

DocStory

ENDPOINT 데이터보호 솔루션 (EDR 확장팩 Ai edition)



BEONE SYSTEM

EDR과 상호보완

DOCSTORY는 기존의 EDR, 백신 등 타 보안 제품들에서 취약한 부분인 데이터 보호를 중점적으로 할 수 있는 최적의 솔루션 (상호 보완 제품)
EDR이 없는 기업도 해킹, 데이터 감염, 유출 피해 방지에 꼭 필요한 최적의 데이터 보안솔루션 (단독 제품 사용 가능)

DOCSTORY (EDR 확장팩)



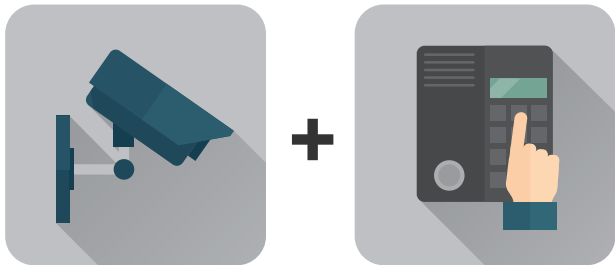
정보 보안과 시설(물리) 보안

무단 침입자를 방지하고, 화재 등 안전사고를 막는 일.
대표적으로 신분증과 출입통제 시스템(도어락), CCTV, 보안검색대, 소방시설 관리 등이 있음. 주로 기관, 기업 등에서는 물리보안이라고 함.

< EDR (Endpoint Detection & Response) 개념 >

출처 - 서울 시청

구 분		EDR (사이버 보안)	CCTV (물리 보안)
목 적		IT환경에서 신종 보안위협 탐지·대응	물리적 공간의 모니터링, 감시
대 상		PC, 서버 등 엔드포인트	물리적 특정공간(건물 내부 등)
역 할	수 집	PC 행위 정보 저장	영상 데이터 녹화
	탐 지	이상행위탐지 및 분석	침입자 및 비정상적 행동 감지
	대 응	파일 격리, 네트워크 차단 등	보안 요원 출동, 알람 울림 등
	분 석	사고시 공격경로와 침해사고 원인분석	사고시 영상 재확인 및 증거 활용



< DOCSTORY AI edition(EDR확장팩) 개념 >

구 분		DOCSTORY(데이터 보안)	도어락 (물리 보안)
목 적		IT 환경에서 신종 보안위협 탐지·대응	물리적 행위의 출입 방지, 차단
대 상		PC의 모든 데이터 파일	물리적 특정공간(건물 입구, 내부 등)
역 할	보 안	AI 자동 판단으로 높은 보안과 편리한 관리	상시 경비 인력에 대한 부담감 해소
	탐 지	주요 실행 파일 이상 행위 탐지 및 분석	정해진 출입자 외 출입 금지
	대 응	주요 실행 파일 탈취 시도 시 차단 및 종료	비정상 출입 시도 시 도어락 차단
	알 림	훼손된 파일 자동복구 및 관리자 알림	출입자 기록 확인 및 관리자 알림



기업 시설 보안시스템



DocStory

100여가지 국가용 보안기능 요구사항에 대한 시험을 통과하여 확보된
DOCSTORY의 차세대 데이터솔루션
10만개 이상의 DATA를 AI를 기반으로 자동 차단



GS 인증
1등급 Software



국가정보원
보안기능 확인서
국내 최초 발급



나라장터 등록
물품식별번호
23181932

대상

✓ 지자체 등 관공서 ✓ 공사/공단등 정부 산하기관 ✓ 지방 교육청등 교육기관 ✓ 공기업 ✓ 사기업 ✓ 병원 ✓ 학교 등

특징



보안기능확인서의
내용에 충실한 구성



사전차단 보안 엔진
(능동형 화이트리스트 엔진)

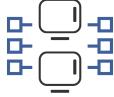


관리서버의
에이전트 통제

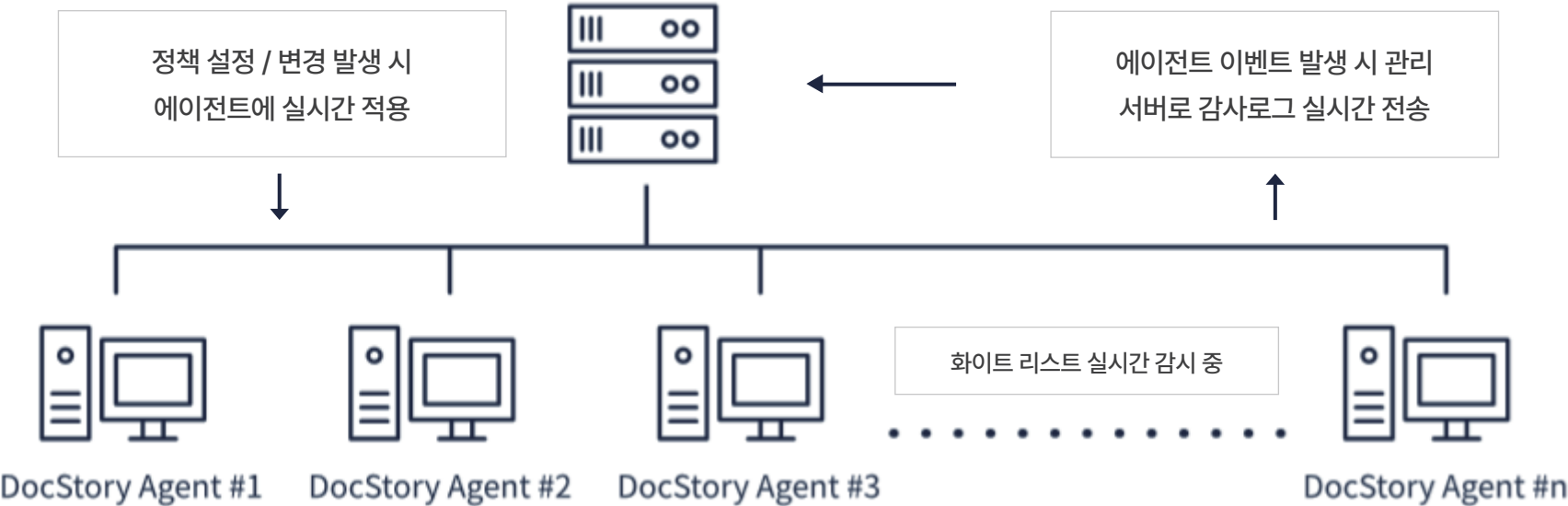


다양한 감사로그



 서브스크립션 형태의 그룹 별 보안 서비스	 전산실 운영 여건 어려운 환경에도 가능
 보안 관리자 부재 또는 상시 관리가 어려운 환경에도 가능	 신속하게 대응하는 기술 지원 서비스

관리 서버



자체 보안 엔진

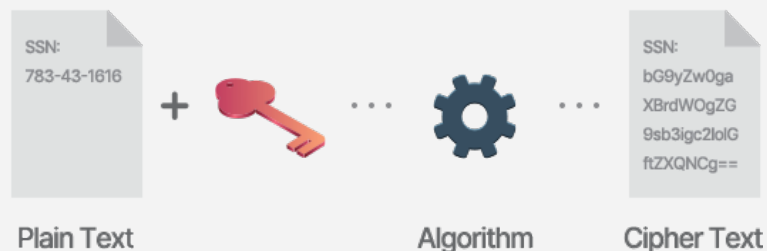
국정원 검증 기준에 따른 기밀성/무결성/가용성 검증 테스트 충족

| 우리나라 국가, 공공기관에 대한 사이버 위협에 대응하기 위한 '보안요구사항'의 모든 항목을 준수하여 관리서버와 에이전트의 보안 기능을 구현

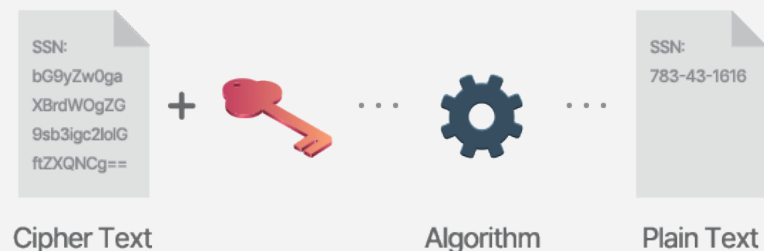
기밀성 확보

- 로그인 시 비밀번호 생성 규칙을 준수하고, 사용자 계정 정보의 암호화 하여 안전하게 저장합니다.
- 관리서버와 에이전트의 운용 중 발생하거나 전달되는 주요 데이터는 암호화되어 저장되거나 암호화되어 통신 됩니다.
- 주요 파일은 숨겨진 상태로 보관되고 사용되는 암호키는 국정원 보안 인증 규격을 준수합니다.

Encryption

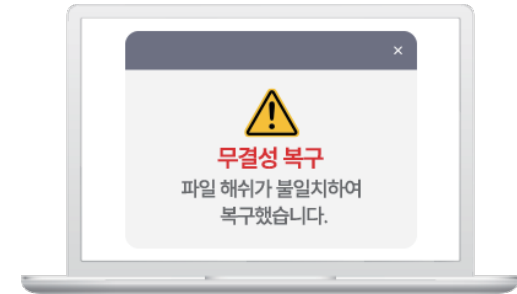


Decryption



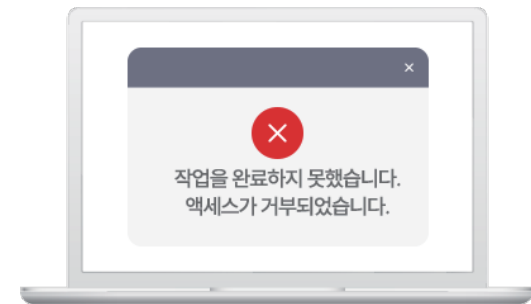
무결성 확보

- 에이전트와 관리서버의 주요 실행파일과 운용되고 있는 주요 프로세스들은 안전한 운용을 위하여 주기적인 무결성 검증을 진행합니다.
- 무결성 검증 시 훼손된 파일들은 자동 복구되며, 이에 대한 정보는 즉각 관리자에게 통보됩니다.
- 무결성 검증 진행 절차는 국정원 보안 인증 규격을 준수합니다.



가용성 확보

- 파일 변경 권한을 얻기 위한 권한 변경 시도를 차단합니다.
- 주요 실행 파일 삭제 시도를 차단합니다.
- 주요 실행 프로세스 중지 시도를 즉시 합니다.
- 세션 탈취 시도를 차단하고 정지된 상황이 일정 시간 이상인 경우 세션 자동 종료됩니다.



사전 차단 엔진

실시간 랜섬웨어 자동 탐지 및 차단 기능

| DOCSTORY는 고정된 패턴이 아닌 방식으로 동작하여, 탐지 기능이 별도 갱신 없이도 최신 보안 위협에 대응

위험한 프로세스 및 데이터로부터 보호 대상 파일 접근을 실시간 사전 차단 함으로써 **훼손 및 유출방지**



AI 자동분류 엔진

불편하고 어려울 수 있는 화이트 리스트 보안의 관리 구간을 AI가 자동으로 분류

| 차별화된 'AI 능동형 화이트 리스트' 알고리즘

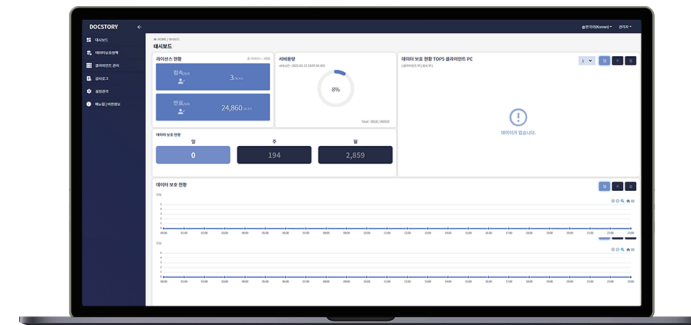
DOCSTORY AI 자동분류 엔진을 통한 화이트 리스트 보안



업무에 영향을 주지 않고 설치되며, 안전한 시스템 운용 환경

설치부터 실 운용까지 안전하고 편리한 진행

| 사용자 개입이 없는 스텔스 설치부터 사용자 PC에 아무 영향 없는 운용 시뮬레이션으로
최적의 정책을 설정하고, 안정적 환경에서 점진적으로 실 운용 전환



PMS 설치

업무 중단 없는
스텔스 설치

업무중단 無

레거시 충돌 無

운용 시뮬레이션

실 운용과 동일한 환경에서
정책 설정 안정화

단계별 실 운용

부서별, 지역별
실 운용 환경으로 전환

업무 연속성 유지

리소스 사용 최소화

안정적 운용

지속적 기술지원
안정적인 패치지원

DocStory 화이트리스트 보안 기술

인가되지 않은 프로세스가 보호대상에 접근하는 것을 **사전 탐지** 하여 악성행위에 대응합니다. DocStory는 랜섬웨어를 포함한 모든 악성코드의 공격으로부터 **데이터를 보호** 합니다. 검증받은 자동분류 엔진과 AI를 접목하여 **높은 보안**과 **관리의 편의성**을 극대화 하였습니다.

DocStory 화이트리스트 보안 기술

승인된 파일 이외 모든 외부 접근 사전 차단 신/변종 악성 위협요소를 사전 차단하여 근본적인 대응이 가능



DocStory 도입효과 및 장점



DocStory

알려지지 않은, 그리고 진화하는 악성행위의 공격으로부터 최선의 방어는 “완벽한 사전차단” 입니다.



사전 위협 차단 엔진

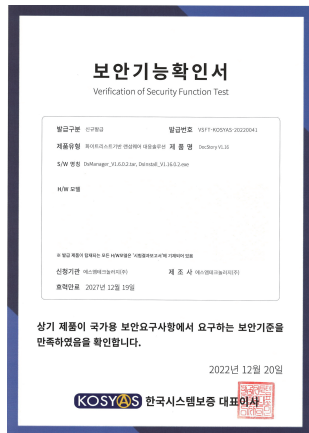
DocStory는 ‘제로트러스트’ 방식을 이용하여 인가되지 않은 접근으로부터 데이터를 보호함으로써 암호화, 삭제 및 유출 등의 위협에 사전 대응합니다. (특허취득)

지능형 자동화 (AI) 엔진

제로 트러스트의 불편함을 극복하기 위하여 신뢰할 수 있는 프로세스를 자동 선별함으로써 관리자의 업무능률을 최적화 하였습니다. (특허취득)

강력한 자체 보호

보안기능확인서를 통한 ‘국가용 보안요구사항’ 만족에 그치지 않고, 더욱 철저한 자체 보안 기준에 충족하도록 개발되어 위협에 적극적으로 대응합니다. (보안기능확인서)



DocStory 프로세스



관리 모듈의 주요 기능

설치 및 감사 로그 기능

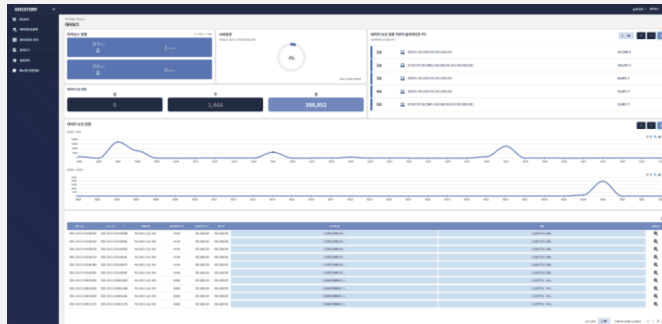
| 대시보드를 통한 직관적인 정보 제공, 다양한 설정을 통한 효과적인 정책 설정, 다양한 상황에 따른 감사 로그

대시보드를 통한 직관적인 정보 제공

- 시간/주간/월간 별 실시간 보호 이벤트 발생 현황을 제공합니다.
- 대시보드 그래프의 특정 상황에 대하여 상세한 정보를 제공합니다.

다양한 설정을 통한 정책 설정

- 솔루션 기능/클라이언트 버전 주기/에이전트 삭제 권한 등 기본 환경 정책 설정을 제공합니다.
- 프로세스 중지 기능/프로세스 차단 한계 설정 등 보호 환경 정책 설정을 제공합니다.
- 로그보존일수/클라이언트 로그/로그 표시 시간/로그 제목 및 내용 등 로그환경에 대한 정책 설정을 제공합니다.
- 관리자 정보 및 권한/업데이트 파일 등록 및 배포 등 다양한 정책 설정을 제공합니다.

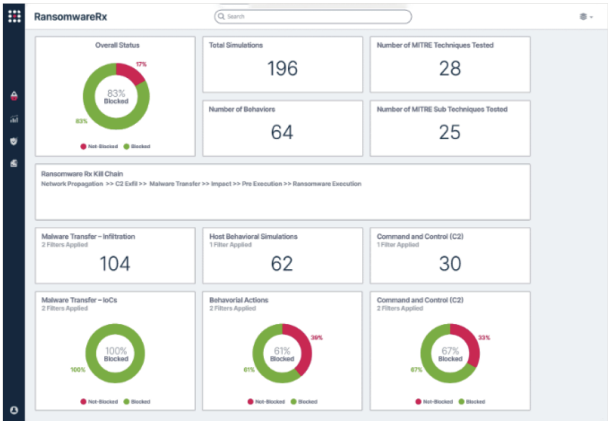
[illegible]

다양한 상황에 따른 감사 로그

- 비인가 프로세스가 보호 대상 파일에 접근과 차단 등 파일 보호 이벤트 로그를 제공합니다.
- 관리자 모듈의 설정 변경하거나 운영 환경에 이벤트 발생할 시 이벤트 로그를 제공합니다.
- 관리자의 로그인/로그아웃에 관한 로그와 로그인 시도 실패에 대한 로그를 제공합니다.
- 에이전트의 무결성/기밀성/가용성과 관련된 주요 이벤트에 대한 로그를 제공합니다.
- 관리자에 의한 감사로그 열람 이외 수정/삭제와 관련한 접근 기능을 제공하지 않습니다.
- 리포팅을 위한 주요 보안 위협에 대한 감사로그를 엑셀 파일로 변환하여 받을 수 있도록 기능을 제공합니다.

DocStory의 보안성

- 국내 공기업 및 관계사 도입을 위한 실제 시험 평가 데이터
- 해당 공기업 보안 책임자가 직접 시험 주관
- 세이프브리치라는 사이버 킬체인과 마이터 어택을 접목한 해킹 및 공격 시뮬레이션 솔루션을 이용한 보안 검증 테스트
- 비교 평가를 위해 실 업무와 동일한 환경의 PC에 V3와 **Docstory**, 윈도우 디펜더를 각각 설치하여 검증 테스트 실시

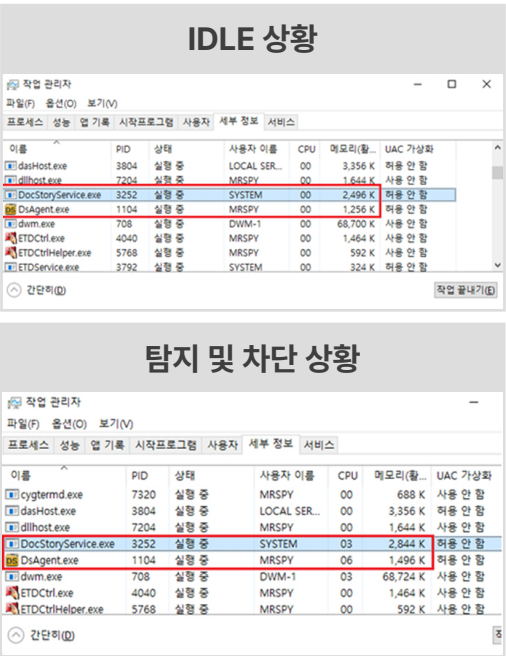


테스트 환경	총 침투 테스트 수	차단 성공	차단 실패	차단 성공률
V3	281	158	123	56.23%
윈도우 디펜더	281	165	116	58.72%
Docstory	281	272	9	96.80%

[테스트PC 사양: Windows10 Professional 64Bit, CPU 4코어, RAM 16GB, HDD SSD500G]

DocStoryPC는 내 최소의 부하로 충돌없이 운용 가능한
저용량의 에이전트 솔루션입니다.

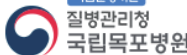
- 비인가 프로세스의 보호대상 접근 시 외에는 부하 발생 최소화
- 관리서버와 통신을 최소화하여 네트워크 부하 없음
- 많은 시간, 다수의 PC에서 운용 보완하여 타 솔루션과 충돌 없음
- 저용량의 에이전트 운용으로 설치가 용이



구분	IDLE 상황		탐지 및 차단 상황	
	Docstory Service	DsAgent	Docstory Service	DsAgent
CPU 점유율	0%	0%	3%	6%
메모리 사용량	2,496Kbyte	1,256Kbyte	2,844Kbyte	1,496Kbyte

주요 구축 실적

국내 기업을 비롯, 공공 기관 및 지자체 30여곳 이상 서비스 중

광역지자체		지자체				기타 공공					
경북도청	대구시청	광주북구청	강릉시청	원주시청	구미시청	 청와대	 해양경찰청 KOREA COAST GUARD	 책임운영기관 질병관리청 국립목포병원			
		평창군청	상주시청	양양군청	영천시청						
		김제시청	속초시청	영암군청	인제군청						
		안동시청	군위군청	양구군청	순천시청						
강원도청	전남도청	목포시청	해남군청	의왕시청	고성군청				 한국농어촌공사	 경상북도 소방본부 Gyeongsangbuk-do Fire Service Headquarters	 문화체육관광부 국립국어원
		영월군청	강진군청	보성군청	신안군청						
		칠곡군청									

대기업군		중견기업군		방송 및 금융		교육 및 기타	
 LS전선		 arneg KOREA  YOUNGYIEL  SENSORVIEW		 TBC 더케이 한국고직원공제회 The·K 저축은행		 KUKKIWON WORLD FREEDOMSHIP HEADQUARTERS  남부대학교 NAMBU UNIVERSITY	
		 trueFriend 한국투자증권		 은행연합회 KOREA FEDERATION OF BANKS			

구매 상담 문의 | T. 02-719-2494 / E. b1system@b1sys.co.kr

Endpoint Data Protection

BEONE SYSTEM

(주)비원시스템

서울 강서구 공항대로46길 13-20

T. 02-719-2494

H. www.b1sys.co.kr

E. b1system@b1sys.co.kr