SMT
Security Mechanism Technology

DocStory

랜섬웨어 팬더믹 대응 솔루션

Endpoint Data Protection

에스엠테크놀러지

증가하는 신/변종 사이버공격 피해 규모. 4차 산업혁명으로 정보자산 범위 확대 및 보안 중요성 대두

2021년, **랜섬웨어 피해 금액** [출처: 소닉월, 사이버시큐리티벤처스]

전세계 전년 대비 **33%** ↑

24조 500억원

(랜섬웨어 피해 건수 **약 4억건**)

국내 전년 대비 **25%** ↑

2조 5,000억원

(랜섬웨어 피해 건수 **약 150건**)

기존 보안 방식

실시간 모니터링

사람의 행위 기반으로
관리 비용 발생, 오탐률 존재

데이터 백업

백업 데이터 삭제/암호화,
정보유출 피해 가능

산업 동향

**산업의 성장과 디지털화로
정보자산 피해 급증 예상**

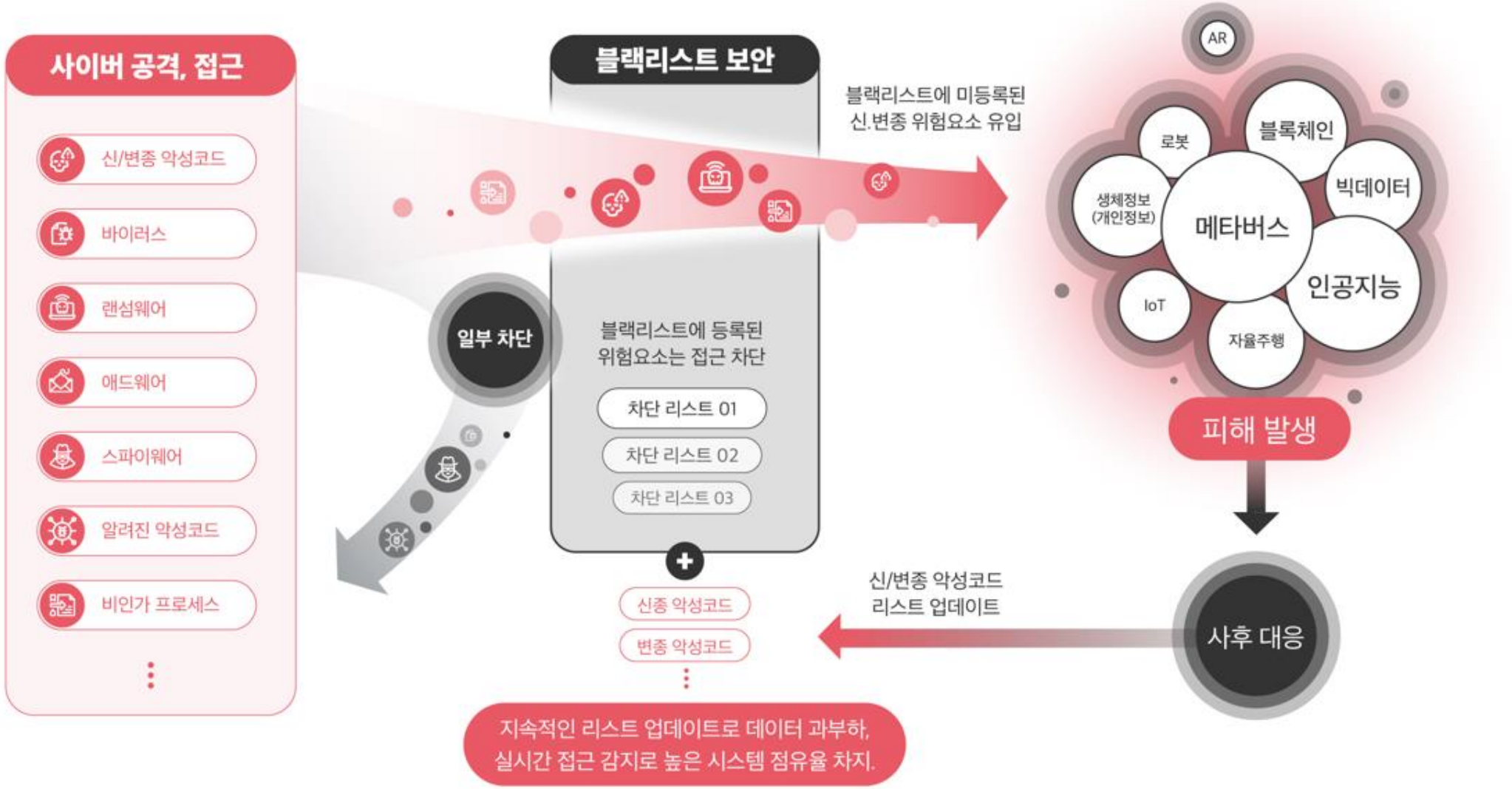
기존 보안 기술

블랙리스트 기술

리스트된 악성코드들만 차단
신/변종 진화 악성코드에 취약

SMT
Security Mechanism Technology

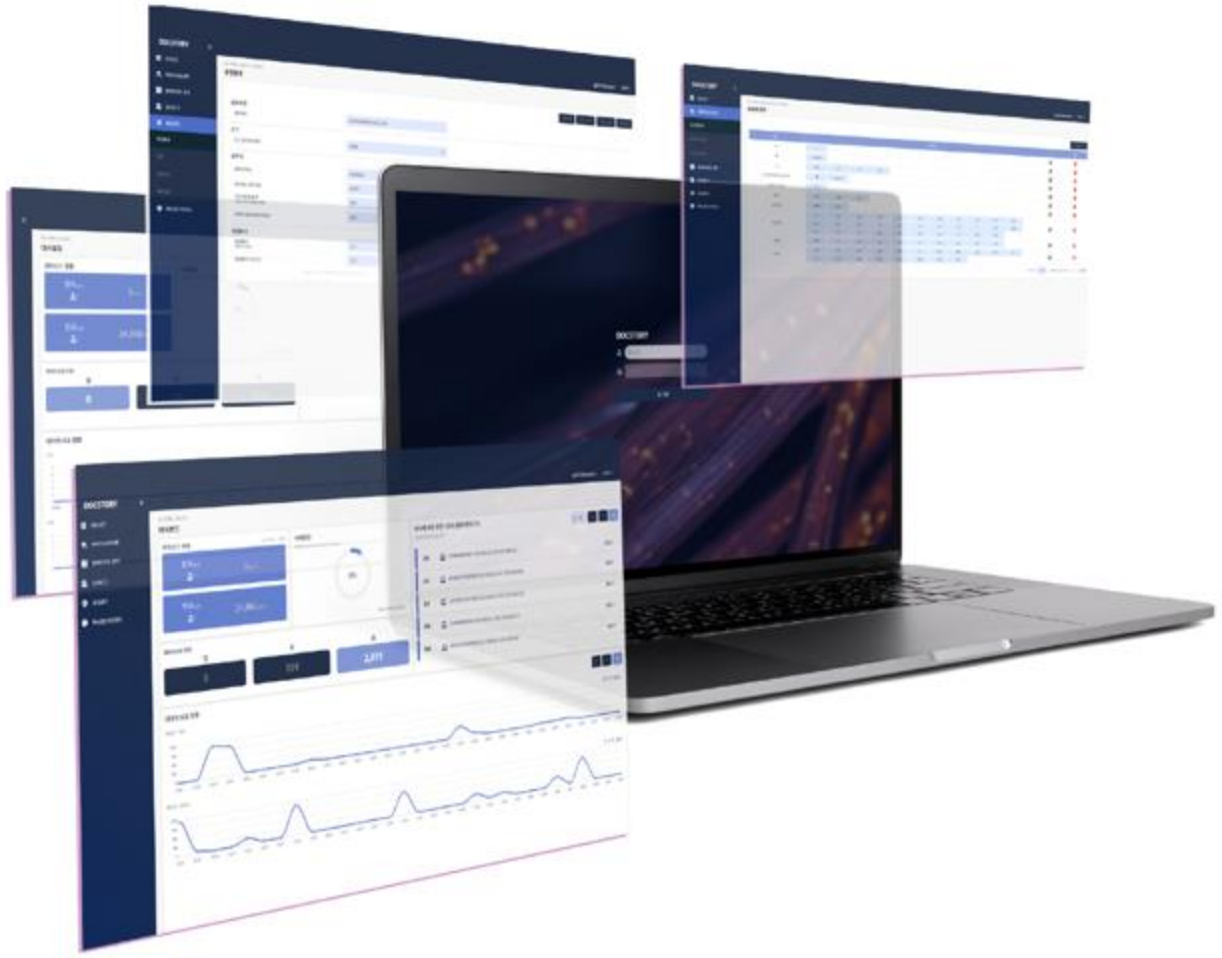
블랙리스트 보안 기술: 진화하는 신·변종 랜섬웨어 대응 불가능한 기존 보안 방식의 기술적 한계



SMT
Security Mechanism Technology

화이트리스트 보안 솔루션; 승인된 파일 이외 모든 외부 접근 사전 차단.
신 변종 악성 위험요소를 사전 차단하여 근본적인 대응 가능

SMT
Security Mechanism Technology



DocStory

- **국내 최초** 능동형 **화이트리스트 기술**
- 검증된 **자체 보안 엔진** 적용
- 신·변종 악성코드를 **사전 차단**

GS 인증
1등급 Software

국가정보원
보안기능 확인서
국내 최초 발급

조달청
나라장터 쇼핑몰 등록
- 물품식별번호 -
23181932

SMT
Security Mechanism Technology

화이트리스트 자동 분류 기술력

자체 개발한 분류 엔진으로
화이트리스트 기술의 난제였던
관리 포인트 95% 이상 절감

국내 유일 국정원 보안 인증서 및 기술 특허

국정원 검증 기준의 무결성 / 기밀성 / 가용성
검증테스트 충족. 보안인증서 및 기술특허
취득하여 기술적 우위 선점

국내 유일 화이트리스트 기술 상용화

화이트리스트 기술을 상용화한
국내 유일 보안 솔루션.
7만개 이상 납품으로 Data 지속적 확보

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

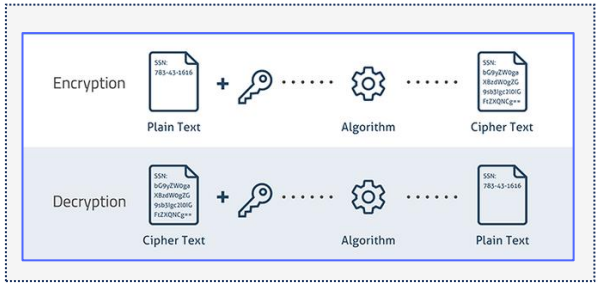
- 로그인 시 패스워드 생성 규칙을 준수하고, 사용자 계정 정보의 암호화 하여 안전하게 저장합니다.
- 관리서버와 에이전트의 운용 중 발생하거나 전달되는 주요 데이터는 암호화되어 저장되거나 암호화 되어 통신 됩니다.
- 주요 파일은 숨겨진 상태로 보관되고 사용되는 암호키는 국정원 보안 인증 규격을 준수합니다.

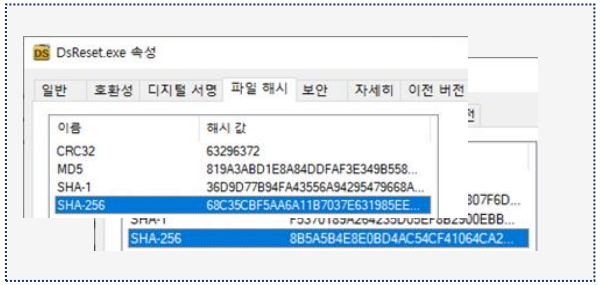
무결성 확보

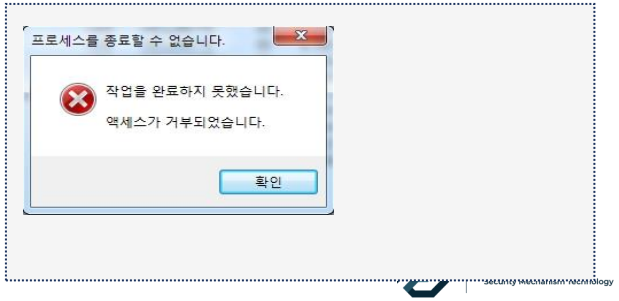
- 에이전트와 관리서버의 주요 실행파일과 운용되고 있는 주요 프로세스들은 안전한 운용을 위하여 주기적인 무결성 검증을 진행합니다.
- 무결성 검증 시 훼손된 파일들은 자동 복구되며, 이에 대한 정보는 즉각 관리자에게 통보됩니다.
- 무결성 검증 진행 절차는 국정원 보안 인증 규격을 준수합니다.

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.







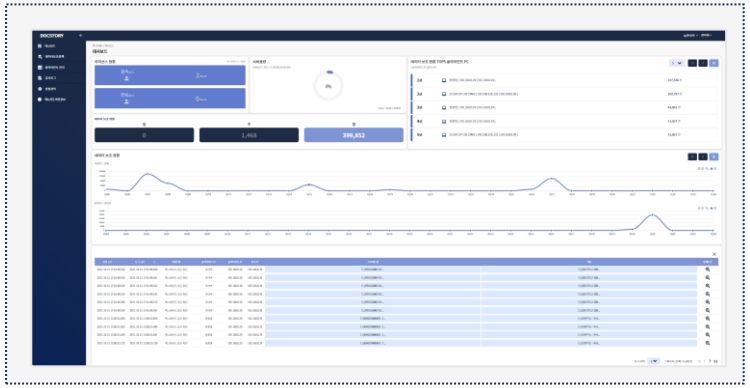
관리 모듈의 주요 기능

설정 및 감사 로그 기능

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

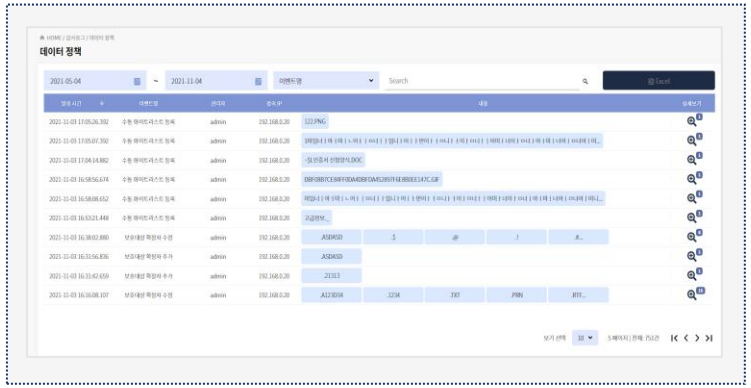
대시보드를 통한 직관적인 정보 제공

- 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.

운용 안정성 테스트

7만 대 이상의 PC에서 다년간 안정적으로 운용하고 있습니다.

| 안정성 테스트를 위하여 테스트 전용 프로그램을 다수 개발하여 테스트에 적용 다양한 자체 평가를 함으로써 안정성을 입증합니다.

[테스트PC 평균 사양 : Windows10 Professional 64Bit, CPU 4코어, RAM 8GB, HDD SSD64G]

구 분	내 용
탐지/차단 속도	커널 드라이버 레벨의 차단 진행으로 속도 측정 불가
단위 시간당 처리량	평균 초당 처리량 250건 이상
위협탐지 신뢰도(탐지율/오탐율)	인가된 프로세스만 허용함으로 오탐에 대한 관련 없습니다. 악의적인 프로세스가 보호 대상 파일에 대한 접근을 커널 레벨에서 차단함으로 악의적인 행위 이외 리소스 점유 추가 없습니다
CPU점유율/메모리 사용량	IDLE상황 대비 탐지 및 차단 상황에서 주요 프로세스의 부하 증가는 체감하기 힘든 수준입니다.
네트워크 부하	운영 초기 정책 설정 이후 낮은 빈도로 발생하고, 탐지/차단 시 해당PC와 관리서버간 짧은 시간 동안 비교적 높은 빈도 발생합니다.
타 보안 솔루션Agent와 충돌 회피	다년간 20 곳 넘는 지자체 안정적인 운용. 대기업을 포함한 일반 기업에서도 충돌없이 안정적인 운용 중 입니다.

업무 중단 없는 설치/안전한 운용 환경

설치부터 실 운용까지 안전하고 편리한 진행.

| 사용자 개입 없는 스텔스 설치부터 사용자PC에 영향 없는 운용 시뮬레이션으로 최적의 정책을 설정하고, 안정적 환경에서 점진적으로 실 운용 전환합니다.

SMT
Security Mechanism Technology

소비자 가격 및 조달등록 가격

DocStory Standard Edition V1.0

| 가격 및 납품 관련 세부사항은 총판사인 '㈜소프트일레븐'과 협의 가능합니다.

No	제품명		물품식별번호 및 구분	라이선스	가격(원)	비고
1		DocStory V1.0, Standard Edition, 랜섬웨어차단솔루션	23181932 (조달청 나라장터 쇼핑몰)	1조 : 1~100 PC 영구라이선스 (관리모듈 포함)	(1조) 7,440,000 (부가세포함)	H/W 제외, 구매 후 1년간 무상 유지 보수
			24294543 (조달청 나라장터 쇼핑몰)	1조 : 1 PC 연간라이선스 (100PC이상 계약 시 관리모듈 모함)	(1조) 32,000 (부가세포함)	H/W 제외, 1년 단위 계약 갱신
2		DocStory V1.0, Enterprise Edition, 랜섬웨어차단솔루션	기업용	1조 : 1~100 PC 영구라이선스 (관리모듈 포함)	(1조) 8,000,000 (부가세제외)	H/W 제외, 구매 후 1년간 무상 유지 보수

현재 국내 기업을 비롯하여 공공기관 및 지자체 30여 군데 서비스 납품 실적 보유

기업 / 공공기관

8곳
납품

5,700대
설치 완료

LS전선 · 한국전력 · TBC

arneg KOREA · true friend 한국투자증권 · 한국교직원공제회 The K 저축은행

청와대 · 국기원 · 특임운영기관 질병관리청 국립목포병원

지자체

23곳
납품

66,000대
설치 완료

경북도청	강릉시청	대구시청	구미시청
평창군청	상주시청	양양군청	영천시청
김제시청	속초시청	영암군청	인제군청
안동시청	군위군청	양구군청	춘천시청
목포시청	원주시청	의왕시청	고성군청
영월군청			