멀웨어로부터 데이터를 보호하는 스토리지 프로텍션

FilingBox MEGA
제품 소개서

FILINGCLOUD

FILINGCLOUD

01

제품 개요

02

주요 특징

03

성과 및 레퍼런스

04

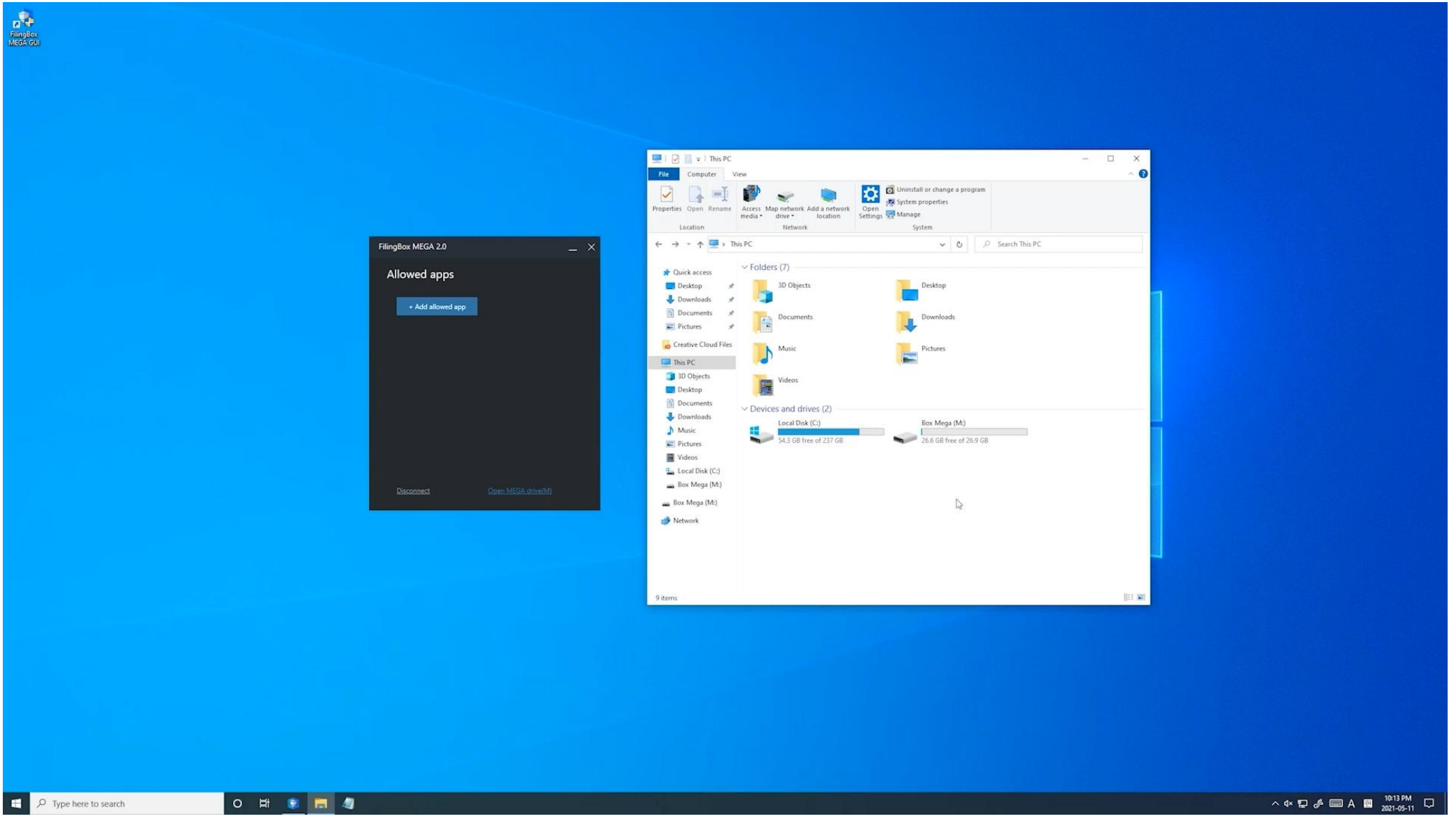
회사 소개

어플리케이션 레벨 스토리지 프로텍션

FILINGBOX MEGA

어플리케이션 레벨 스토리지 프로텍션 솔루션인 파일링박스 메가는 스토리지에 접근가능한 애플리케이션을 미리 등록하고, 등록된 애플리케이션의 데이터 요청만 데이터를 제공하고 그 이외 애플리케이션에서 데이터를 요청하면 읽기 전용 가짜 데이터를 제공하여 스토리지내 데이터를 멀웨어 공격으로 부터 사전에 보호하는 기술입니다. (국제표준 X.1220, 국제 CC인증, GS인증)

01 제품 개요

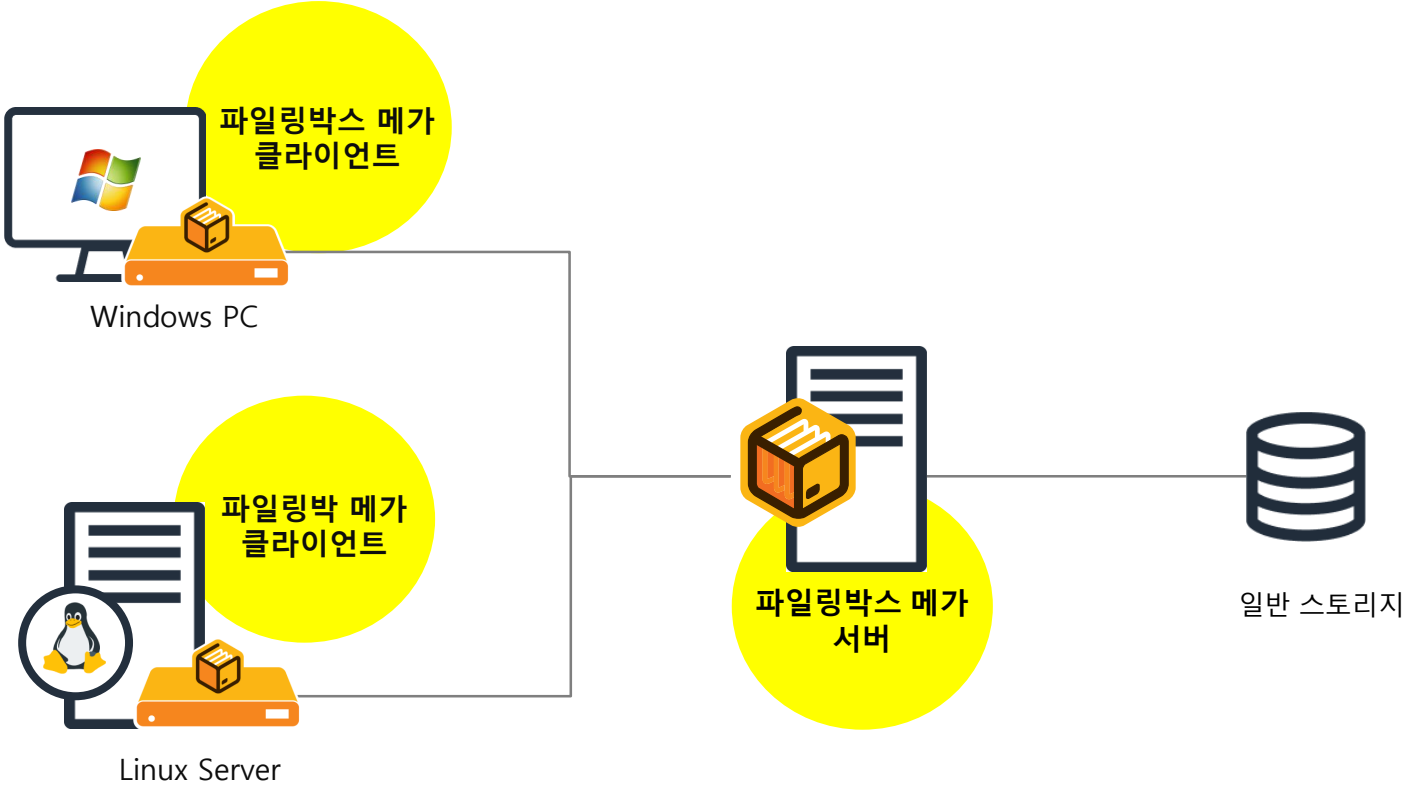


https://youtu.be/VByVeKEYorE

https://youtu.be/zNMKlIyJ4uU

FilingBox MEGA 아키텍처

파일링박스 메가는 애플리케이션 레벨 스토리지 프로텍션 솔루션으로, 메가 서버와 메가 클라이언트로 구성됩니다. 메가 서버는 스토리지가 연결된 서버 장치에 설치되어 클라이언트 장치에 보안 스토리지 볼륨을 제공합니다. 메가 클라이언트는 보안 스토리지 볼륨이 필요한 윈도우와 리눅스 장치에 설치되며, 사용자 인증을 거친 후 보안 스토리지 볼륨(메가 드라이브)에 접근할 수 있습니다.



FILINGCLOUD

01

제품 개요

02

주요 특징

03

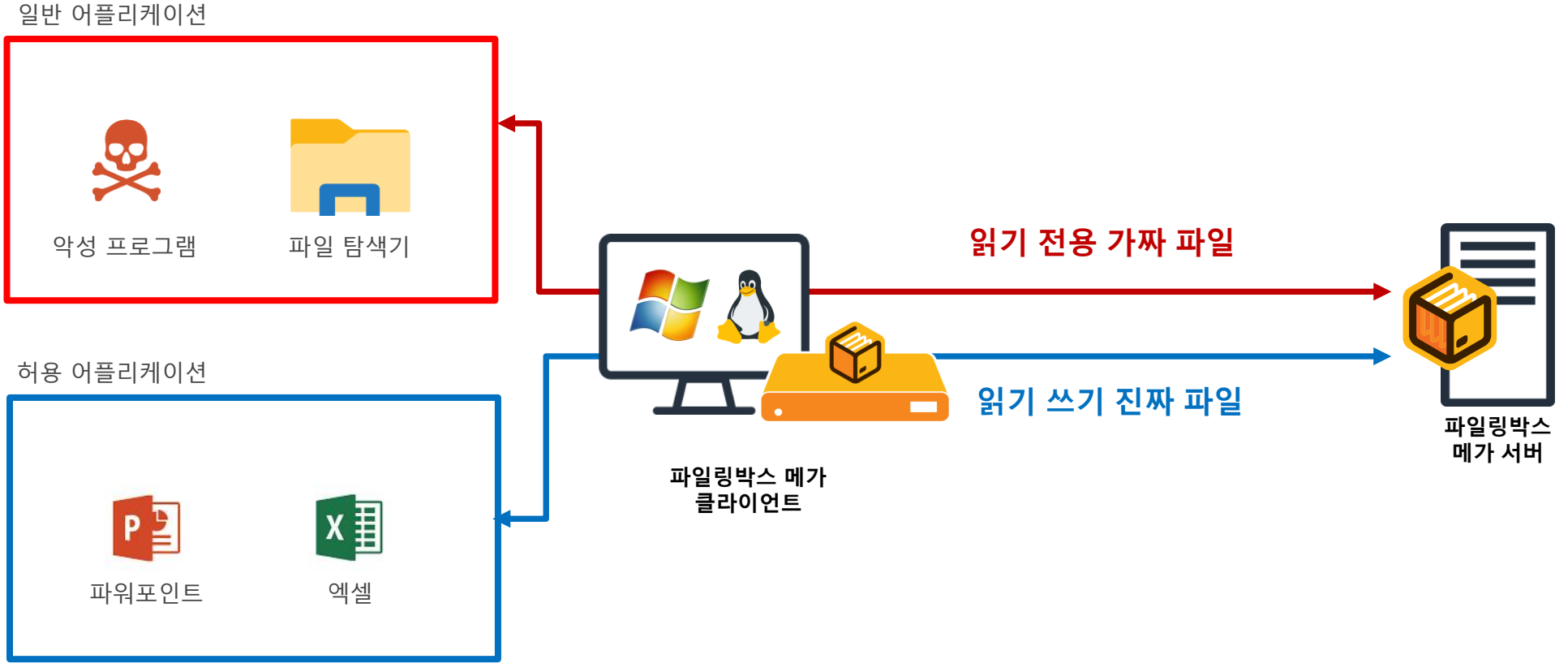
성과 및 레퍼런스

04

회사 소개

특징 1 – 최신 사이버 공격으로 관리자 권한이 탈취되어도 데이터를 보호

RCE(Remote Code Execution), 제로데이 익스플로잇트(Zero-day Exploit)등 최신 사이버 공격으로 관리자 권한이 탈취되더라도, FilingBox Mega에 저장된 데이터는 탈취되거나 암호화되지 않습니다. Mega 서버에는 데이터에 접근하는 어플리케이션에 대한 검사 모듈이 탑재되어 있어, 메가 드라이브에 접근하는 어플리케이션을 확인합니다. 사전에 등록된 허용 어플리케이션에는 읽기·쓰기 권한의 실제 파일을 제공하지만, 등록되지 않은 일반 어플리케이션에는 읽기 전용 속성의 가짜 파일만 제공합니다. 따라서 공격자가 관리자 계정과 권한을 탈취하더라도, 일반 어플리케이션으로 FilingBox Mega 드라이브 내부의 데이터를 암호화하거나 탈취할 수 없습니다.



특징 2 – OTP를 이용한 허용 어플리케이션 등록과 권한 설정

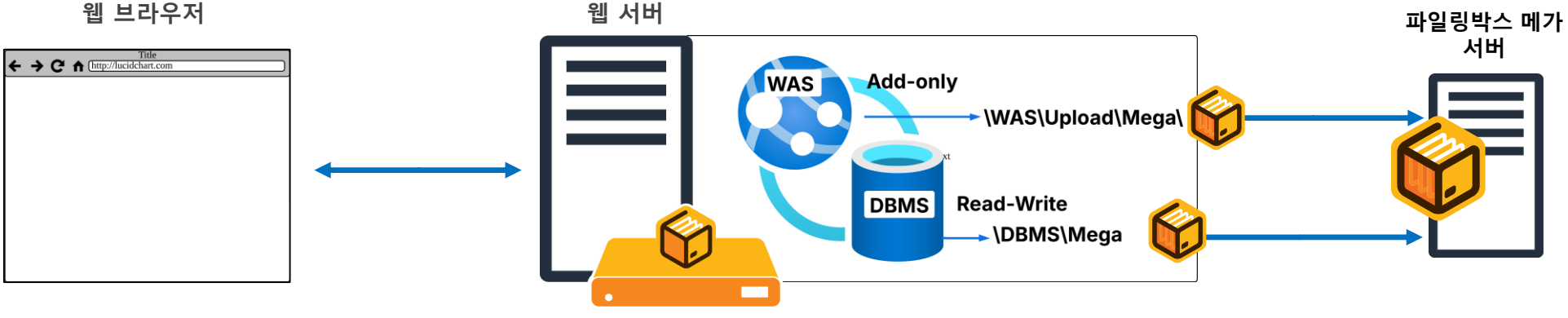
FilingBox MEGA는 스토리지 접근할 수 있는 어플리케이션을 안전하게 통제하기 위해 OTP(One-Time Password) 기반의 어플리케이션 등록 및 권한 설정 기능을 제공합니다. 이 OTP 인증 구조는 공격자가 관리자 계정을 탈취하더라도 OTP 인증 없이는 새로운 어플리케이션 등록이나 권한 변경이 불가능해 저장 데이터를 안전하게 보호합니다.

또한 PC나 서버에서 구동하는 일반 어플리케이션을 MEGA 드라이브에 허용 어플리케이션으로 등록할 때, 읽기-쓰기(Read-Write), 읽기 전용(Read-Only), 추가 전용(Add-Only), 읽기-쓰기 버저닝(Read-Write Versioning) 등 권한을 지정할 수 있습니다. 예를 들어 읽기 전용은 열람만 가능하고 수정·삭제는 불가하며, 추가 전용은 신규 생성만 허용됩니다. 읽기-쓰기 버저닝은 수정·삭제가 가능하지만 이전 파일을 보존하여 데이터 안전성을 강화합니다.

특징 3 – 중요 서버 어플리케이션의 사용중인 데이터까지 보호

FilingBox MEGA는 리눅스 서버에서 구동되는 서버 어플리케이션(DBMS, WAS 등)이 사용 중인 데이터를 보호합니다. 공격자가 서버의 관리자 계정을 탈취하더라도, 사전에 등록된 서버 어플리케이션만 MEGA 드라이브의 데이터에 접근할 수 있습니다. 예를 들어 DBMS와 WAS로 구성된 웹 서비스의 경우, MEGA 드라이브 내에 DBMS의 데이터 파일이나 사용자가 업로드한 데이터 파일만 보관하여 지정된 서버 어플리케이션 이외에 다른 어플리케이션이 접근하지 못하도록 데이터를 보호합니다.

특히 DBMS 서버 어플리케이션은 **읽기-쓰기**로 등록하고, 업무 파일을 업로드하는 WAS 어플케이션은 **추가 전용**으로 설정하여 어플리케이션별 특성에 따라 세밀하게 데이터 보호를 설정 할 수 있습니다. 이러한 서버 어플리케이션 기반의 데이터 보호 설정 방식은 사용 중인 최신 데이터를 직접적으로 보호하기 때문에, 특정 시점으로 복구하면서 최신 데이터 유실을 감수해야 했던 기존 백업/복구 방식보다 뛰어납니다.



FILINGCLOUD

01

제품 개요

02

주요 특징

03

성과 및 레퍼런스

04

회사 소개

03 성과 및 레퍼런스

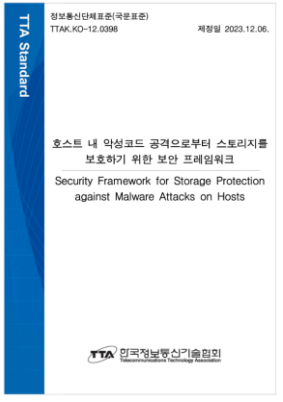
주요 시상

장영실상

지식경제부 장관상

특허청장상

표준 기술



https://tta.or.kr/tta/

https://www.itu.int/rec/T-REC-X.1220

주요 발표

AI for Good

https://youtu.be/0BokcJ6ZmLI?list=PLQqkkIwS_4kV0fRMgyl8F3oAejtgjTV98&t=8671

eGISEC 2025

https://youtu.be/xVZBZ_MM4_I

ISEC 2024
INTERNATIONAL SECURITY CONFERENCE

https://youtu.be/Vct8PdaU34k

https://youtu.be/rBUK45fdBtY?t=838

DATACON LA

https://youtu.be/CGKFihLeTZ0

주요 인증

ISO/IEC 25023, 25051, 25041

Cloud Service
Accredited by KACI

ioXt
internet of secure things

FIPS VALIDATED 140-2

03 성과 및 레퍼런스

금 융

- KB카드 – 내부 및 협력업체 개인정보 보호용 협업파일 서버 구축
- 미래에셋생명–협업용 보안파일서버 시스템 구축
- 한국투자파트너스–랜섬웨어 방어 등을 위한 보안 파일 공유 시스템 구축
- 엠캐피탈–(구)효성캐피탈 랜섬웨어 대응 위한 업무 자료 백업시스템 구축

기 업

- CMB대전방송–랜섬웨어 방지를 위한 파일공유 시스템 도입
- 삼영순화(주) 삼영순화–MS Azure 기반의 파일공유 서비스 공급
- 아성코리아–랜섬웨어 방어 위한 보안 파일 공유 시스템 구축
- (주)우원기술 우원기술–중요 자료 보안 강화 및 랜섬웨어 방지 파일 공유 시스템 구축

공 공

- 통계청 통계청–인구 총조사 자료에 대한 문서중앙화 시스템 구축
- 한국철도공사 – 차세대 나라장터 시스템 사용자 PC의 중요 데이터 보호 및 랜섬웨어 방지 파일서버 구축
- 한국석유공사–랜섬웨어 대응 PC 자료 백업 및 공유체계 구축
- 한국철강협회–문서 통합 관리시스템 구축
- 안동시 경북 안동시청–랜섬웨어 방지을 위한 보안 웹하드 구축
- 단양군 충북 단양군청–랜섬웨어 대응 PC자료 백업시스템 구축
- 전남 진도군청–내부 직원 간의 협업을 위한 클라우드 파일공유 시스템 구축
- 보은군 충남 보은군청–직원 PC의 행정자료 손상 및 유출방지용 보안 웹하드 시스템 도입
- 칠곡군 경북 칠곡군청–랜섬웨어 방어 및 협업을 위한 파일공유시스템 구축
- 인천광역시 남동구 인천 남동구청–파일 중앙관리 시스템 구축
- 대전광역시 대덕구 대전 대덕구청–랜섬웨어 대응 PC자료 백업시스템 구축
- 대구광역시북구 광주 북구청–랜섬웨어 방지를 목적으로 클라우드 저장소 구축
- 충청북도교육청 충북교육연구정보원–충북소통메신저 고도화를 위한 파일공유 협업시스템 도입
- 한국건설생활환경시험연구원 한국건설생활환경시험연구원–랜섬웨어 대비 파일공유시스템 구축
- 아동권리보장원 아동권리보장원–(구)중앙입양원 보안 파일 공유 시스템 구축

FILINGCLOUD

01

제품 개요

02

주요 특징

03

성과 및 레퍼런스

04

회사 소개

멀웨어 공격으로부터 데이터를 보호하는 스토리지 프로텍션

파일링클라우드는 랜섬웨어나 데이터 탈취 멀웨어로부터 데이터를 보호하는 스토리지 프로텍션 솔루션을 제공하는 기술회사입니다. 스토리지 프로텍션 기술은 데이터를 보관하고 있는 스토리지 관점에서 데이터를 보호하는 기술로 작동 방식에 따라 애플리케이션 레벨 스토리지 프로텍션, 폴더 레벨 스토리지 프로텍션, 유저 엑션레벨 스토리지 프로텍션으로 구분됩니다. 이 기술들은 UN산하 국제표준화기구인 ITU에서 X.1220와 X.nspam으로 권고되고 있으며, 국제 CCRA에서 CC 인증될 만큼 뛰어난 사용성과 보안성을 갖추고 있습니다. 스토리지 프로텍션 기술은 제로트러스트 시대에 데이터 보호에 관한 핵심 기술입니다. 파일링클라우드는 ESG 실현을 위하여 전세계 의료기관을 대상으로, 무료 라이선스를 제공하고 있습니다.

제로트러스트 시대의 데이터 보호를 위한 스토리지 프로텍션 기술

애플리케이션 레벨 스토리지 프로텍션	폴더 레벨 스토리지 프로텍션	유저 액션 레벨 스토리지 프로텍션
FILINGBOX MEGA	FILINGBOX GIGA	FILINGBOX ENTERPRISE
리눅스및 윈도우 서버의 데이터 보호	NAS를 사용하는 전문가 및 AI/OT/IoT 기기의 데이터 보호	기업이나 기관의 데이터 보호 및 관리

FILINGCLOUD

- 회 사 명 : ㈜파일링클라우드
- 홈페이지 : www.filingbox.com
- 문의메일 : support@filingbox.com

도입 문의

- 주소 : (08589) 서울특별시 금천구 디지털로 130 남성프라자 13층
- 전화번호 : +82-2-6925-1305
- 사업문의 : sales@filingbox.com

감사합니다.