DocStory

Your data is safe.

SMTechnology

1등급 GOOD Software

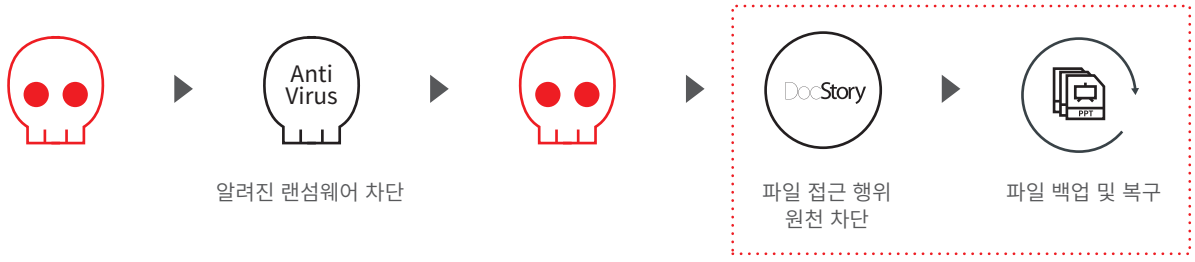
랜섬웨어에 대응하는 바른 자세는 선제적 방어입니다.

감염을 원천 차단하고 감염 즉시 완벽한 복구가 가능하여야 합니다.

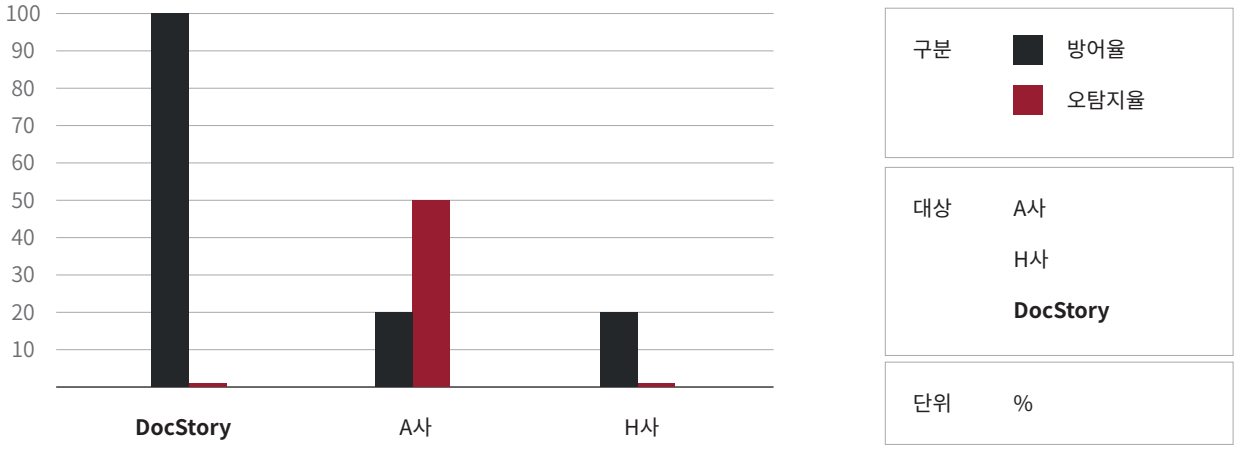
DocStory 솔루션 설치 시 클린 PC를 요구하지 않습니다. 사용하던 PC에 DocStory 프로그램을 설치 후 사용합니다.

- 화이트리스트 알고리즘 적용
- 윈도우 드라이버 차원의 엔진
- 유연한 데이터 접근성
- 시점 백업으로 잘못 저장된 데이터 복구
- 통합 관리툴(사이트) 지원

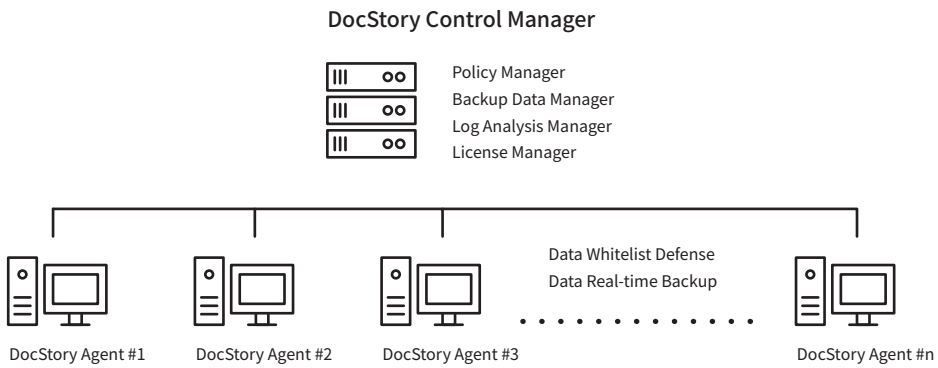
이상적인 랜섬웨어 차단도



한국랜섬웨어침해대응센터 테스트 결과



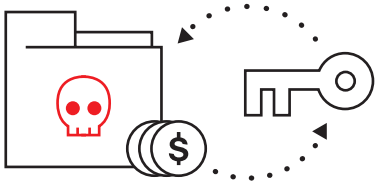
솔루션 구성도



랜섬웨어 바이러스

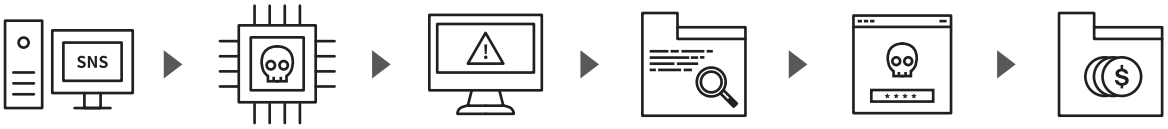
랜섬웨어(Ransomware)란 몸값을 뜻하는 '랜섬(Ransom)'과 '소프트웨어(Software)'의 합성어이며, 파일을 인질로 잡아 금전을 요구하는 악성코드입니다.

- 디지털 파일을 인질로 삼고 비트코인을 대가로 요구합니다.
- 해커가 수익을 얻기 때문에 변종 프로그램이 빠르게 진화하고 있습니다.
- 복구 과정에서 중요/기밀 데이터의 유출 가능성이 있습니다.
- 검증된 인터넷 사이트의 접속만으로 감염될 수 있습니다.



랜섬웨어 침해 프로세스

이메일 등에 악성코드를 심어 PC에 침투를 하거나 오염된 웹사이트 방문 시 침투하여 문서 파일 등을 검색 후 복구할 수 없는 코드로 암호화합니다.



포털 및 SNS 접속 → 악성코드 다운로드 → 랜섬웨어 동작 → 문서 파일 등 검색 → 암호화 수정 → 결제유도

랜섬웨어 해커의 공격대상

데이터 구분	데이터 종류	보관 위치	관리 주체	백업시스템 보유
정형 데이터	ERP DB 전자결재 DB 웹서버 DB	중앙서버/ 스토리지	전산실	대기업/공공: 95% 중소기업: 20%
비정형 데이터	설계도, 인사 회계 자료 구매자료, 공문서 업무관련 사진 외부 수신문서	직원 PC	직원 개인	5% 미만 [설계실 중심]

복구피해

감염 후 데이터 사용 중지 > 업무 중지 또는 비정상적 업무 진행 > 회사/기관의 유무형적 손실 발생

복구 과정에서 금전적 피해 발생과 중요/기밀 데이터 유출 가능성 상존

비트코인 송금 후 복호화 키 미접수 혹은 오류 키 접수로 복구 불가능

국내 랜섬웨어 공격 특징

2016년부터 4GB 이상 대용량 파일도 암호화 시키고 서버의 DB를 감염시키기 시작했습니다. 특히 XTBL과 Glove3와 같은 랜섬웨어는 주로 병원의 EMF DB와 같은 민감한 데이터를 감염시켜 1,000만 원 이상의 복구비용과 업무 진행의 어려움을 겪은 사례가 있습니다.

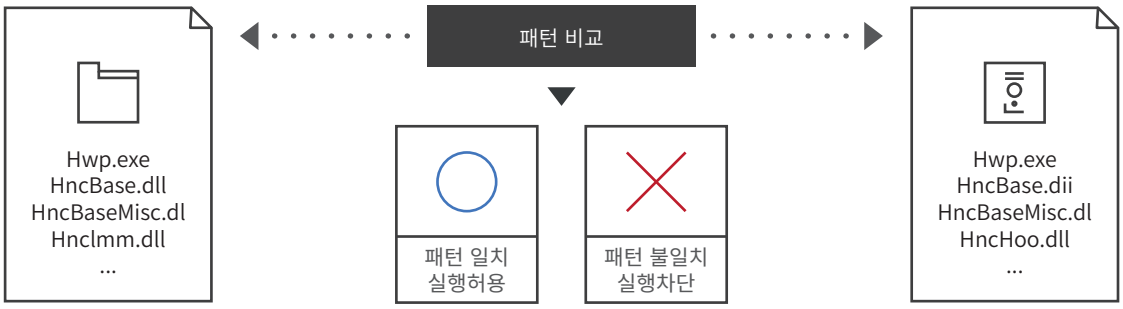
국내 랜섬웨어 피해자의 공통점

피해자들은 대부분 최소 백신을 사용하고 있었고, 50% 이상의 기업과 기관이 방화벽 등 보안 솔루션을 도입하고 있었습니다.

화이트리스트 알고리즘

AWD(Adaptive WhiteList Defense)

문서를 편집하려는 애플리케이션 경로와 디지털 서명 등을 화이트리스트와 비교하여 지능적이고
능동적인 데이터 입출력 신뢰성을 검증합니다.



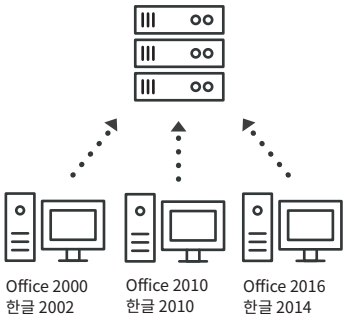
명령어 및 목적 프로세스 기반의 화이트리스트 제어

신뢰하지 않는 애플리케이션, 프로세스에 의한 파일 공격 시도가 발생하면 해당 행위를 중지하고,
해당 로그를 실시간 서버로 전송하고 관리자에게 직관적인 알림과 보안 상태 정보를 알립니다.

타사	DocStory
실행 파일에 대한 화이트리스트 방식	윈도우 드라이버 차원의 엔진
중앙 통제 방식의 관리 이슈 발생	유연한 데이터 접근성 확보
사용자 불편 가중	주요 데이터 탈취 통제
백업 중심	설정에 따른 화이트리스트에 없는 직접 접근 가능
	자동화 화이트리스트 생성

화이트리스트 자동화

개별 PC마다 사용하는 프로그램의 버전이 다를 경우 화이트리스트를 자동적으로
생성하여 운영 관리의 유연화와 사용자 편의성을 높게 고도화하였습니다.



1. 파일에 대한 접근 권한을 화이트리스트 목록에 맞게 권한을 설정한다.
2. 화이트리스트 목록에 없더라도 사용자 실행일 경우 허용한다.

PC 별 화이트리스트를 서버로 전달 > 다수의 PC에서 동일한 화이트리스트가 존재할 경우 Group으로 생성 > 그룹원의 PC에서 화이트리스트를 추가할 경우 Group 전체에 동일한 화이트리스트 정책 사용

사용자 실행 허용 및 불허 2가지 권한 조정

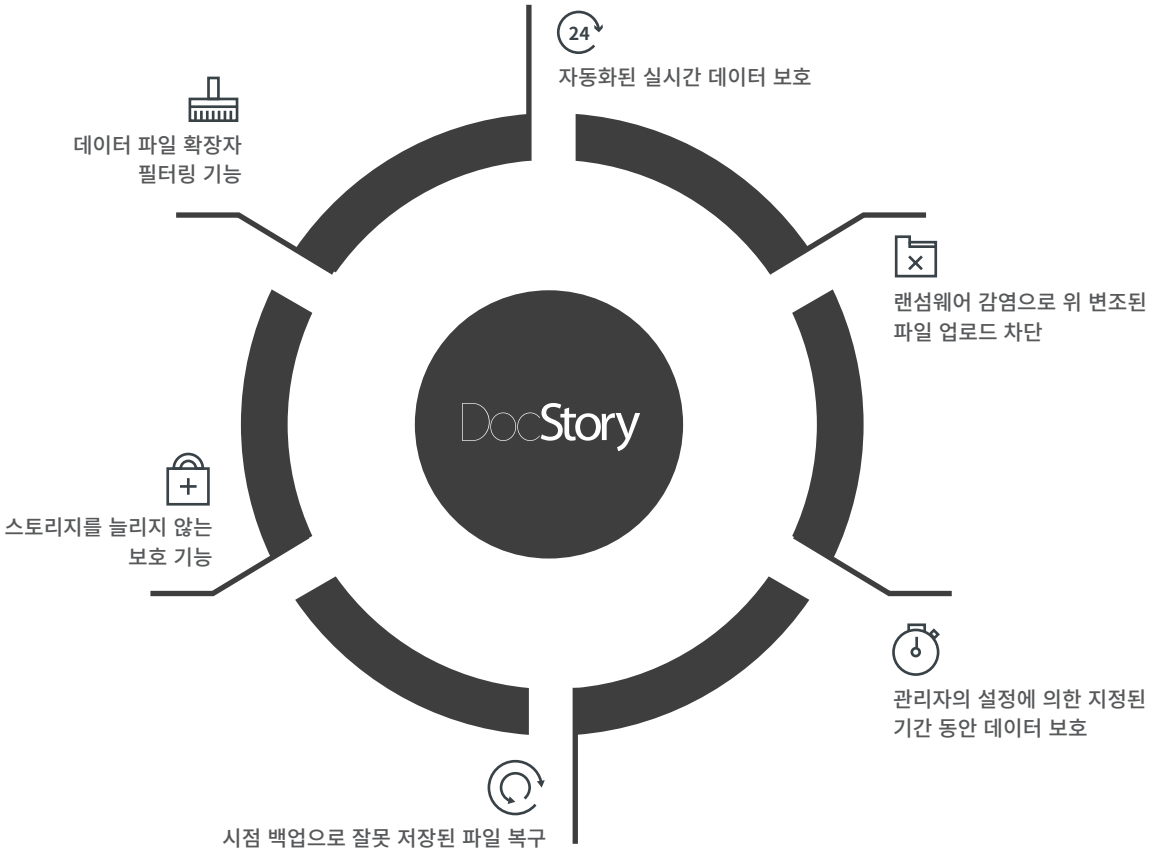
사용자의 실행에 대하여 허용 및 불허에 대한 두 가지 권한을 조정할 수 있습니다.
관리자의 보안 설정으로 조직의 특성에 맞게 유연성을 높일 수 있는 장점이 있습니다.

실시간 자동 백업 및 툴

DocStory 시스템

DRB(Data Realtime Backup)

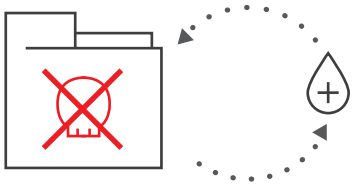
생성·수정되는 주요 문서에 대하여 서버로 실시간 백업하는 기능을 하고, 설사 랜섬웨어 등 악성코드로 인하여 자료가 훼손되는 경우가 발생하더라도 원하는 시점의 자료로 원상 복구할 수 있습니다.



2가지 복구 기능

시스템 과부하를 최소화하면서 실시간 백업의 막강한 기능을 탑재했습니다.
시점별 백업 기능으로 특정 시점 이전으로 되돌릴 수 있고, 파일 하나하나 확인 후 복구 가능합니다.

1 감염된 파일을 백업 파일로 복구



2 웹브라우저에서 다운로드 형태로 백업 파일 제공

랜섬웨어에 대응하는 바른 자세는 'DocStory'입니다.

평생 모은 자료를 집어 삼키는 최악의 바이러스 랜섬웨어로부터 지킬 수 있는 유일한 방법은 'DocStory'입니다.

운영을 위한 클라이언트 컴퓨터 사양

구분	최소 사양	권장 사양
프로세서(CPU)	1GHz 이상 32 비트(x86) 프로세서	1GHz 이상 64 비트(x64) 프로세서
램(RAM)	1GB RAM(32 비트) 이상	2GB RAM(64 비트) 이상
하드디스크(HDD)	16GB 사용 가능 하드디스크	20GB 사용 가능한 하드디스크
운영체계(OS)	Microsoft Window 7 (32bit, 64bit) Microsoft Window 8 (32bit, 64bit) Microsoft Window 8.1 (32bit, 64bit) Microsoft Window 10 (32bit, 64bit)	

관리자 모듈 운영 및 백업 공간 확보를 위한 서버 사양

하드웨어 권장 사양		지원 환경	
프로세서(CPU)	Intel Pentium급 이상	운영체계(OS)	CentOS 6.5 이상
램(RAM)	16GB 이상	지원 WAS	Apache Tomcat
하드디스크(HDD)	1TB 이상	지원 DB	MariaDB 5.0 이상
HDD 여유 공간	4TB 이상		