METIS AI

RansomEye V3.0

에이전트 사용 설명서

㈜베일리테크 기술연구소

1. RansomEye Agent

RansomEye Agent 는 윈도우 계열의 PC 또는 서버에 설치되는 응용프로그램으로, 악성코드로 의심되는 파일의 수집 및 랜섬웨어로 의심되는 악성코드로부터 암호화 행위를 사전에 탐지, 차단(프로세스 종료)하고 격리합니다. 차단/격리된 의심파일은 Manager 로 전송합니다.

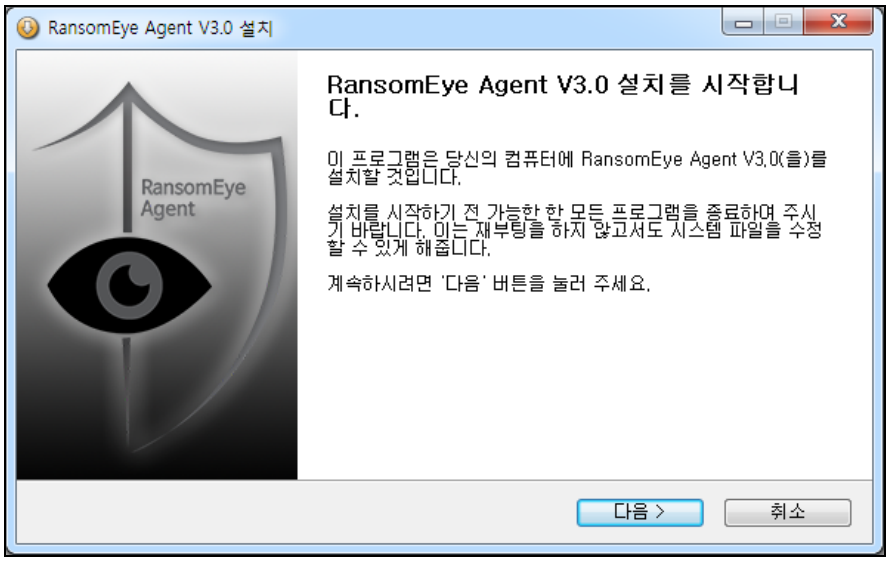
1.1 설치

- **설치파일 다운로드**

  RansomEye Agent 설치파일(RansomEyeSetup.exe)은 RansomEye Manager 의 관리자 웹에 접속후 "에이전트관리> 설치파일다운로드" 페이지에서 다운로드 할 수 있습니다. 또는 제공되는 CD 또는 담당자 e-mail 을 통해서 설치파일이 제공됩니다.

- **설치**

  RansomEye Agent 설치파일 (RansomEyeSetup.exe)을 실행하여 설치를 진행합니다.



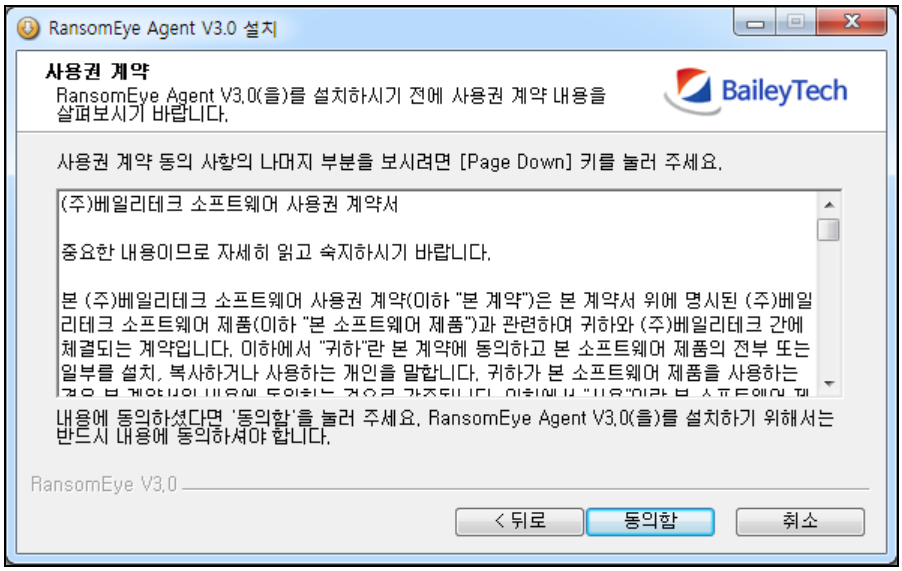
RansomEye Agent 설치 전 .NET Framework 4.0 이 설치되어 있지 않은 환경에서는 .NET Framework 설치를 자동으로 진행합니다.

> Windows 7 sp1 이상의 환경에서 대부분 .NET Framework 4.0 이 기본 설치되어 있습니다.

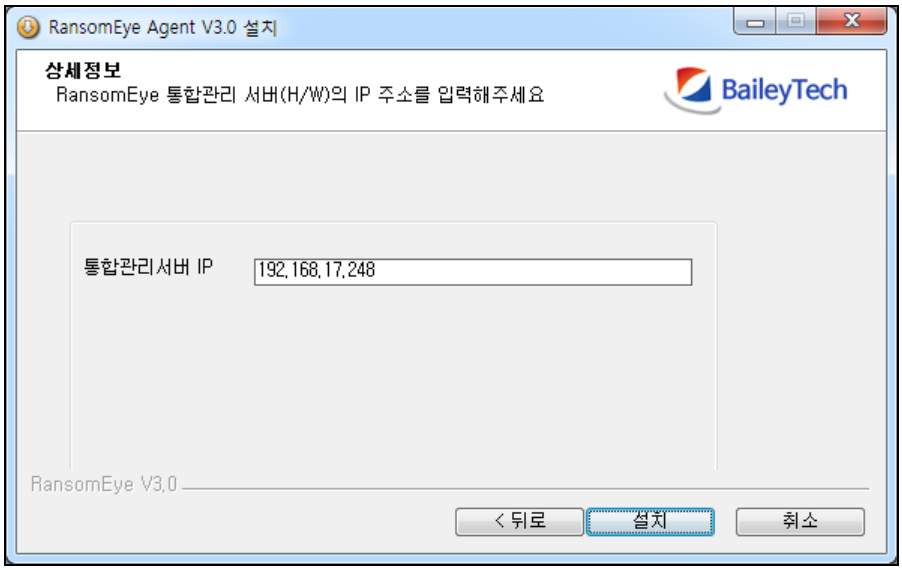
.NET Framework 설치를 진행한 경우에는 OS 가 요구하는 시스템 재시작이 될수도 있습니다.

.NET Framework 설치 후 RansomEye Agent 설치가 계속해서 진행됩니다.

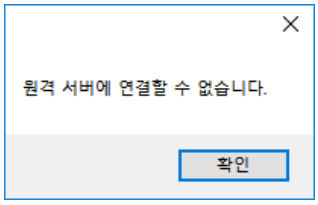
소프트웨어 사용권 계약사항에 동의하고 설치를 계속해서 진행합니다.

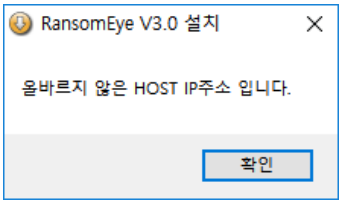


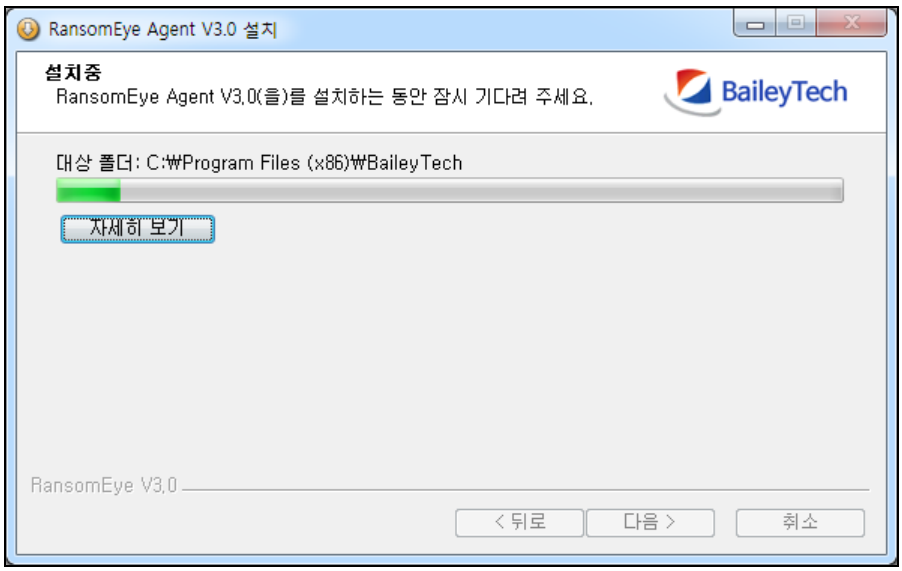
"통합관리서버 IP"란에 RansomEye Manager 의 IP 를 입력하고 설치를 진행합니다.



만일 잘못된 IP 가 입력되면 다음과 같이 "원격 서버에 연결할 수 없습니다." 라는 메시지와 "올바르지 않은 HOST IP 주소입니다." 라는 메시지가 출력됩니다.

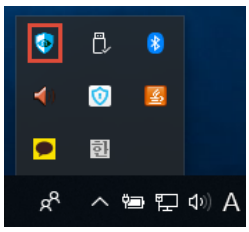




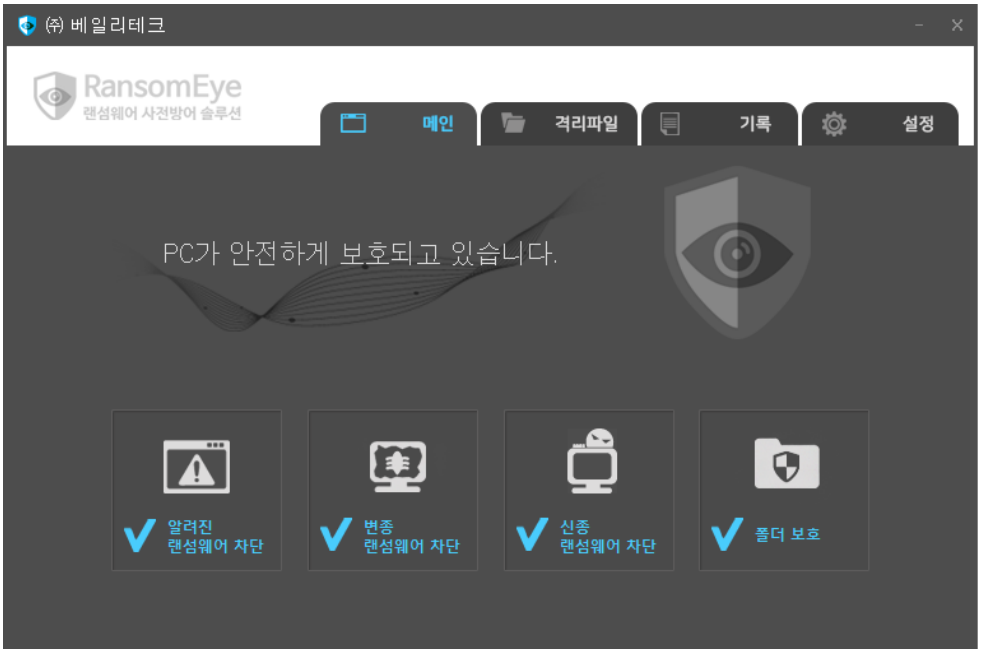


설치가 모두 완료되면 설치를 마칩니다.

설치가 완료되면 트레이에 다음과 같이 RansomEye Agent 아이콘이 보입니다.



아이콘을 더블클릭하여 화면을 엽니다.



메인 화면의 아래에 Agent 의 기능 활성화 정보를 확인합니다.
다음 4 가지 기능의 활성화 정보가 표시됩니다.

- ✓ 알려진 랜섬웨어 차단 기능
- ✓ 신변종 랜섬웨어 차단 기능
- ✓ 신종 랜섬웨어 행위 차단 기능
- ✓ 폴더 보호 기능

1.2 주요 기능

- **알려진 랜섬웨어 차단**

  RansomEye Agent 는 알려진 랜섬웨어 파일이 PC 내로 유입(인터넷 다운로드, USB 카피, FTP 다운로드 등)되면 보유중인 700 여 종의 알려진 랜섬웨어 정보와 비교하여 즉시 안전한 장소로 격리 보관합니다. 단, 압축된 파일은 알려진 랜섬웨어 차단 기능을 지원하지 않습니다.

- **변종 랜섬웨어 유사 코드 비교 기법을 이용한 탐지**

  PC 내로 유입되는 모든 파일은 보유중인 700 여 종의 알려진 랜섬웨어와 유사코드 비교를 수행하여 변종 여부를 확인합니다. 비교결과 60% 이상 동일 코드인 경우 즉시 안전한 장소로 격리합니다. 단, 압축된 파일은 유사코드 비교 탐지 기능을 지원하지 않습니다.

- **랜섬웨어 행위(암호화) 탐지센서에 의한 차단**

  랜섬웨어의 암호화 행위의 사전 징후를 탐지하여 암화 공격 수행 이전에 의심이 되는 프로세스를 Kill 하고 해당 프로세스를 안전한 장소로 격리보관합니다.

  일부 프로그램이 암호화와 유사한 행위 패턴으로 실행되는 경우가 있습니다. 이 경우 RansomEye Agent 는 해당 프로세스를 차단하나, 허용프로세스 등록처리로 차단되지 않게 할 수 있습니다.

- **보호폴더**

  사용자가 보호폴더로 지정한 폴더에 있는 모든 파일은 허용되지 않은 프로세스로부터 접근을 차단합니다. 단, 허용 프로그램으로 등록된 프로세스 이거나 코드싸인 된 프로세스인 경우에는 접근이 허용됩니다.

- **의심 파일 매니저로 전송**

  악성코드 및 랜섬웨어로 의심되는 프로세스 또는 프로그램 파일은 차단, 격리 후 상세분석을 위해 RansomEye Manager 로 전송합니다.

  랜섬웨어 의심파일 전송시 RansomEye Manager 와의 통신이 단절되어 있거나 파일을 전송에 실패했을경우, 이후에 통신 상태가 정상으로 복구되면 RasomEye Agent 자체 파일 업로드 스케쥴러에 의해 RansomEye Manager 로 재전송합니다.

- **허용프로세스 등록**

  허용프로세스로 등록된 프로세스는 사용자가 폴더보호로 지정한 폴더에 접근이 허용됩니다.

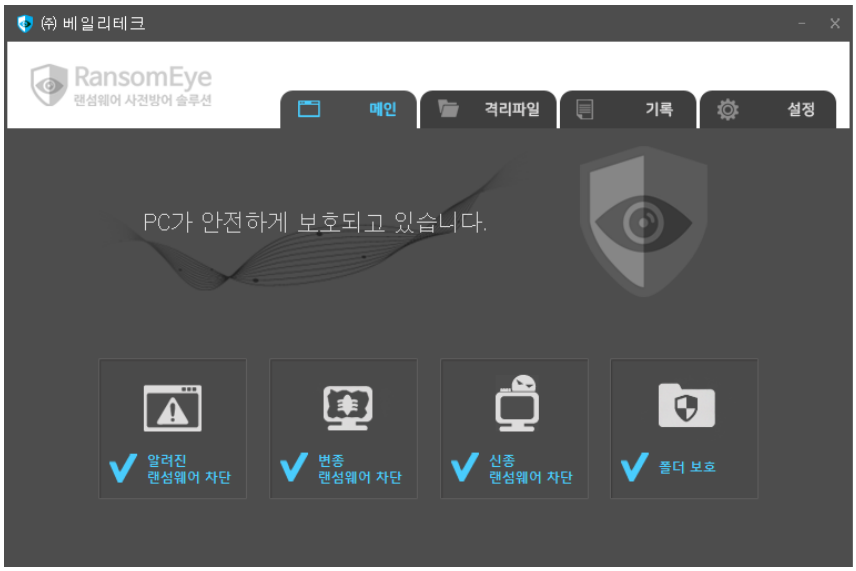
- **자체 프로세스 보호**

  RansomEye Agent 는 관련 프로세스간 실시간 상태체크를 하면서 외부적인 요인 또는 내부적인 요인에 의한 오류가 발생하더라도 자동복구되도록 설계되어있습니다.

1.3 사용법

- **메인**

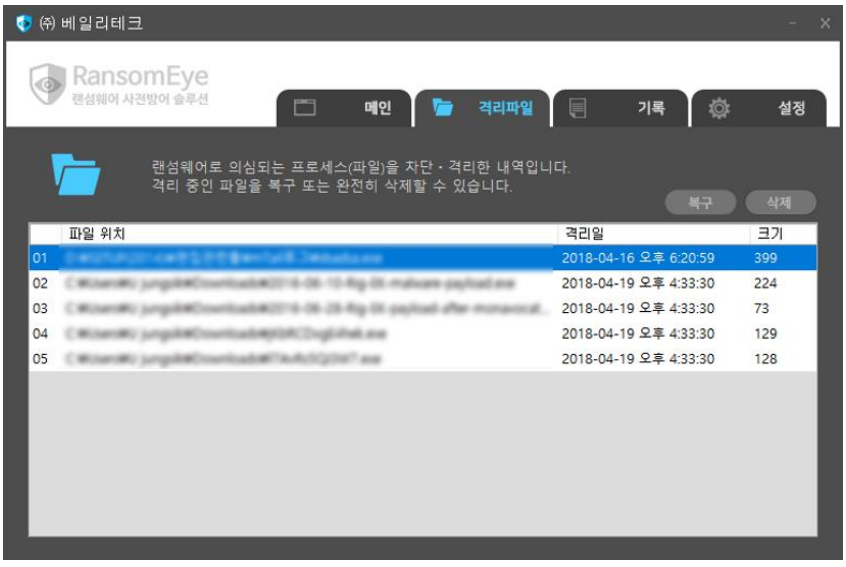
RansomEye Agent 는 4 개의 화면으로 구성되어 있습니다.
메인 화면에는 에이전트 기능 활성화 정보가 표시됩니다.



- **격리파일**

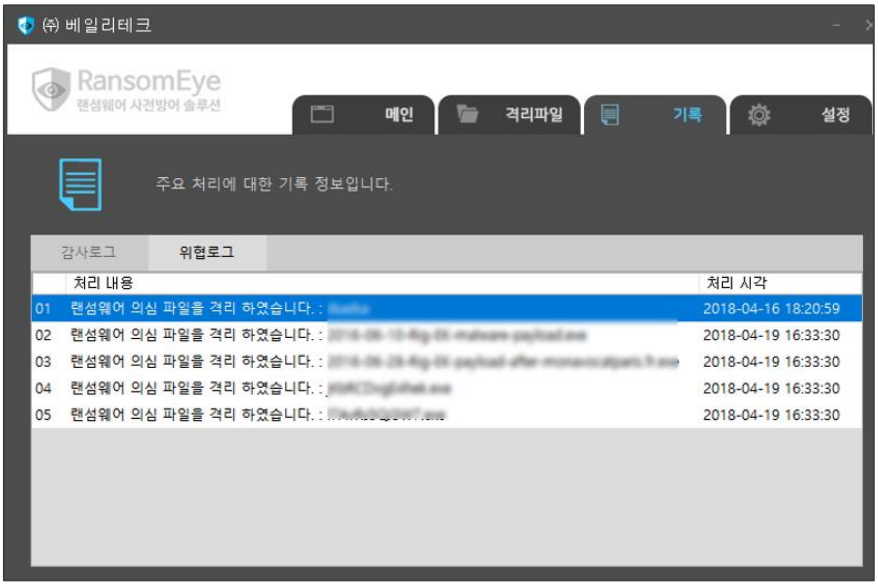
RansomEye Agent 는 랜섬웨어로 의심되는 프로세스가 발견되면 우선 차단(Process Kill)하고 해당 프로그램(exe, bin 등)을 안전한 장소로 격리보관합니다.

차단 이후에 악성 프로그램이 아닌경우 해당 프로그램을 복구할 수 있습니다.



- **기록**

RansomEye Agent 에 관한 기록 정보를 확인합니다. 랜섬웨어의 위협에 관한 기록과 시스템의 일반적인 처리 기록에 대한 정보로 구분되어있습니다.



- **설정**

에이전트 설정기능은 관리자가 개인 설정 권한을 부여 한 경우에만 설정 가능합니다.
설정은 보호폴더 설정, 허용프로그램 등록, 확장기능 설정, 업데이트 등이 있습니다.

- **보호폴더** 등록

보호된 폴더 내에 있는 모든 정보는 인가되지 않은 프로그램의 접근을 차단하여 정보를 보호합니다.

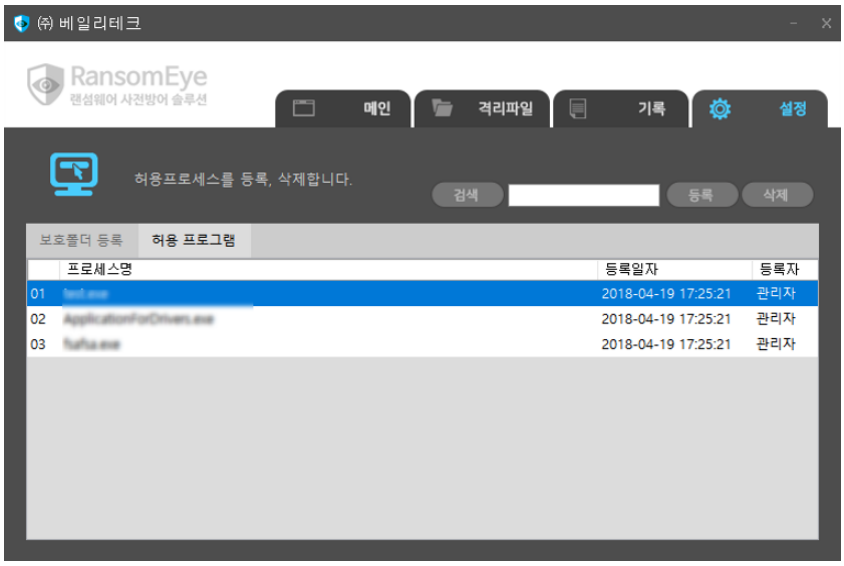
① 기본값은 관리자가 설정하며, 권한이 있으면 설정 할 수 있습니다.
② 사용자가 별도의 설정을 추가하고자 할 경우 보호할 폴더를 등록 할 수 있습니다.
③ 관리자가 설정한 값은 '등록자' 항목에 '관리자'라고 표시되며, 개인 사용자는 삭제 할 수 없습니다.
④ 입력값은 사용자가 직접 폴더명을 입력하거나 "검색"버튼을 이용하여 탐색기에서 폴더를 선택할 수 있습니다.
⑤ 폴더명 직접 입력 시 디스크 볼륨 정보 (C:\ 또는 D:\)로 시작하여 정확하게 입력하여야합니다. (예: C:\작성문서보관함, C:\mydoc)
⑥ 보호된 폴더에 접근이 불가한 프로그램이 있을 경우 허용프로그램 등록으로 접근 허용할 수 있습니다. (4-나 참고)

[입력제한 사항]

보호폴더	한글, 영문, 숫자를 사용하여 "C:₩temp1"형태로 3 자리에서 250 자리
허용프로그램	한글, 영문, 숫자를 사용하여 5 자리에서 250 자리

- **허용프로그램**

랜섬웨어 의심행위로 차단되거나 보호된 폴더에 접근이 필요한 프로세스를 등록하여 접근을 허용합니다.



① 기본값은 관리자가 설정하며, 권한이 있으면 설정할 수 있습니다.
② 안전한 프로그램 임이 100% 확실 한 경우에만 등록하여야 하며, 가급적 관리자에 의한 통합 설정을 권장합니다.
③ 관리자가 설정한 값은 '등록자' 항목에 '관리자'라고 표시되며, 개인 사용자는 삭제할 수 없습니다.
④ 입력값은 사용자가 직접 프로그램명(프로세스명)을 입력하거나 "검색"버튼을 이용하여 탐색기에서 해당 프로그램을 선택할 수 있습니다.

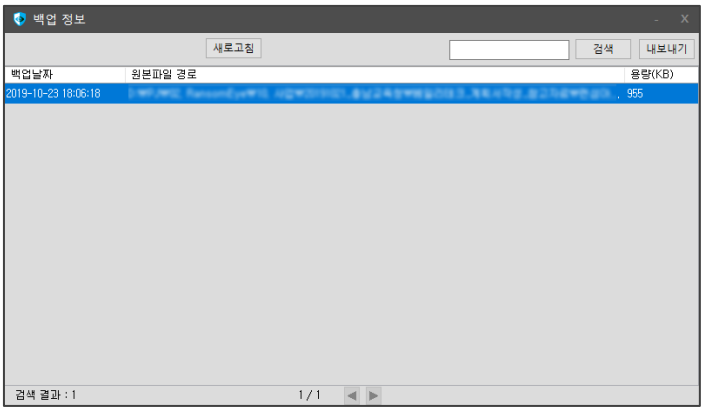
[입력제한 사항]

보호폴더	한글, 영문, 숫자를 사용하여 3 자리에서 250 자리
허용프로그램	한글, 영문, 숫자를 사용하여 5 자리에서 250 자리

- **확장 기능**

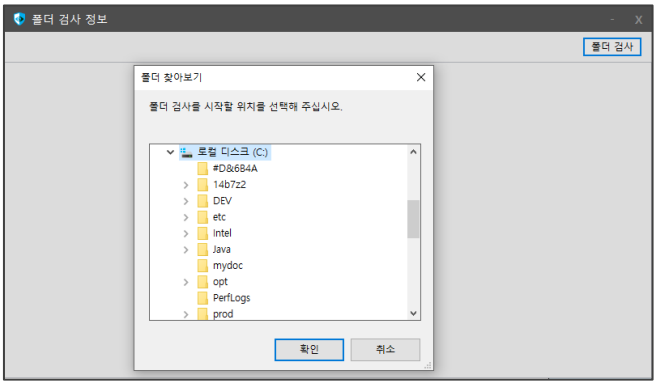
백업 기능의 백업할 확장자 추가, 삭제, 백업파일 확인 및 내보내기 등의 기능을 제공합니다.

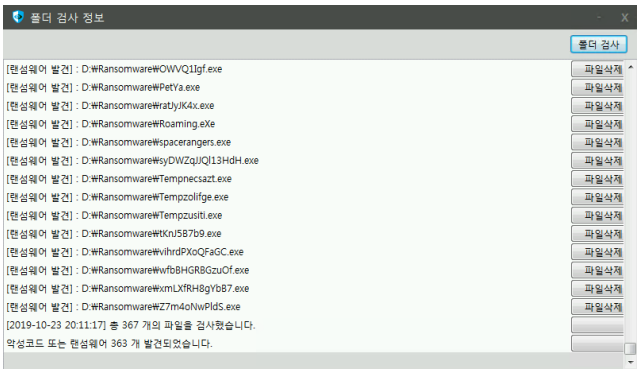
① 백업 확장자 기본값은 관리자가 설정하며, 권한이 있으면 설정 할 수 있습니다.
② 백업할 문서의 확장자를 추가 또는 삭제 할 수 있습니다.
③ 관리자가 설정한 확장자는 삭제 할 수 없습니다.
④ MBR 보호 기능은 관리자가 설정하면 자동으로 설정됩니다.
⑤ 로그파일 내보내기
에이전트 자체 로그 파일을 가져올 수 있는 기능입니다. 장애시 또는 기능 점검 시에 사용합니다.
⑥ 백업 목록
+ 에이전트의 백업 기능에 의해 백업되어 있는 정보를 확인하고 백업된 파일을 가져올 수 있는 기능입니다.
+ 검색버튼을 클릭하여 현재 백업되어있는 목록을 불러오거나, 검색어 입력후 검색버튼을 클릭하여 검색합니다.
+ 파일 목록 선택 후 내보내기 버튼을 클릭하여 파일을 가져올 수 있습니다.



⑦ 폴더검사

+ PC 내에 침투되어 있는 알려진 랜섬웨어 또는 악성코드가 있는지 검사하는 기능입니다.
+ 폴더검사 버튼을 클릭하여 디스크 볼륨(C 또는 D) 또는 폴더를 선택하고 확인버튼을 선택하면 해당 폴더를 검사합니다.

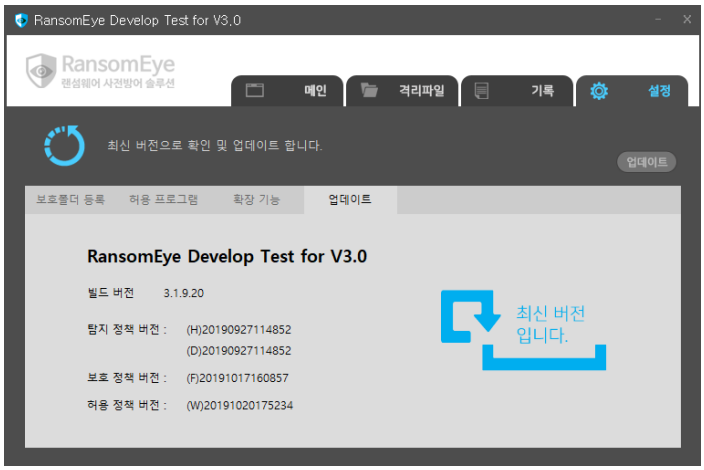




+ 알려진 램섬웨어 또는 악성코드가 발견되면 검사 결과창에 파일의 위치와 파일명이 표시되며 삭제할 수 있습니다.

- **업데이트(자동업데이트 및 수동 업데이트)**

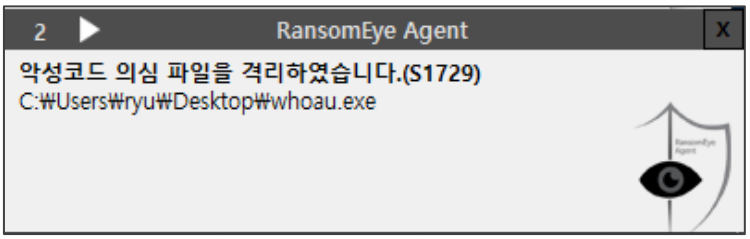
에이전트 프로그램의 버전 정보, 탐지 정책 버전, 보호 정책, 허용 정책 등의 버전 정보를 표시하는 화면입니다.
업데이트 스케쥴에 의해 RansomEye Agent 의 버전 및 탐지 정책 정보를 매 10 분 마다 체크하여 RansomEye Manager 서버로부터 자동 업데이트를 수행합니다.



① 로그램 버전 및 모든 정책 버전은 자동으로 업데이트됩니다.
② 업데이트 버튼을 클릭하여 수동으로 업데이트 할 수 있습니다.
③ 새로운 버전이 있으면 업데이트를 진행합니다.

▪ 차단 팝업

- 악성코드 의심파일 차단, 격리 알림창

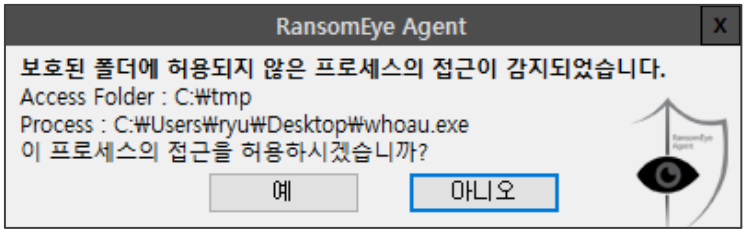


+ 랜섬웨어로 의심되는 프로세스를 에이전트가 탐지하여 차단한 경우입니다.
+ 에이전트는 랜섬웨어 행위로 의심이 되는 프로세스를 차단하므로 랜섬웨어가 아닌 경우에도 차단될 수 있습니다. 이 경우에는 관리자에게 해당 프로그램을 허용등록 요청하십시오.
+ 관리자가 허용프로그램에 등록 완료하면 해당 프로그램은 차단되지 않고 계속해서 실행됩니다.

- 알려진 악성코드 차단, 격리 알림창

+ 악성코드로 알려진 프로세스를 에이전트가 탐지하여 차단한 경우입니다.

- 보호된 폴더에 비인가 프로세스 접근 알림창



+ 보호된 폴더에 인가되지 않은 프로세스가 접근하려고 했을때 에이전트가 탐지하여 차단한 경우입니다.
+ 관리자에 의해 권한이 부여된 경우 접근 허용 처리를 할 수 있습니다.
+ "예"를 선택하면 보호된 폴더에 프로세스의 접근이 허용됩니다.
+ 관리자에 의해 권한이 부여되지 않은 경우 다음과 같이 프로세스 접근허용 버튼이 제공되지 않습니다.

※ 차단팝업은 사용자가 창을 닫지 않거나 추가 발생되는 팝업이 없을경우 5 분 동안 계속해서 유지됩니다.

1.4 데이터 백업 및 복구

- **탐지 정책 데이터**

탐지정책 데이터는 알려진 랜섬웨어 정보와 유사도 정보, 허용프로세스 정책 데이터로서, 정보의 추가 및 변경은 RansomEye Manager 의 관리자가 배포 관리하므로 별도의 백업은 하지않습니다.

- **로그파일**

RansomEye Agent 로그파일은 이벤트 발생시 RansomEye Manager 로 전송되었던 정보이므로 별도의 백업은 하지않습니다. (6 개월 이상 로그파일은 자동 삭제됨)

1.5 장애 처리

RansomEye Agent 운영중 발생하는 각종 오류에 대한 대처방법입니다.

- **사용자 장애 처리 방법**

항목	장애유형	해결방법
하드웨어 장애	디스크용량 장애 발생	디스크 용량 확인 후 불필요한 파일 삭제
	네트워크 장애	▪ 랜카드와 랜케이블 연결상태 확인 ▪ 허브 및 라우터 상태 확인 ▪ 네트워크 담장자에 문의
소프트웨어 장애	수동 업데이트 불능	▪ 네트워크 상태 확인 ▪ 관리서버 상태 확인(관리용 H/W(RansomEye Manager)가 설치되어 있는 고객사에 해당)
	제품 소프트웨어 운영중 예외오류 발생	▪ 시스템과 충돌의 원인이 있는지 점검 ▪ 필요시 PC 재기동