랜섬웨어 대응 솔루션 제안서

EST

INDEX

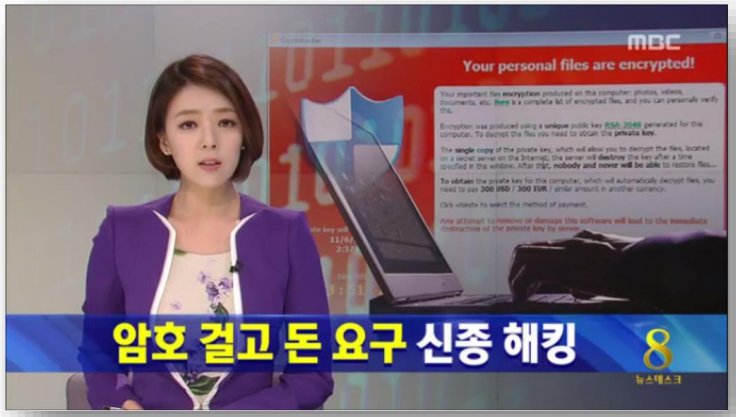
01 랜섬웨어 란?

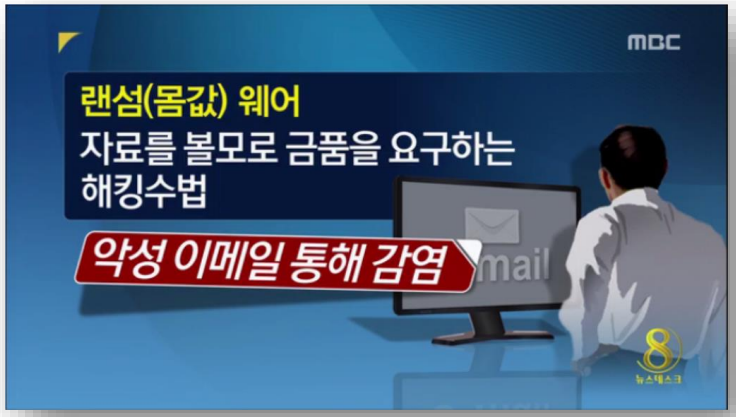
랜섬웨어(Ransomware) ?

- 사용자PC에 있는 파일들을 불법적으로 암호화하고 복호화를 대가로 금적전인 보상을 요구하는 악성코드
- 복호화 키는 공격자의 서버에 저장되기 때문에 사용자는 암호화된 파일 복구 불가

랜섬웨어 확산

- 2015년부터 한글화 된 랜섬웨어 발견, 피해 신고 및 사례 급증
- 국내 대형 커뮤니티 사이트 변조 등 다양한 수법으로 진화
- 2017년 5월 전세계 150개국, 20만대 이상의 PC를 감염시킨 '워너크라이' 랜섬웨어 강타





발췌 - MBC 뉴스데스크

랜섬웨어 침투 경로

- 웹 취약점, 악성코드 첨부 메일, APT 공격 등 다양한 경로로 지능적인 악성코드 침투
- 1대만 감염되어도 조직 전체가 랜섬웨어 공격에 노출되어 업무 마비

악성코드 침투

이메일 및 악의적인
링크를 통해 감염

숙주 PC 감염

악성코드 암호화 명령
(Command & Control 서버)

감염되면 사용자의
시스템 및 파일에 접근 불가

암호화 / 금전적 요구
(비트코인 등)

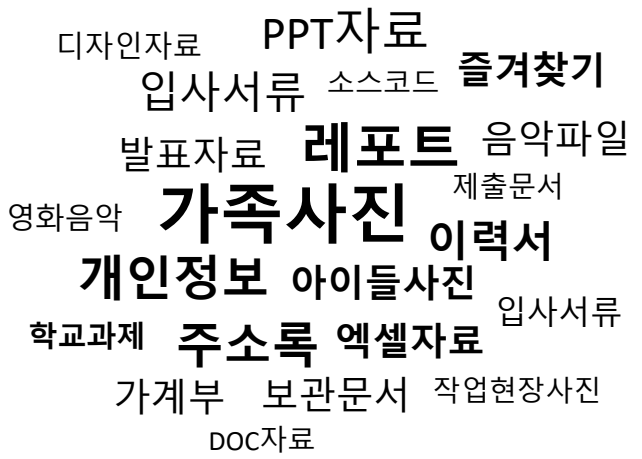
몸값을 지불하거나
해당 파일은 영구 이용 불가

평생 모았던 소중한 자료, 디지털 지식 자산을 한 순간에 모두 날려버릴 수 있습니다.

랜섬웨어 공격대상

- 개인과 기업 구분없이 인질로 가치가 있다고 판단되는 자료는 랜섬웨어 주 공격 대상
- 보안이 취약하고 백업이 미비한 비정형 데이터의 피해 규모 확대

개인 피해 자료



- 개인의 경우 대부분 자료 손실 후 HDD 포멧 (복구불가)
- 정확한 피해액 산출 불가

기업 피해 대상

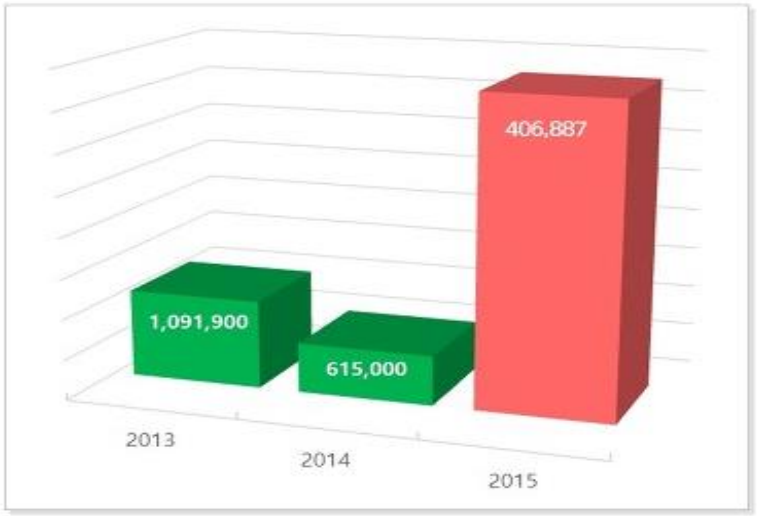
데이터구분	데이터종류	보관위치	관리주체	백업시스템 보유
정형 데이터	• ERP DB • 전자결재 DB • 웹서버 DB	중앙 서버/ 스토리지	전산실	• 대기업/공공 :95% • 중소기업 :20%
비정형 데이터	• CAD 설계도면 • 인사, 회계 자료 • 기술 문서 • 업무관련 자료 • 외부 수신문서	직원PC	직원 개인	5% 미만 (설계실 중심)

- 공공기관, 병원, 대기업 분야 구분없이 공격 대상
- 특히, 중견&중소기업의 피해가 전체의 약 60%이상

출처 : 랜섬웨어침해대응센터/보안뉴스

랜섬웨어 침해사례 통계

전세계 피해 현황



- 2016년 전세계 랜섬웨어 피해액 약 10억 달러(3조원)에 달하는 것으로 추산(Herjavec Group)
- 2015년 크립토라커와 데슬라크립토 두 종류의 랜섬웨어가 전체 공격의 82%를 차지

출처 : McAfee Lab

국내 피해 현황

- 2016년에는 상반기에만 벌써 13종류의 랜섬웨어가 등장, 2천19건으로 3.7배 증가
- 15만명이 랜섬웨어에 감염 총 3천억원의 피해를 입을 수 있을 것으로 추정

출처 : 보안뉴스

02 제안 배경

랜섬웨어 대응 방안

- 끊임없이 진화하고 다양한 경로로 유포되고 있어 기존 솔루션 대응의 한계 도달
- 개인 뿐만 아니라 다양한 보안 솔루션으로 방어하고 있는 다수의 기업에서도 랜섬웨어 감염 피해 확산

랜섬웨어 기본 대응 방안

✓ APT 탐지 및 메일 보안SW 도입

✓ OS 및 응용SW 보안 업데이트

✓ 스팸메일 첨부파일 실행 금지

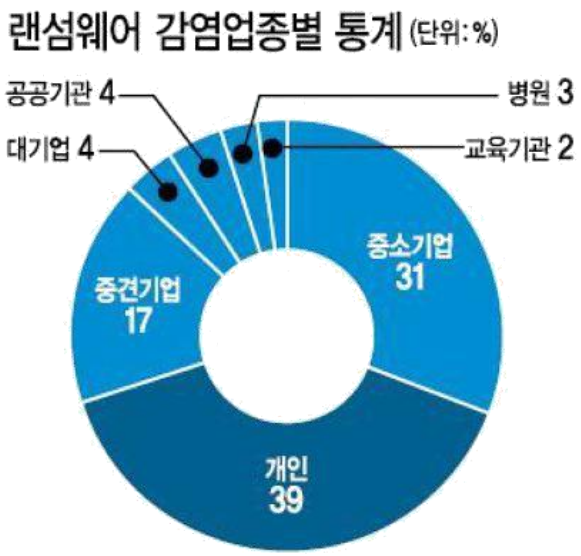
✓ 웹 페이지 접속 URL 안전 확인

✓ 백신 프로그램 최신 업데이트

✓ 읽기 전용 폴더 설정

•
•
•

하지만.. 현실은 ?



출처 : 헤럴드경제

랜섬웨어 대응 방안 (계속)

- 예측 불가능한 공격에 대한 최적의 대응 방법은 데이터 안전한 백업 뿐!

(과거) "악성코드"에 집중

진화&변종을 거듭하는
랜섬웨어는
기존 악성코드 차단 솔루션으로

대응의 한계 도달

(변화) "데이터보호"에 집중

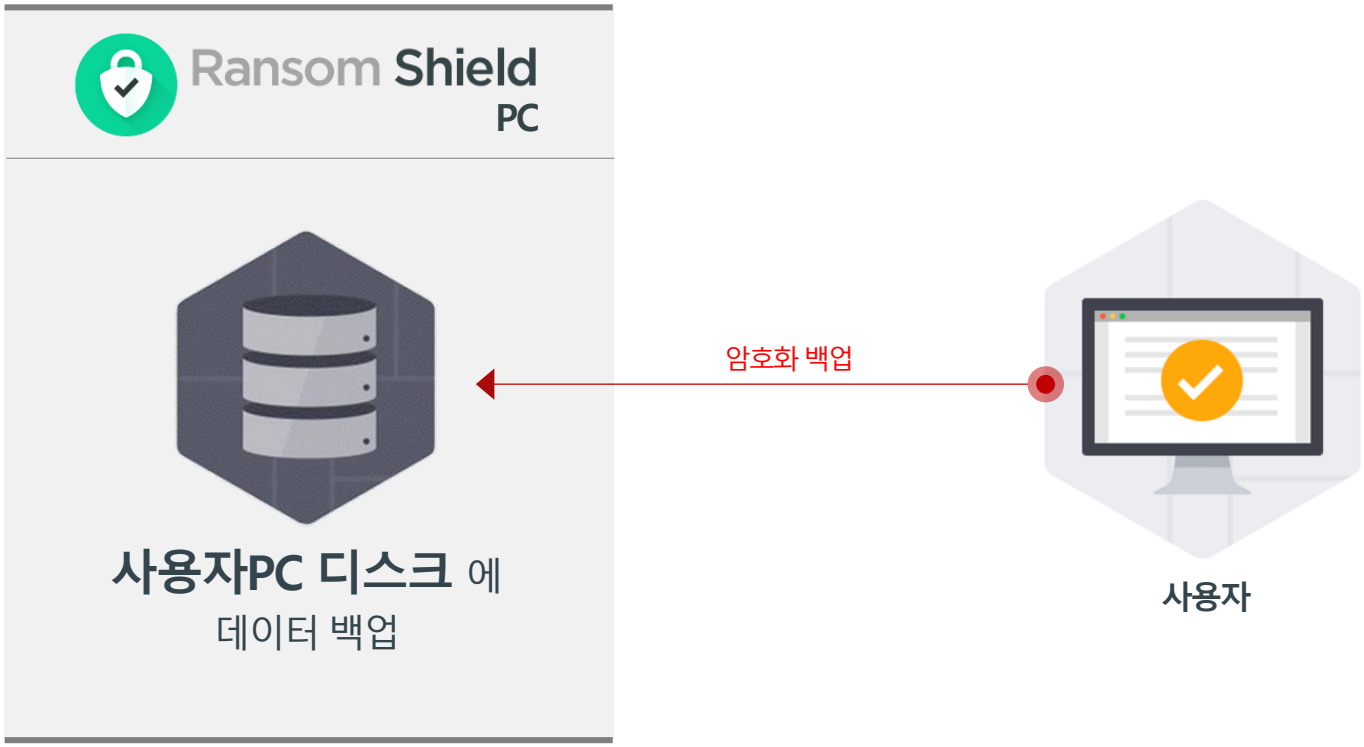
예측 불가능한
랜섬웨어 공격에는
데이터의 안전한

백업만이 최적의 대응

끊임없는 악성코드 방어에 집중하는 것보다 랜섬웨어의 주 공격 대상인 **데이터 보호**가 최적의 대응책

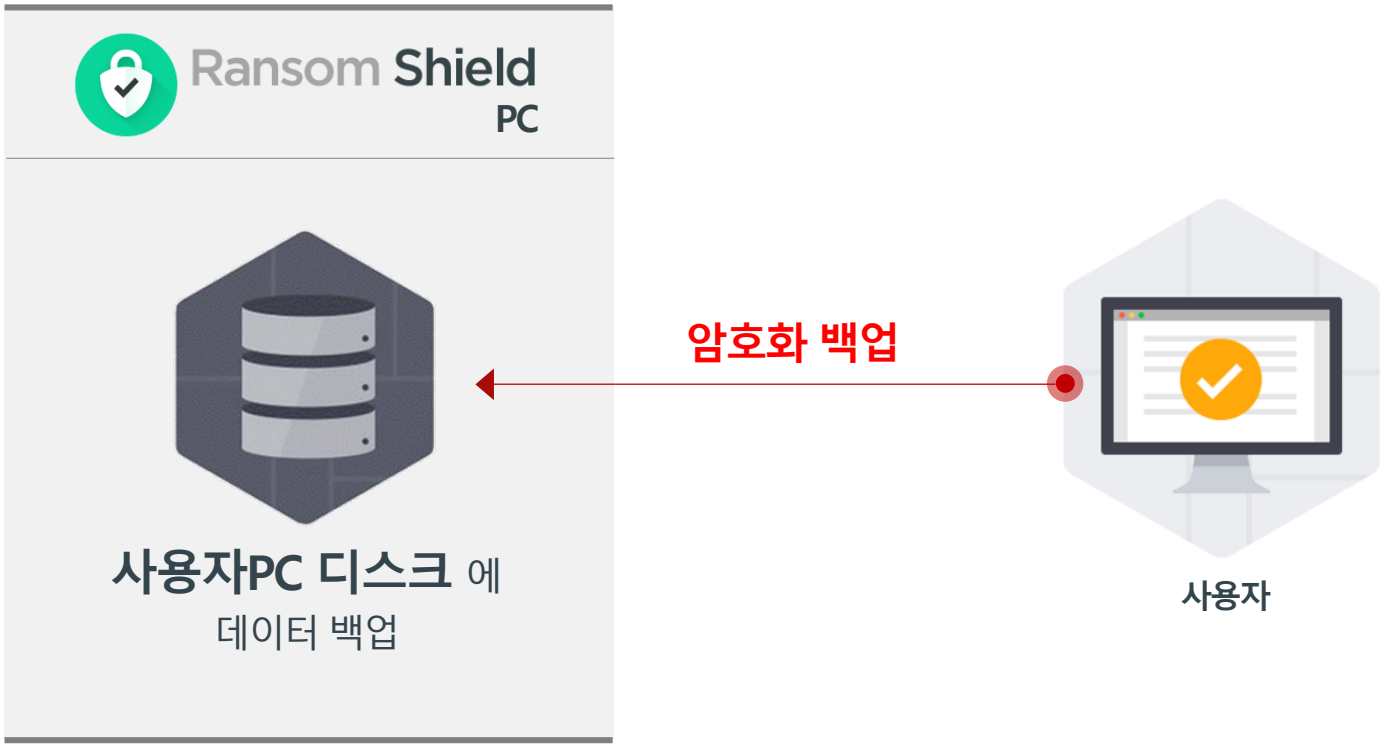
랜섬웨어 대응 솔루션 제안

랜섬웨어 및 바이러스 등 침해 공격에도 실시간 백업된 자료를 통해 안전하게 복구할 수 있는 솔루션



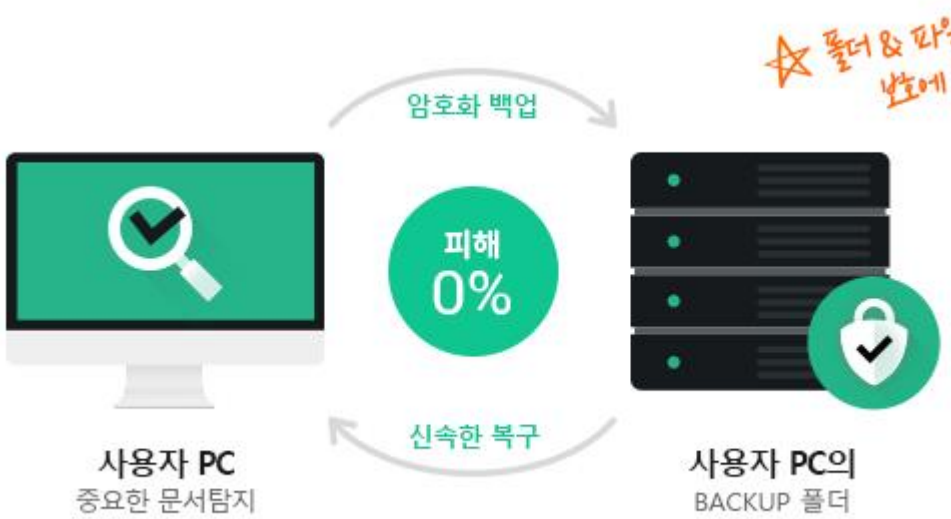
03 솔루션 소개

랜섬쉴드 PC



랜섬쉴드 PC (계속)

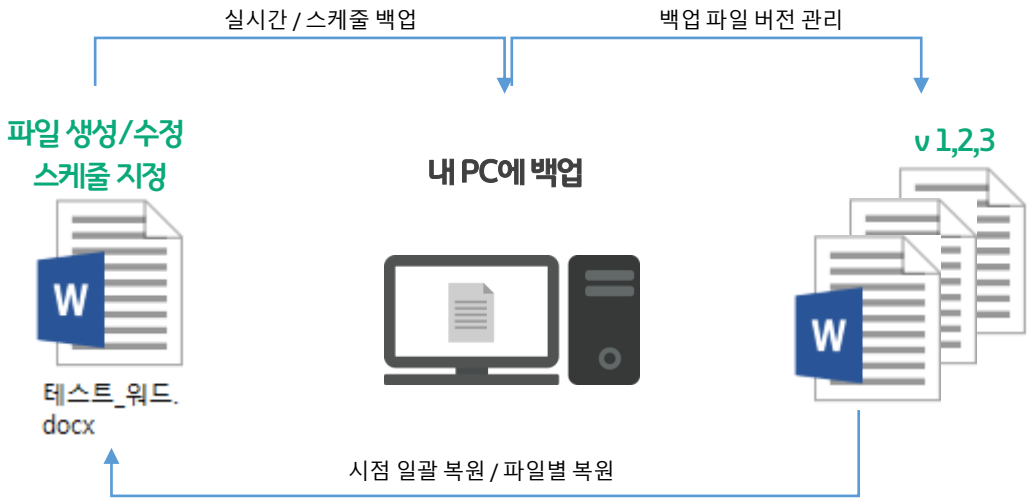
Ransom Shield PC



랜섬쉴드 PC는 사용자 로컬 PC의 데이터 파일 이름과 확장자 내용을 암호화 백업하여 관리합니다.
랜섬쉴드 프로그램 및 백업된 데이터는 자가보호 기능을 통해 랜섬웨어로부터 보호됩니다.

랜섬쉴드 PC (계속)

Ransom Shield PC



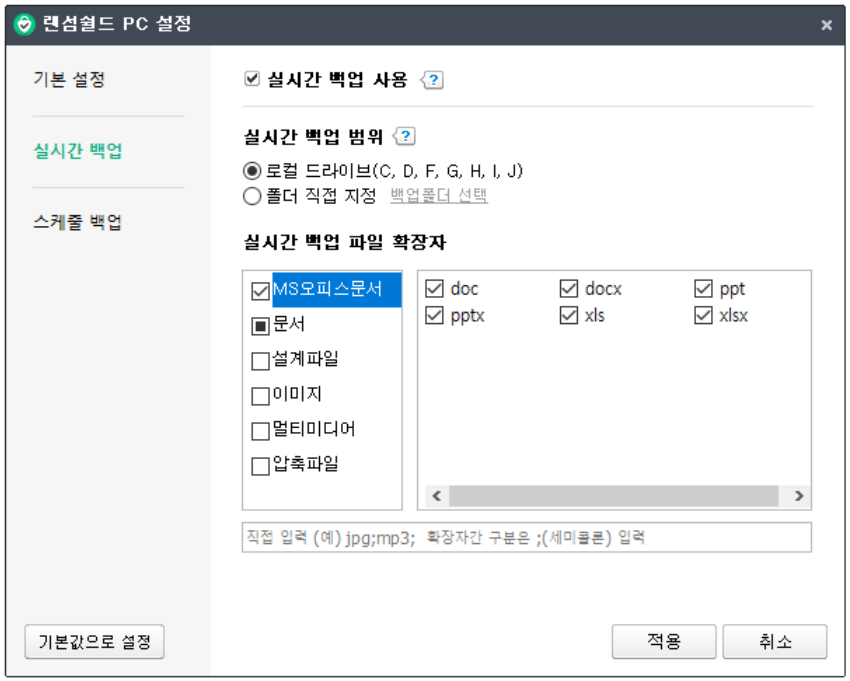
- 암호화 백업과 백업폴더 보호
- 확장자 기반 실시간/스케줄 백업
- 백업 이력 및 사용자 복원/삭제 내역
- 시점 일괄 복원, 선택 버전 복원 지원

랜섬쉴드 PC (계속)

Ransom Shield PC

실시간 백업

- 실시간 백업 기능 on/off 가능
- 실시간 백업 할 범위 및 파일 확장자 선택
- 자주 쓰는 주요 파일 확장자를 카테고리 별로 제공하며, 이 외의 확장자 직접 입력 가능
- 백업 정책에 해당 하는 파일을 생성하거나 수정하면 실시간으로 확인하여 백업

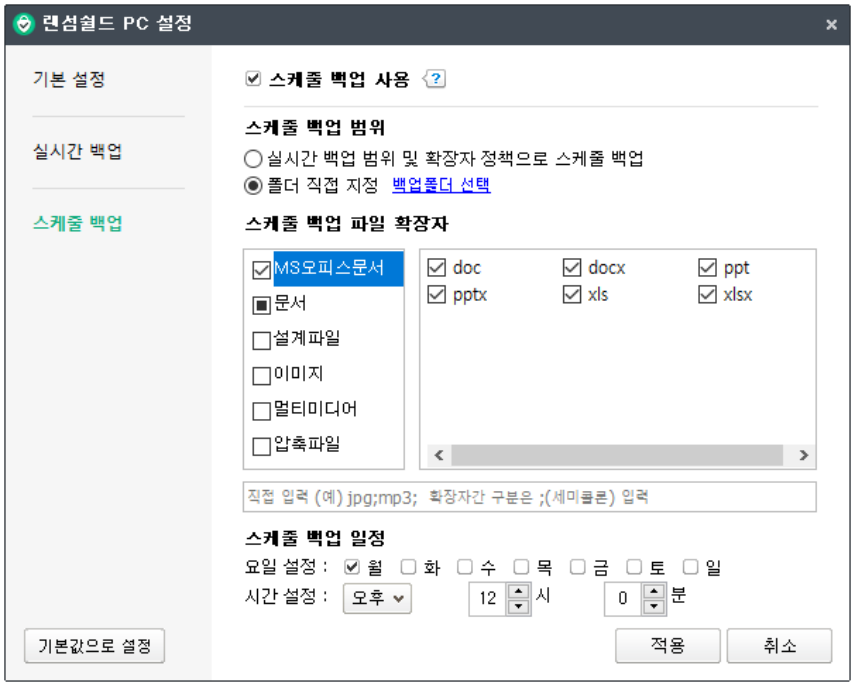


랜섬쉴드 PC (계속)

Ransom Shield PC

스케줄 백업

- 스케줄 백업 기능 on/off 가능
- 스케줄 백업 할 범위 및 파일 확장자 선택
- 실시간 백업과는 별개로 스케줄 백업 정책을 별도로 설정 가능
- 원하는 요일 및 시간을 설정하면 매주 해당 요일, 시간에 백업 정책에 따라 일괄 백업 진행

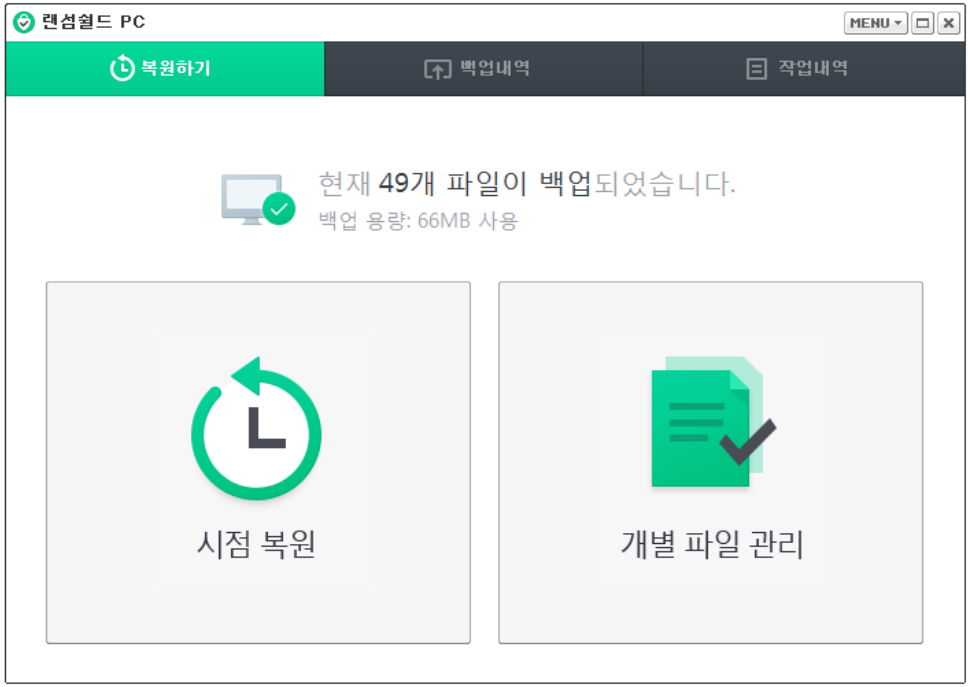


랜섬쉴드 PC (계속)

Ransom Shield PC

쉽고 빠른 복원

- 백업된 총 파일 수와 백업 용량 제공
- 시점 복원 : 지정한 날짜와 시간을 기준으로 전체 파일을 일괄 복원
- 개별 파일 관리: 특정 폴더, 파일만 개별 복원하거나 백업 파일 관리 가능

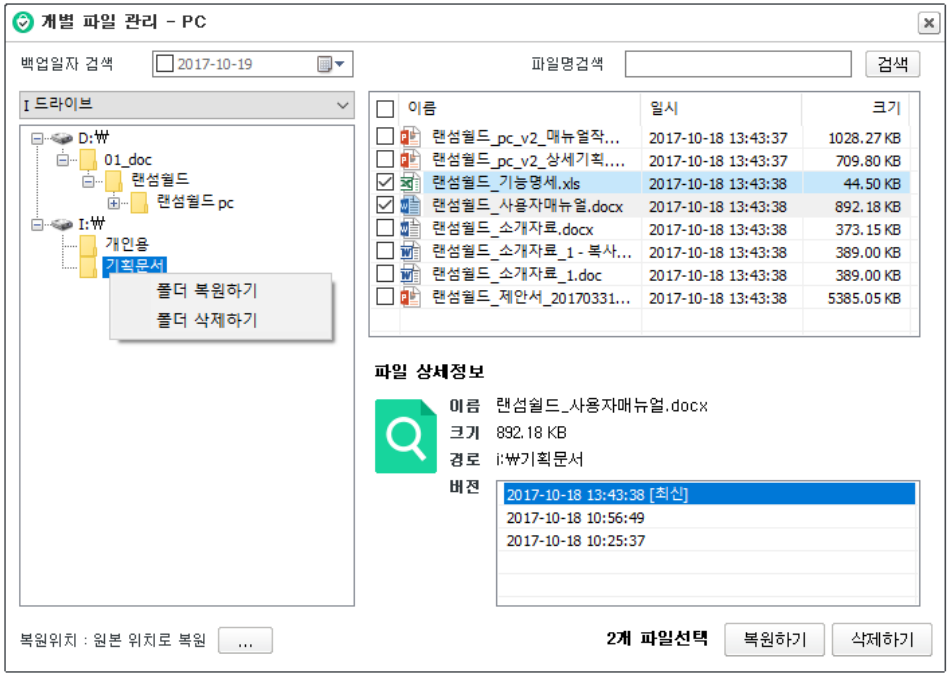


랜섬쉴드 PC (계속)

Ransom Shield PC

쉽고 빠른 복원

- 개별 파일 관리 : 백업 파일 탐색기 제공
- 복원할 폴더/파일을 선택하여 특정 버전으로 복원
- 불필요한 백업 폴더/파일 삭제 가능



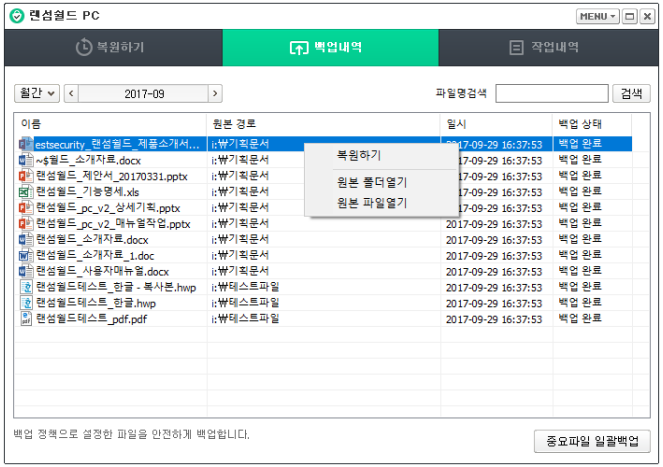
랜섬쉴드 PC (계속)

Ransom Shield PC

백업 내역, 작업 내역

백업과 작업 내역을 통해 히스토리 추적이 가능

- 백업 내역 : 백업 대상 파일의 확인 및 백업 성공 여부 제공
- 작업 내역 : 백업된 파일을 사용자가 복원 하거나 삭제한 내역 제공



랜섬쉴드 PC (계속)

Ransom Shield PC

시스템 운영 환경

사용자 PC

상세 정보

운영체제	기타 사양
Microsoft Windows Vista Microsoft Windows 7 (32/64bit) Microsoft Windows 8 Microsoft Windows 10	■ CPU : Intel Pentium, AMD ■ Memmory : 512M 이상 ■ HDD : 10GB 이상 ■ File System : FAT32, NTFS, GPT ■ 지원 HDD : IDE, SCSI, SATA, SSD HDD 지원

04 Appendix

감사합니다

Contact

TEL : +82-2-3470-2970
FAX : +82-2-6442-9744
E-mail : altools@estsoft.com

EST