RansomDefense v1.0

사용자가이드

목 차

일러두기

이 사용자 가이드에서는 RansomDefense V1.0의 구성 및 기능별 상세 설명이 소개되어 있습니다.

표기규칙

표기 규칙	내용
'일반 폰트'	기능 또는 설정 이름, 메시지 내용 입니다.(예: '리스트 관리')
[버튼]	버튼의 이름입니다.(예: [확인])
<>	창의 이름 입니다.(예: <알림>)
>	메뉴 실행 순서 입니다.(예: '백업'>'초기화')
※Note	참고할 사항입니다.
※주의	반드시 주의해야 할 사항입니다.

기술지원 안내

㈜위젯누리에서는 다양한 형태의 고객지원을 제공하고 있습니다.

제품 사용 중 문제 및 불편사항이 발생할 시에는 본사 기술지원부로 문의하시기 바랍니다.

연락처

㈜위젯누리 http://www.widgetnuri.com

Tel. 02-2043-8292

1. 제품 소개

1.1 RansomDefense 소개

RansomDefense 솔루션은 평판기반, 시그니처, 행위 기반, 상황인식 기반의 방식 보다 빠른 대응과 예상하지 못하는 악성 행위를 차단하기 위하여 소프트웨어 인증방식을 도입, 사용자가 알 수 없거나 불필요한 소프트웨어가 중요 자료에 접근 하는 것을 원천적으로 제어 할 수 있는 강력한 보안 솔루션 입니다.

1.2 주요기능

■ 소프트웨어 인증

정보가 없는 새로운 소프트웨어를 발견했을 경우 해당 소프트웨어의 중요 자료의 접근을 제한 합니다. 사용자의 소프트웨어 평판 정보와 분석을 통해 소프트웨어 인증 기능을 사용자에게 실시간으로 업데이트 하여 정보가 없는 소프트웨어에 대해 빠르게 대처 할 수 있습니다.

■ 행위 감시

소프트웨어 인증을 통과한 소프트웨어라도 부적절한 접근, 무분별한 변조 행위 등을 실행 할 경우 해당 소프트웨어의 접근을 실시간으로 차단하여 강력한 보안 기능을 발휘 합니다.

■ 자동백업

사용자의 중요 파일에 소프트웨어가 접근하는 경우 자동으로 백업하여 사용자가 인지하지 못한 순간에도 대비 할 수 있도록 합니다.
또한 사용자의 어떤 자료들이 접근되고 있는지를 분석할 수 있습니다.

■ 폴더 보호

사용자가 중요 자료라고 판단되는 폴더들을 직접 선택하여 자동 백업 기능과 같이 수동적인 대처가 아닌 사용자의 능동적인 대처로 중요 자료의 보안을 강화 할 수 있습니다.

2. Agent 설치하기

2.1 시스템 사양

RansomDefense Agent를 설치하기 위해서는 다음의 시스템 사양 이상의 하드웨어 사양과 소프트웨어 환경을 만족해야 합니다. 시스템 사양을 확인하신 후 설치하여 주시기 바랍니다.

※ 주의

다음의 시스템 사양 이상의 하드웨어와 소프트웨어 환경을 만족하지 않는 경우 프로그램이 정상 작동하지 않을 수 있으며, 위젯누리는 이로 인한 책임을 지지 않습니다.

■ 하드웨어 최소 사양

- CPU: Intel i3 3.1GHz 이상
- Memory: 4GB 이상
- HDD: 100GB 이상의 여유공간

■ 지원 언어

- 한국어

■ 지원 OS

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

※ Note

지원 가능한 운영 체제는 32bit와 64bit를 모두 지원합니다.

2.2 설치하기

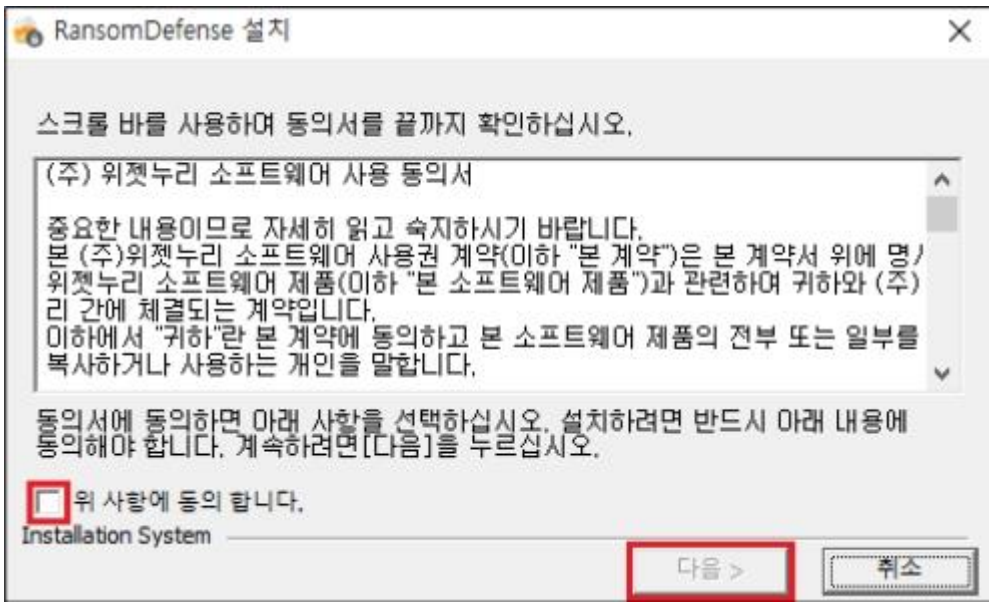
RansomDefense Agent 설치 파일을 실행하면, PC에 Agent를 설치 할 수 있습니다.

※ Note

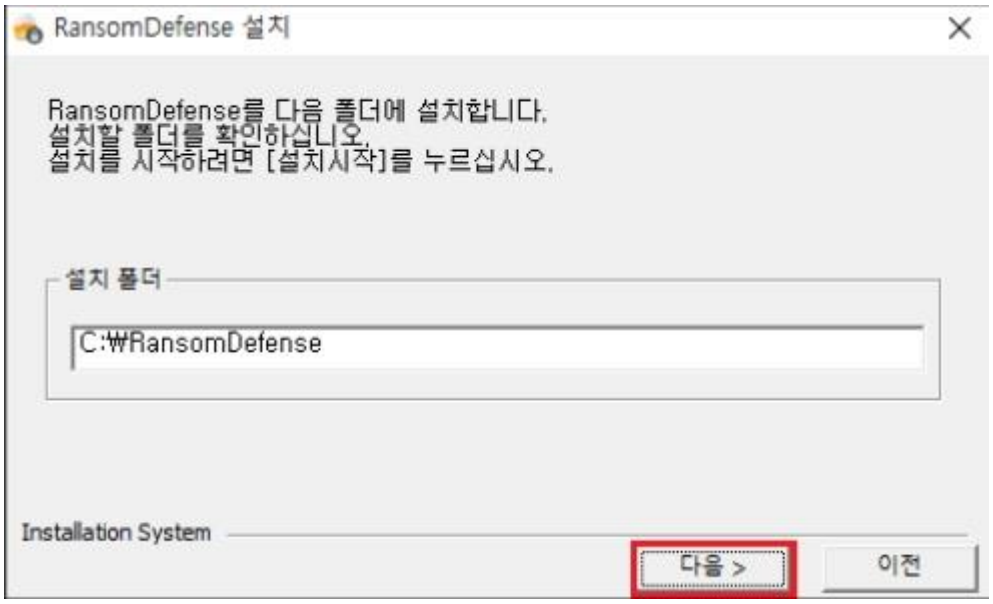
설치하기 전에 이전에 실행중인 작업을 미리 저장 및 종료하여 주시기 바랍니다

1. RansomDefense

2. <동의서> 확인 후 '위 사항에 동의합니다.'를 체크 한 뒤 [다음]을 누릅니다.

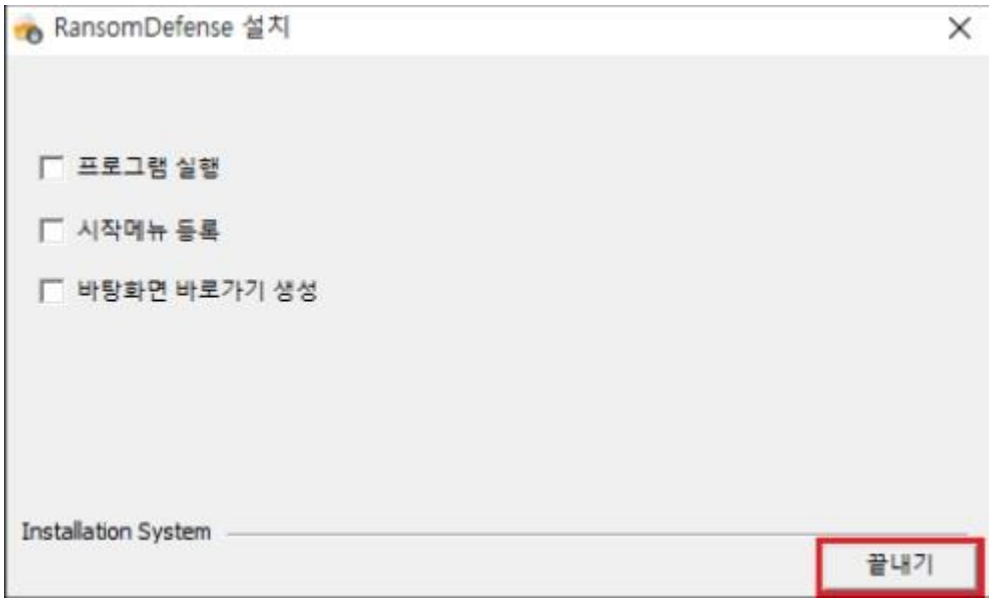


3. 설치 경로를 확인 후 [다음]을 누릅니다.



4. [설치시작]을 누릅니다.

5. 설치가 완료되면 원하는 선택사항을 선택 후 [끝내기]를 누릅니다.



◆ 프로그램 실행 : 설치 종료 후 RansomDefense를 실행 합니다.

◆ 시작메뉴 등록 : 시작메뉴에 RansomDefense 메뉴를 등록합니다.

◆ 바탕화면 바로가기 생성 : 바탕화면에 RansomDefense 바로가기를 생성합니다.

2.3 제거하기

RansomDefense를 PC에서 제거하기 위한 방법은 다음과 같습니다.

◆ 제어판에서 제거하기

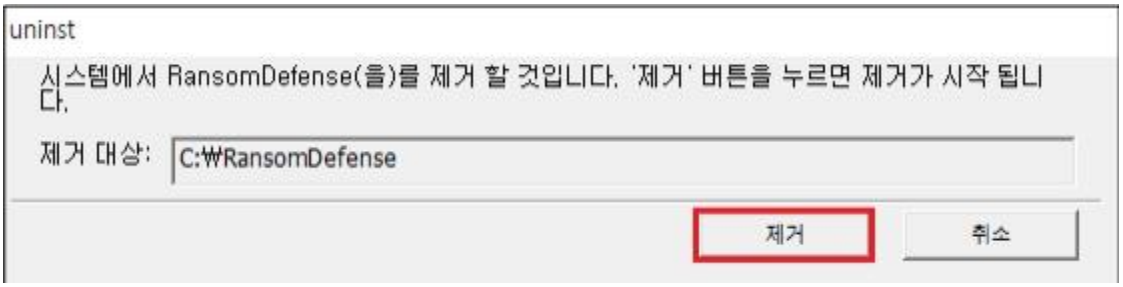
1. '제어판' > '프로그램' > '프로그램 및 기능'을 선택합니다.
2. 프로그램 제거 또는 변경 목록의 'RansomDefense'에서 마우스 오른쪽 클릭 '제거/변경'을 선택 또는 더블 클릭 합니다.

◆ 시작 메뉴에서 제거하기

1. '시작' > '모든 프로그램' > 'RansomDefense'를 선택합니다.
2. 'RansomDefense 제거'를 선택합니다.

◆ 제거 진행 과정

1. <uninst>에서 [제거]를 누릅니다.



2. 제거가 끝날 때까지 잠시 기다려 주십시오.
3. 파일 삭제 과정을 마친 후 [닫기]를 누르면 제거가 완료 됩니다.

3. RansomDefense Agent 둘러보기

3.1 Agent 실행 방법

RansomDefense Agent가 종료되어 있을 때 실행하는 방법 입니다.

※ Note

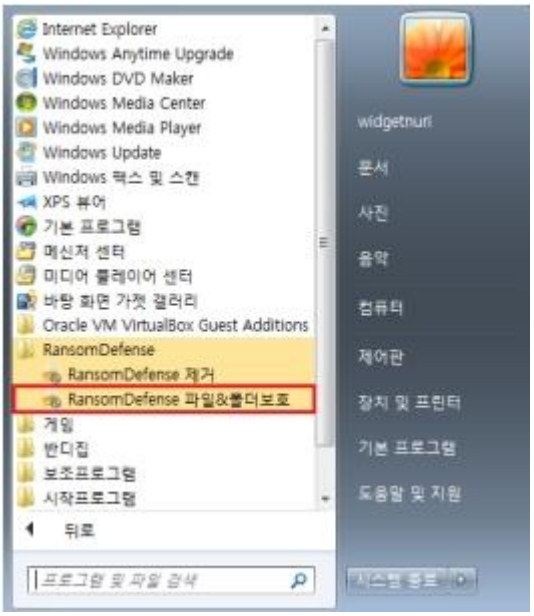
PC부팅시 자동으로 Agent가 실행 됩니다.

◆ 바탕화면에서 실행하기

'바탕화면'의 'RansomDefense 바로가기' 아이콘[ ]을 더블 클릭합니다.

◆ 시작 메뉴에서 실행하기

1. '시작' > '모든 프로그램' > 'RansomDefense' > 'RansomDefense 파일&보호폴더'를 선택합니다.



2. 관리자권한으로 실행합니다.

3.2 RansomDefense Agent 트레이 아이콘

◆ Agent 메인 화면 팝업

작업 표시줄의 RansomDefense 트레이 아이콘을 더블 클릭하여 실행중인 RansomDefense의 메인 화면을 띄울 수 있습니다.

4. RansomDefense Agent HOME 화면

4.1 화면 구성

RansomDefense를 메인 화면으로써 현재 프로그램의 기능 설정 상태 및 업데이트, 라이선스 등 정보를 표시 합니다.

◆ HOME 화면

A 영역

: 환경 설정 실행 합니다. 환경설정에서 랜섬디펜스의 각종 옵션 및 정보를 확인 할 수 있습니다.

: 화면을 최소화 합니다.

: 현재 화면을 닫습니다.

B 영역

Anti-Ransomware
RansomDefense

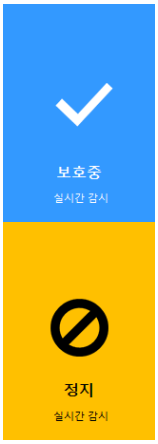
: 메인 화면으로 이동 합니다.

C 영역

1. 실시간 감시 기능

중요 문서에 접근하는 소프트웨어를 실시간으로 감시하여 중요 문서 위변조 시 소프트웨어를 검출 하는 기능 입니다.

1.1 기능 ON/OFF



: 중요 문서 위변조를 실시간으로 감시하고 있는 상태 입니다.

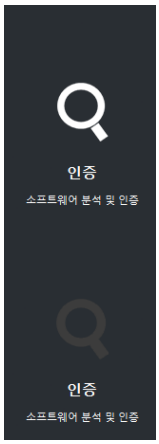
: 중요 문서 위변조를 실시간으로 감시하지 않는 상태 입니다.

D 영역

2 소프트웨어 인증 기능

중요 문서에 접근하는 알 수 없는(미확인) 소프트웨어의 신뢰성을 검사하여 사용자의 중요문서를 보호합니다.

2.1 기능 ON/OFF



: 소프트웨어의 신뢰성을 검사 하고 있는 상태 입니다.

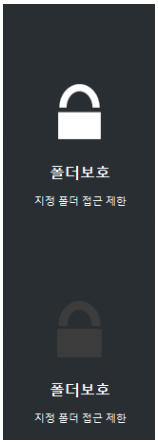
: 소프트웨어의 신뢰성을 검사 하지 않는 상태 입니다.

E 영역

3. 보호폴더

사용자가 지정한 폴더를 문서의 종류와 상관 없이 랜섬웨어 및 다른 프로그램의 접근을 차단하여 파일을 보호 할 수 있습니다.

3.1 기능 ON/OFF



: 사용자가 지정한 폴더를 보호하고 있습니다.

: 사용자가 지정한 폴더를 보호하지 않습니다.

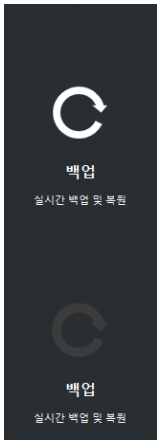
※ **Note** : 사용자가 지정한 폴더가 없다면 기능 ON/OFF를 하여도 보호할 폴더가 없기 때문에 ON/OFF는 상관 없습니다.

F 영역

4. 실시간 백업

소프트웨어가 중요 문서 접근할 때 실시간으로 백업하고 보호하여 랜섬웨어 및 다른 프로그램의 접근 차단 및 보호 합니다.

4.1 기능 ON/OFF



: 중요문서를 실시간으로 백업 및 복원을 합니다.

: 중요문서를 실시간으로 백업 및 복원을 하지 않습니다.

G 영역

5. 업데이트

마지막으로 업데이트한 날짜를 보여줍니다.

※ Note : 최신 파일을 PC 부팅 시 체크하여 업데이트 되며 내부 데이터를 주기적으로 업데이트를 체크하여 업데이트합니다.

H 영역

6. 라이선스

남은 라이선스 기간으로 라이선스 기간이 지나면 랜섬디펜스를 사용 할 수 없게 됩니다.

I 영역

7. 도움말

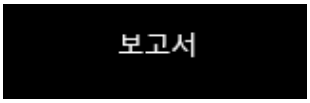
FAQ를 클릭 시 ㈜위젯누리 FAQ 게시판으로 이동 합니다.

J 영역

8. 정보

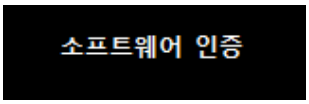
현재 PC의 안전 상태를 표시하여 줍니다.

K 영역



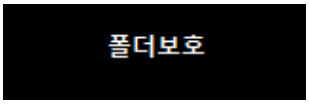
: 실시간 감시, 소프트웨어 인증에 의하여 검출 된 소프트웨어 및 검출 로그를 확인할 수 있는 화면을 보여줍니다.

L 영역



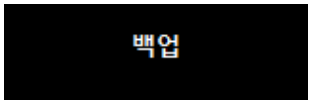
: 소프트웨어의 신뢰성 기준에 부합하지 않아 검출 된 소프트웨어를 보여줍니다.

M 영역



: 사용자가 지정한 보호폴더를 보여줍니다.

N 영역



: 실시간으로 백업 된 파일을 보여줍니다

5. 환경 설정

5.1 설정

각 기능에 대한 간략한 설명과 기능을 ON/OFF 할 수 있습니다.

5.2. 정보

랜섬디펜스의 업데이트, 제품 정보를 보여주며 기술 문의 및 매뉴얼을 확인 할 수 있습니다.

5.2.1 화면 설명

최신 업데이트 확인 : 최신 업데이트 확인 및 최신 버전으로 업데이트

㈜ 위젯누리 홈페이지 : 랜섬디펜스 개발사 홈페이지 이동

㈜ 인프라허브 : 파트너사 홈페이지 이동

기술 문의 : 개발사 기술문의 홈페이지로 이동

매뉴얼 확인 : 랜섬디펜스 매뉴얼 홈페이지로 이동

6. 보고서

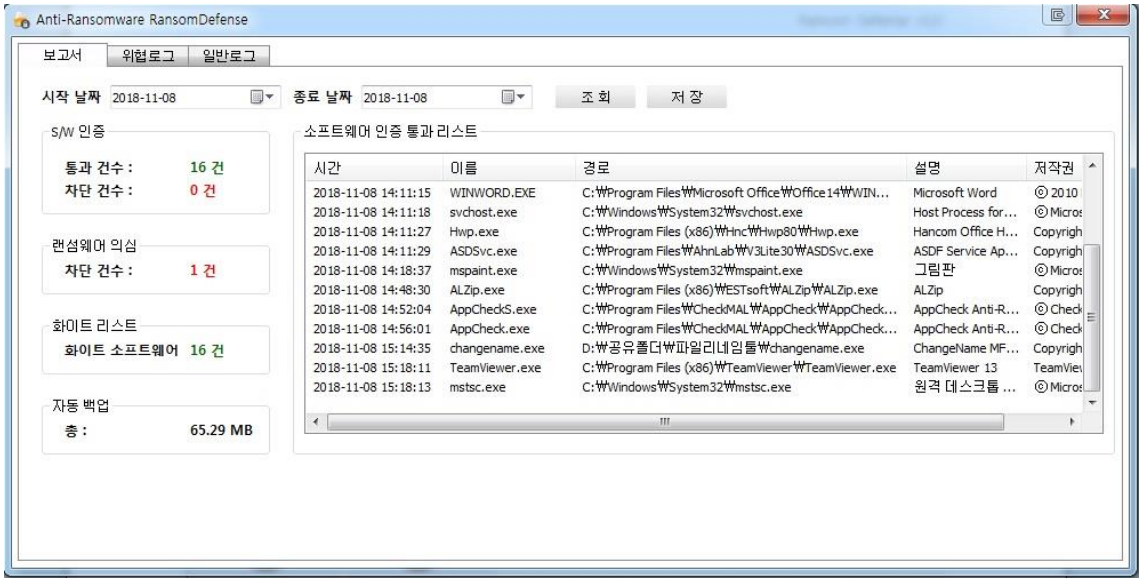
[메인 화면] – [보고서] – [클릭]

보고서, 위협로그, 일반로그 탭으로 구성되어 있으며 정보를 확인 할 수 있습니다.

6.1 보고서 설명

[메인 화면] – [보고서] – [보고서]

최소 1일에서 최대 30일까지 최근에 중요 문서에 접근 및 검출 된 소프트웨어를 보여줍니다.



시작 날짜 : 소프트웨어 검출이력 조회 할 시작 날짜 입니다.

종료 날짜 : 소프트웨어 검출이력 조회 할 종료 날짜 입니다.

조회 버튼 : 시작, 종료 날짜 설정 후 조회 시 위와 같은 화면을 보여줍니다.

저장 버튼 : 조회 결과를 엑셀 파일로 저장 합니다.

S/W 인증 – 통과 건수

: 조회 기간 내 소프트웨어의 신뢰성 검증에 통과 된 정보를 출력합니다.

S/W 인증 – 차단 건수

: 조회 기간 내 소프트웨어의 신뢰성 검증에 통과 되지 못한 정보를 출력합니다.

랜섬웨어 의심 : 조회 기간 내 중요 문서에 접근하여 문서를 위변조 시킨 소프트웨어의 검출된 정보를 출력합니다.

화이트 소프트웨어 : 소프트웨어 신뢰성 검증을 통과 및 사용자가 인증 시킨 소프트웨어 정보를 출력합니다.

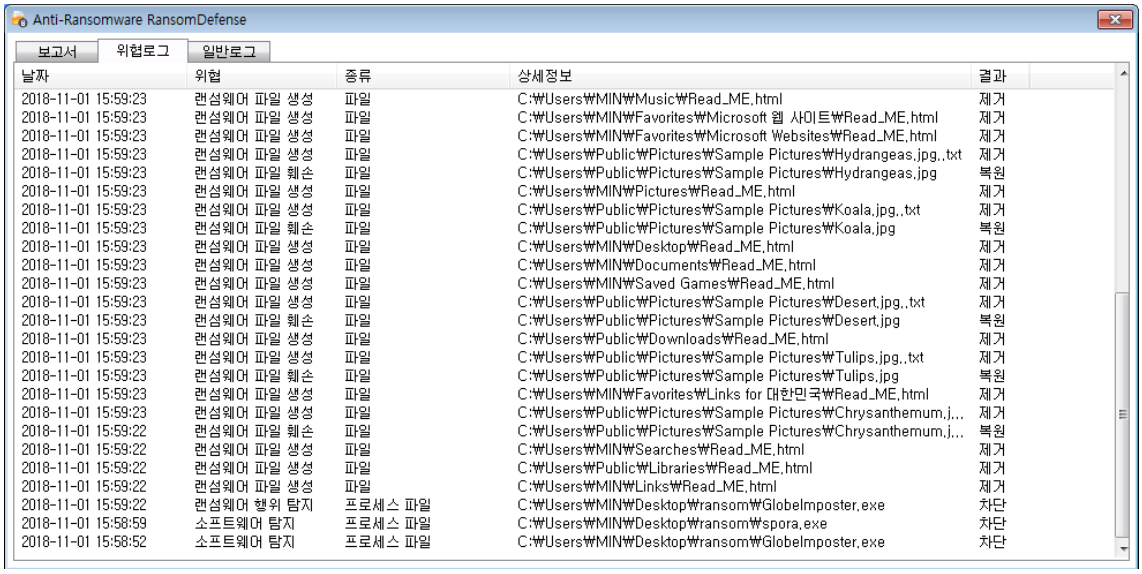
자동 백업 : 실시간으로 자동 백업된 파일 용량을 보여줍니다.

※ **Note** : [메인 화면] – [보고서] 클릭 시 기본으로 오늘 날짜로 조회 된 정보를 보여줍니다.

6.2 위협로그

[메인 화면] – [보고서] – [위협로그]

랜섬웨어 및 알 수 없는 소프트웨어의 위협(중요 문서 위변조)을 받아 소프트웨어 검출 및 감염 파일 삭제, 원본파일 복원한 이력을 조회 할 수 있습니다.

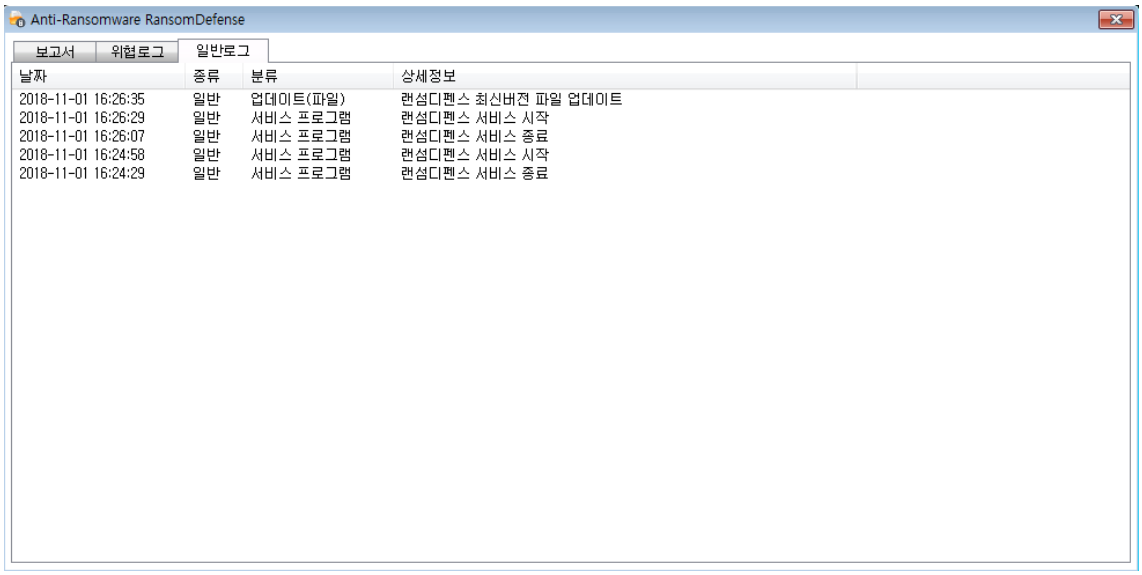


날짜	위협	종류	상세정보	결과
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Music₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Favorites₩Microsoft 웹 사이트₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Favorites₩Microsoft Websites₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Hydrangeas.jpg.,.txt	제거
2018-11-01 15:59:23	랜섬웨어 파일 훼손	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Hydrangeas.jpg	복원
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Pictures₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Koala.jpg.,.txt	제거
2018-11-01 15:59:23	랜섬웨어 파일 훼손	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Koala.jpg	복원
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Desktop₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Documents₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Saved Games₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Desert.jpg.,.txt	제거
2018-11-01 15:59:23	랜섬웨어 파일 훼손	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Desert.jpg	복원
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Downloads₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Tulips.jpg.,.txt	제거
2018-11-01 15:59:23	랜섬웨어 파일 훼손	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Tulips.jpg	복원
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Favorites₩Links for 대한민국₩Read_ME.html	제거
2018-11-01 15:59:23	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Chrysanthemum.j...	제거
2018-11-01 15:59:22	랜섬웨어 파일 훼손	파일	C:₩Users₩Public₩Pictures₩Sample Pictures₩Chrysanthemum.j...	복원
2018-11-01 15:59:22	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Searches₩Read_ME.html	제거
2018-11-01 15:59:22	랜섬웨어 파일 생성	파일	C:₩Users₩Public₩Libraries₩Read_ME.html	제거
2018-11-01 15:59:22	랜섬웨어 파일 생성	파일	C:₩Users₩MIN₩Links₩Read_ME.html	제거
2018-11-01 15:59:22	랜섬웨어 행위 탐지	프로세스 파일	C:₩Users₩MIN₩Desktop₩ransom₩GlobeImposter.exe	차단
2018-11-01 15:58:59	소프트웨어 탐지	프로세스 파일	C:₩Users₩MIN₩Desktop₩ransom₩spora.exe	차단
2018-11-01 15:58:52	소프트웨어 탐지	프로세스 파일	C:₩Users₩MIN₩Desktop₩ransom₩GlobeImposter.exe	차단

6.3 일반로그

[메인 화면] – [보고서] – [일반로그]

서비스의 시작, 종료 및 업데이트 내역을 확인 할 수 있습니다.



날짜	종류	분류	상세정보
2018-11-01 16:26:35	일반	업데이트(파일)	랜섬디펜스 최신버전 파일 업데이트
2018-11-01 16:26:29	일반	서비스 프로그램	랜섬디펜스 서비스 시작
2018-11-01 16:26:07	일반	서비스 프로그램	랜섬디펜스 서비스 종료
2018-11-01 16:24:58	일반	서비스 프로그램	랜섬디펜스 서비스 시작
2018-11-01 16:24:29	일반	서비스 프로그램	랜섬디펜스 서비스 종료

7. 소프트웨어 인증

[메인 화면] – [소프트웨어 인증]

신뢰성이 검증 되지 않은 소프트웨어 또는 중요문서를 위변조 시도한 소프트웨어 검출 정보를 보여줍니다.

7.1 화면 설명

시간 : 소프트웨어 검출 시간

이름 : 소프트웨어 이름

저작권 : 소프트웨어의 저작권 이름

경로 : 소프트웨어의 파일 경로

차단 기반 – 인증차단

: 소프트웨어의 신뢰성이 검증되지 않아 차단된 목록 입니다.

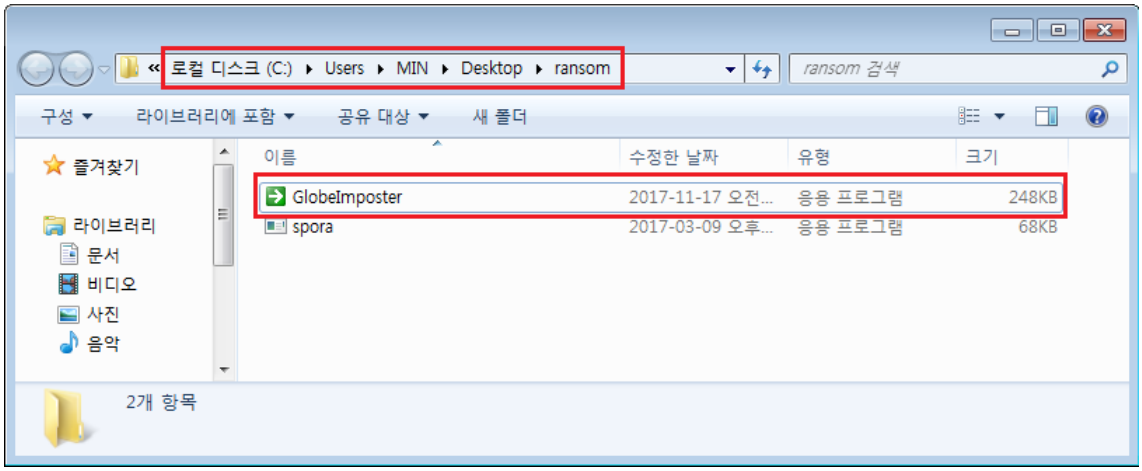
차단 기반 – 행위차단

: 중요문서를 위변조하여 차단된 목록 입니다.

7.2 기능 설명

1. 해당 소프트웨어의 위치로 이동 방법

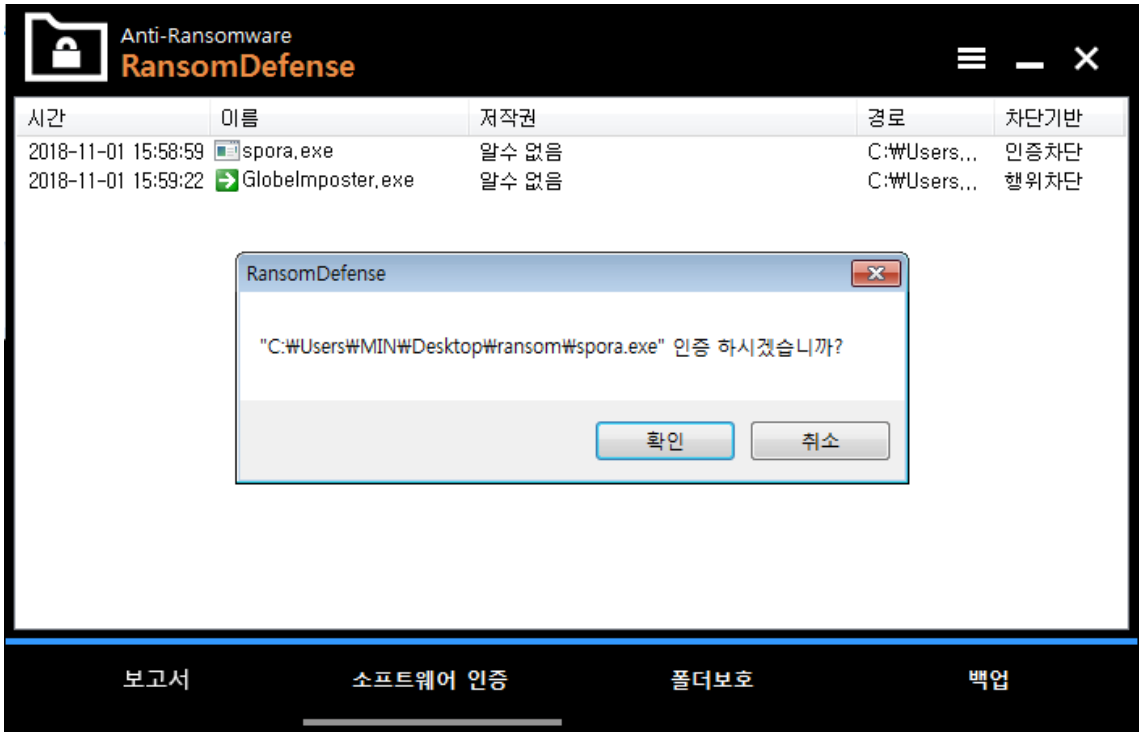
해당 소프트웨어를 더블 클릭 시 파일이 존재하는 경로로 이동 합니다.



Ex) GlobeImposter 더블클릭 화면

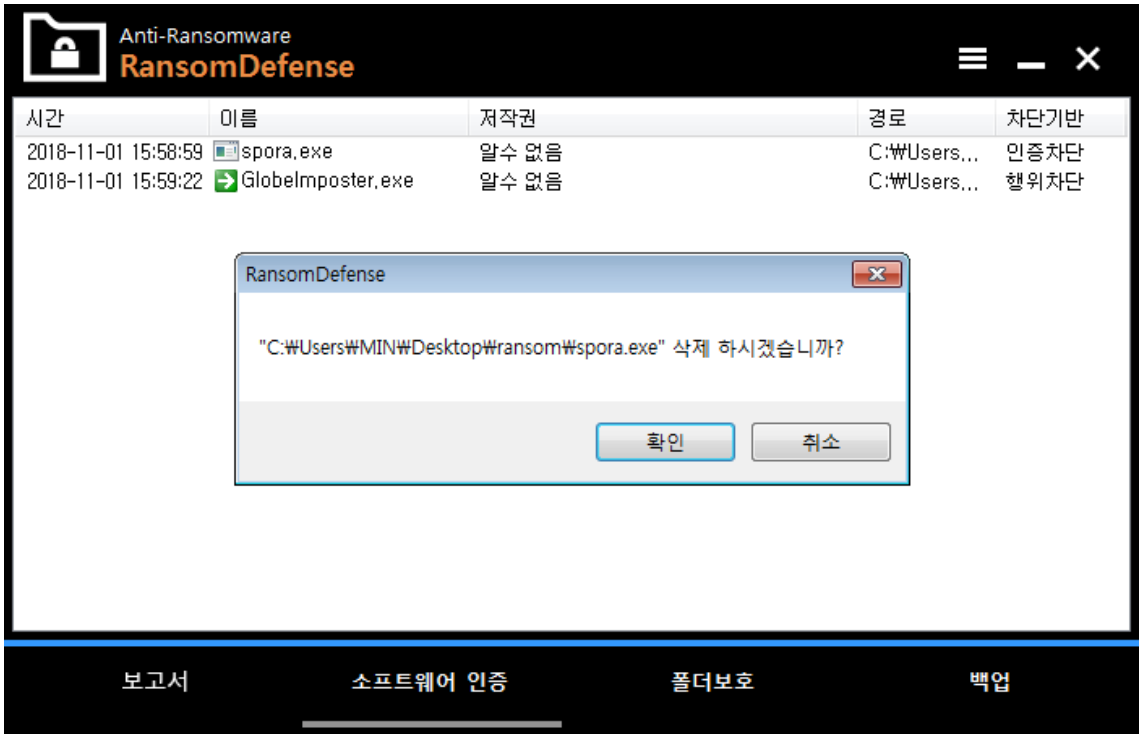
2. 해당 소프트웨어의 인증, 삭제, 상제 정보

인증 : 해당 소프트웨어를 인증(신뢰 할 수 있는 소프트웨어로 등록) 합니다.



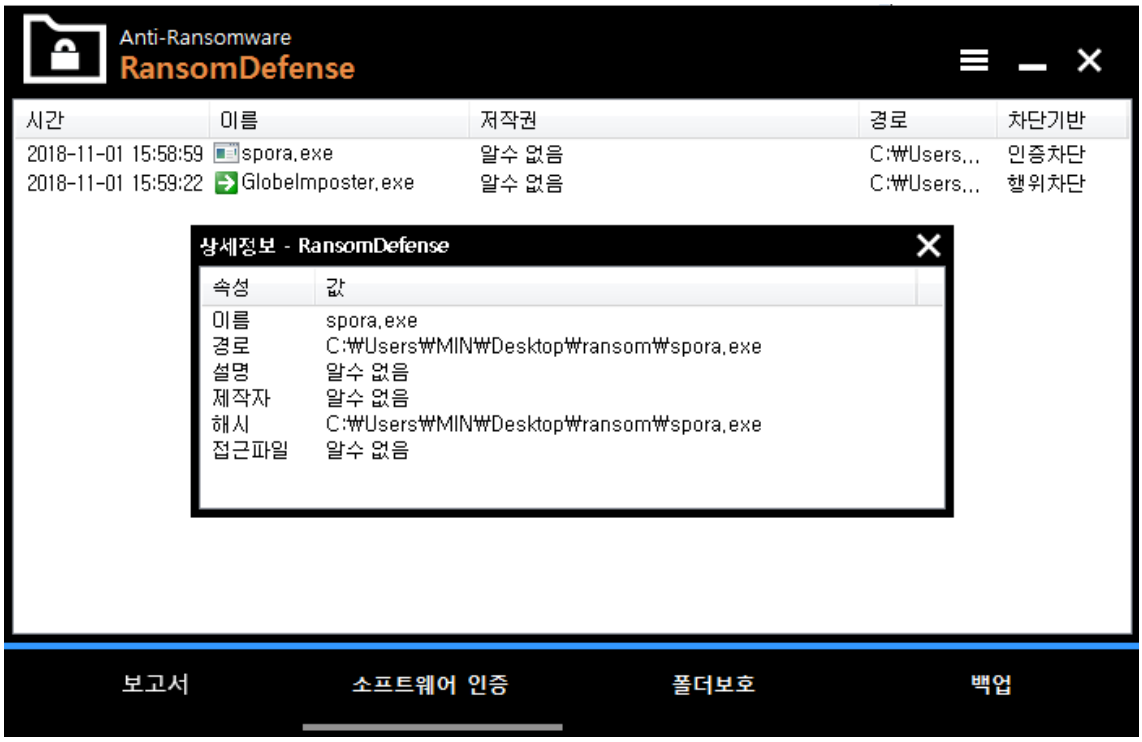
[소프트웨어 우클릭] – [인증] – [확인] or [취소]

삭제 : 해당 소프트웨어를 삭제(소프트웨어 신뢰성 재검증) 합니다.



[소프트웨어 우클릭] – [삭제] – [확인] or [취소]

상세 정보 : 해당 소프트웨어의 상세 정보를 확인 할 수 있습니다.



[소프트웨어 우클릭] – [상세정보]

8. 보호폴더

[메인 화면] – [폴더 보호]

사용자가 지정한 폴더를 문서의 종류와 상관 없이 랜섬웨어 및 다른 프로그램의 접근 차단하여 보호합니다.

8.1 화면 설명

폴더 이름 : 사용자가 보호한 폴더 이름 입니다.

폴더 경로 : 사용자가 보호한 폴더 이름 입니다.

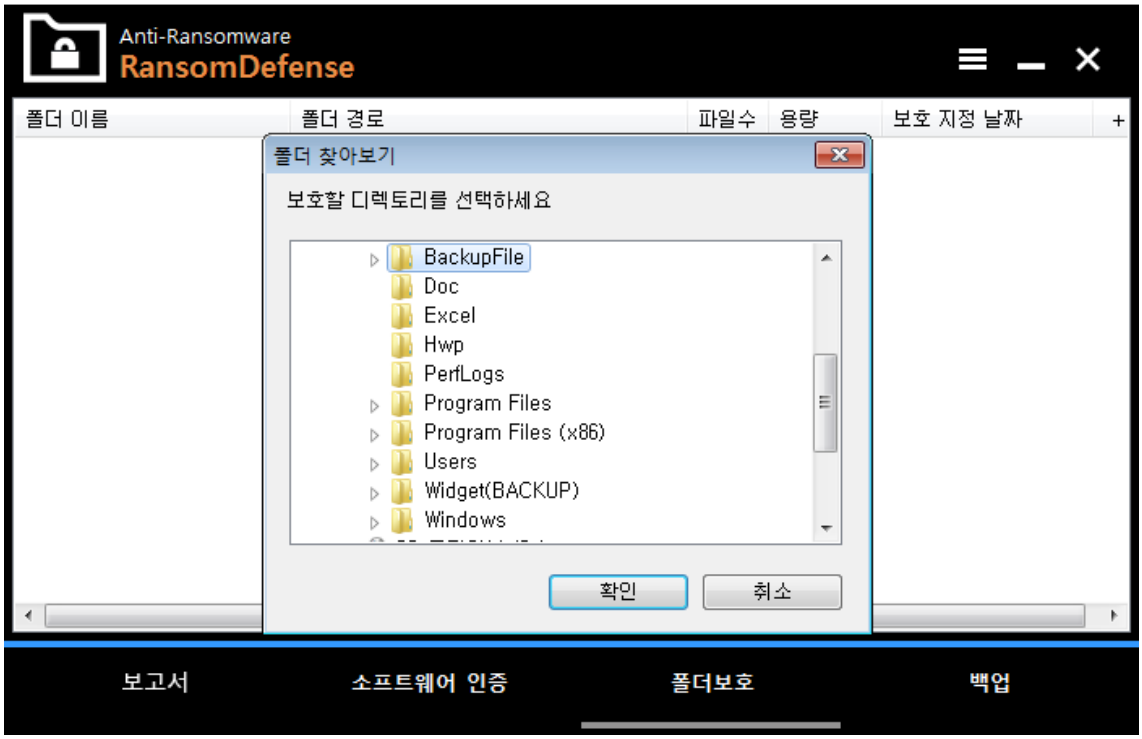
파일수 : 사용자가 지정한 폴더에 있는 파일 개수입니다.

용량 : 사용자가 지정한 폴더에 있는 파일 용량 입니다.

보호 지정 날짜 : 사용자가 보호폴더를 지정한 날짜 입니다.

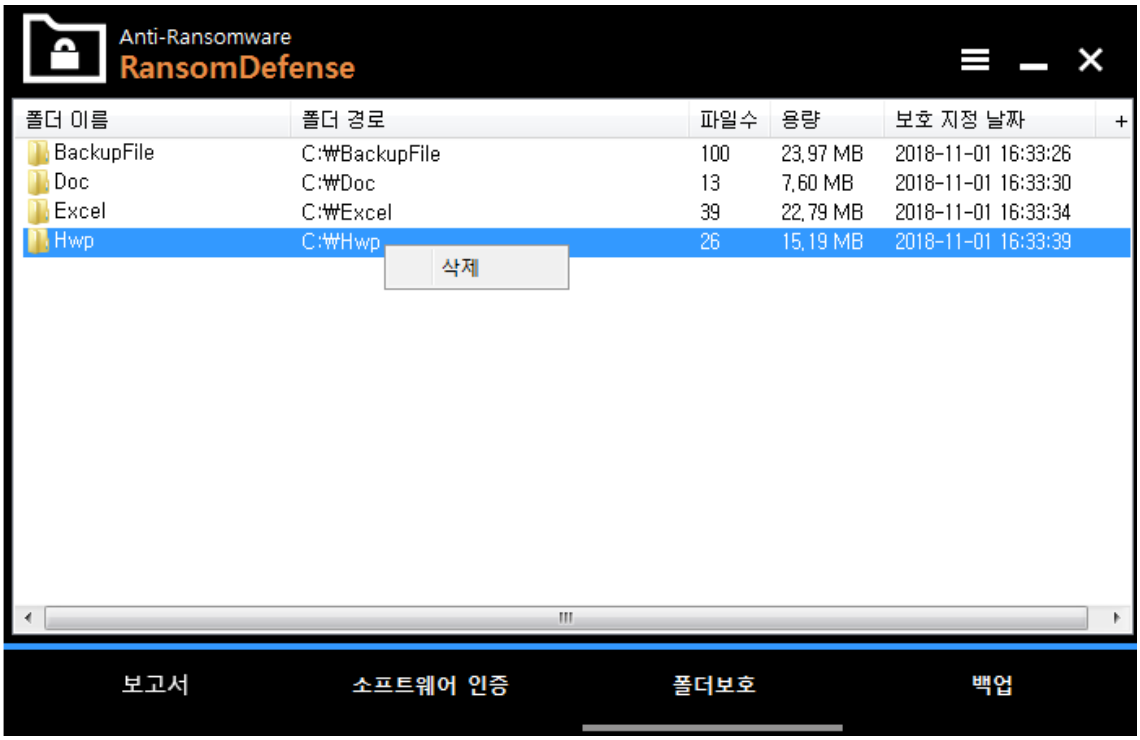
8.2 보호폴더 추가

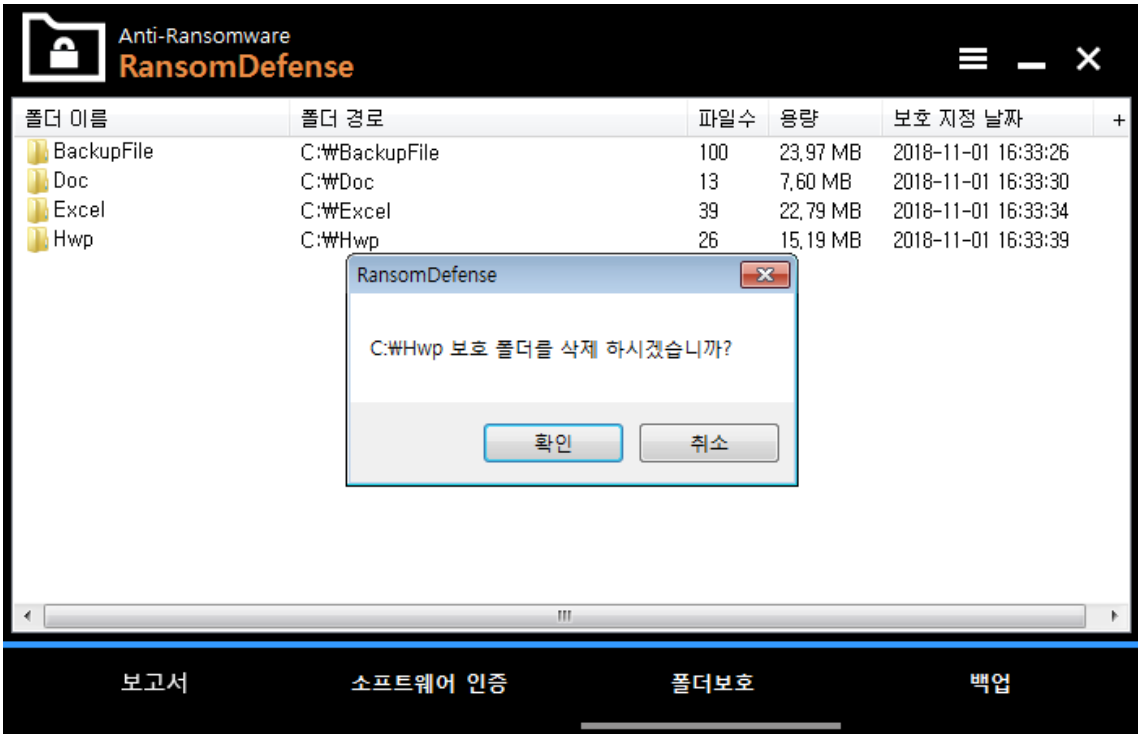
상단 우측의 '+'를 클릭하면 폴더를 지정 할 수 있는 창이 띄어집니다.

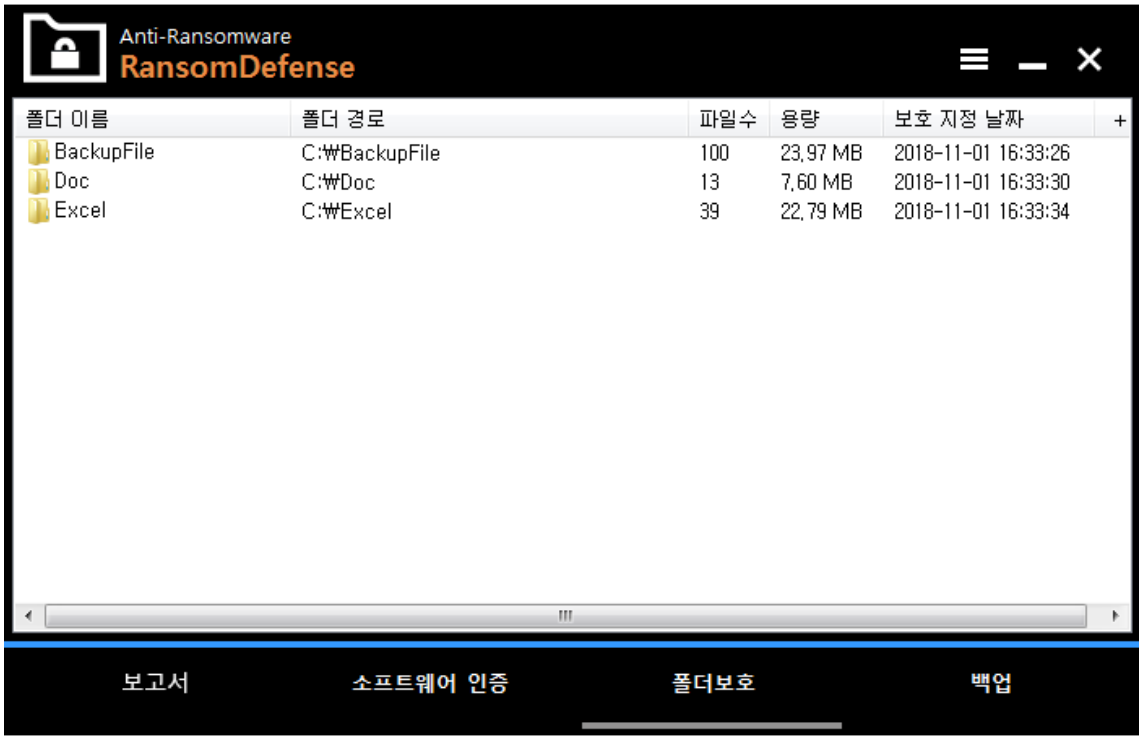


8.3 보호 폴더 삭제

원하는 [폴더 명 우클릭] - [삭제] 클릭






Anti-Ransomware
RansomDefense
폴더 이름
폴더 경로
파일수
용량
보호 지정 날짜
BackupFile
C:₩BackupFile
100
23,97 MB
2018-11-01 16:33:26
Doc
C:₩Doc
13
7,60 MB
2018-11-01 16:33:30
Excel
C:₩Excel
39
22,79 MB
2018-11-01 16:33:34
보고서
소프트웨어 인증
폴더보호
백업

9. 실시간 자동 백업

실시간으로 소프트웨어가 접근한 중요문서를 자동으로 각각의 하드디스크에 백업 합니다.

9.1 화면 설명

이름 : 백업된 폴더의 최상위 폴더 명 입니다.

비율 : 각각에 자동 백업 된 폴더의 저장 비율 입니다.

크기 : 각각에 자동 백업 된 폴더의 저장 용량 입니다.

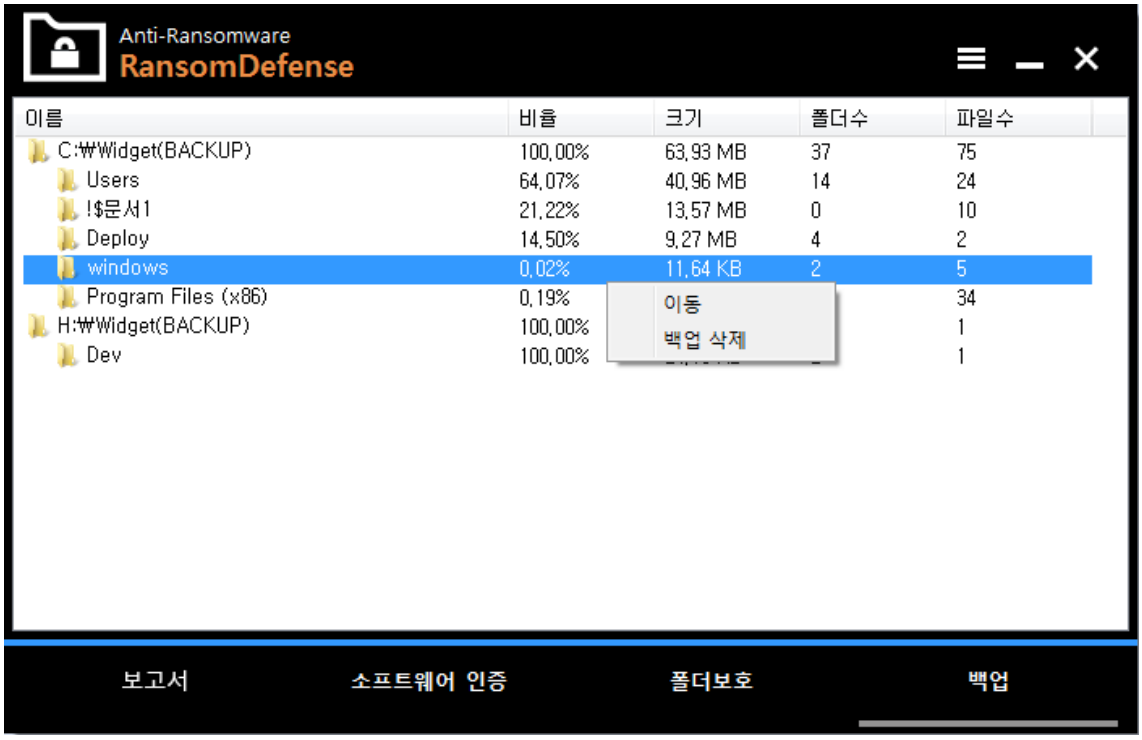
폴더수 : 각각에 자동 백업 된 폴더 개수 입니다.

파일수 : 각각에 자동 백업 된 파일 개수 입니다.

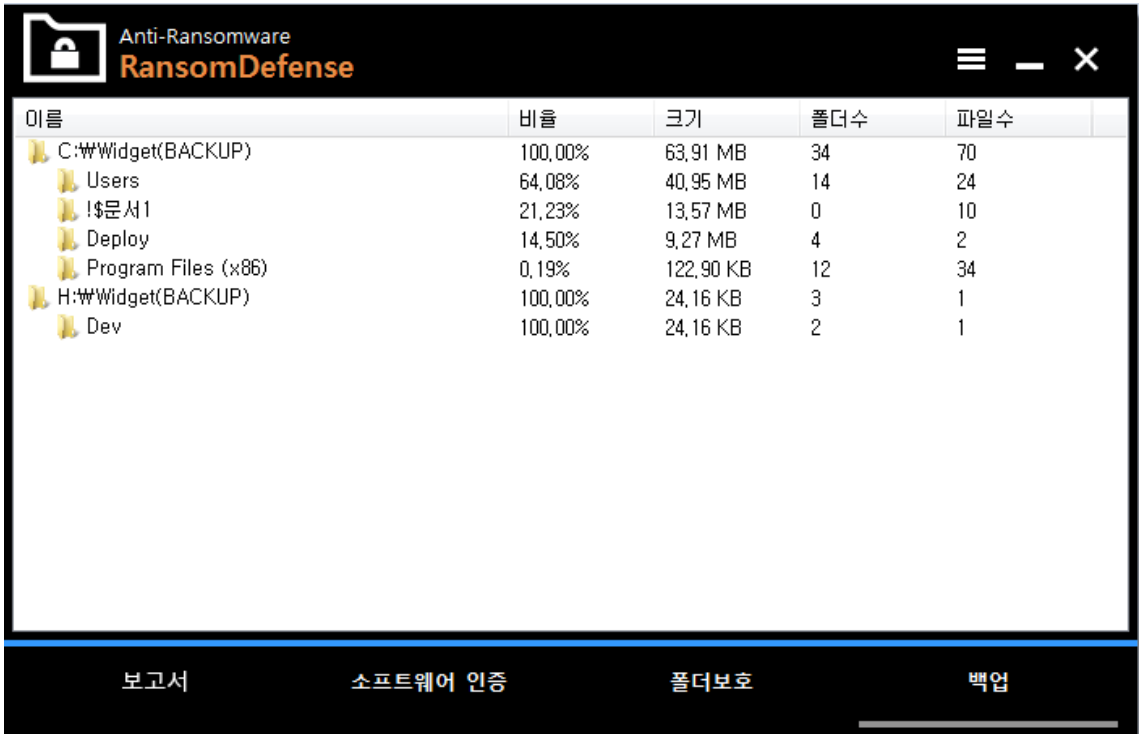
9.2 기능 설명

1. 자동 백업 된 파일 삭제 방법

[폴더 우클릭] – [백업 삭제] 클릭하여 해당 폴더를 삭제 할 수 있습니다.



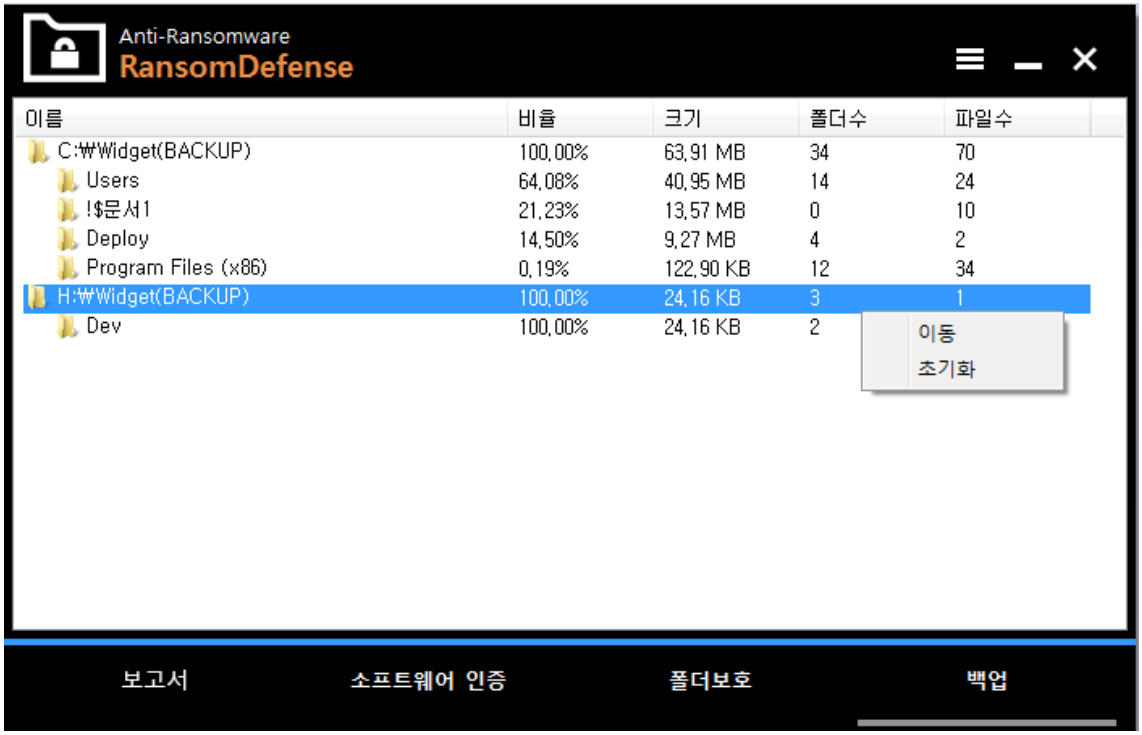
'Windows' 폴더 [백업 삭제] 클릭 합니다.



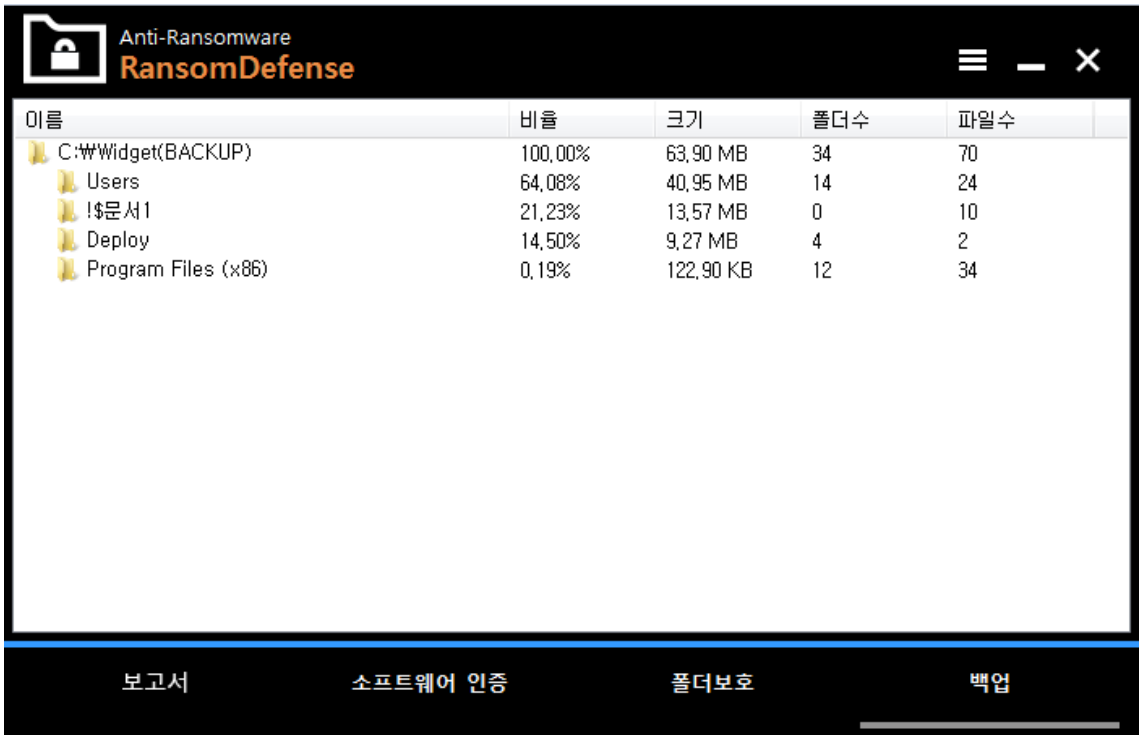
'Windows' 폴더가 삭제 되었습니다.

2. 자동 백업 된 파일 초기화

하드디스크가 표기된 폴더 명 우클릭 후 [초기화]를 클릭하여 모두 삭제 할 수 있습니다.



하드디스크가 표기된 폴더 명 우클릭 및 [초기화] 클릭



H 하드디스크에 자동 백업된 파일이 삭제 되었습니다.

3. 백업 폴더로 이동 방법

[폴더 우클릭] – [이동] or [폴더 더블 클릭] 하여 백업된 폴더로 이동 할 수 있습니다.