조달청 / 나라장터 물품식별번호 : 23181932

지금까지 경험해보지 못한 새로운 보안
랜섬웨어 차단 솔루션

DocStory

1등급

GOOD Software

보안기능확인서

현재상황

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

이에 국가정보원은 2021년부터 “정보보안 관리실태 평가지표”에 보안 위규로 인한 랜섬웨어 피해 발생 시 감점 항목을 신설하는 등 랜섬웨어에 대한 보안 대책을 강구하고 있습니다.

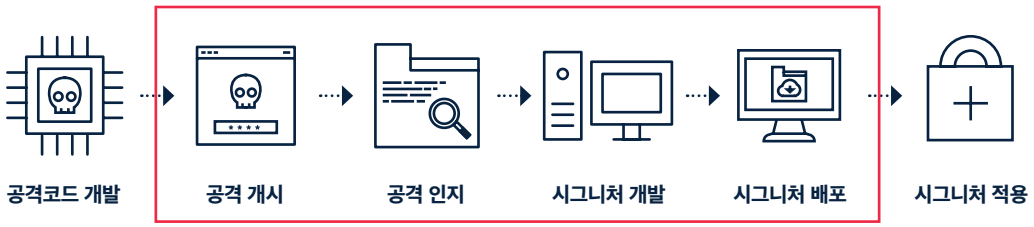
또한 개인정보보호위원회는 “개인정보 침해행위가 발생할 경우 기업 등 개인정보 처리자에게 “연간 매출액의 최대 3%까지 과징금을 부과할 수 있도록 한 조항”을 주요 내용으로 개인정보보호법 개정안을 추진하고 있는 등 기업경영에 있어 개인 정보보호 및 정보 유출에 대하여 매우 중요한 사항으로 자리 잡고 있습니다.

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



은행의 ATM이나 공장자동화 등 최고의 보안을 요구하는 곳에서 사용되는 화이트리스트 보안방식은 제로 데이(Zero Day)를 극복할 수 있는 최선의 기술이지만 사용자 편의성이 현저히 떨어지는 이유로 일반적인 컴퓨터에는 적용이 불가능하다고 알려져 있습니다.

DocStory 소개

DocStory는 화이트리스트방식의 보안프로그램으로 PC내에서 운용가능한 프로세스를 사전에 능동적으로 정의하고 정의되지 않은 프로세스는 보호대상파일에 접근이 불가능하도록 하여 랜섬웨어, 자료유출 등의 악성코드로부터 데이터를 보호하는 솔루션입니다.

자동화된 DocStory의 엔진은 기존 화이트리스트 보안방식의 한계를 극복하여 최선의 보안성능을 유지하면서 사용자 편의성을 극대화 하였습니다.

DocStory의 능동형 화이트리스트엔진은 보호대상 데이터에 접근하는 프로세스의 위험도를 분석하여 안전한 프로세스의 접근만을 허용합니다.

DocStory 특징

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

사전차단 엔진

비인가 프로세스가 보호대상 데이터 접근 시도 시 사전 차단

프로세스 자동 분류 엔진

안전한 프로세스의 접근을 허용함으로써 관리자의 관리포인트 최소화

자체 보호 엔진

국정원 검증 기준에 따른 무결성 / 기밀성 / 가용성 검증테스트 충족

보안기능확인서 인증 및 도입효과

감사정책, 보호, 랜섬웨어 차단 수준 등 모든 기본 사항을 국가정보원에서 제시한 규격을 준수하고 있습니다.

“DocStory”는 현재 광역지자체 등을 포함하여 관공서, 기업 등에서 운용되고 있습니다.
설치 후 단 한 차례의 피해사례도 접수되지 않고 있습니다.

Q & A

Q. 타 제품과의 가장 큰 차이점은?

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

Q. 화이트리스트 방식 보안 솔루션의 문제점인 수많은 프로세스를 일일이 화이트리스 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. 30여개 관공서 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.

에스엠테크놀러지(주) | T. 02 407 0680 | F. 02 6455 2342 | W. www.smtechnology.kr
A. 경기도 하남시 조정대로 45 미사센텀비즈 F902