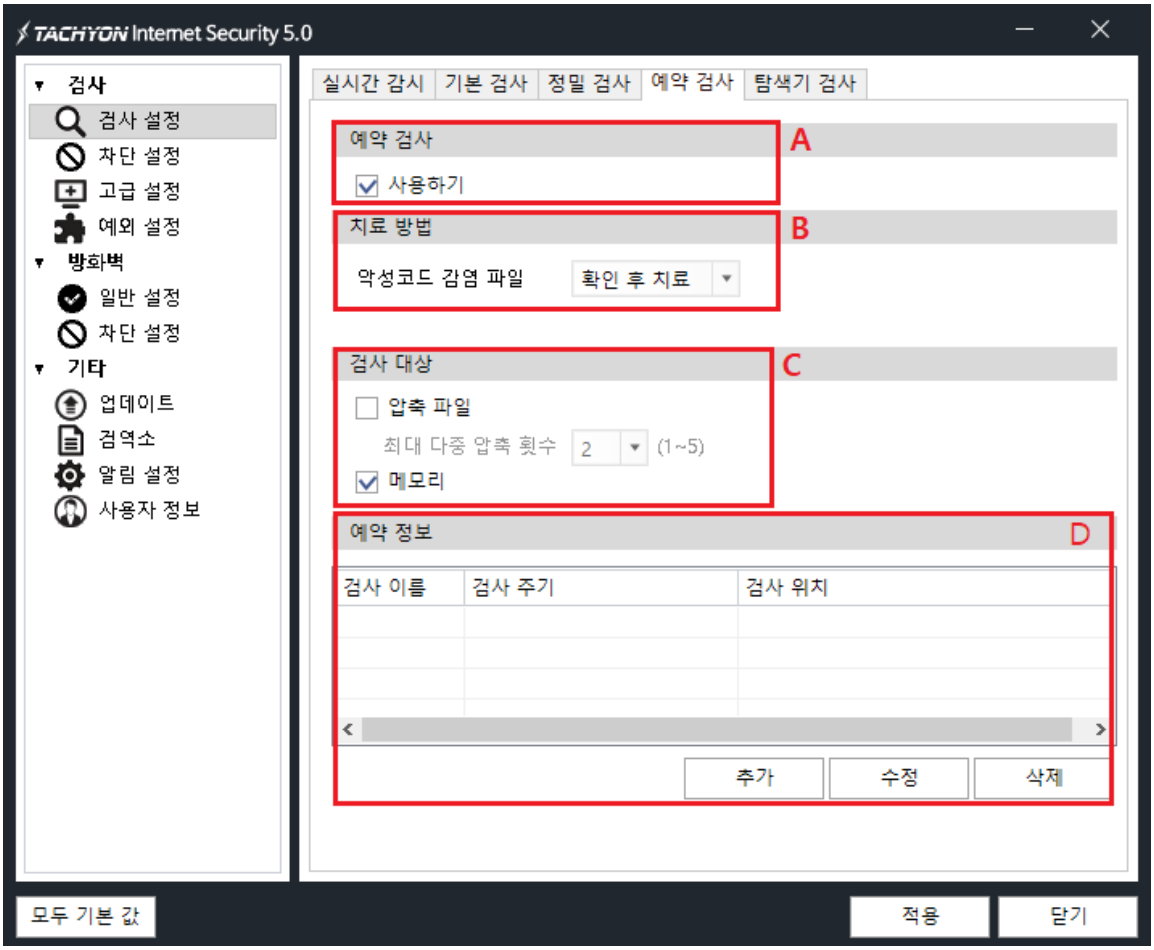
따라서 검사 시간은 사용자의 작업이 없거나, 작업량이 적을 때 선택하는 것이 효율적이며, 파일 수, 디스크 용량 등에 따라 예약 검사 시간이 달라질 수 있습니다.

또한 두 개 이상의 예약 검사를 등록하는 경우, 예약 검사 실행 중에는 다른 예약 검사가 중복으로 실행되지 않으니 예약 시간 설정 시 이를 고려해 주시기를 바랍니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 예약 검사 탭을 선택합니다.



A 영역

예약 검사 사용 여부를 선택합니다. 예약 검사 사용을 선택하면, 예약 정보에서 추가를 클릭하여 예약 검사 주기와 검사 위치를 설정할 수 있습니다.

B 영역

예약 검사에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

- 자동 치료 : 악성코드 감염 파일을 발견과 동시에 치료를 진행합니다.
- 확인 후 치료 : 악성코드 감염 파일 발견 시 사용자에게 알린 후 악성코드를 치료하지 않습니다.

C 영역

예약 검사에서 검사할 대상으로 압축 파일과 메모리에 실행중인 악성코드를 선택할 수 있습니다.

- 압축 파일 : 일반 압축 파일을 검사합니다. ZIP, CAB, TAR, JAR, RAR, LZH, TGZ 등 다양한 압축 파일을 지원하며 최대 5 회까지 다중 압축된 파일도 검사 가능합니다.
- 메모리 : 메모리에 실행 중인 악성코드를 진단하고 치료합니다.

D 영역

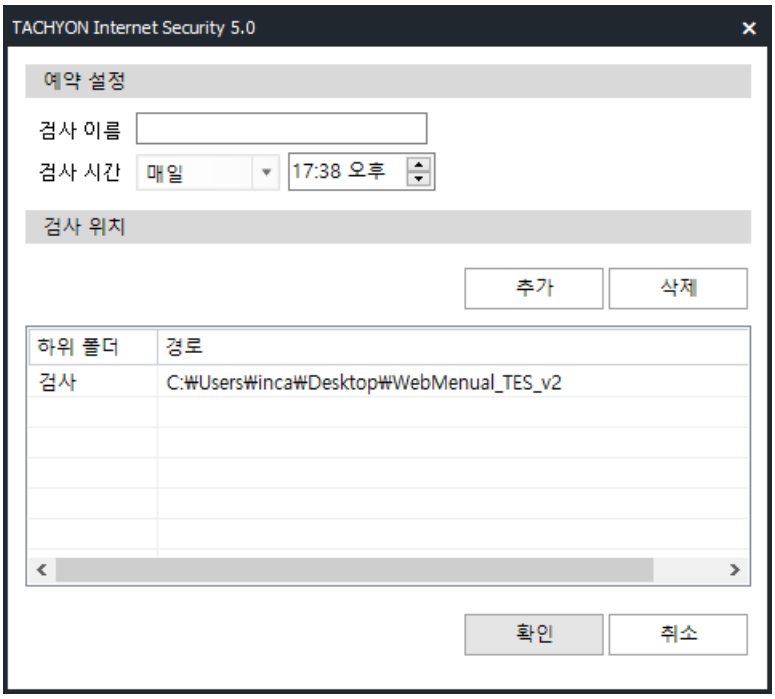
예약 검사 사용하기 체크 여부에 따라 예약 정보를 설정할 수 있습니다.

- 검사 이름 : 예약 검사를 구분할 수 있는 이름을 입력합니다.
- 검사 주기 : 예약 검사를 실행할 시간을 선택합니다.(매일/매주/매월/한번만)
- 검사 위치 : 예약 검사를 실행할 대상 경로를 설정할 수 있습니다.
- 추가 : 예약 검사를 추가할 수 있습니다.

- 수정 : 수정할 예약 검사 리스트를 선택 후 [수정]을 클릭하면 선택된 예약 검사 리스트를 수정할 수 있습니다.
- 삭제 : 삭제할 예약 검사 리스트를 선택 후 [삭제]를 클릭하면 선택된 예약 검사 리스트를 삭제할 수 있습니다.

예약 검사 추가

예약 정보의 [추가]를 클릭하면 예약 설정 창을 통하여 예약 검사 설정을 할 수 있습니다.



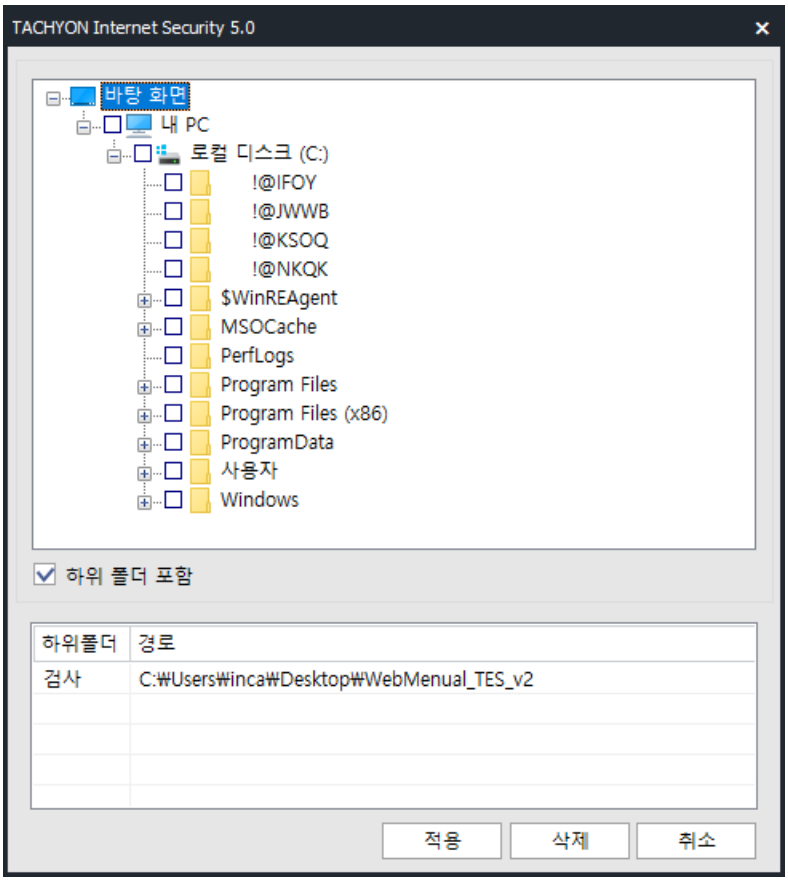
- 검사 이름 : 예약 검사 항목 이름을 설정합니다. 단, 같은 검사 이름이 존재할 경우 추가/수정할 수 없습니다.
- 검사 시간 : 예약 검사 시간을 설정합니다.
  - 매일 : 매일 실행하며, 검사 시간을 설정할 수 있습니다.
  - 매주 : 특정 요일/검사 시간을 설정할 수 있습니다.
  - 매월 : 특정 일/검사 시간을 설정할 수 있습니다.

- 한번만 : 검사할 날짜와 시간을 설정할 수 있습니다.

■ 검사 위치

사용자가 지정한 검사 대상 영역을 검사합니다. 특정 대상(폴더, 드라이브) 또는 사용자 컴퓨터 전체를 선택하여 검사를 할 수 있습니다.

[추가]를 클릭하면 검사 위치를 지정할 수 있는 폴더 탐색기 창이 나타납니다.



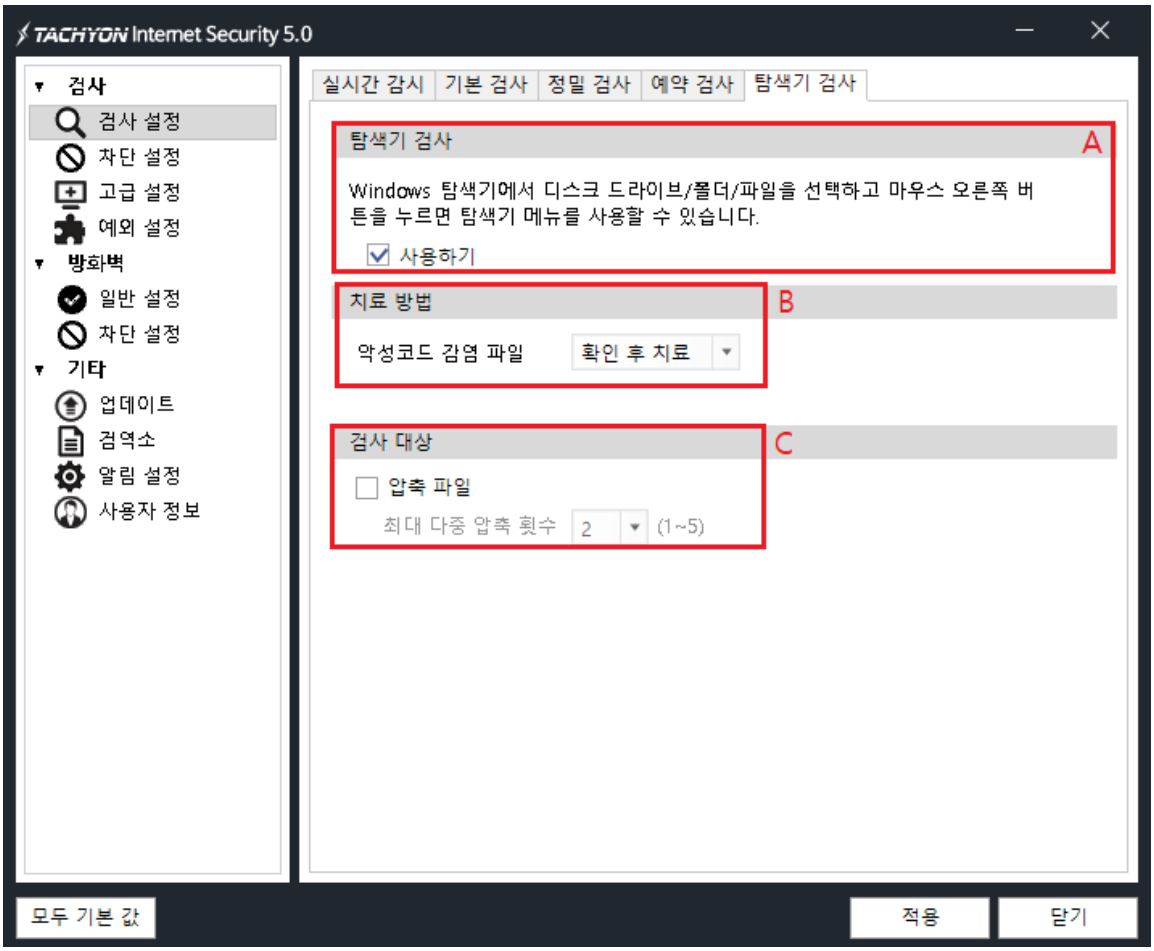
6. 탐색기 검사

파일 또는 폴더를 선택하여 마우스의 오른쪽 버튼을 클릭 시 발생하는 탐색 메뉴에 악성코드 검사 메뉴를 추가합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 탐색기 검사 탭을 선택합니다.



A 영역

탐색기 검사 사용 여부를 선택합니다. 탐색기 검사를 사용하게 되면 파일 또는 폴더를 선택하여 마우스의 오른쪽 버튼을 클릭 시 발생하는 탐색 메뉴에 “사용자 선택 검사” 메뉴가 추가 됩니다.

B 영역

탐색기 검사에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

- 자동 치료 : 악성코드 감염 파일을 발견과 동시에 치료를 진행합니다.
- 확인 후 치료 : 악성코드 감염 파일 발견 시 사용자에게 알린 후 악성코드를 치료하지 않습니다.

C 영역

탐색기 검사에서 검사할 대상으로 압축 파일을 선택할 수 있습니다.

- 압축 파일 : 반 압축 파일을 검사합니다. ZIP, CAB, TAR, JAR, RAR, LZH, TGZ 등 다양한 압축 파일을 지원하며 최대 5 회까지 다중 압축된 파일도 검사 가능합니다.

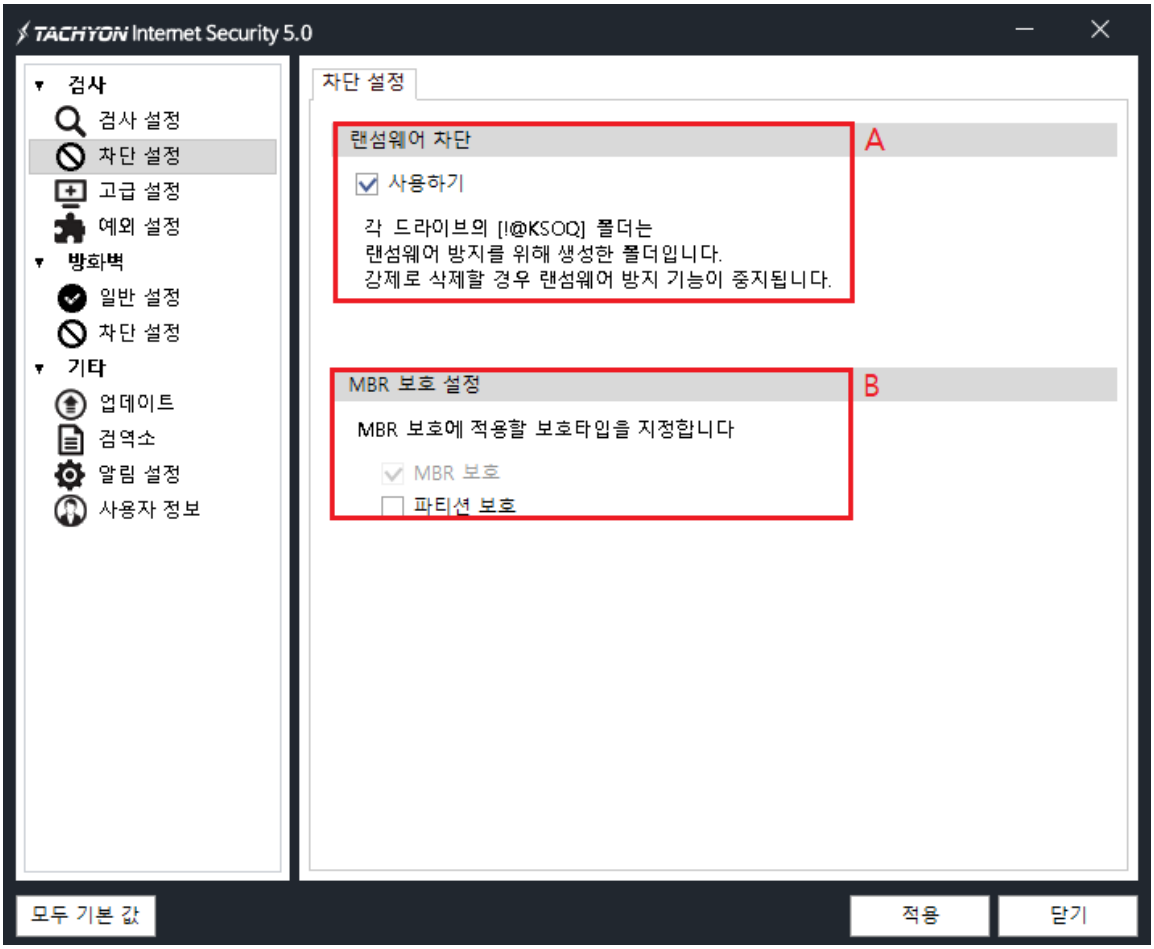
7. 차단 설정

차단 설정에는 랜섬웨어 차단 기능과 MBR 보호 설정에 대한 사용 설정이 가능합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 차단 설정 탭을 선택합니다.



A 영역

■ 랜섬웨어 차단

사용하기 체크 여부에 따라 랜섬웨어 차단 기능 사용 유무를 설정할 수 있습니다.

랜섬웨어 차단 설정에 따라 사용자에게 알림 창이 표시됩니다.

랜섬웨어 차단의 결과는 알림창과 “로그 > 위협요소 > 랜섬웨어”에서 확인 가능합니다.

B 영역

■ MBR 보호 설정

MBR 보호에 적용할 보호 타입을 지정할 수 있습니다.

- MBR 보호 : 다른 프로그램에서 MBR 영역에 접근을 시도하였을 경우 이를 차단하고 사용자에게 알림 창을 표시하여 알립니다.
- 파티션 보호 : 다른 프로그램에서 볼륨 영역에 접근을 시도하였을 경우 이를 차단하고 사용자에게 알림 창을 표시하여 알립니다.

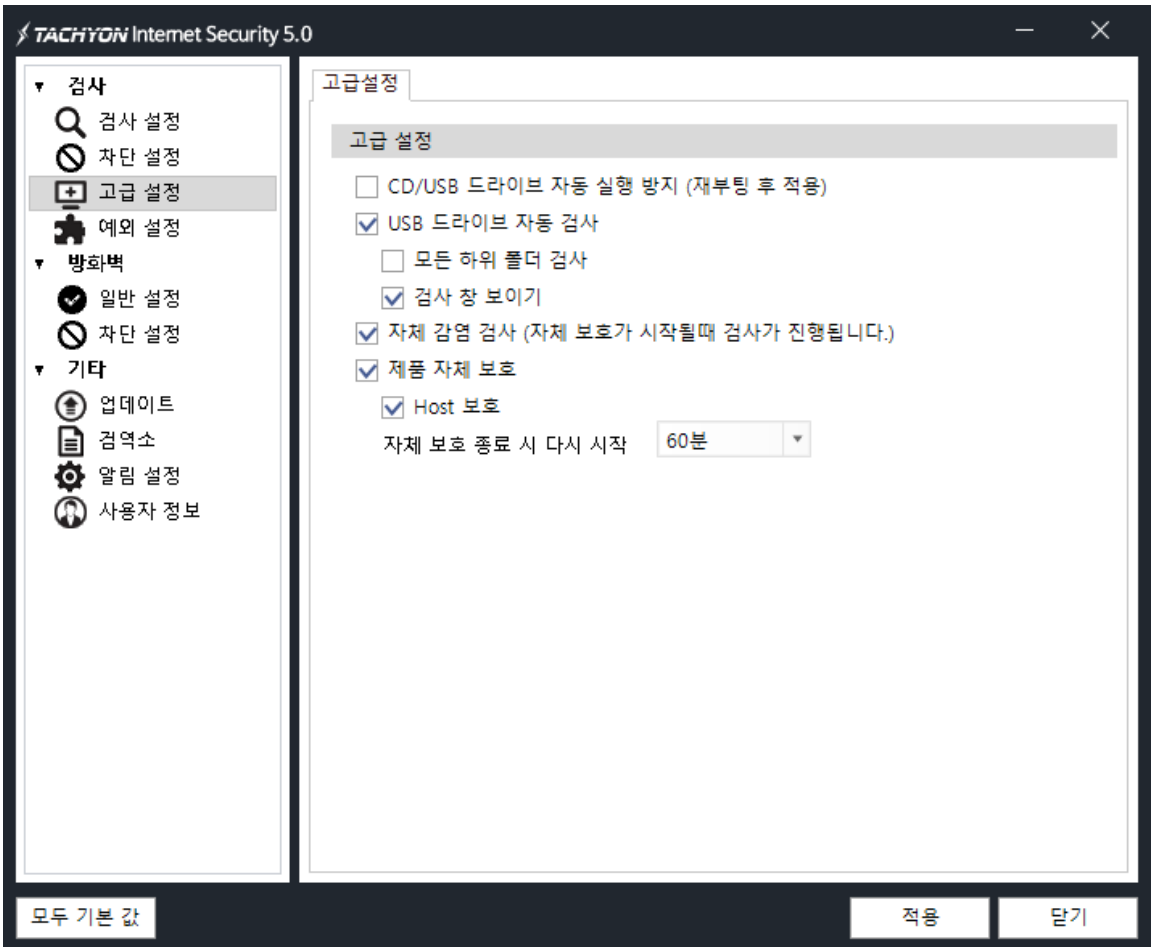
8. 고급 설정

고급 설정에서는 PC 검사에서 사용할 수 있는 기본적인 검사 옵션 외의 다양한 검사 옵션을 사용자가 직접 선택할 수 있습니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 고급 설정 탭을 선택합니다.



CD/USB 드라이브 자동 실행 방지

■ CD/USB 드라이브 자동 실행 방지

USB 메모리를 연결했을 때 이동식 디스크의 내용을 보여주는 창이 실행되지 않아 폴더 구조를 보이지 않게 하고 CD 삽입시 자동 실행되지 않게 합니다.

자동 실행 기능을 이용하여 감염되는 악성코드로부터 사용자 PC 를 보호하려면 CD 나 USB 메모리에 저장된 파일을 자동 실행하지 않고 사용자가 직접 실행하여 감염된 파일의 자동 실행으로 인해 PC 가 감염되는 것을 예방할 수 있습니다.

■ USB 드라이브 자동 검사

- 모든 하위 폴더 검사

  USB 드라이브에 저장된 하위 폴더를 모두 검사합니다.

- 검사 창 보이기

  USB 드라이브 자동 검사를 할 때 검사 창을 화면에 표시합니다.

■ 자체 감염 검사

TACHYON Internet Security 5.0 프로그램의 악성코드 감염 여부를 검사합니다.

■ 제품 자체 보호

TACHYON Internet Security 5.0 이외의 다른 프로그램에서 TACHYON Internet Security 5.0 이 사용하는 프로세스, 레지스트리, 파일, TACHYON Internet Security 5.0 설치 볼륨에 접근하는 것을 차단합니다.

- Host 보호

  악성코드에 의해 Host 파일이 변조되는 것을 차단합니다.

- 자체 보호 종료 시 다시 시작

  TACHYON Internet Security 5.0 자체 보호를 종료했을 경우 자동으로 다시 시작할 시간을 설정합니다. 자동으로 다시 시작할 주기는 10분, 30분, 60분, 재부팅 시를 선택할 수 있으며, 선택한 시간이 지난 후에 TACHYON Internet Security 5.0 자체 보호를 시작합니다. 사용 안함을 선택하면, TACHYON Internet Security 5.0 자체 보호를 종료한 후 자동으로 다시 시작하지 않습니다.

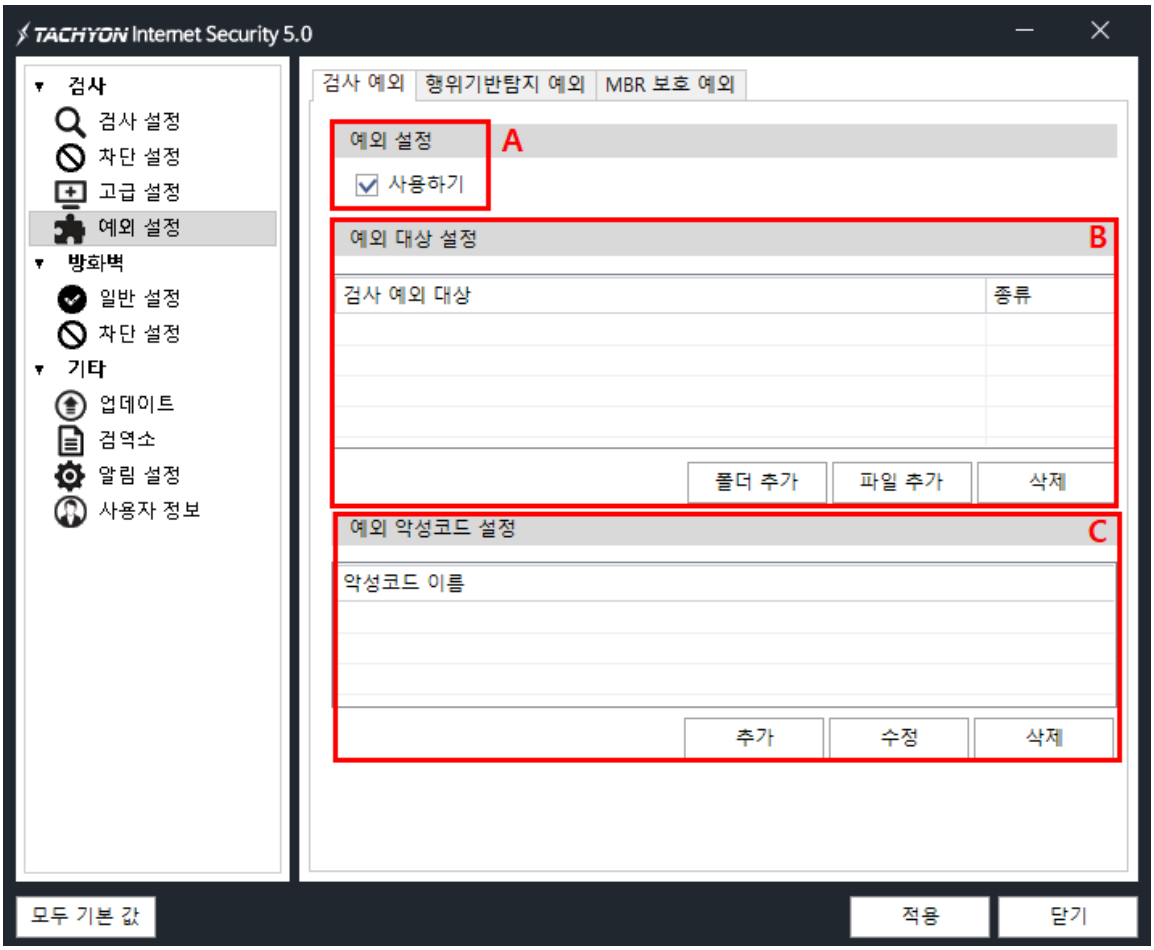
9. 예외 설정

예외 설정은 PC 검사의 검사 대상에 포함되더라도 사용자가 설정한 검사 예외 대상이거나 악성코드이지만 사용자가 검사 예외 악성코드로 설정한 경우에는 설정된 대상과 항목에 대해서는 검사하지 않는 기능입니다.

검사 예외 실행

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 검사 예외 탭을 선택합니다.



A 영역

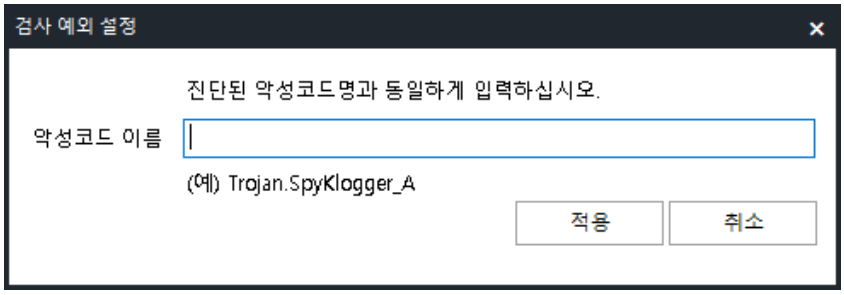
- 검사 예외 설정
  - 사용하기 : 검사 예외 대상이나 검사 예외 악성코드를 설정하려면 예외 설정 사용하기를 선택해야 합니다.

B 영역

- 검사 예외 대상 설정
  - 검사 예외 대상 : 검사하지 않을 폴더나 파일 리스트를 보여줍니다.
  - 종류 : 검사하지 않을 대상의 종류를 표시합니다.(폴더, 파일)
  - 폴더 추가 : 검사하지 않을 폴더를 추가합니다.
  - 파일 추가 : 검사하지 않을 파일을 추가합니다.
  - 삭제 : 검사 예외 대상 리스트에서 선택된 항목을 삭제합니다. 삭제된 항목은 예외 처리 되지 않습니다.

C 영역

- 검사 예외 악성코드 설정 : 검사하지 않을 악성코드를 추가하는 기능입니다.
  - 악성코드 이름 : 검사하지 않을 악성코드 리스트를 보여줍니다.
  - 추가 : 검사하지 않을 악성코드 명을 입력합니다. 단, TACHYON Internet Security 5.0 이 검사하여 진단된 악성코드 명과 동일할 경우에만 제외할 수 있습니다.

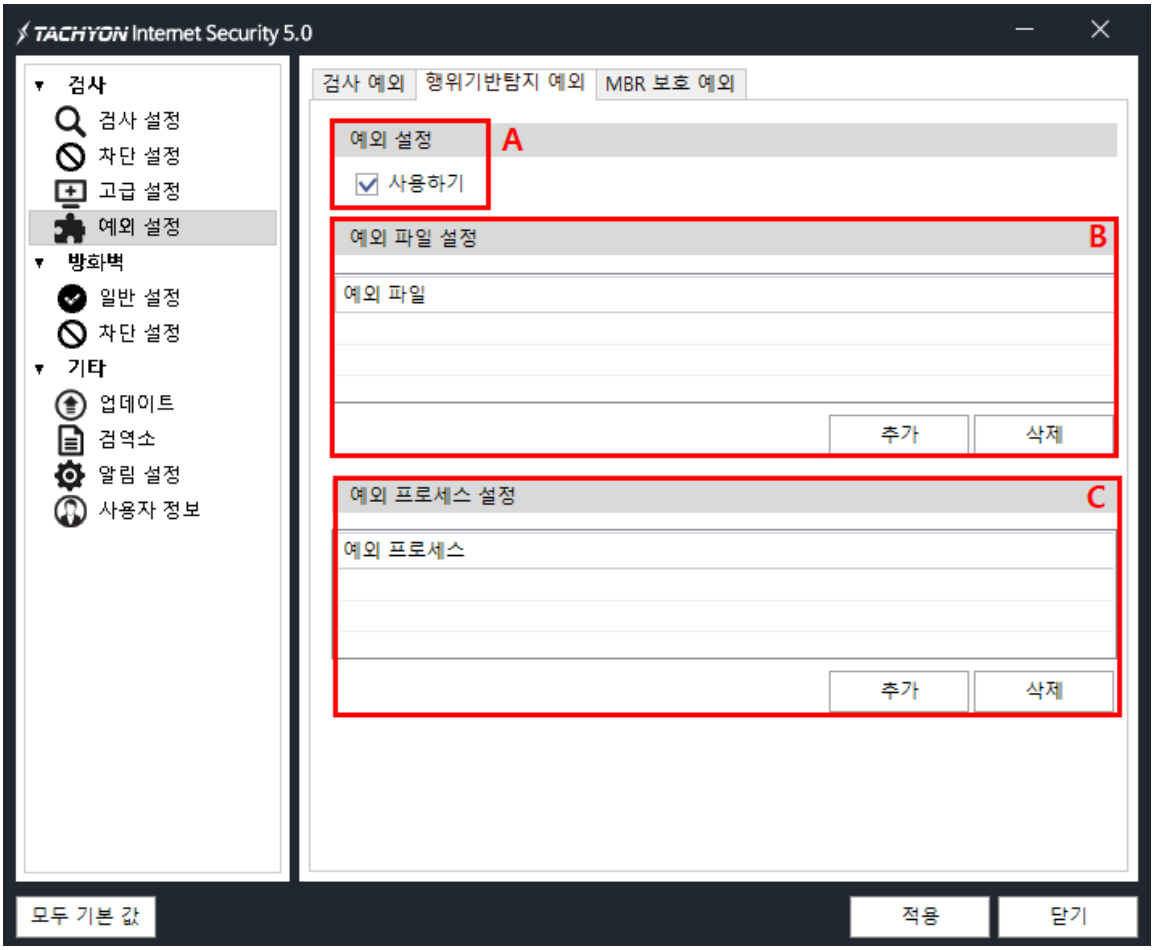


- 수정 : 예외 악성코드 리스트에서 선택된 항목의 악성코드 이름을 수정합니다.
- 삭제 : 예외 악성코드 리스트에서 선택된 항목의 악성코드를 삭제합니다.

행위기반탐지 예외 실행

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 예외 설정 > 행위기반탐지 예외 탭을 선택합니다.



A 영역

■ 행위기반탐지 예외 설정

- 사용하기 : 행위기반탐지 예외 대상이나 행위기반탐지 예외 프로세스를 설정하려면 예외 설정 사용하기를 선택해야 합니다.

B 영역

■ 행위기반탐지 예외 파일 설정 : 행위기반탐지 기능의 예외 파일을 설정할 수 있습니다.

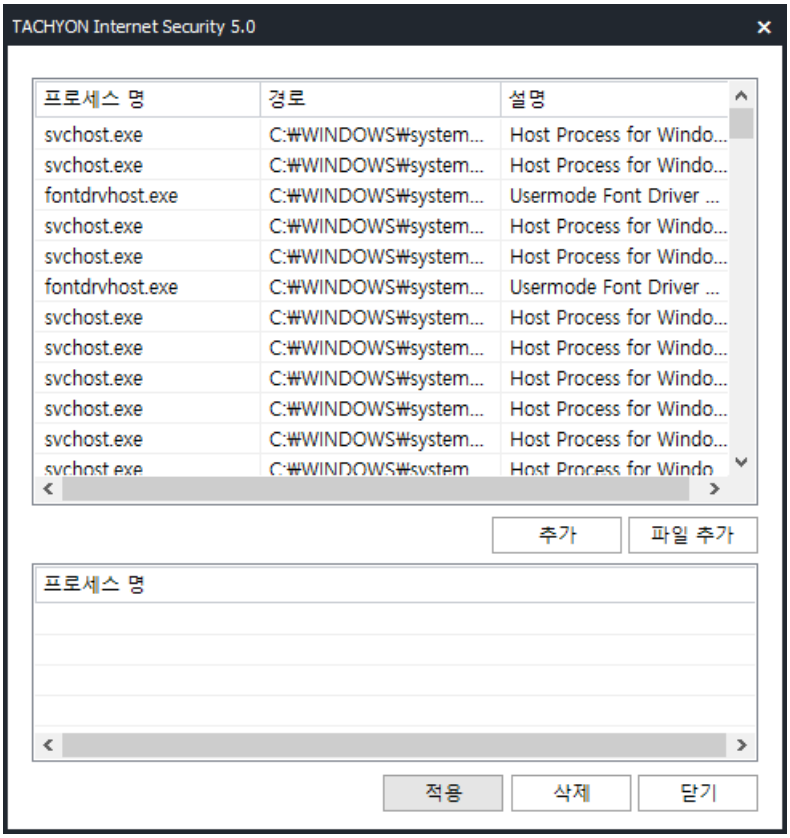
- 예외 파일 : 행위기반탐지 기능의 예외 파일 리스트를 보여줍니다.
- 추가 : 행위기반탐지 기능의 예외 파일을 추가합니다.
- 삭제 : 예외 파일 리스트 중 선택된 항목을 삭제합니다.

C 영역

■ 행위기반탐지 예외 프로세스 설정

행위기반탐지 기능의 예외 프로세스를 설정할 수 있습니다. 예외 설정 시 해당하는 프로세스 실행, 생성되는 파일이 행위기반탐지 공격에 이용된 파일이라도 진단하지 않습니다.

- 예외 프로세스 : 행위기반탐지 기능의 예외 프로세스 리스트를 보여줍니다.
- 추가 : 행위기반탐지 기능의 예외 프로세스를 추가합니다. 현재 실행 중인 프로세스 리스트에서 예외 설정에 추가할 프로세서를 추가할 수 있으며, 설치된 파일 경로에서 직접 프로세스를 추가할 수 있습니다.

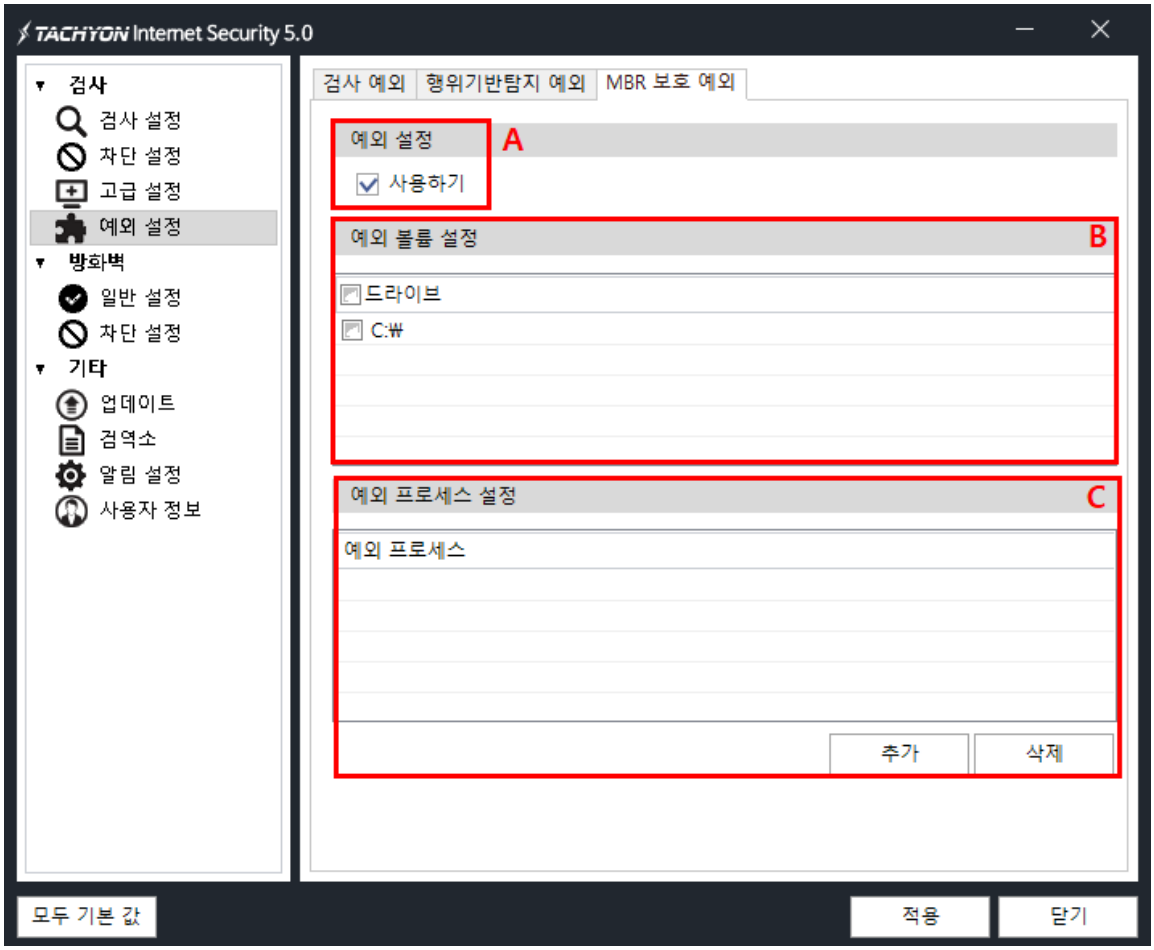


- 삭제 : 예외 프로세스 리스트 중 선택된 항목을 삭제합니다.

MBR 보호 예외 실행

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 예외 설정 > MBR 보호 예외 탭을 선택합니다.



A 영역

- MBR 보호 예외 설정
  - 사용하기 : MBR 보호 예외 볼륨이나 MBR 보호 예외 프로세스를 설정하면 예외 설정 사용하기를 선택해야 합니다.

B 영역

■ MBR 보호 예외 볼륨 설정

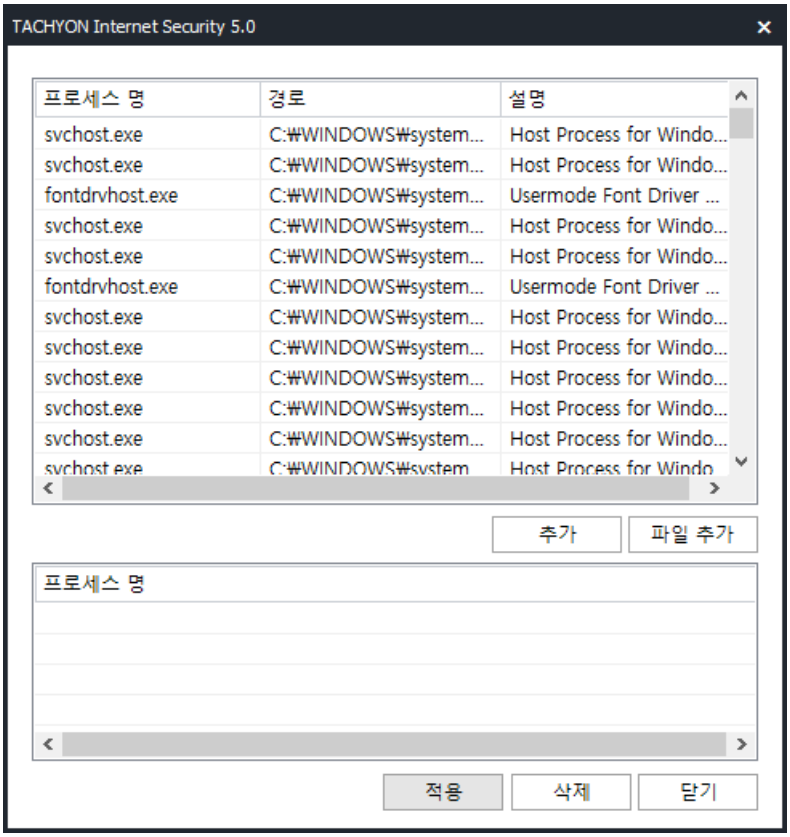
MBR 보호 기능 중 볼륨 보호 기능의 예외 되는 볼륨을 선택할 수 있습니다. 이때, 설정된 예외 볼륨에는 다른 프로세스로부터 볼륨 접근이 가능합니다.

C 영역

■ MBR 보호 예외 프로세스 설정

MBR 영역 및 볼륨에 접근 가능한 프로세스를 설정할 수 있습니다.

- 예외 프로세스 : MBR 영역 및 볼륨에 접근 가능한 프로세스 리스트를 표시합니다.
- 추가 : 예외 프로세스를 추가합니다. 현재 실행 중인 프로세스 리스트에서 예외 설정에 추가할 프로세서를 추가할 수 있으며, 설치된 파일 경로에서 직접 프로세스를 추가할 수도 있습니다.



- 삭제 : 예외 프로세스 리스트 중 선택된 항목을 삭제합니다.

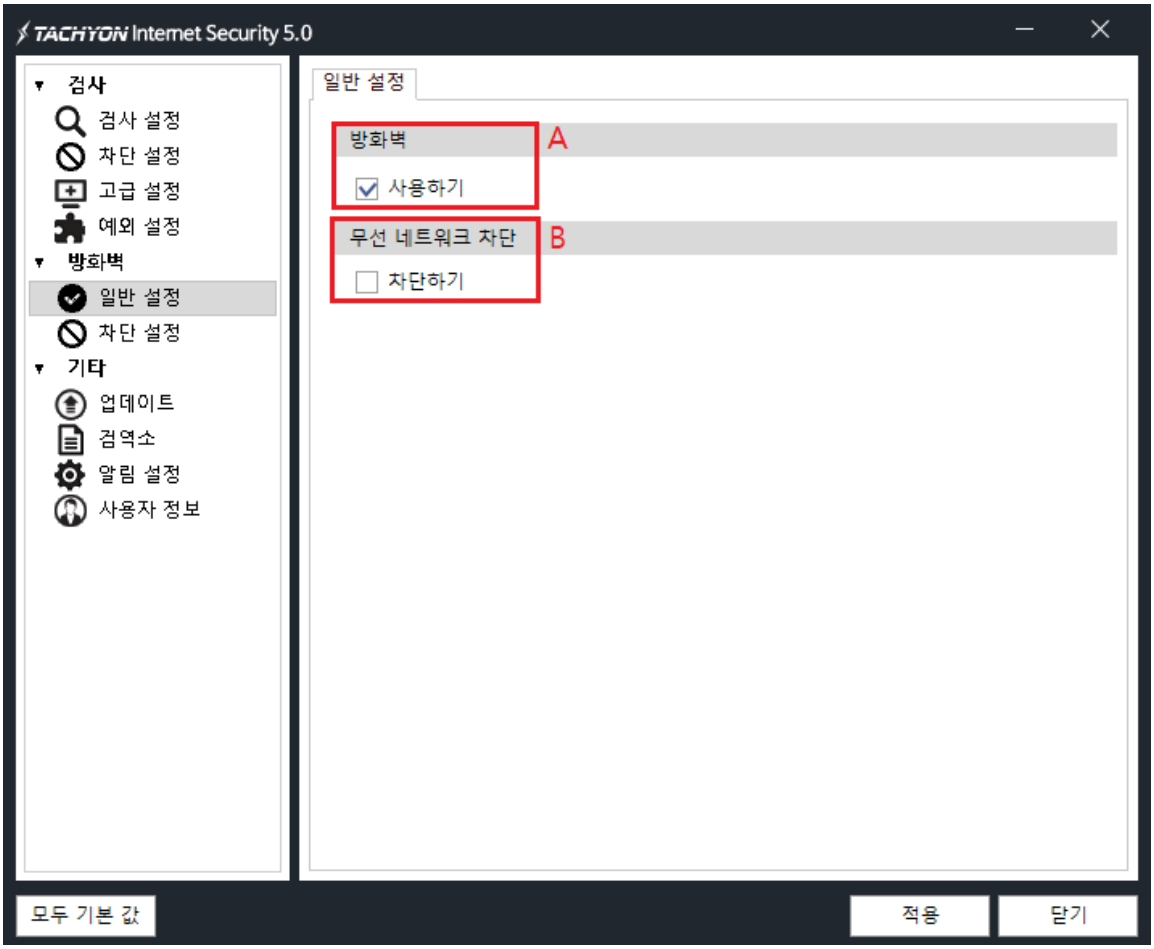
10. 방화벽 설정

방화벽 일반 설정에서는 각 항목을 선택하여 해당 기능을 ON/OFF할 수 있습니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 방화벽 > 일반 설정 > 일반 설정 탭을 선택합니다.



A 영역

- 방화벽
  - 사용하기 : 방화벽 기능에서 사용하기를 체크하면 방화벽 기능 사용이 가능합니다.

B 영역

- 무선 네트워크 차단
  - 차단하기 : 무선 네트워크와의 모든 통신을 차단합니다. IEEE 에서 인가한 802.1* 표준을 사용하는 무선 통신은 모두 차단합니다.

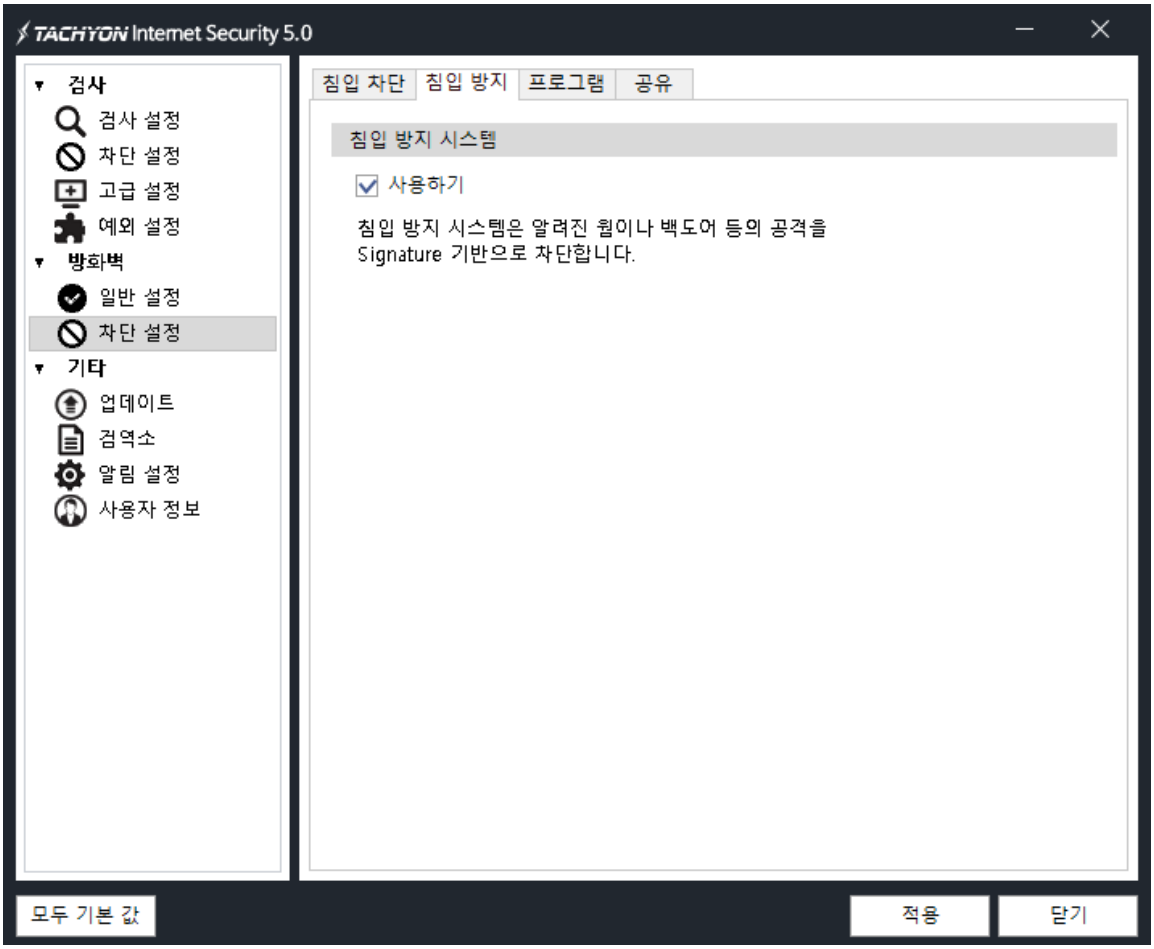
11. 침입 차단

침입 차단에서는 접근 차단 모드에 대한 세부 설정이 가능합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 검사 > 검사 설정 > 일반 설정 탭을 선택합니다.



A 영역

■ 침입 차단 시스템

- 사용하기 : 사용하기 체크 여부에 따라 접근 차단 모드 사용 유무를 설정 할 수 있습니다. 사용하기 체크가 되어 있어야 하위 메뉴가 활성화 됩니다.

B 영역

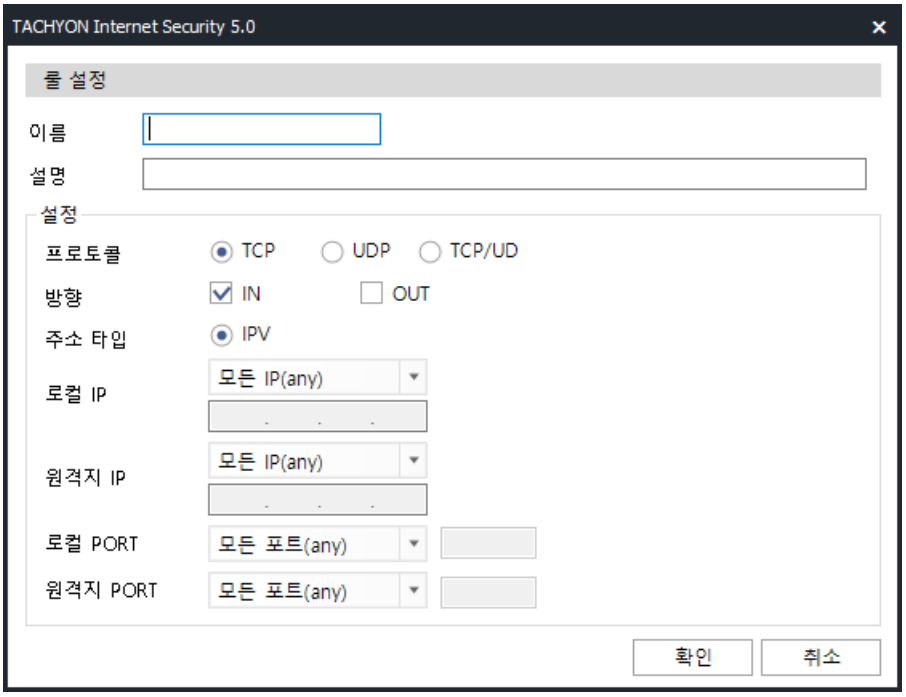
■ 접근 차단 모드

PC 에서 모든 포트를 사용할 수 있도록 우선 허용하고 사용자의 접근 차단 정책에 의해 시스템을 보호하는 차단(Black List) 목록 방식의 방화벽입니다.

침입 차단에서 접근 차단에 대한 세부 설정이 가능하며 프로트콜, ICMP 옵션, ARP 옵션, IP, PORT 에 대한 룰 설정이 가능합니다.

접근 차단 모드는 사용자가 지정한 정책만을 차단합니다.

- 사용 : 등록된 접근 차단 모드 리스트의 사용 유무를 체크합니다.
- 이름 : 접근 차단 모드 리스트를 구분하기 위한 이름을 표시합니다.
- 동작 : 등록된 접근 차단 모드 리스트의 동작을 표시합니다.
- 방향 : 등록된 접근 차단 모드 리스트의 방향을 표시합니다.(IN, OUT, IN/OUT)
- 프로토콜 : 등록된 접근 차단 모드 리스트의 프로트콜을 표시합니다.(TCP, UDP, TCP/UDP)
- 설명 : 접근 차단 모드 리스트의 설명 입니다.
- 추가 : 접근 차단 룰을 설정할 수 있습니다.



- 수정 : 수정할 접근 차단 모드 리스트를 선택 후, [수정]을 클릭하면 선택된 접근 차단 모드 리스트를 수정할 수 있습니다.

- 삭제 : 삭제할 접근 차단 모드 리스트를 선택한 후, [삭제]를 클릭하면 선택된 접근 차단 모드 리스트를 삭제할 수 있습니다.

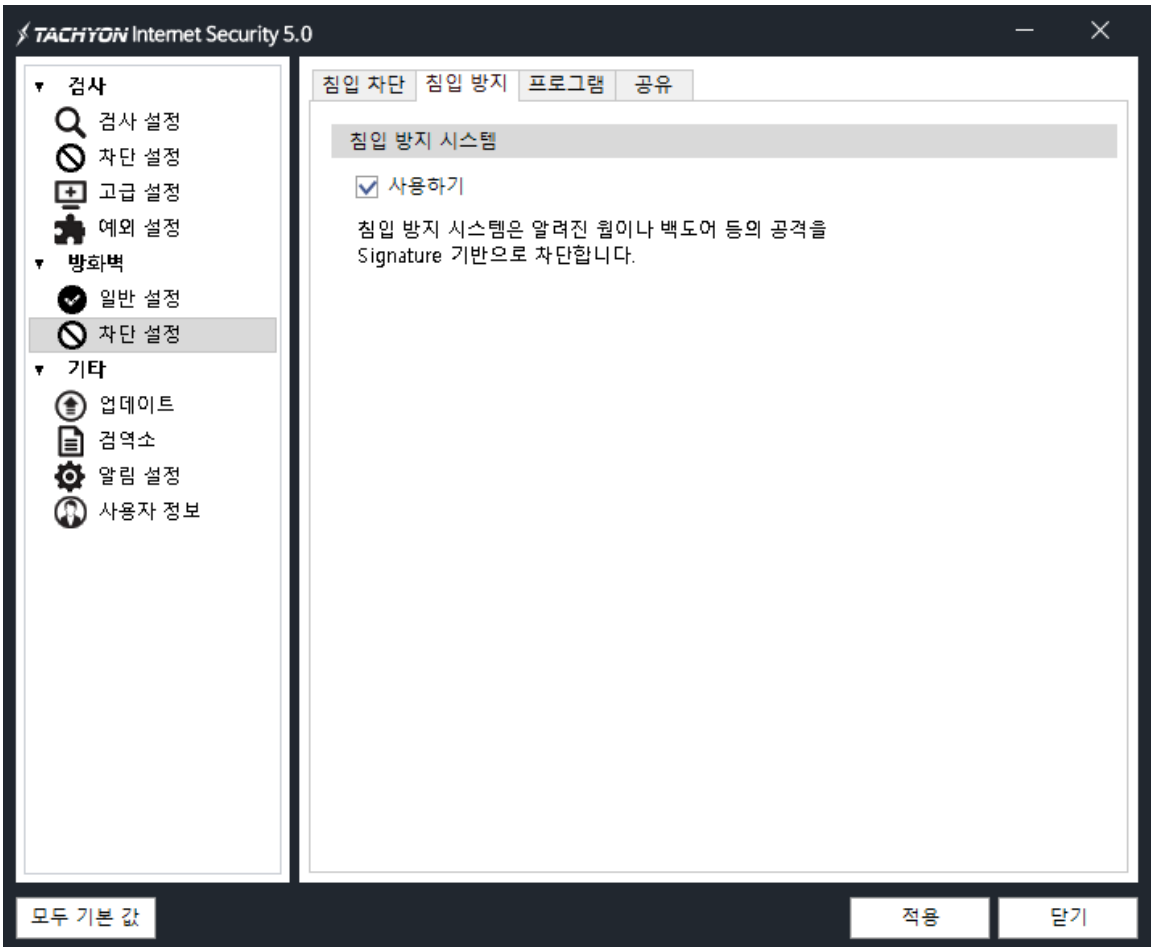
12. 침입 방지

침입 방지에서는 알려진 웜이나 백도어 등의 공격을 Signature 기반으로 차단하는 침입방지 시스템 설정이 가능합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 방화벽 > 차단 설정 > 침입 방지 탭을 선택합니다.



침입 방지 시스템

■ 침입 방지 시스템

- 사용하기 : 침입 방지 시스템은 알려진 웜이나 백도어 등의 공격을 Signature 기반으로 차단합니다. 사용하기 체크 여부에 따라 침입 방지 시스템 사용 유무를 설정할 수 있습니다.

13. 프로그램

프로그램에서는 인증된 프로그램만 실행되도록 설정이 가능합니다.

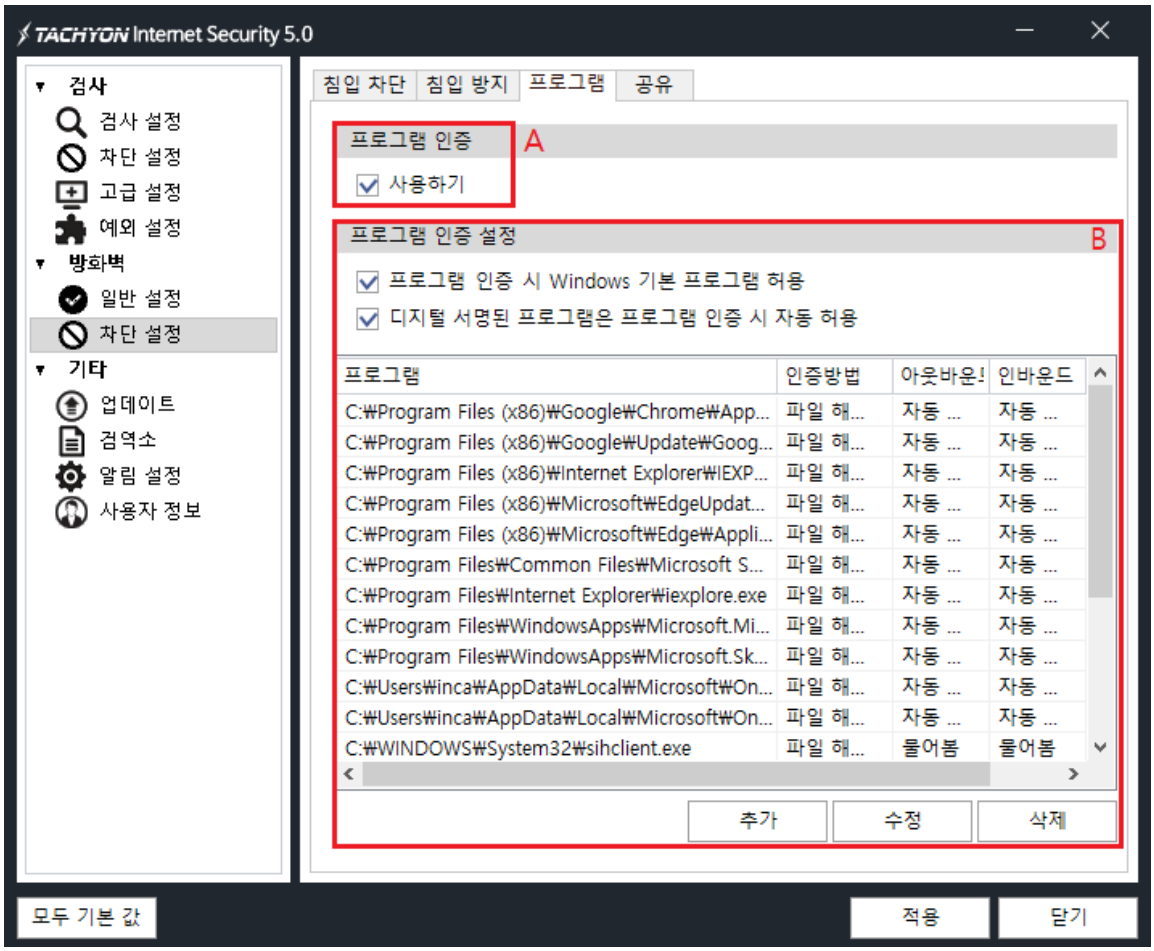
프로그램 인증은 프로그램 네트워크 접근 시도를 인증하여 동작합니다.

네트워크 자원을 사용하는 프로그램을 인증하는 이유는 사용자 몰래 설치되어 시스템 정보를 유출하는 행위를 차단하고, 공공 자원인 네트워크를 보호하기 위해서입니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 방화벽 > 차단 설정 > 프로그램 탭을 선택합니다.



A 영역

■ 프로그램 인증

- 사용하기 : 프로그램 인증 사용 유무를 설정할 수 있습니다. 사용하기 체크가 되어 있어야 하위 메뉴가 활성화 됩니다.

B 영역

■ 프로그램 인증 설정

- 프로그램 인증 시 Windows 기본 프로그램 허용

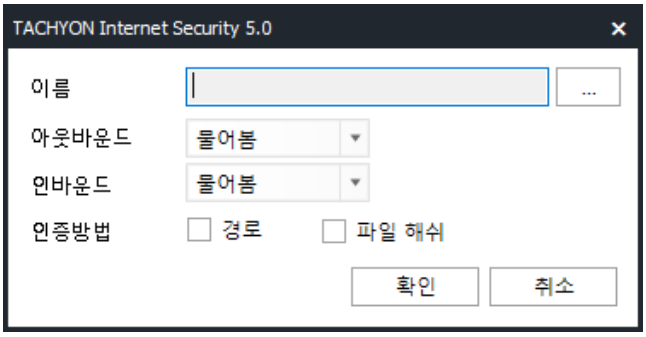
  프로그램 인증 사용 시, 윈도우 기본 프로그램인 경우 자동 허용되어 실행될 때에 프로그램 인증 알림 창을 표시하지 않습니다.

  윈도우 기본 프로그램이 차단될 경우에는 시스템 장애가 발생할 수 있으므로 기본적으로 허용해 주시기 바랍니다.

- 디지털 서명된 프로그램은 프로그램 인증 시 자동 허용

  프로그램 인증 사용시, 디지털 서명이 된 프로그램이 실행될 때에 프로그램 인증 알림 창을 표시하지 않습니다.

- 프로그램 : 프로그램 인증을 한 프로그램의 리스트를 표시합니다.
- 인증방법 : 프로그램의 인증방법을 표시합니다.(파일 해쉬/경로/파일 해쉬+경로)
- 아웃바운드 : 아웃바운드 설정을 선택할 수 있습니다.(물어봄/허용/차단)
- 인바운드 : 인바운드 설정을 선택할 수 있습니다.(물어봄/허용/차단)
- 파일 해쉬 : 프로그램 리스트의 파일의 해쉬를 표시합니다.
- 추가 : [추가]를 클릭하면 수동으로 프로그램 등록이 가능합니다.



- 수정 : 수정할 프로그램 인증 리스트를 선택 후, [수정]을 클릭하면 선택된 프로그램 인증 리스트를 수정할 수 있습니다.

- 삭제 : 삭제할 프로그램 인증 리스트를 선택 후, [삭제]를 클릭하면 선택된 프로그램 인증 리스트를 삭제할 수 있습니다.

14. 공유

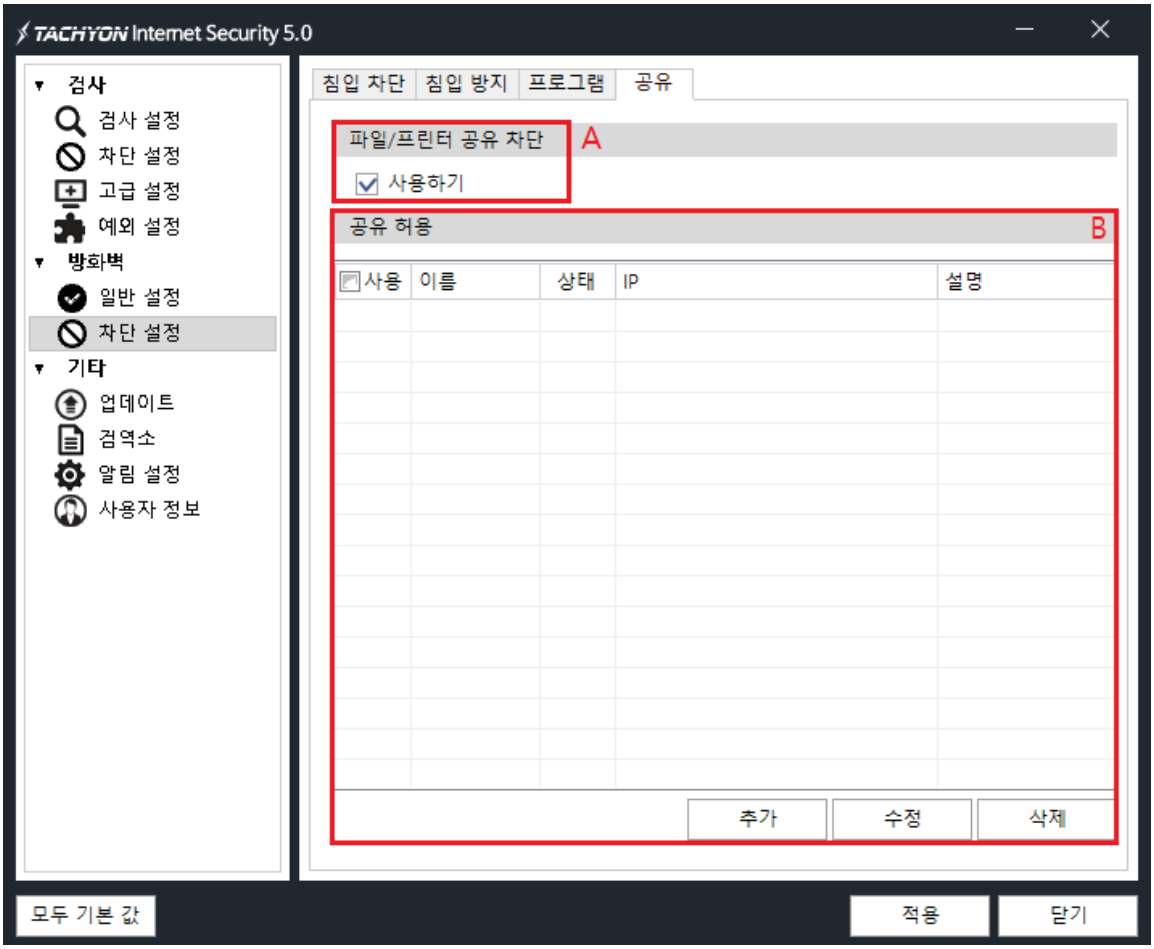
공유에서는 등록이 된 IP로 공유가 가능하도록 설정이 가능합니다.

공유 허용은 사용자가 사용하는 PC의 공유 자원을 사용자가 지정한 컴퓨터만이 이용할 수 있도록 허용하는 기능입니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 방화벽 > 차단 설정 > 공유 탭을 선택합니다.



A 영역

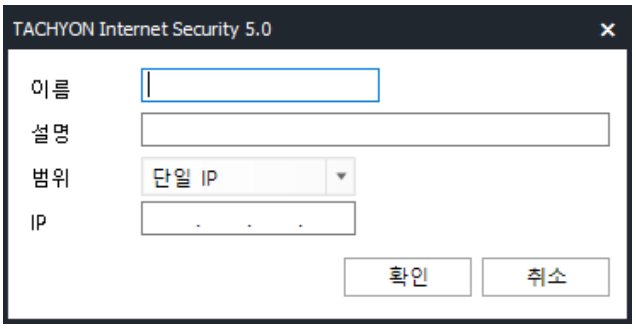
■ 파일/프린터 공유 차단

- 사용하기 : 파일/프린터 공유 차단 사용 유무를 설정할 수 있습니다. 사용하기 체크가 되어 있어야 하위 메뉴가 활성화 됩니다.

B 영역

■ 공유 허용

- 사용 : 등록된 공유 허용 리스트의 사용 여부를 체크할 수 있습니다.
- 이름 : 공유 허용 리스트를 구분할 수 있는 이름을 입력합니다.
- 상태 : 허용 유무를 표시합니다.
- IP : 공유 허용할 IP 값을 입력합니다. 단일 IP 와 IP 범위로 입력할 수 있습니다.
- 설명 : 공유 허용 리스트를 구분할 수 있는 설명을 입력합니다.
- 추가 : [추가]를 클릭하면 공유를 허용할 IP 를 등록할 수 있는 설정 창이 나타납니다.



- 수정 : 수정할 공유 허용 리스트를 선택 후, [수정]을 클릭하면 선택된 공유 허용 리스트를 수정할 수 있습니다.
- 삭제 : 삭제할 공유 허용 리스트를 선택 후, [삭제]를 클릭하면 공유 허용 리스트를 삭제할 수 있습니다.

15. 업데이트

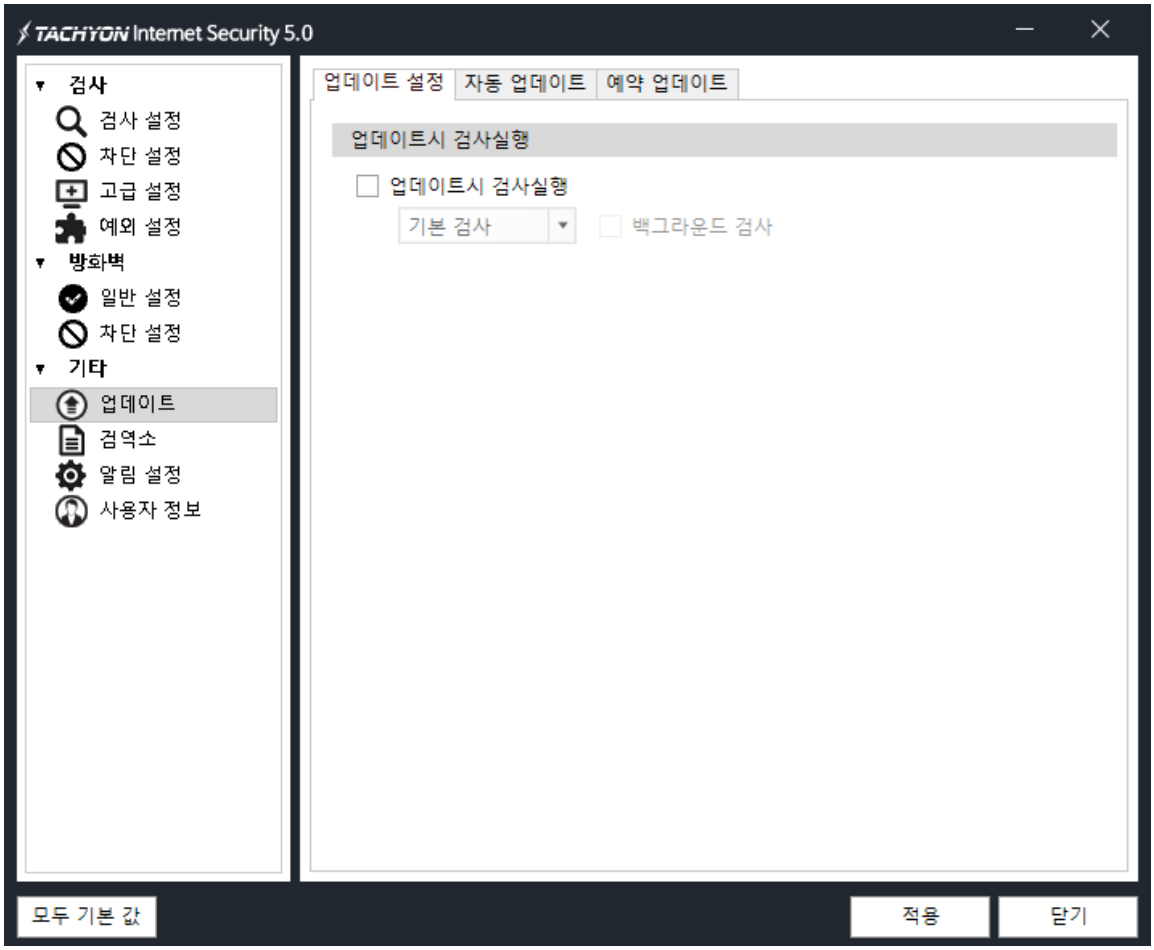
TACHYON Internet Security 5.0 이 최신 보안 위협으로부터 사용자 PC 를 지키려면 관련 정보 파일을 항상 최신 버전으로 업데이트 해야 합니다.

업데이트 설정에서는 좀 더 편리하게 업데이트 하기 위해 자동 업데이트를 선택하거나, 사용자가 선택한 시간에 업데이트를 할 수 있도록 예약 업데이트 옵션을 설정할 수 있습니다.

업데이트 설정 실행

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 기타 > 업데이트 > 업데이트 설정 탭을 선택합니다.



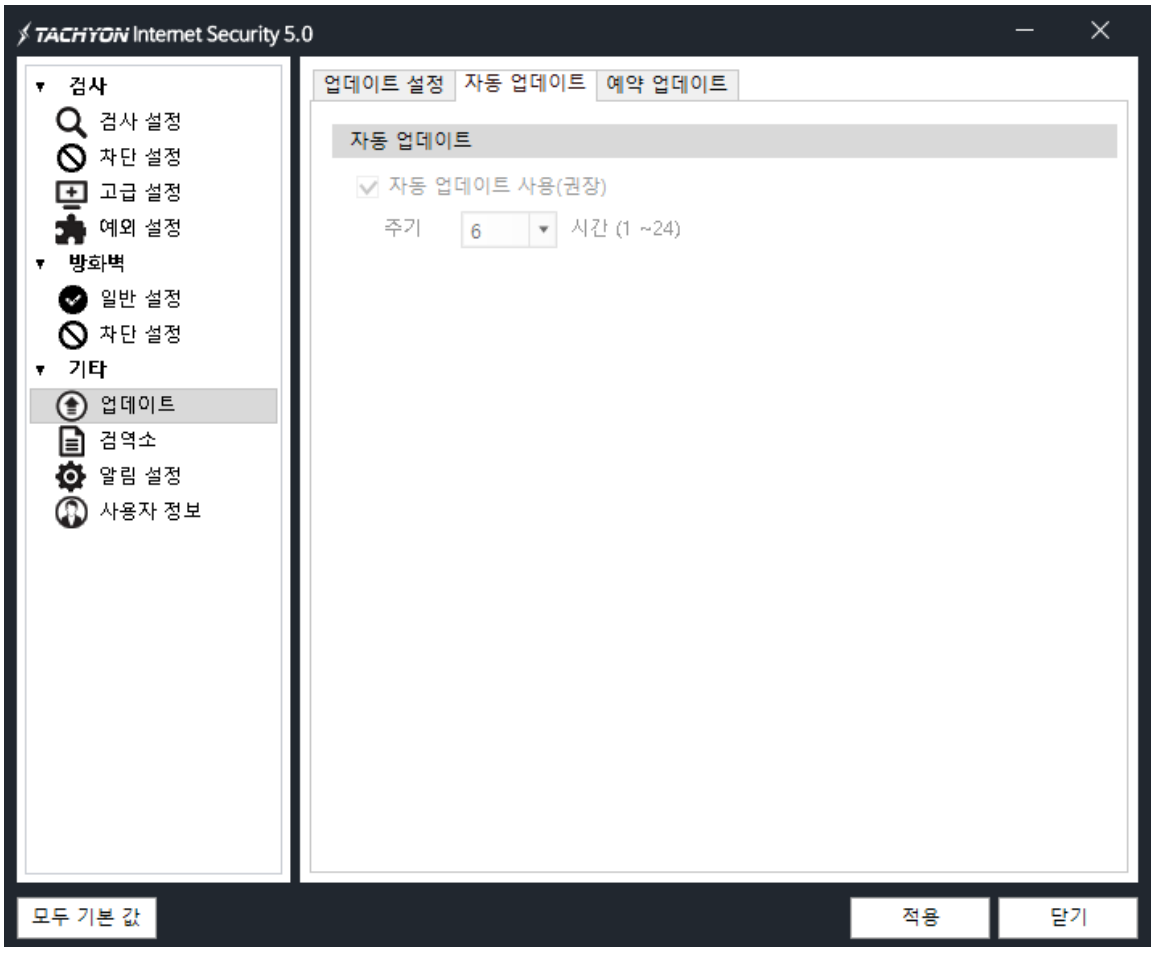
업데이트시 검사 실행

업데이트 설정에서 업데이트시 검사 실행을 체크하면 업데이트 설정 기능이 활성화 되며, 기본 검사 및 정밀 검사, 백그라운드 검사 등을 선택이 가능합니다.

자동 업데이트 실행

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 기타 > 업데이트 > 자동 업데이트 설정 탭을 선택합니다.



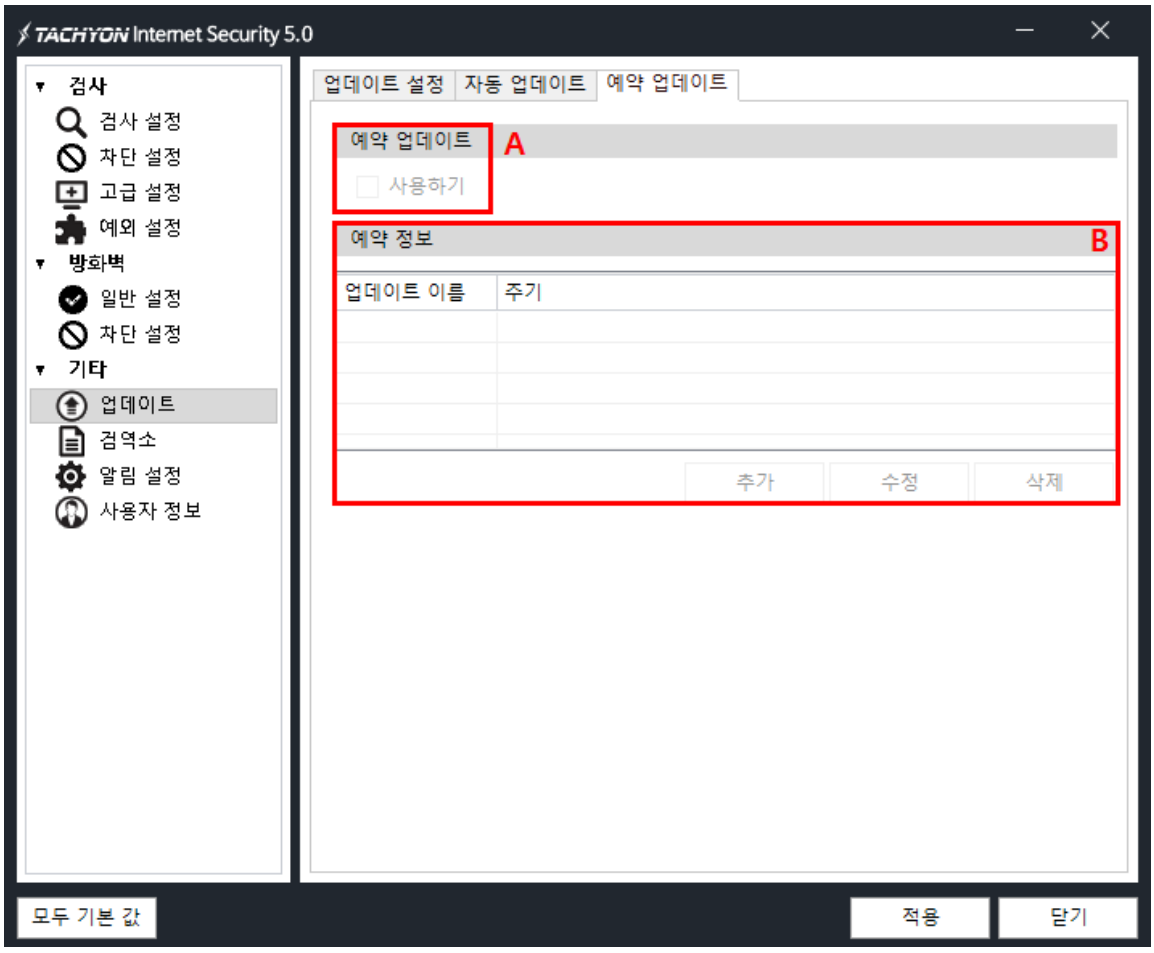
자동 업데이트

자동 업데이트 사용(권장)을 사용하게 되면 PC 부팅 이후 설정한 자동 업데이트 주기에 따라 업데이트 여부를 확인하여 업데이트를 진행합니다. 업데이트 주기는 1~24 시간까지 설정 가능합니다.

예약 업데이트 실행

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 기타 > 업데이트 > 예약 업데이트 탭을 선택합니다.



A 영역

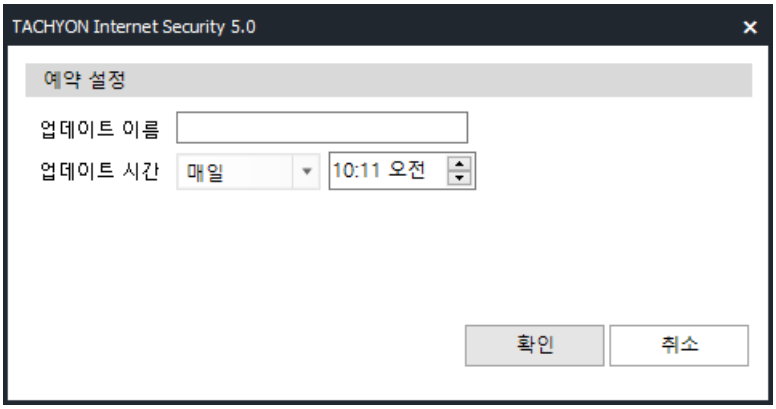
■ 예약 업데이트

- 사용하기 : 예약 업데이트 사용하기를 선택하면 사용자가 설정한 예약 시간 마다 엔진 파일이 최신 버전인지 확인하여 업데이트 할 수 있습니다.

B 영역

■ 예약 업데이트 예약 정보

- 업데이트 이름 : 예약 업데이트를 구분할 수 있는 이름을 표시합니다.
- 주기 : 예약 업데이트가 실행될 주기입니다.(매일/매주/매월/한번만)
- 추가 : 예약 업데이트 스케줄을 추가합니다.



- 수정 : 등록된 예약 업데이트 스케줄을 수정합니다.
- 삭제 : 등록된 예약 업데이트 스케줄을 삭제합니다..

16. 검역소

검역소는 악성코드에 감염된 파일을 치료하거나 삭제하기 전에 감염된 원본 파일을 백업하여 보관하는 기능입니다.

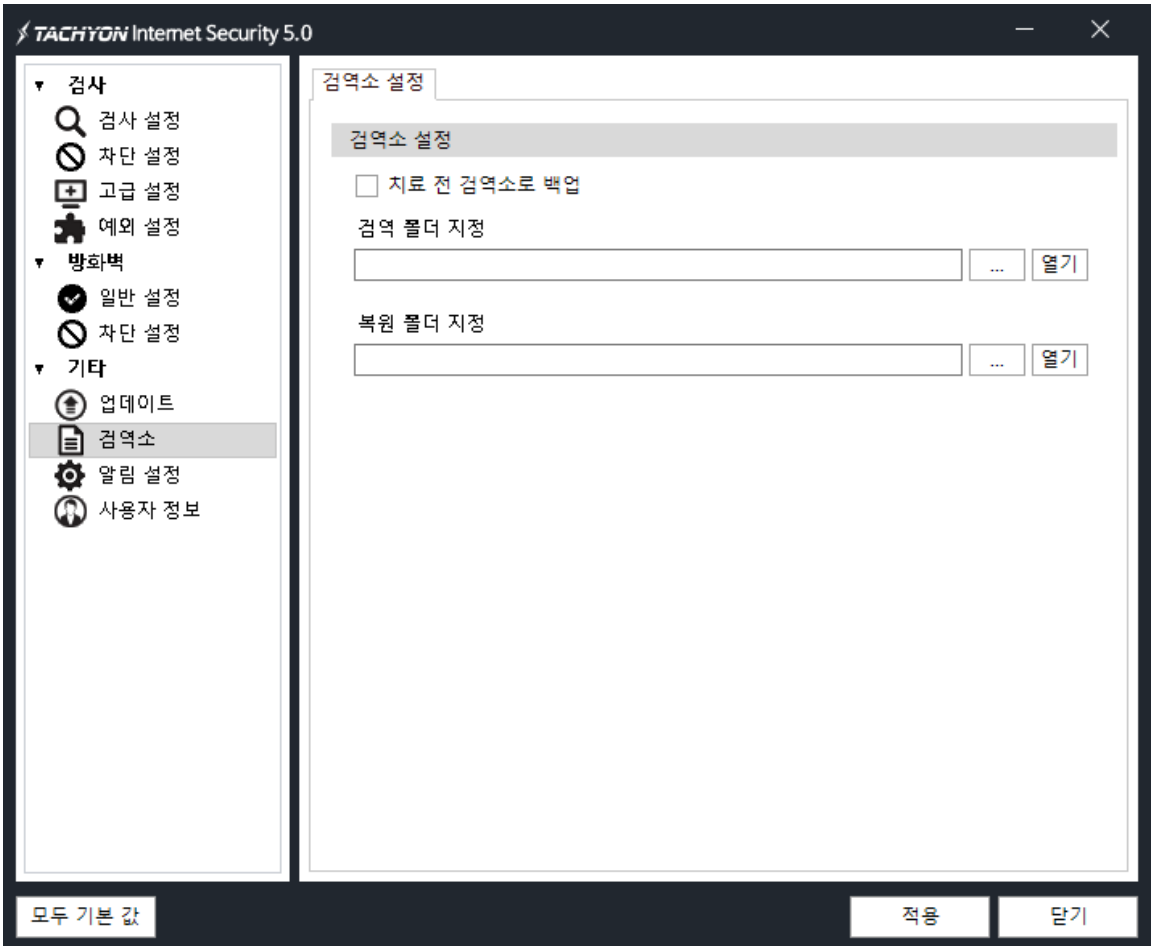
검역소 기능이 설정된 후에 백업 파일이 삭제되지 않고 계속 생성되면 디스크 공간 부족으로 인하여 시스템 및 프로그램 실행에 오류가 발생할 수 있습니다.

따라서 검역소 관리가 필요합니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 기타 > 검역소 > 검역소 설정 탭을 선택합니다.



검역소 설정

- 치료 전 검역소로 백업 : 악성코드 치료 전 감염된 파일을 검역소 폴더로 복사합니다.
- 검역 폴더 지정

  검역소 폴더를 지정합니다. [열기]를 통하여 지정된 폴더로 바로 이동이 가능합니다.

  검역 폴더의 기본값은 다음과 같습니다.

  32bit : C:\Program Files\Common Files\TACHYON\T5\Quarantine

  64bit : C:\Program Files (x86)\Common Files\TACHYON\T5\Quarantine
- 복원 폴더 지정

  검역소 파일 복원 시 파일이 저장될 폴더를 지정합니다. [열기]를 통하여 지정된 폴더로 바로 이동이 가능합니다.

  복원 폴더의 기본값은 다음과 같습니다.

  32bit : C:\Program Files\Common Files\TACHYON\T5\Quarantine\Restore

  64bit : C:\Program Files (x86)\Common Files\TACHYON\T5\Quarantine\Restore

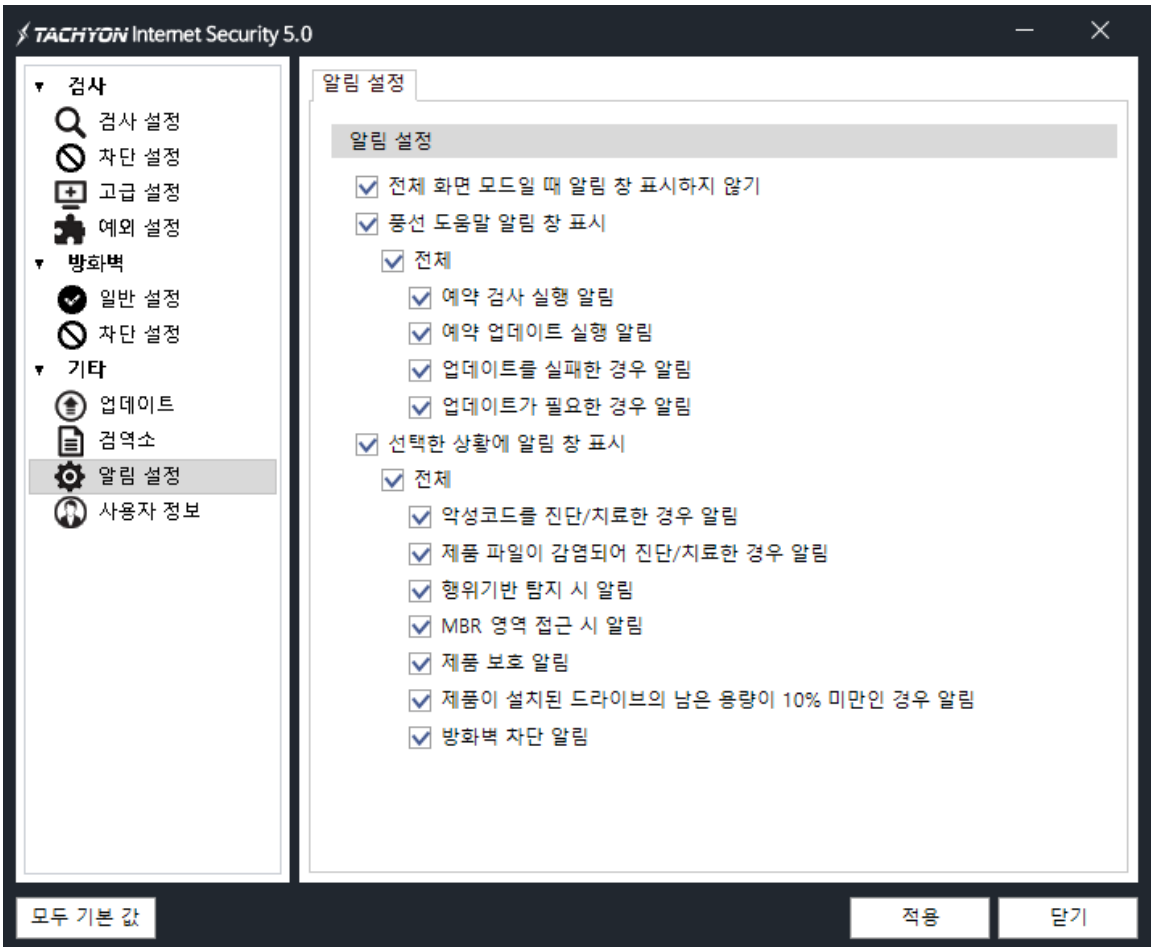
17. 알림 설정

알림 설정에서는 TACHYON Internet Security 5.0 제품을 사용할 때, 각 기능이나 상황에 대해 알림을 설정할 수 있습니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 기타 > 알림 설정 > 알림 설정 탭을 선택합니다.



알림 설정

■ 전체 화면 모드일 때, 알림 창 표시하지 않기

파워포인트에서 프레젠테이션을 하거나 워드 같은 프로그램에서 전체 화면 모드를 사용할 때, 알림 창 발생을 금지합니다.

■ 풍선 도움말 알림 창 표시

사용자에게 일회성 정보를 알려줄 때, 나타나는 풍선 도움말의 표시 여부를 선택합니다.

- 예약 검사 실행 알림 : 예약된 검사가 시작될 때 풍선 도움말 알림 창으로 예약 검사의 시작을 표시합니다.
- 예약 업데이트 실행 알림 : 예약된 업데이트가 시작될 때 풍선 도움말 알림 창으로 예약 업데이트의 시작을 표시합니다.
- 업데이트를 실패한 경우 알림 : 업데이트가 실패하였을 때 풍선 도움말 알림 창으로 업데이트가 실패하였음을 표시합니다.
- 업데이트가 필요한 경우 알림 : 구 버전을 사용하는 사용자에게 업데이트가 필요할 때 풍선 도움말로 업데이트 알림을 표시합니다.

■ 선텍한 상황에 알림 창 효시

알림 설정에서 사용자가 선택한 상황이 발생했을 때 작업 표시줄에 알림 창을 보여줍니다.

- 악성코드를 진단/치료한 경우 알림 : 악성코드를 진단 또는 치료된 경우 알림 창을 표시합니다.
- 제품 파일이 감염되어 진단/치료한 경우 알림 : 제품 파일이 감염되어 악성코드가 진단 또는 치료된 경우 알림 창을 표시합니다.
- 행위기반 탐지 시 알림 : 행위 기반의 악성코드가 탐지될 경우 알림 창을 표시합니다.

- MBR 영역 접근 시 알림 : 다른 프로그램이 MBR 영역에 접근할 경우 알림 창을 표시합니다.
- 제품 보호 알림 : 바이러스 또는 외부/내부의 위협으로 제품 자체에 허락 받지 않은 접근이 탐지될 경우 알림 창을 표시합니다.
- 제품이 설치된 드라이브의 남은 용량이 10% 미만인 경우 알림 : HDD 의 남은 용량이 전체 용량의 10% 미만인 경우 알림 창을 표시합니다.
- 방화벽 차단 알림 : 방화벽 차단 알림 창을 표시합니다.

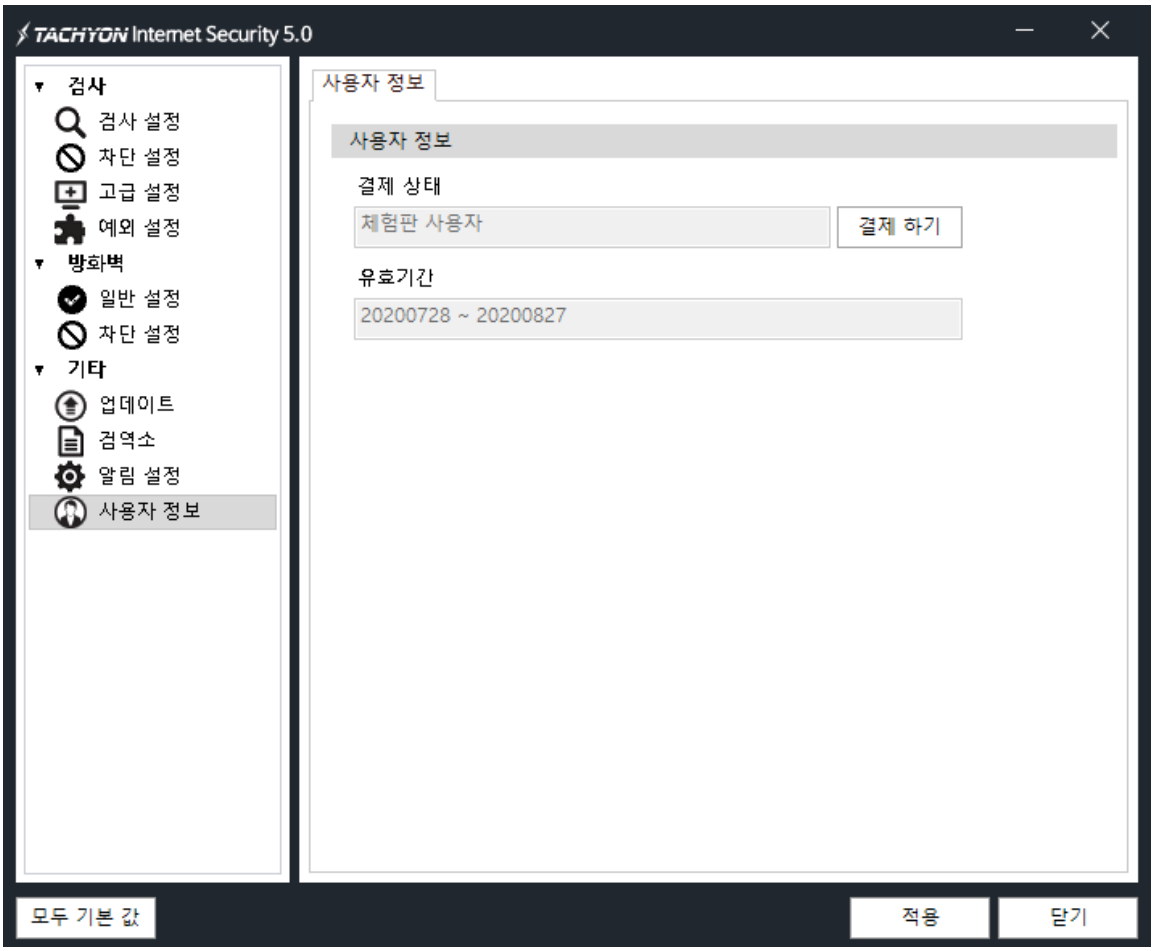
18. 사용자 정보

현재 설치된 TACHYON Internet Security 5.0 제품 사용자의 결제 상태, 사용자 ID, 유효기간을 확인할 수 있습니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후 “환경설정”을 클릭합니다.

2. 기타 > 사용자 정보 > 사용자 정보 탭을 선택합니다.



사용자 정보

- 결제 상태 : 현재 설치된 TACHYON Internet Security 5.0 제품 사용자의 결제 상태를 표시합니다.(체험판 사용자/유료 사용자)
- 결제 하기 : 회원 로그인 페이지로 이동합니다.
- 사용자 ID : 현재 설치된 TACHYON Internet Security 5.0 제품을 사용 중인 유료 사용자의 ID 를 표시합니다.
- 유효기간 : 유료 사용자의 경우 결제 후 사용할 수 있는 유효기간을 표시합니다.

14장

회원 가입

1. 회원 가입

1. 회원 가입

TACHYON Internet Security 5.0 의 모든 기능을 사용하기 위해서는 회원 가입이 필요합니다.

회원 가입을 하려면 다음 절차에 따라서 가입하시면 됩니다.

실행 방법

- 홈페이지에서 실행

  https://my.tachyonlab.com 페이지로 이동하여 가입 하시면 됩니다.

- TACHYON Internet Security 5.0 프로그램에서 실행

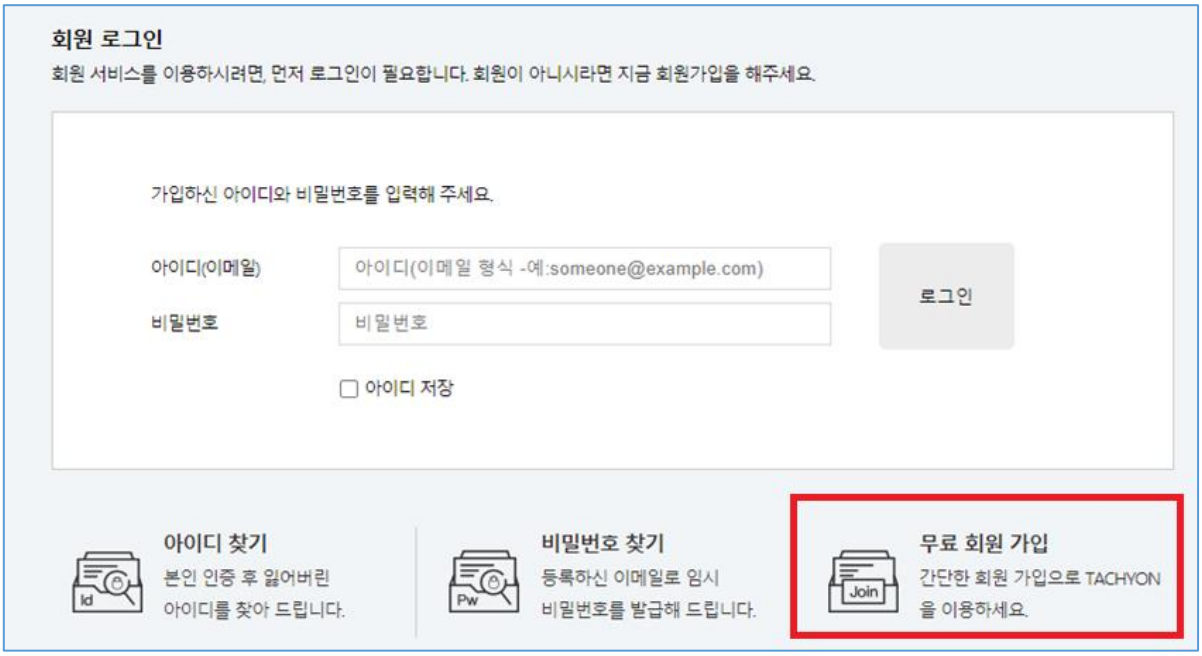
  1. TACHYON Internet Security 5.0 실행 후, '환경설정'을 클릭합니다.

  2. 기타 > 사용자 정보 > 사용자 정보 탭을 선택합니다.

  3. 결제 하기를 클릭합니다.

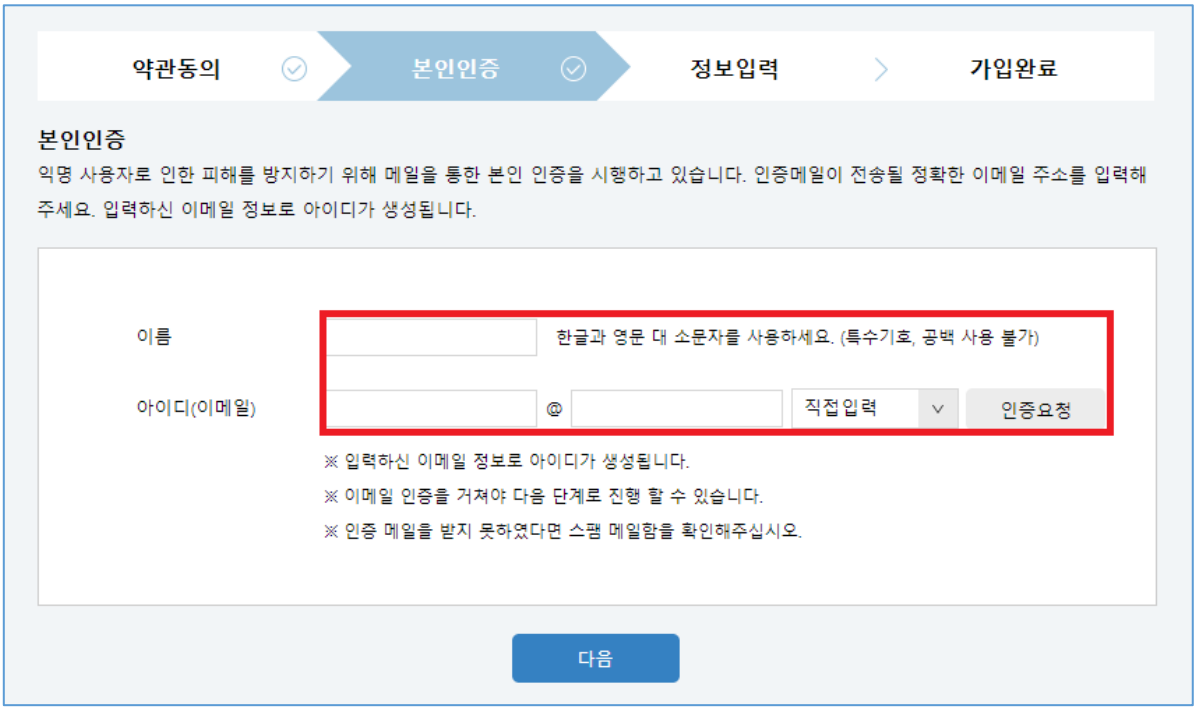
회원 가입

1. 로그인 페이지에서 [무료 회원 가입]을 클릭합니다.

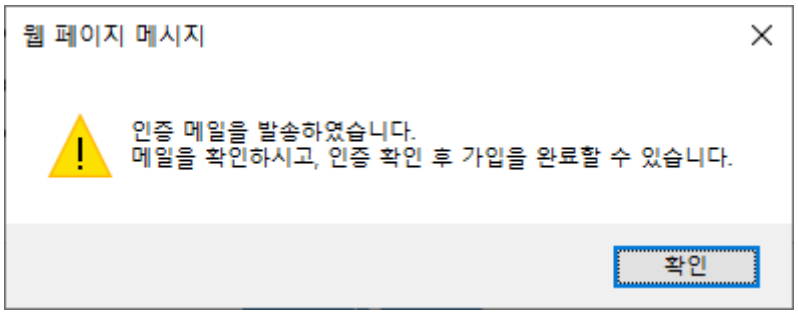


2. 약관 동의에 체크 후, [다음]을 클릭합니다.

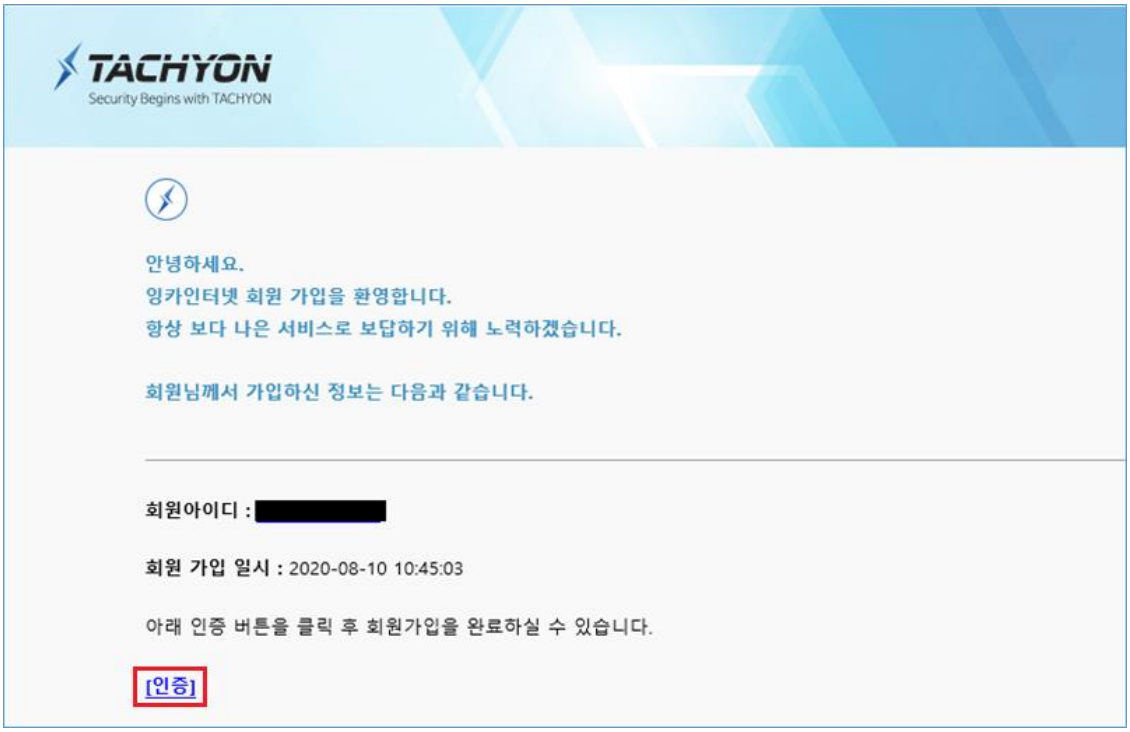
3. 이름과 이메일 주소를 입력 후, [인증요청]을 클릭합니다.



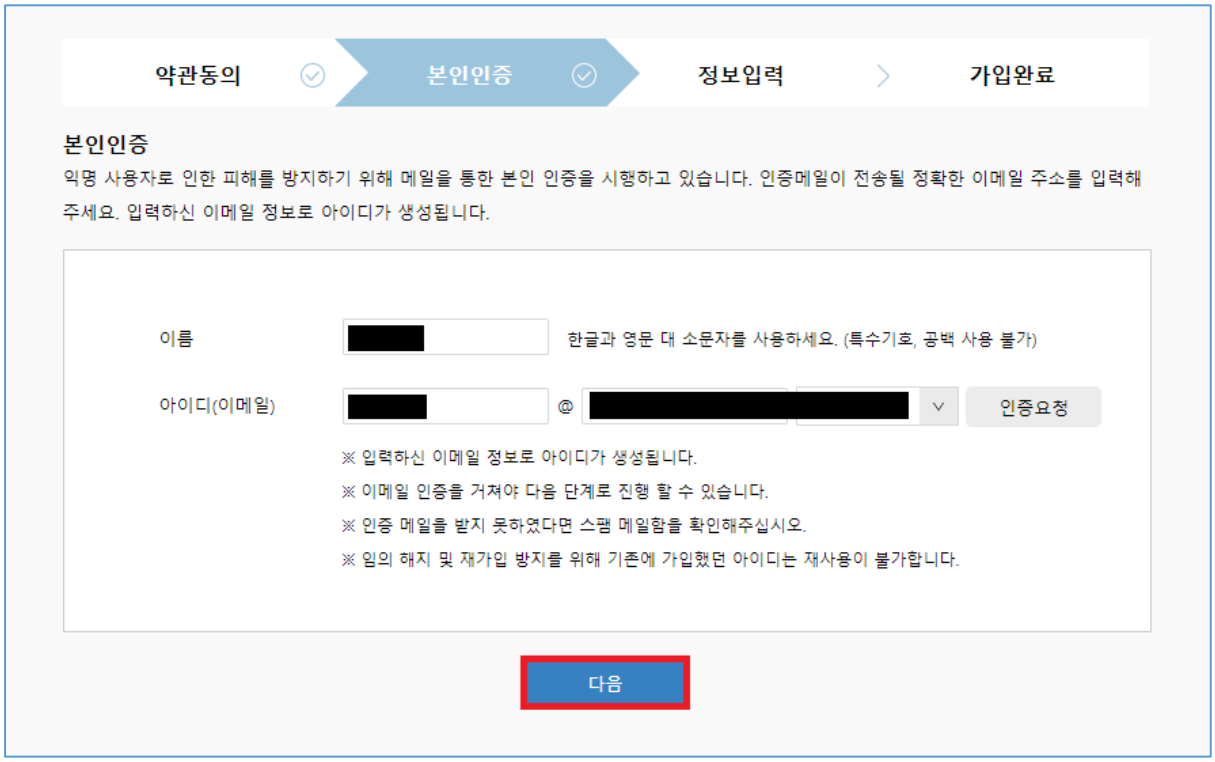
4. 입력한 이메일 주소로 인증 메일을 발송하였다는 메시지가 나타나면 [확인]을 클릭합니다.



5. 입력한 이메일을 통해 회원가입 이메일 인증 메일을 받으셨다면, [인증]을 클릭하여 회원 가입을 계속 진행할 수 있습니다.



6. 이메일 인증까지 마쳤다면 하단에 [다음]을 클릭합니다.



7. 사용자 개인 정보를 입력한 후, [다음]을 클릭합니다.

8. [확인]을 클릭하여 회원 가입을 완료합니다.

15장

로그인

1. 로그인

1. 로그인

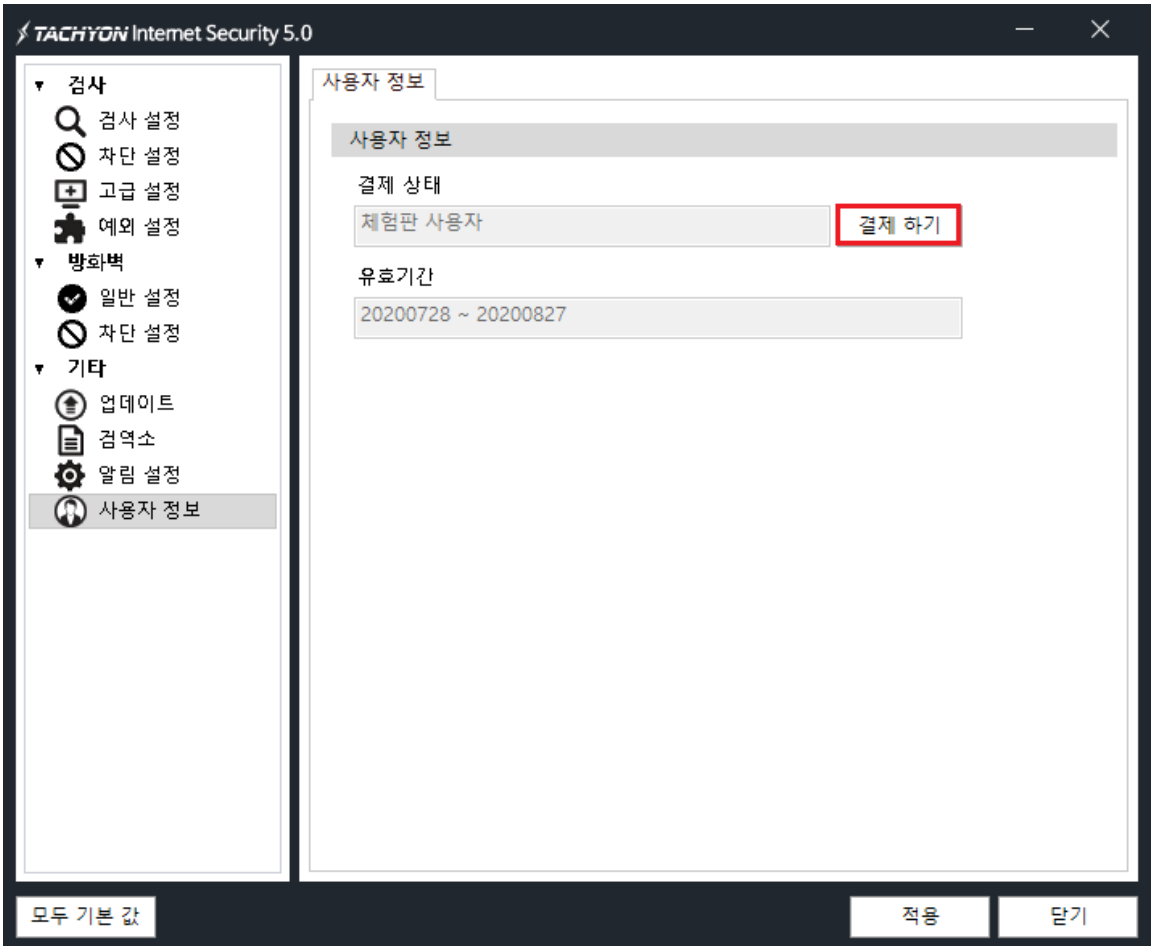
TACHYON Internet Security 5.0 유료 회원으로 전환 후, 로그인하면 모든 기능들을 사용할 수 있습니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후, '환경설정'을 클릭합니다.

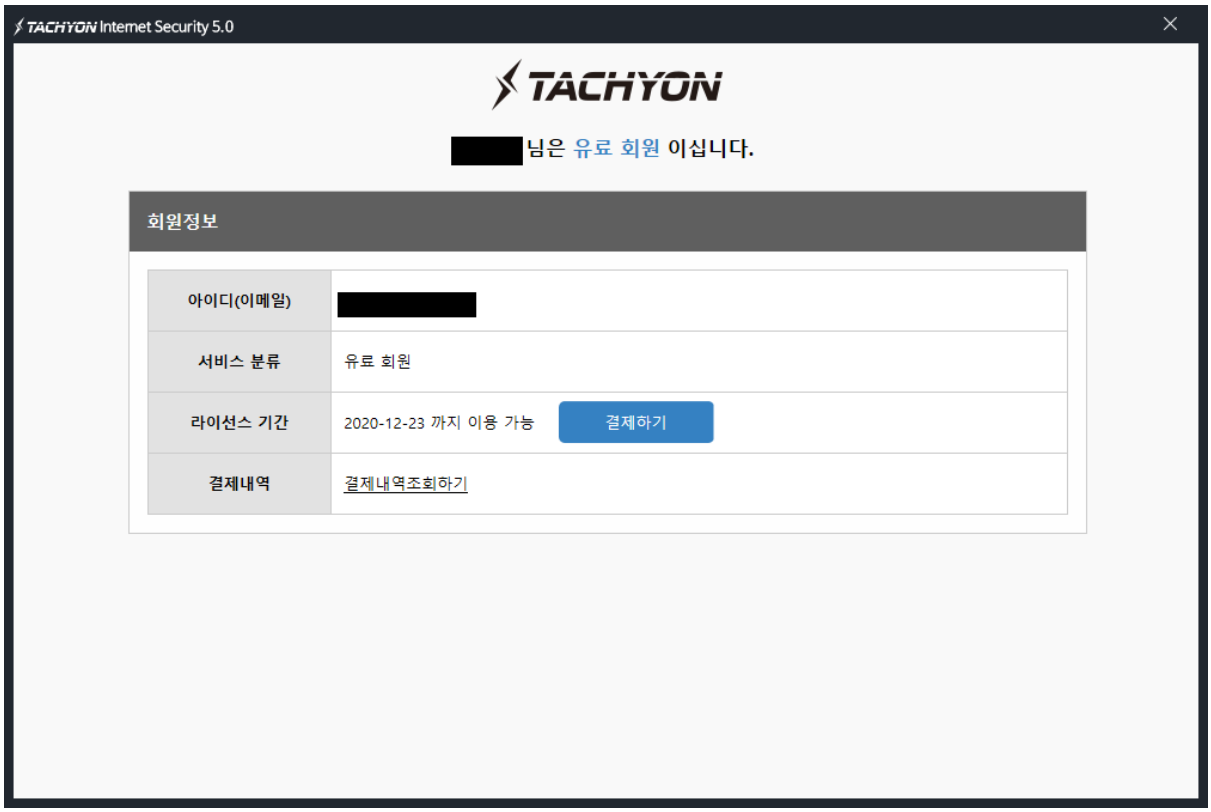
2. 기타 > 사용자 정보 > 사용자 정보 탭을 선택합니다.

3. 결제 하기를 클릭합니다.

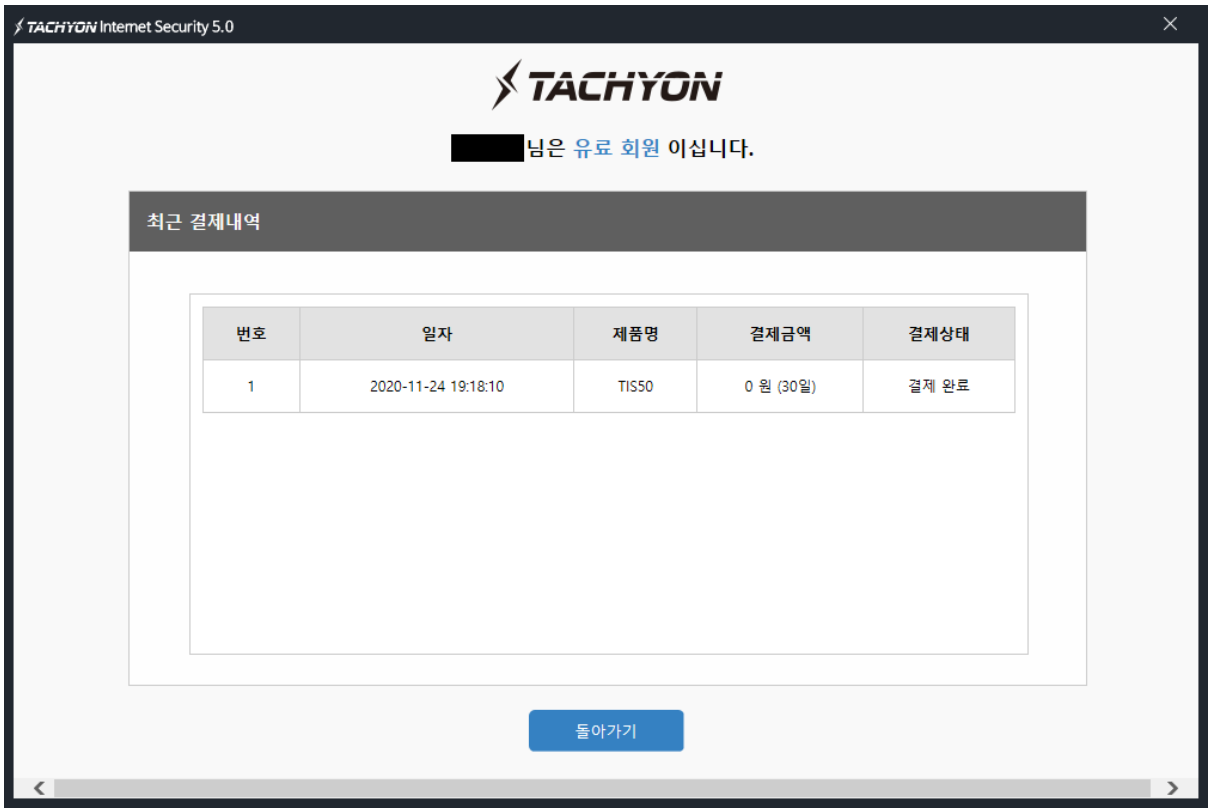


1. 결제 하기를 클릭하면 로그인 화면으로 이동합니다.

2. 회원 로그인을 하면 유료 회원으로 전환된 정보를 확인할 수 있습니다.



3. 결제내역을 조회하려면 [결제내역조회하기]를 클릭하면 됩니다.



16장

결제하기

1. 결제하기

1. 결제 하기

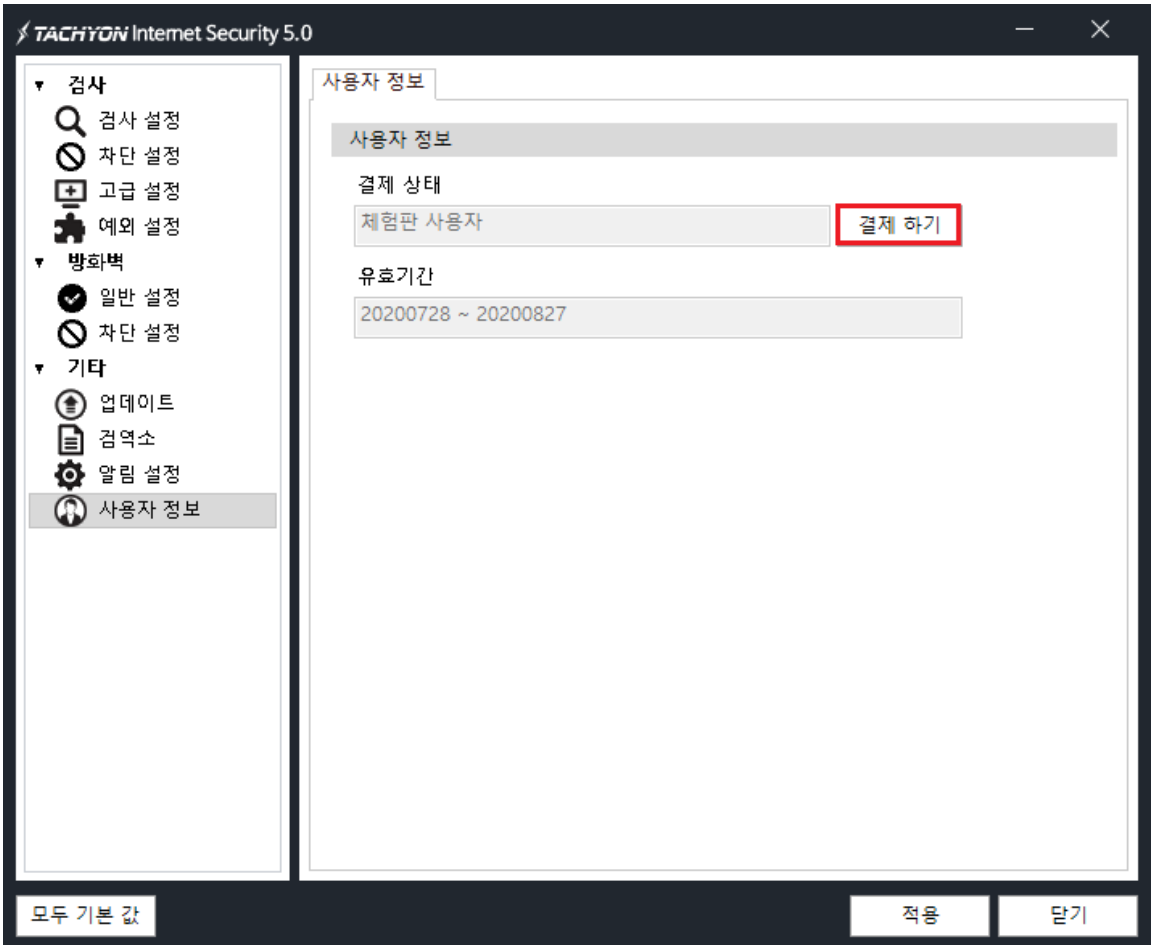
TACHYON Internet Security 5.0 체험판 기간이 만료되면 일부 기능들을 사용할 수 없습니다. 제험판 기간이 만료되기 전 유료 회원으로 전환하면 계속해서 모든 기능들을 사용할 수 있습니다.

실행 방법

1. TACHYON Internet Security 5.0 실행 후, '환경설정'을 클릭합니다.

2. 기타 > 사용자 정보 > 사용자 정보 탭을 선택합니다.

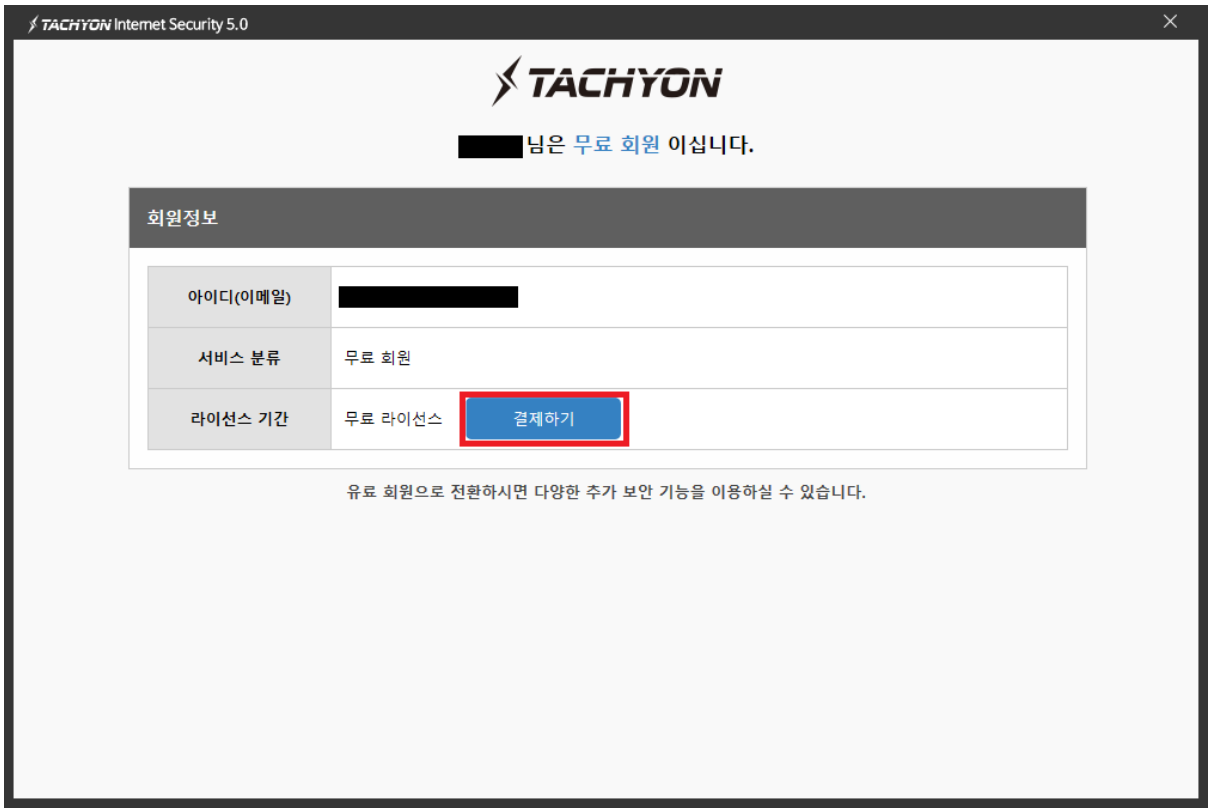
3. 결제 하기를 클릭합니다.



결제 하기

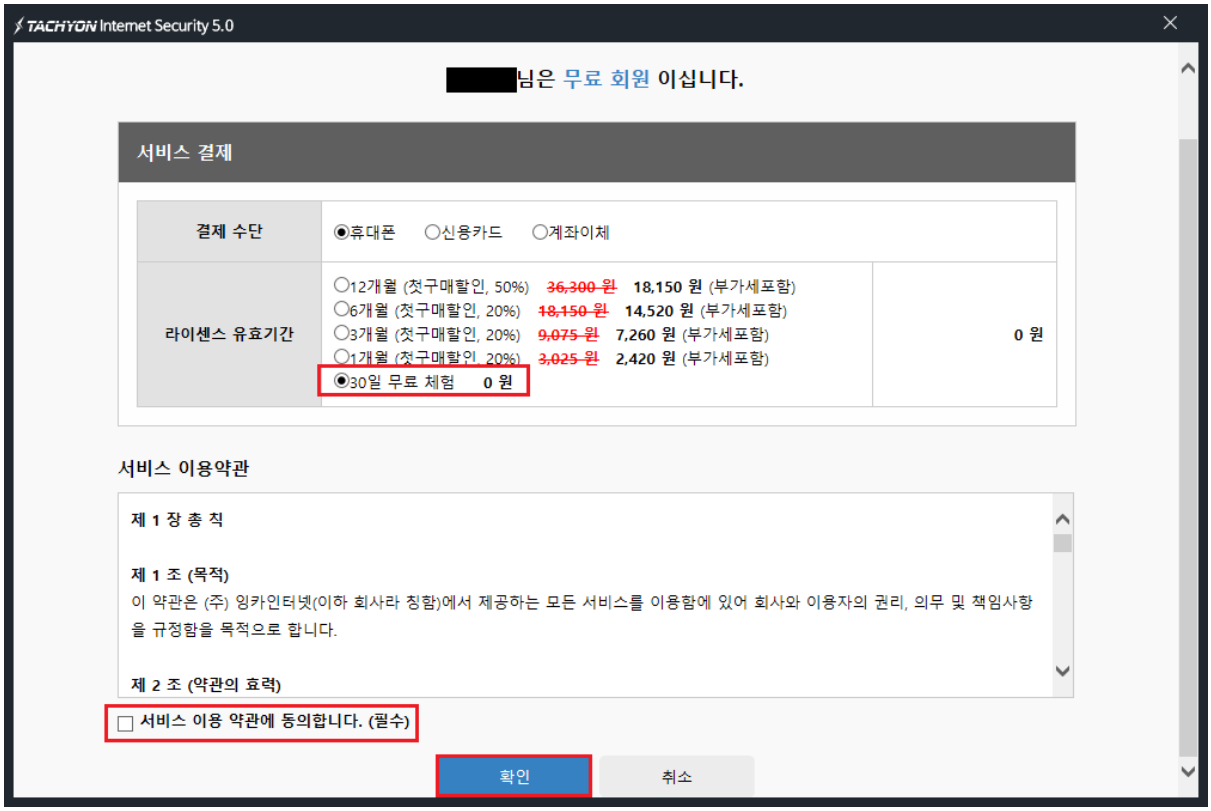
4. [결제 하기]를 클릭하면 로그인 화면으로 이동합니다.

5. 회원 로그인 후 [결제 하기]를 클릭합니다.

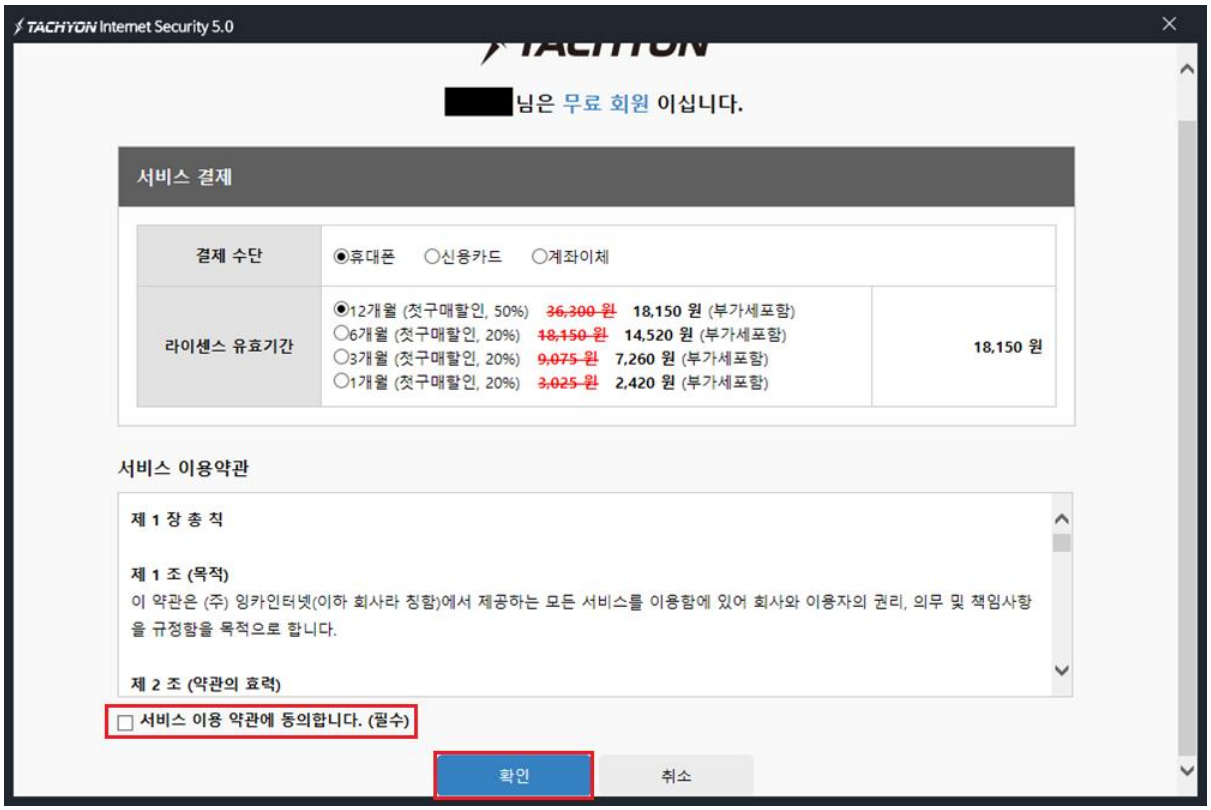


6. 원하는 결제 수단을 선택하여 결제를 진행합니다.

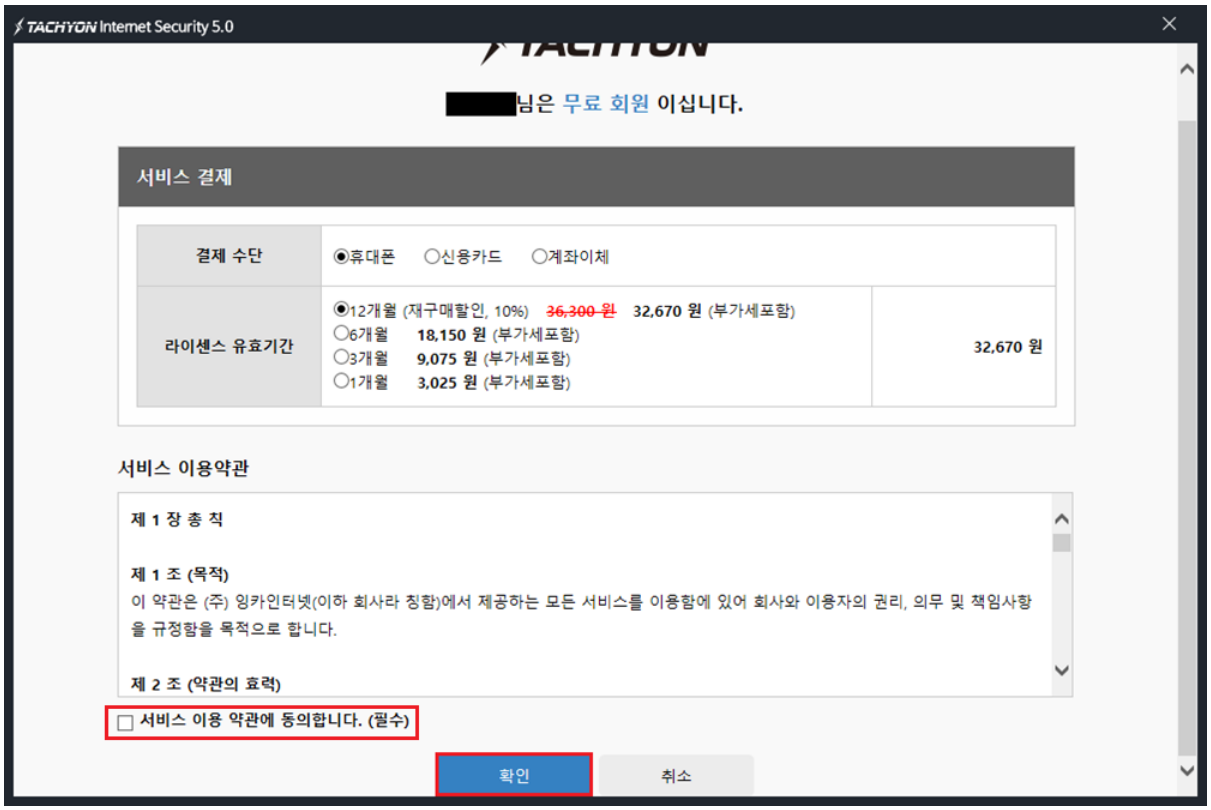
30 일 무료 체험 상품을 이용하여 TACHYON Internet Security 5.0 제품을 30 일간 무료로 이용하실 수 있습니다.



30 일 무료 체험 종료 후, 첫 구매시에는 할인된 가격이 적용됩니다.



이후, 재구매시에는 아래와 같은 가격이 적용됩니다.



※ 회원이 아니라면 회원 가입부터 진행해주세요.

TACHYON

서울특별시 강서구 마곡중앙 14 로 53 (주) 잉카인터넷

www.tachyonlab.com

대표번호 02-6411-8000 | 고객지원 1566-0808 | Fax 02-6411-8080