

지금까지 경험해보지 못한 새로운 보안
랜섬웨어 차단 솔루션

DocStory



보안기능확인서

현재상황

전 세계적으로 랜섬웨어 고도화 . 지능화되고, 이로 인한 피해 규모는 급속도로 확산되고 있습니다.

이에 국가정보원은 2023년부터 “정보보안 관리실태 평가지표”에 보안 취약 요인을 사전 발굴/제거함을 목적으로 “랜섬웨어 대응” 점검항목을 추가하고 관련 보안 솔루션 적용을 권고하고 있습니다.

질의 내용 : 랜섬웨어 등 악성코드 감염 예방을 위한 자체 보안대책이 강구되어 있는가?

1. 관련 보안솔루션 적용 등 보안대책을 수립.시행하고 있다.	1점
2. 보안대책을 수립.시행하고 있으나 일부 미흡하다.	0.5점
3. 보안대책이 수립되어 있지 않거나 시행하고 있지 않다.	0점

기존보안의 한계

일반적으로 PC를 위협하는 모든 공격으로부터 백신이 보호해 준다고 믿고 있습니다.

하지만, 백신만으로는 지능화 되어가는 신.변종의 악성코드에는 취약합니다.

백신은 악성코드 사후 보완방식으로 감염된 컴퓨터를 치료하는 제품이기 때문입니다.

Zero Day

새로운 악성코드가 발견되지 않은 상태로 활동하며 피해를 주는 기간



랜섬웨어의 진화

랜섬웨어는 계속해서 진화하고 있습니다. 행위기반, 시그니처 기반으로 대응하기 힘든 이유입니다.



알려지지 않은, 그리고 진화하는 악성행위의 공격으로부터 최선의 방어는 **사전차단** 입니다.

DocStory 소개

- DocStory는 화이트리스트 기술을 이용한 제로트러스트 솔루션으로 인가되지 않은 접근으로부터 데이터를 보호함으로써 암호화, 삭제 및 유출 등의 위협에 사전 대응합니다.
- 제로트러스트의 불편함을 극복하기 위하여 신뢰할 수 있는 프로세스를 자동 선별함으로써 관리자의 업무능률을 최적화 하였습니다.
- 보안기능확인서를 통한 '국가용 보안요구사항' 만족에 그치지않고, 강화된 자체 보안 기준에 충족하도록 개발되어 위협에 적극적으로 대응합니다.

[제로트러스트 : '아무것도 신뢰하지 않는다.'는 원칙을 바탕으로한 보안 접근 전략]

DocStory 특징

DocStory는 3가지 강력한 엔진이 유기적으로 결합되어 랜섬웨어 등의 신.변종악성코드로부터 데이터를 안전하게 보호합니다.

사전차단 엔진



주요 데이터
훼손 방지 및 유출 방지

비인가 프로세스가
데이터 접근 시도 시
사전 차단

프로세스 자동 분류 엔진



시스템 및 상용프로세스
자동 판별 및 분류

안전한 프로세스의 접근을
허용함으로써 관리자의
관리포인트 최소화

자체 보호 엔진



악성코드로부터
Agent 보호

국정원 검증 기준에 따른
무결성 / 기밀성 / 가용성
검증테스트 충족

DocStory 성능 검증

글로벌 해킹 및 공격 시뮬레이션 업계의 리더인 이스라엘의 세이프브리지(SafeBreach) 제품으로 사이버 킬체인과 마이터어택(MITRE ATT&CK)을 접목한 공격 시뮬레이션 검증하였습니다.(2023년11월)

테스트 환경	총 침투 테스트 수	차단 성공 수	차단 실패 수	차단 성공률(%)
국내 A사 백신	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 SSD 500GB]

Q & A

Q. 타 제품과의 가장 큰 차이점은?

A. 화이트리스트 방식의 솔루션으로 화이트리스트에 등록되지 않은 비인가 프로세스의 데이터 접근을 원천 차단하여, 보호 데이터의 유출, 삭제, 위.변조 등의 어떠한 악성행위도 차단이 가능합니다.

Q. 화이트리스트 방식 보안 솔루션의 난제인 수많은 프로세스를 일일이 화이트리스트로 등록하는 불편함은 해결되었는가?

A. 프로세스 자동 분류 엔진을 통하여 화이트리스트를 95%이상 자동 판별하여 적용합니다.
따라서 PC에서 사용하는 대부분의 정상 프로세스는 화이트리스트로 등록할 필요가 없습니다.
보안에 취약한 일부분의 프로세스만 관리하면 됩니다.
화이트리스트 방식 솔루션의 문제점인 관리포인트 가중화를 대폭 절감하였습니다.

Q. 에이전트 설치 후 PC 성능 저하는 일어나지 않는가?

A. 평상 시 에이전트 운영 자원 소모량은 CPU 0%, Memory 5Mbyte 이내 입니다. 에이전트 설치 후 PC 성능 저하 현상은 일어나지 않습니다.

Q. 에이전트 설치 후, 기 운영중인 솔루션 이상 동작 및 충돌 등의 증상이 일어나지 않는가?

A. 다수의 공공기관 및 기업에서 수 년 이상 운영 중, 솔루션 이상 동작 및 충돌은 일어나지 않았습니다.

Q. 랜섬웨어 및 악성코드 실시간 탐지/방어 시 알림기능을 제공하는가?

A. 사용자 및 관리자에게 즉시 팝업창을 통해 알림을 제공합니다.

Q. 폐쇄망에서 운영 가능한가?

A. 화이트리스트 방식 솔루션이므로 시그니처 등의 업데이트가 불필요 합니다.
따라서 외부 서버와의 연결이 필요하지 않습니다.
DocStory는 폐쇄망에 최적화된 솔루션이고 외부망 또한 운영 가능합니다.