

랜섬웨어 공격을 원천 차단하는 기업용 스토리지

FILINGBOX ENTERPRISE



Q&A 1 FilingBox Enterprise 왜 랜섬웨어로부터 100% 안전한가요?

한국 및 PCT 특허 출원



FilingBox Enterprise는 업무 PC에 랜섬웨어가 원천 차단된 하이브리드 WORM 디스크를 제공합니다. 한번 자료가 생성되면 읽기만 가능한 일반적인 WORM (Write Once Read Many) 디스크와 달리 하이브리드 WORM 디스크는 윈도우 탐색기에 한하여 WORM 디스크 내 자료를 수정/삭제할 수 있는 전환 기능을 갖추고 있습니다. 따라서 랜섬웨어에 의한 자료 위변조는 불가능하고, 윈도우 탐색기를 통한 조작에 의해서만 자료 변경이 가능하게 됩니다.

Q&A 2 FilingBox Enterprise를 직접 체험해 볼 수 있나요?

홈페이지에 무료 체험을 신청하시면 클라우드 기반의 데모 환경을 제공해드립니다.

Q&A 3 FilingBox가 랜섬웨어를 예방하는 동영상을 어디서 볼 수 있나요?

YouTube에서 FilingBox를 검색하시면 업무 PC에 랜섬웨어가 감염되어 있더라도 파일링박스 내에 보관된 문서가 암호화되지 않는 동영상을 보실 수 있습니다.



Ransomware Issue

Issue 1 왜 PC에 설치되는 백신 소프트웨어가 랜섬웨어를 막지 못하나요?

악성 소프트웨어인 랜섬웨어 역시 백신이나 예방 소프트웨어처럼 운영체제 위에서 구동되는 소프트웨어입니다. 랜섬웨어 중에는 백신이나 예방 소프트웨어를 먼저 중단시키고 파일을 위변조하는 경우까지 있어서 소프트웨어 방식으로 랜섬웨어 예방을 100% 장담할 수 없습니다.

또한 매일같이 쏟아지는 새로운 랜섬웨어의 시그니처를 확보하여 백신을 갱신하기도 어렵고, 하드디스크에 읽기 쓰기 행위가 계속된다고 해서 랜섬웨어로 간주하여 차단하는 것도 모호합니다. 느슨하면 랜섬웨어에 노출되고 철저하면 정상 프로그램까지 차단하는 상황이 발생합니다.

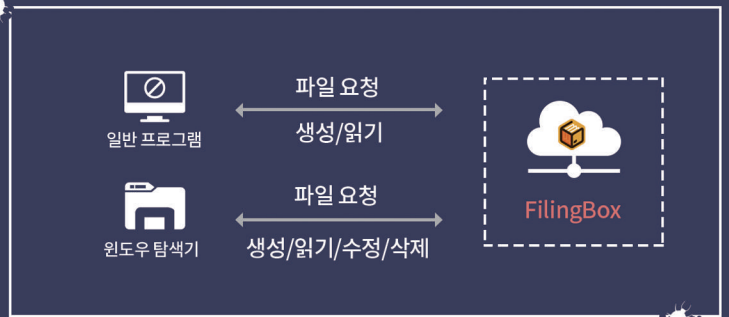
게다가 파일 단위 암호화가 아니라 하드디스크 전체를 암호화하는 FDE(Full Disk Encryption)이나 MBR(Master Boot Record) 공격의 경우 소프트웨어 예방 방식을 우회하기 때문에 100% 예방을 보장하지 못합니다.

Issue 2 랜섬웨어 예방 디스크가 일반디스크나 기존 WORM 디스크와 무엇이 다른가요?

일반적인 하드디스크, 외장형 USB 디스크, 네트워크 디스크 등이 PC에 연결되면 어떤 프로그램이든 디스크 내 파일을 수정하거나 삭제할 수 있습니다. 따라서 PC에서 랜섬웨어가 구동되면 모든 파일이 암호화됩니다.

그에 반해 WORM(Write Once Read Many) 디스크는 어떤 프로그램이 파일을 생성하던 처음은 생성할 수 있지만 생성된 이후 파일은 더 이상 변경되지 못하고 읽을 수만 있게 제공하여 PC가 랜섬웨어에 감염돼도 데이터가 안전하게 보관됩니다. 그러나 기존의 WORM 디스크는 가격이 고가이면서 한번 생성된 파일을 삭제하거나 편집할 수 없어서 수시로 변경되는 업무 데이터를 보관하기에는 부적합했습니다.

이에 반해 랜섬웨어 예방 디스크는 일반적인 프로그램에 대해서는 WORM 디스크로 작동하지만, 지정 프로그램에 한하여 파일을 편집/삭제할 수 있는 하이브리드 WORM 디스크로 작동합니다.



기업용 랜섬웨어 예방 디스크 FilingBox Enterprise의 특징

업무 PC에 랜섬웨어가 예방된 하이브리드 WORM 디스크를 제공하여 모든 암호화 공격을 원천차단

업무 PC에 보관중인 문서파일까지 랜섬웨어 예방디스크로 자동 백업

사용자별 개인디스크 이외에도 부서나 팀간의 자료공유를 위한 조직 디스크 제공

FilingBox Enterprise가 회사PC를 위한 랜섬웨어 예방 스토리저라면 서버나 개인 PC를 위한 랜섬웨어 예방 스토리지는 없나요?



서버를 위한 랜섬웨어 예방스토리지인 FilingBox MEGA와 개인이나 팀을 위한 FilingBox MINI가 준비되어 있습니다.



무료 데모체험을 신청하시면 클라우드 기반의 데모 환경을 제공해 드립니다.