DocStory

ENDPOINT 데이터보호 솔루션

(EDR 확장팩 Ai edition)

SMT

1. 국내 사이버 위협 동향과 리스크

국내 사이버 침해사고 피해가 전년 대비 크게 증가했습니다. 2024년 한 해 침해사고 피해는 전년 대비 약 48% 증가했고,
랜섬웨어 감염은 195건이 공식 집계되었습니다. 피해의 94%가 중견·중소기업에 집중되었습니다.

개인정보 유출 신고도 고위험 양상입니다. 2024년 307건의 유출 신고가 접수되었고, **'해킹이 56%'**로 최다 원인이었습니다.
이는 단순 시스템 장애가 아니라 의도적 침해와 금전·협박 목적의 공격이 다수를 차지함을 의미합니다.

공격은 **'데이터 자체(문서·자료)'**를 직접 겨냥합니다. 감염·침입이 탐지된 이후 대응만으로는 **'유출·변조·삭제·암호화(랜섬)'**를 막기에 늦습니다.

공공/지자체/기업 환경은 결재·보고·대민 업무가 PDF/한글/Word/PPT 등 문서 중심으로 이루어져 **'데이터 실물(파일)'**의 보호가 곧 업무 연속성입니다.

결론 - '탐지 중심(EDR)'만으로는 부족하며, 데이터 접근 단계에서의 사전 차단을 병행해야 실질적인 피해를 줄일 수 있습니다.

< 한국인터넷진흥원(KISA) 유형별 침해사고 신고 건수 >

구분 \ 연도		2023 (상반기)	비율	2023 (하반기)	비율	2024 (상반기)	비율	2024 (하반기)	비율
침해사고 신고	DDoS 공격	124	18.7%	89	14.5%	153	17.0%	132	13.4%
	악성코드	**156**	**23.5%**	**144**	**23.5%**	**106**	**11.8%**	**123**	**12.4%**
	(랜섬웨어)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)	(103)	(10.4%)
	서버 해킹	320	48.2%	263	42.9%	504	56.1%	553	56.0%
	기타	64	9.6%	117	19.1%	136	15.1%	180	18.2%
합 계		664		613		899		988	

2. EDR 한계와 병행 아키텍처

EDR은 엔드포인트에서 발생하는 행위를 탐지·분석·대응하는 도구입니다.
로그·이벤트 분석으로 침투 경로나 이상행위를 찾아내지만, 데이터 접촉 단계에서의 사전 차단은 역할 범위를 벗어납니다.

결론 - EDR은 필수이지만 사후 탐지·대응 중심이므로, 데이터 접근 통제와 보호를 담당할 솔루션을 함께 운영해야 공백이 없습니다.

■ 병행 운용 시 성능·충돌 우려 해소

DOCSTORY는 데이터 접근 시에만 동작하는 경량 에이전트 구조입니다.
관리 서버와의 통신 최소화로 네트워크 부하가 거의 없고, 다수 환경에서 타 솔루션과 충돌 없이 운영 중인 사례가 축적되어 있습니다.

따라서 EDR과 역할 중복 없이 상호 보완하며, 체감 성능 저하 없이 병행 운용 가능합니다.

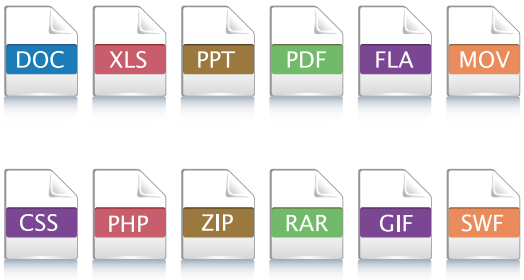
요지: 탐지(EDR) + 차단(DOCSTORY) 병행으로 공백 해소

3. 문서 중심 업무환경의 데이터 보호 필요성

공공기관·지자체·대다수 기업의 업무 산출물은 문서파일입니다.
결재·보고·대민 공지·입찰/계약·감사 대응까지 PDF/한글(HWP)/Word/PowerPoint 등의 직접적인 데이터 파일로 생성·유통·보관됩니다.

즉, 공격자는 바로 이 문서파일을 암호화(랜섬), 유출(내부자/외부자), 변조(위변조 공문), 삭제(감사자료·증빙 파괴)하려고 하며,
이는 EDR의 탐지/분석만으로는 접근 순간의 차단이 어렵습니다.

- 문서 중심 업무 환경에서 발생하는 대표 시나리오
- 결재 전/후 파일이 메일·메신저·클라우드·USB로 이동하는 과정에서 무단 복제·유출
- 편집기/뷰어/변환 프로그램이 위장·악성화되어 민감 문서에 접근 시도
- 외부 민원/제안서 접수 파일 열람 중 매크로·취약점을 노린 공격이 내부 문서에 연쇄 접근
- 프로젝트/입찰 산출물이 압축·전송·백업되는 순간에 벌어지는 권한 외 접근



따라서 보안의 최종 목적(중요 데이터의 안전)을 달성하려면, 문서파일에 대한 접근 자체를 통제하는 데이터 보안 솔루션이 필수입니다.

DOCSTORY는 보호 대상(문서·자료)에 접근하려는 프로세스를 사전 분류/검증 후 차단하여, 유출·삭제·암호화 피해를 접근 단계에서 원천 차단합니다.
또한 정책은 업무 흐름을 방해하지 않도록 설계되어 기존 결재/협업 도구와 병행 운용이 가능합니다.

4. DOCSTORY 적용 제안(도입/운영·기대효과)

도입: 스텔스 설치 → 모니터링 모드 → 단계적 전환(업무 중단 없이)

■ 핵심

- 제로트러스트 기반 사전 차단 엔진: 보호 대상 파일에 접근하려는 프로세스를 AI 자동 분류 → 신뢰 불가 시 즉시 차단.
- AI 능동형 화이트리스트: 승인 애플리케이션은 원활, 미인가 프로세스는 구조적으로 차단.
- 감사·가시성: 접근 이벤트·정책 적용 이력·차단 로그 제공(감사·보안점검 대응).

■ 기대 효과

- 유출·변조·삭제·암호화(랜섬) 등 데이터 피해 시나리오를 접근 단계에서 원천 차단.
- EDR과 역할 중복 없이 상호 보완하여 탐지(EDR)+차단(DOCSTORY) 이중 방어 완성.

■ 도입·운영 방식(업무 연속성 보장)

- 스텔스 설치 → 운용 시뮬레이션(모니터링 모드) → 단계적 실운영 전환으로 업무 중단 없이 안착.
- 부서/현장 단위 점진적 정책 적용으로 레거시 충돌 최소화.
- 관리 서버 통신 최소화와 경량 에이전트로 체감 성능 저하 없이 운영.
- 대시보드·리포트로 정책 최적화와 감사 대응을 지원.

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

대 상

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

특 징

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 환경**에도 가능

보안 관리자 부재 또는 **상시 관리가 어려운 환경에도 가능**

신속하게 대응하는 **기술 지원** 서비스

관리 서버

정책 설정 / 변경 발생 시
에이전트에 실시간 적용

에이전트 이벤트 발생 시 관리
서버로 감사로그 실시간 전송

화이트 리스트 실시간 감시 중

DocStory Agent #1 DocStory Agent #2 DocStory Agent #3 DocStory Agent #n

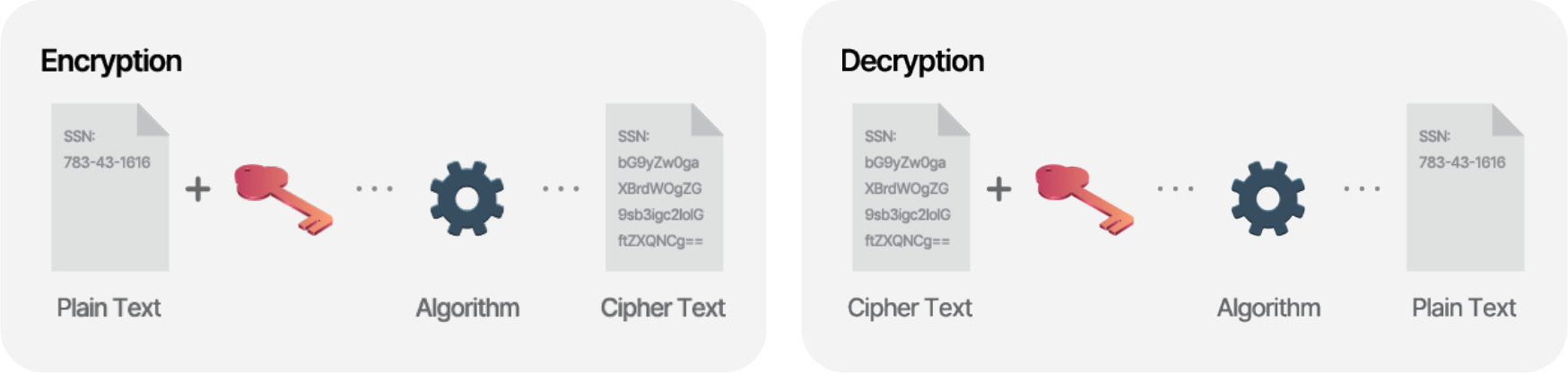
자체 보안 엔진

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

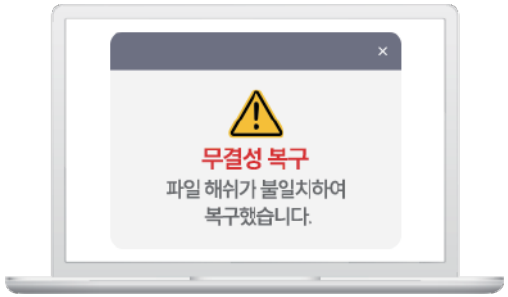
기밀성 확보

- 로그인 시 패스워드 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.



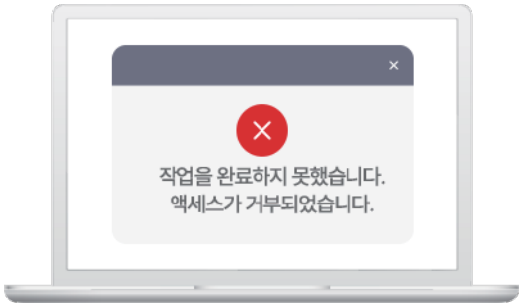
무결성 확보

- 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.

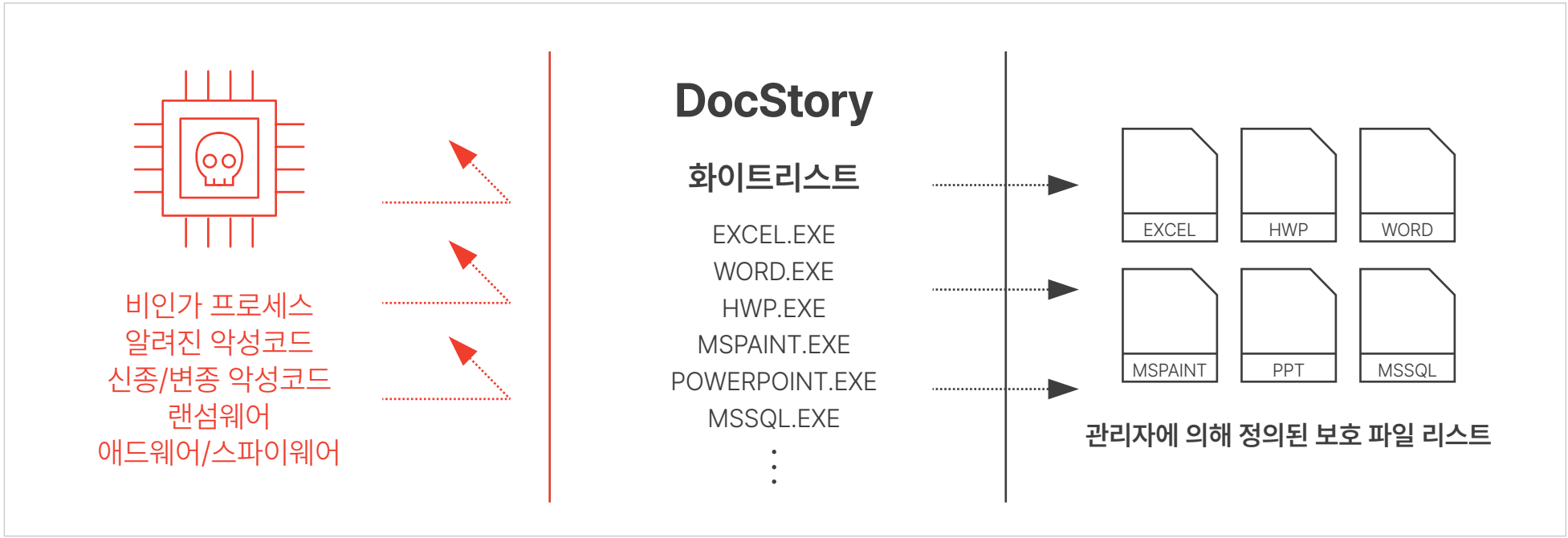


사전 차단 엔진

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 보완

강력한 보안 인가되지 않은 프로세스는 보호대상 파일에 접근이 불가능	**강력한 보안 유지** 기존 화이트리스트 보안 강점을 계승
유연성 부족 새로운 프로그램 도입 및 업데이트 시 매번 화이트리스트 등록이 필요	**AI 를 통한 자동화** AI 를 이용한 프로세스 자동 등록
관리의 어려움 화이트리스트 DB에 없는 프로세스에 대한 관리의 어려움	**관리 부담 감소** 자동 분류 엔진을 통하여 편의성 향상

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

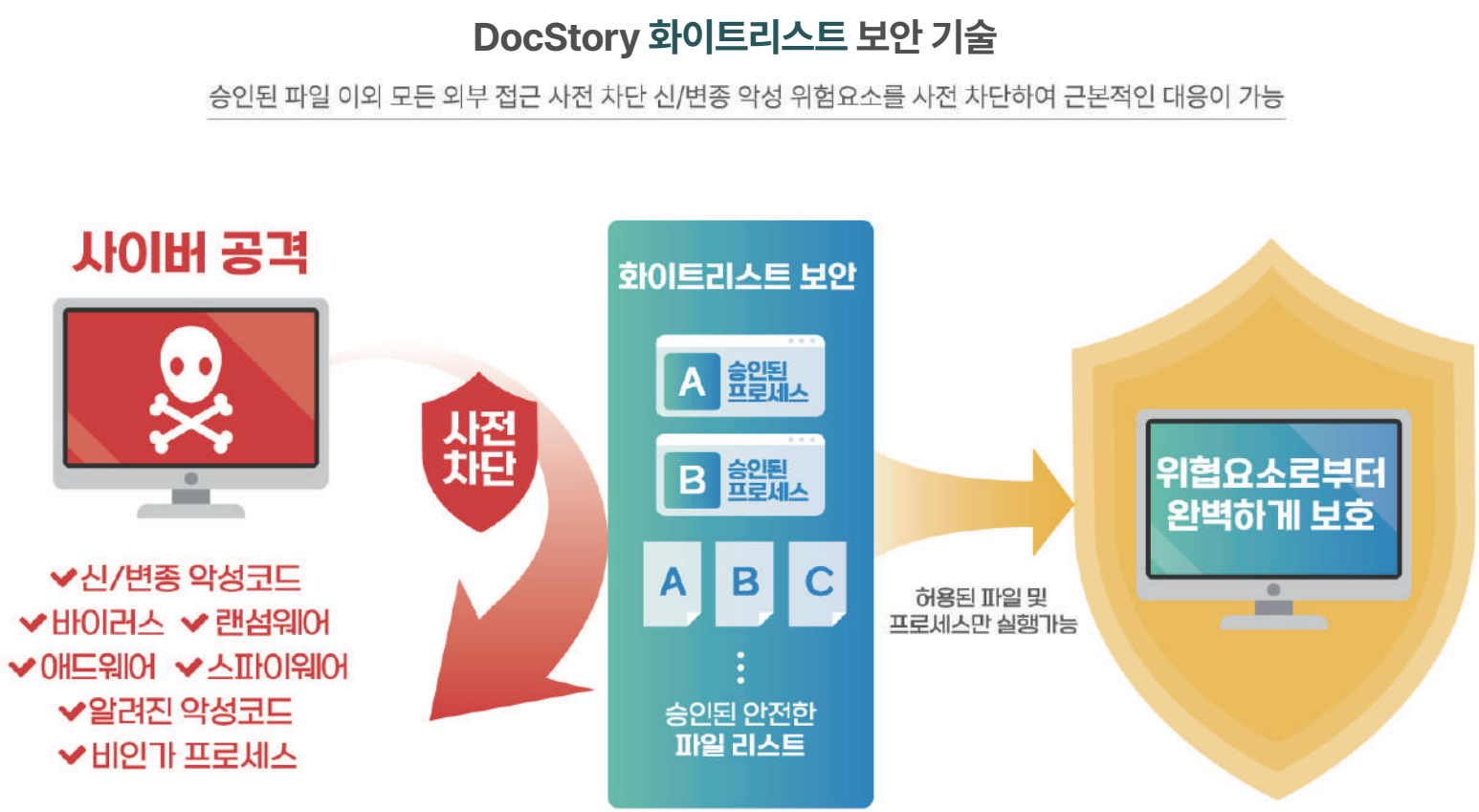
업무 영속성 유지

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 도입효과 및 장점

문제 감지 및 대응
비인가 접근 빠르게
감지 및 대응

향상된 보안
승인된 프로세스만 접근
주요 정보 유출 사전차단

성능 최적화
불필요한 접근 차단하여
시스템 효율적 사용

규제 준수
산업보안 규제 및 컴플라이언스 충족
접근 관리의 체계화로 감사 용이

관리 간소화
화이트 리스트 접근 정책 설정 편리
승인된 접근만 모니터링하여 편리

성능의 확장
모든 악성코드에 대응
운용 중 성능 저하 無

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)

EDR

위협 탐지 후 수동 대응 필요 (제로 데이 발생).
해결 보안의 애로 사항 발생

개발사에서 정의된 이상 행위가 발생해야만
추적하고 관찰하는 방식

모든 프로세스를 분석, 처리가 이루어짐,
리소스를 많이 소모할 수 있음

자동화된 위협 대응

기존 EDR의 한계 보완

경량화된 데이터 기반 시스템

DOCSTORY

자동화된 대응 (문서 접근 사전 차단)으로
신속한 실시간 대응이 가능,관리자의 부담 경감

학습된 AI를 통해 인가된 프로세스 이외의 모든
파일을 실시간으로 자동 판별하고 즉시 차단

데이터접근 시에만 동작하여 리소스 최소화,
엔드포인트에서 독립적으로 동작

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.

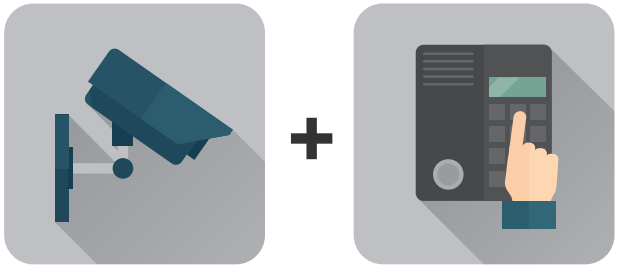
< EDR (Endpoint Detection & Response) 개념 >

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(EDR 확장팩) 개념 >

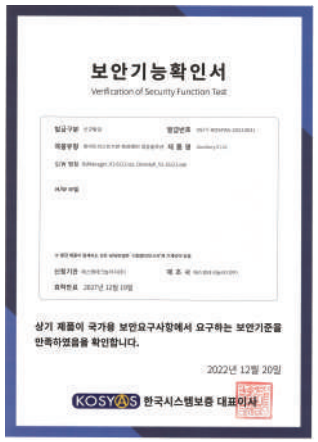
구 분		DOCSTORY(데이터 보안)	도어락 (물리 보안)
목 적		IT 환경에서 신종 보안위협 탐지·대응	물리적 행위의 출입 방지, 차단
대 상		PC의 모든 데이터 파일	물리적 특정공간(건물 입구,내부 등)
역 할	보 안	AI 자동 판단으로 높은 보안과 편리한 관리	상시 경비 인력에 대한 부담감 해소
	탐 지	주요 실행 파일 이상 행위 탐지 및 분석	정해진 출입자 외 출입 금지
	대 응	주요 실행 파일 탈취 시도 시 차단 및 종료	비정상 출입 시도 시 도어락 차단
	알 림	훼손된 파일 자동복구 및 관리자 알림	출입자 기록 확인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



기업 시설 보안시스템

DocStory

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 선별**함으로써 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

보호 대상 파일 접근 시도	자동 분류 엔진 분석	AI 판단	접근 허용 또는 차단
프로세스가 보호 대상 파일에 접근을 시도	프로세스의 특성을 분석하여 분류	학습된 데이터를 기반으로 안전성을 판단	안전한 프로세스는 자동 등록 접근 허용

관리 모듈의 주요 기능

설치 및 감사 로그 기능

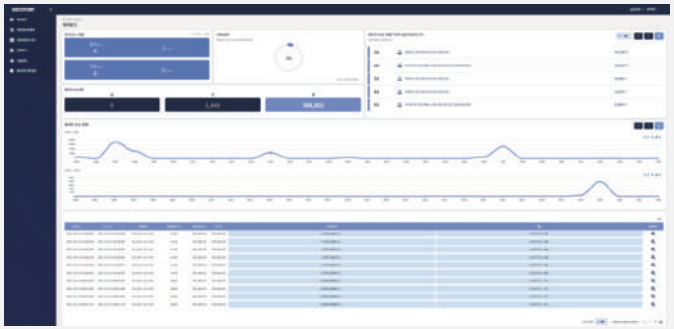
| 대시보드를 통한 직관적인 정보 제공, 다양한 설정을 통한 효과적인 정책 설정, 다양한 상황에 따른 감사 로그

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.

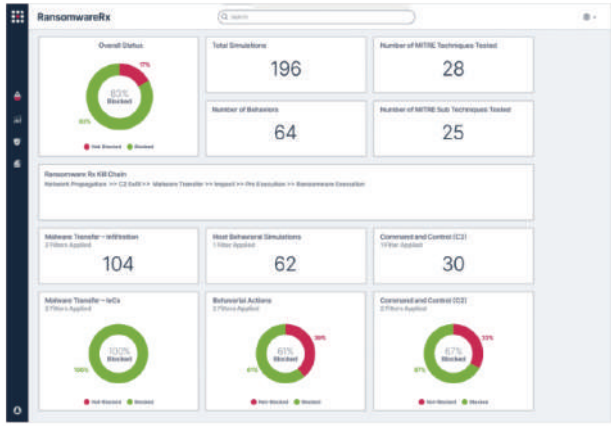


다양한 상황에 따른 감사 로그

- 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

IDLE 상황

탐지 및 차단 상황

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

경북도청 | 대구시청 | 강원도청 | 전남도청

■ 지자체

광주북구청	강릉시청	원주시청	구미시청	평창군청	상주시청	양양군청	영천시청	김제시청	강진군청
속초시청	영암군청	인제군청	안동시청	군위군청	고성군청	영월군청	신안군청	칠곡군청	보성군청
양구군청	순천시청	목포시청	해남군청	의왕시청	포항시청				

■ 기타 공공

청와대 | 경기도교육청 GYEONGGIDO OFFICE OF EDUCATION | 해양경찰청 KOREA COAST GUARD | 질병관리청 국립목포병원 | 한국농어촌공사 | 경상북도 소방본부 | 문화체육관광부 국립국어원 | 전남테크노파크 JEONNAM TECHNOPARK | 과학기술사업화진흥원 | 한국전력

■ 방송 및 금융

TBC | 더케이 한국교직원공제회 The-K 저축은행 | true friend 한국증권 | 은행연합회

■ 교육 및 기타

KUKKIWON | 남부대학교 NAMBU UNIVERSITY

■ 중견기업군

arneg KOREA | YOUNGYIEL | SENSORVIEW

■ 대기업군

LS전선

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

DocStory

검색창에 "DocStory"를 검색하시면, 랜섬웨어 정보를 확인 할 수 있습니다.

DocStory

개발 SMT Security Mechanism Technology

(주) 에스엠테크놀러지
경기도 하남시 조정대로 45 미사센텀비즈, F902호
02-407-0680 | www.smtechnology.kr

판매 BEONE SYSTEM

(주) 비원시스템
서울 강서구 공항대로 46길 13-20 (화곡동 1113-17)
02-719-2494 | www.b1sys.co.kr