Storage Protection to Safeguard Data from Malware

FilingCloud
Company Introduction

FILINGCLOUD

FILINGCLOUD

Storage Protection Provider for Safeguarding Data from Malware Attacks

FilingCloud is a technology company that provides storage protection solutions designed to protect data from ransomware and data-stealing malware. Storage protection technology protects data from the storage perspective, and depending on how it operates, it is categorized into application-level, folder-level, and user-action-level storage protection. These technologies are officially recommended by the International Telecommunication Union (ITU), a United Nations specialized agency, as ITU-T X.1220 and ITU-T X.1560, and have been recognized for their outstanding usability and security by obtaining Common Criteria (CC) certification under the International CCRA. Storage protection is a core technology for data protection in the era of Zero Trust. To promote ESG realization, FilingCloud offers free licenses to medical institutions worldwide.

Storage Protection Technology for Data Protection in the Zero Trust Era

Application-Level Storage Protection	Folder-Level Storage Protection	User-Action-Level Storage Protection
FILINGBOX MEGA	FILINGBOX GIGA	FILINGBOX ENTERPRISE
Protects data on Linux and Windows servers.	Protects data on NAS systems, professional environments, and AI/OT/IoT devices.	Protects and manages data for enterprises and public institutions.

FILINGCLOUD

01

Company Overview

02

Product Introduction

03

Achievements & References

04

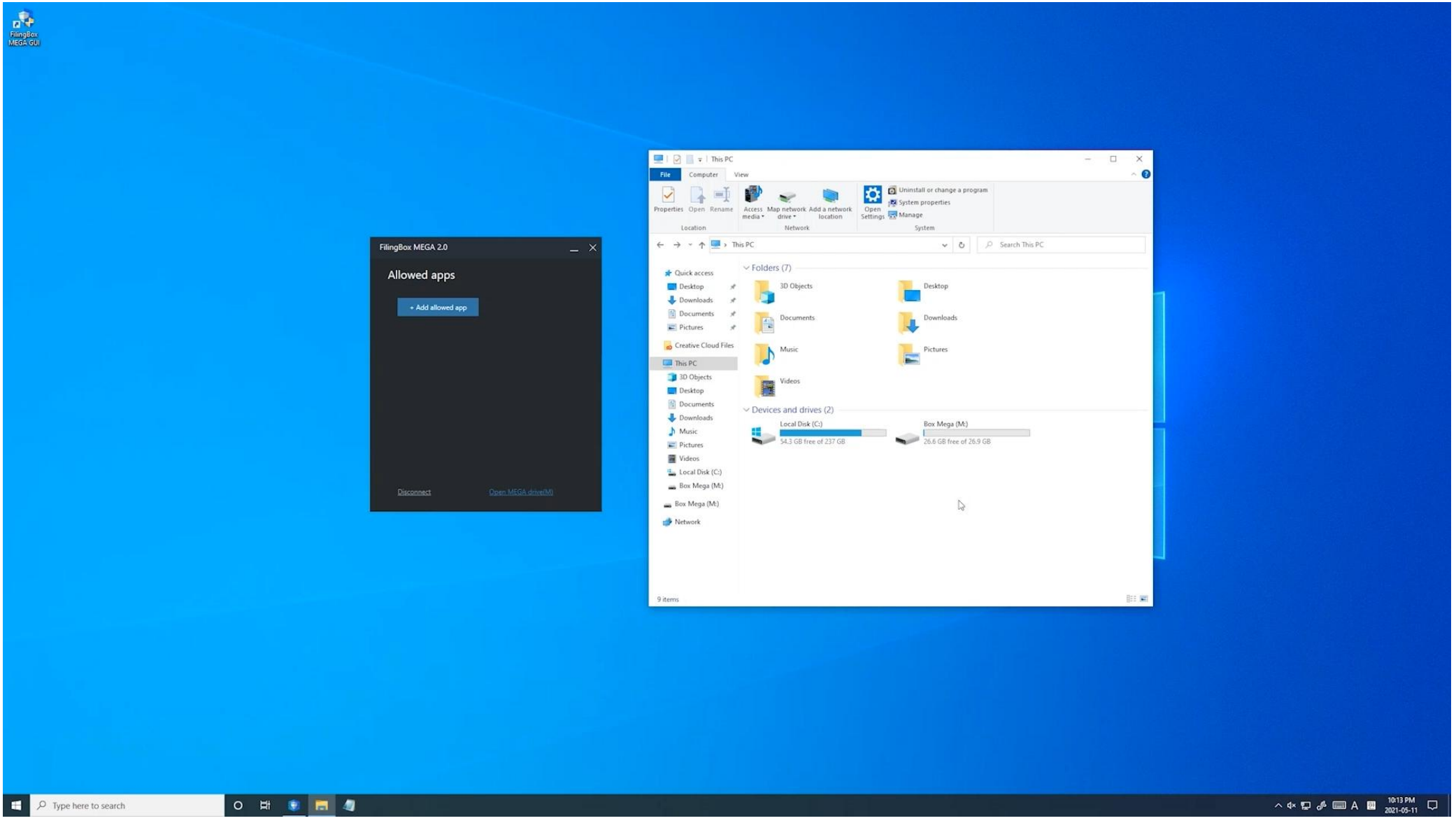
Contact

Application-Level Storage Protection

FILINGBOX MEGA

FilingBox MEGA, an application-level storage protection solution, registers in advance the applications that are allowed to access storage. It provides data only to registered applications, and when unregistered applications request access, it delivers read-only fake data instead. Through this mechanism, it protects data within the storage in advance from malware attacks. (International Standard ITU-T X.1220, International CC Certification, GS Certification)

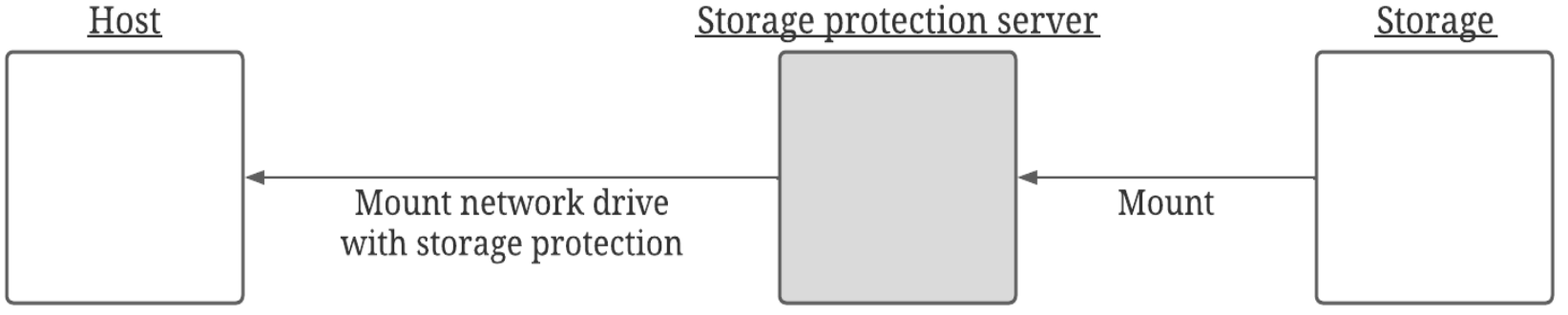
02 Production Introduction – Application-Level Storage Protection



https://youtu.be/VByVeKEYorE

https://youtu.be/zNMKlIyJ4uU

02 Production Introduction – Application-Level Storage Protection



FilingBox Mega Features

Existing technologies for protecting data on servers include antivirus software and EDR (Endpoint Detection & Response). However, these conventional technologies consume a large amount of server computing power and cannot fundamentally block newly evolving viruses or behavioral attacks. Backup-based technologies can only restore data after an incident has occurred, so they cannot prevent ransomware attacks in advance. Furthermore, existing methods are unable to prevent the leakage of important data to external sources beforehand.

FilingBox Mega, on the other hand, pre-registers applications that are allowed to access storage.
It provides data only to registered applications, and when unregistered applications request data, it supplies read-only fake data. In this way, it proactively protects data within storage from malware that attempts to encrypt or steal it. An OTP code is required to register an application in FilingBox Mega, and only authorized administrators can perform the registration.

FIlingBox Mega Benefits

1. Even if an administrator or staff member accidentally runs malware on a server or main PC, or an attacker gains full control over the system, the data stored in the Mega storage cannot be lost or stolen.

2. Because FilingBox Mega inspects applications that request data within the network storage itself, it protects data without slowing down servers or main PCs, unlike EDR or antivirus software.

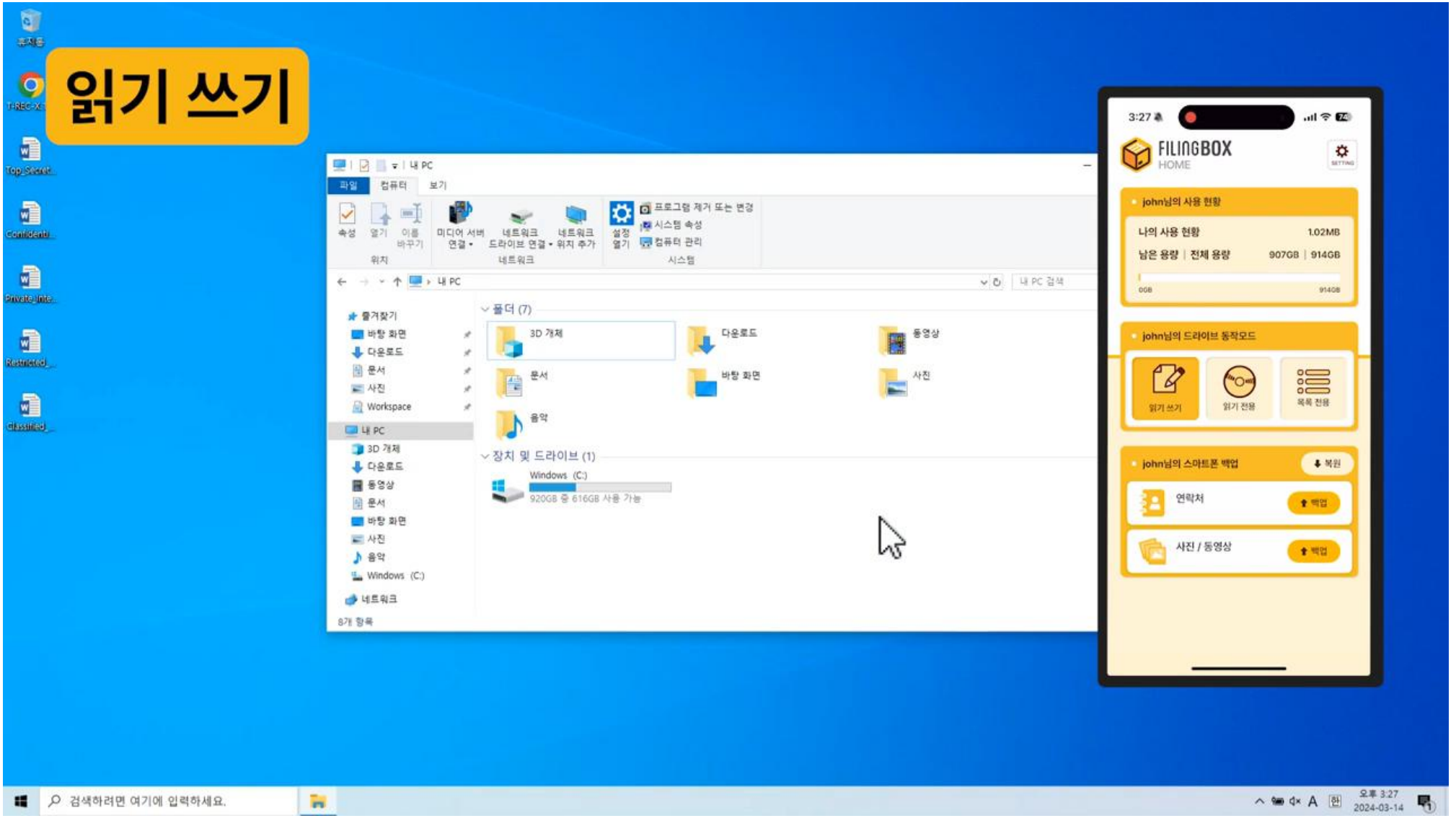
3. FilingBox Mega does not replace existing network or endpoint protection systems — instead, it complements them by addressing their inherent limitations.

Folder-Level Storage Protection

FILINGBOX GIGA

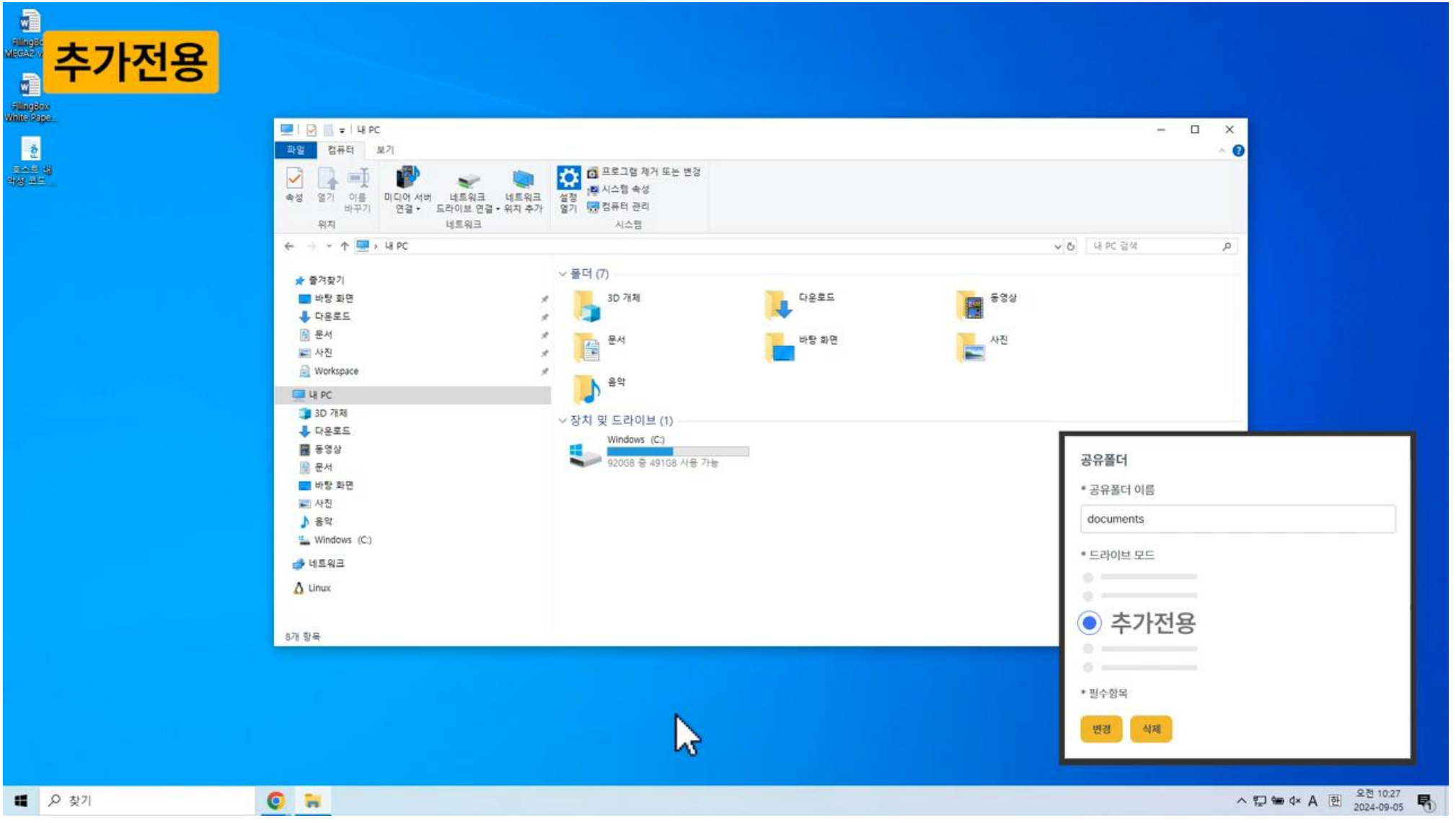
FilingBox GIGA, a folder-level storage protection solution, protects data for professionals who manage large volumes of data and for AI/OT/IoT devices that store sensitive data. It allows users to configure five operating modes per folder on a standard network file server to preemptively protect important data from malware attempting to encrypt or steal it. (International Standard ITU-T X.1560, GS Certification)

Personal Folder Mode Settings (Add-Only, List-Only)



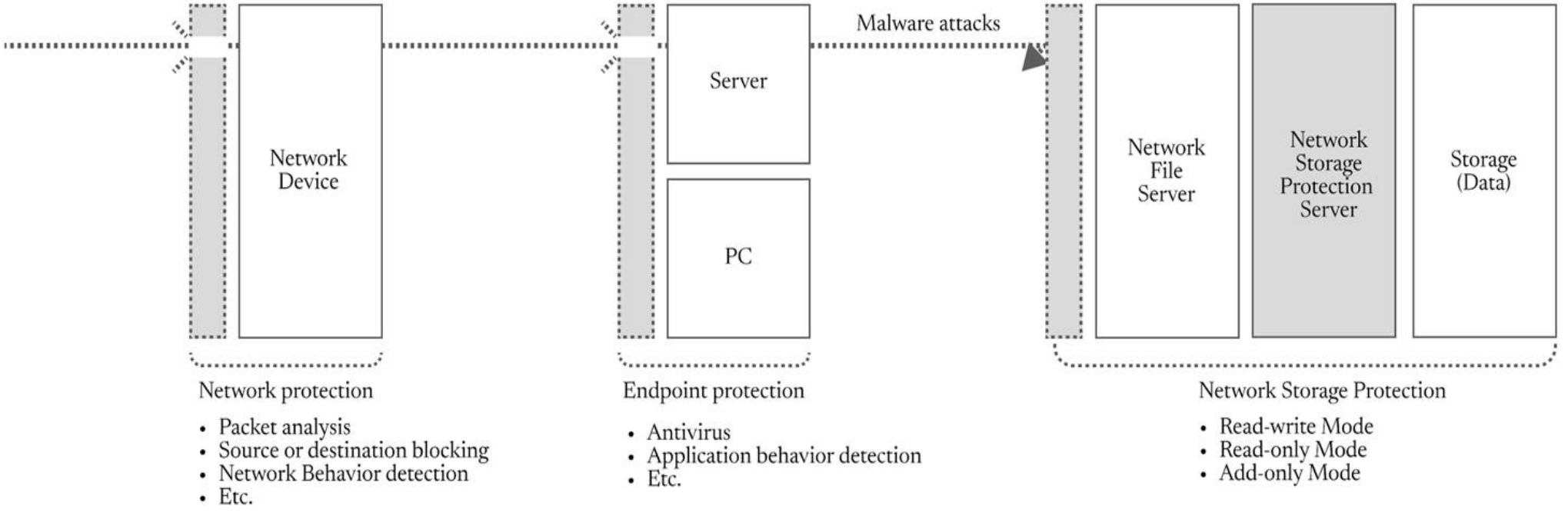
https://youtu.be/CYV2Z4IMgoo

Shared Folder Mode Settings (Add-Only, Read/Write, Hidden-Only)



https://youtu.be/g4OV179HSkg

02 Production Introduction – Folder-Level Storage Protection



FilingBox GIGA Features

Professionals who manage large volumes of data use file servers for systematic data management. However, hackers tend to target file servers first, as attacking them yields greater impact. Conventional file servers are shared storage without built-in protection functions, leaving them vulnerable to ransomware and data theft attacks — and valuable data can be lost instantly. Additionally, AI/OT/IoT devices often generate and store sensitive data, but traditional storage systems have limitations in protecting such data.

FilingBox GIGA, while using the standard SAMBA protocol like ordinary file servers, adds extra configuration for operating modes per folder to protect data from various cyberattacks. When a folder is set to Read-Write Mode, normal file creation, editing, and deletion are allowed. When set to Read-Only Mode, existing files can only be viewed, and creation, modification, or deletion is disabled. In Add-Only Mode, read requests for existing files return read-only fake data, so existing files cannot be opened and only new files can be added. Finally, in List-Only Mode, only file lists can be viewed — no creation, opening, modification, or deletion is permitted — thus ensuring data protection.

FIlingBox GIGA Benefits

1. Even if a file server is accessed through a specific user account or device, each folder’s independent operating mode ensures that data remains protected against ransomware or data-theft attacks coming from authorized accounts or devices.

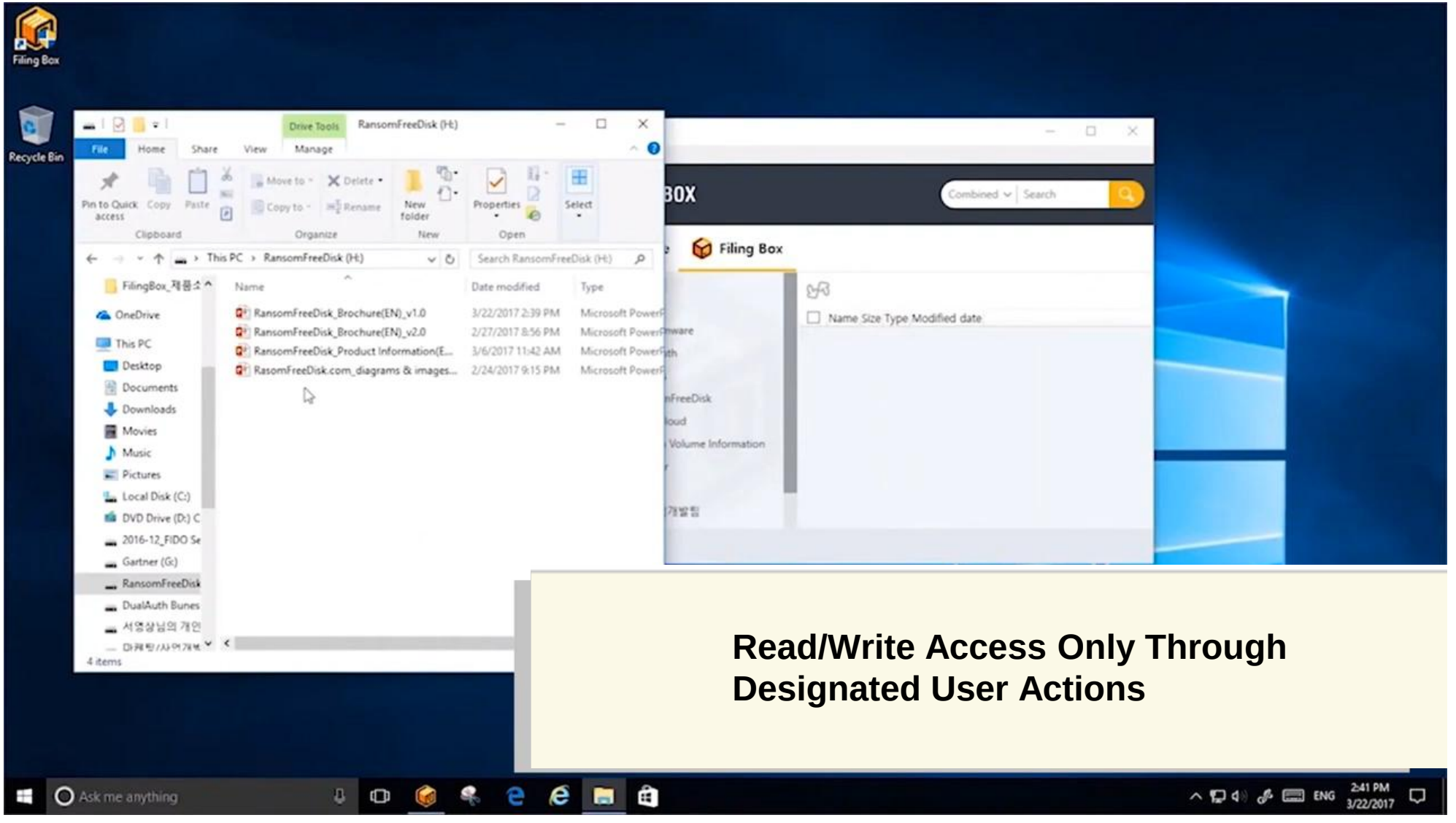
2. Each user in FilingBox GIGA is provided with a personal folder, and users can directly select their folder’s operating mode via a mobile app to protect personal data from malware attacks.

3. Administrators of FilingBox GIGA can also create shared folders, and by selecting the operating mode of each shared folder, they can prevent data within the shared folder from being leaked or encrypted.

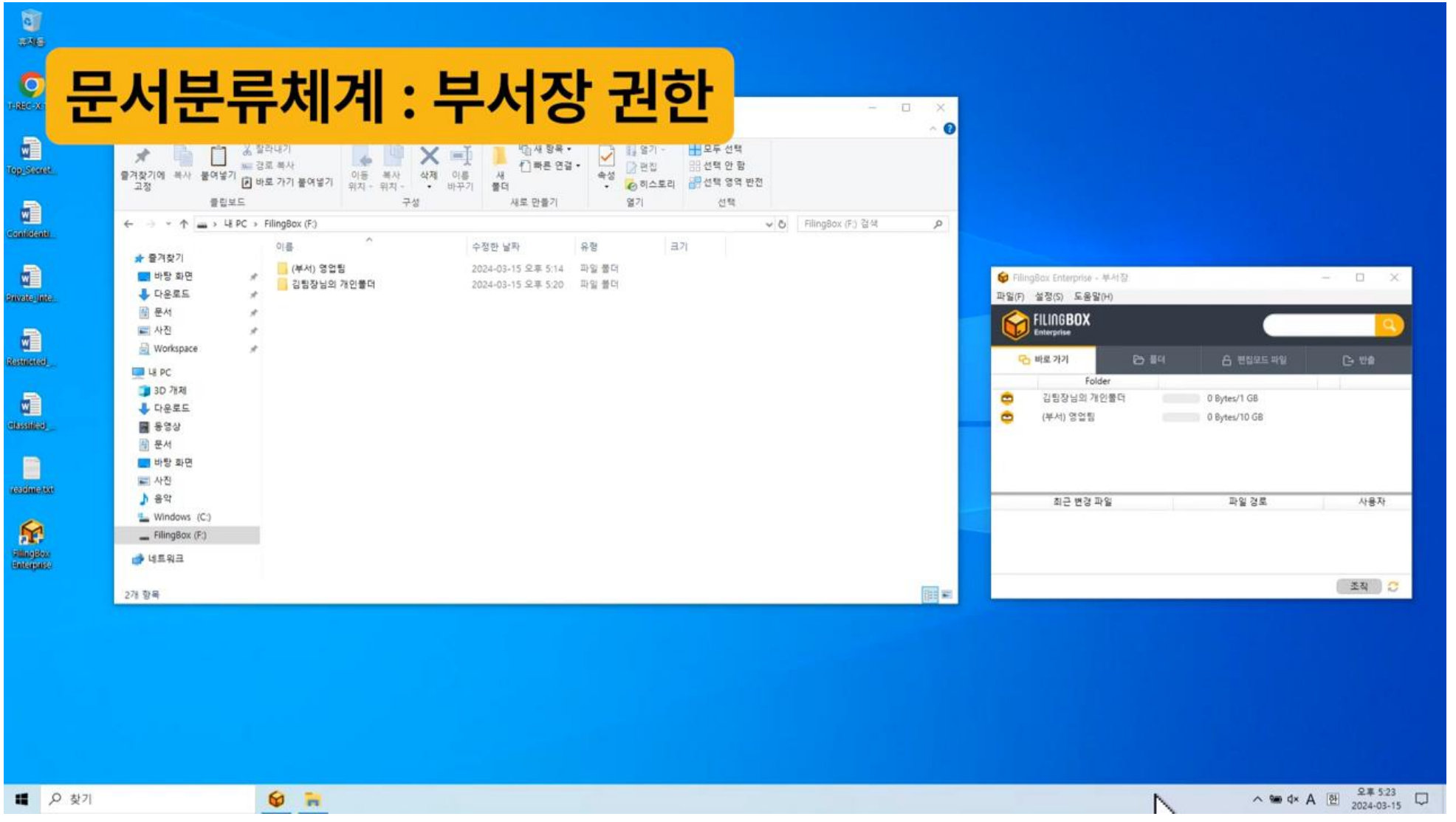
User-Action-Level Storage Protection

FILINGBOX ENTERPRISE

FilingBox Enterprise, a user-action-level storage protection solution, provides data only when a user requests to open a file together with an edit/open action.
For any other data access requests, it supplies read-only data instead. This technology protects data within the storage in advance from ransomware attacks. (GS Certification)

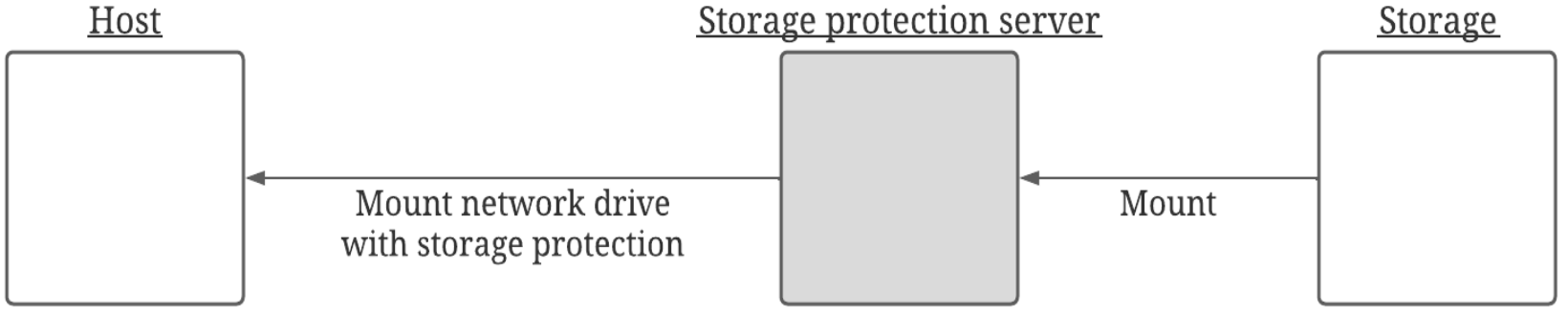


https://youtu.be/CYV2Z4IMgoo



https://youtu.be/U7m03gCA0TM

02 Production Introduction – User-Action-Level Storage Protection



FilingBox Enterprise Features

FilingBox Enterprise, designed for large-scale users, provides editable, genuine data only when files are accessed through explicit user actions such as “Open in Edit Mode.” For all other data requests, it supplies read-only data, thereby protecting storage data in advance from malware that attempts to encrypt files.

FIlingBox Enterprise Benefits

1. Even if a user accidentally executes ransomware on their PC, the data stored in FilingBox Enterprise, used for collaboration with colleagues, remains unencrypted because it is provided as read-only.

2. Since FilingBox Enterprise inspects user actions requesting data at the back-end of the network storage, it protects data without slowing down PCs, unlike antivirus or EDR software.

3. In addition to data protection, FilingBox Enterprise provides team folders, project folders, personal folders, and shared folders, enabling systematic document access control within the organization. It also supports document classification folders and search functions, allowing for comprehensive company-wide document management and protection.

FILINGCLOUD

01

Company Overview

02

Product Introduction

03

Achievements & References

04

Contact

03 Achievements & References

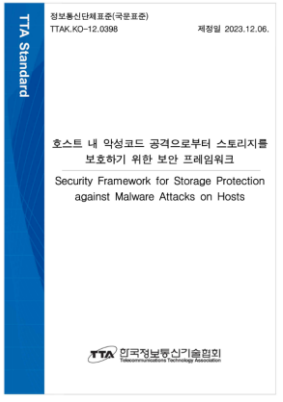
Awards

IR52 Jang Yeong-sil Award

The Minister's Award

The Commissioner's Award

Standard Technologies



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

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

Presentations

AI for Good

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

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

eGISEC 2025

https://youtu.be/xVZBZ_MM4_I

DATACON LA

https://youtu.be/CGKFihLeTZ0

ISEC 2024
INTERNATIONAL SECURITY CONFERENCE

https://youtu.be/Vct8PdaU34k

Certificates

ISO/IEC 25023, 25051, 25041

Cloud Service
Accredited by KACI

ioXt
internet of secure things

FIPS VALIDATED 140-2

03 Achievements & References

Finance

KB Card – Established a collaborative file server for protecting personal information of internal staff and partner companies.

NH Investment & Securities – Built a company-wide file sharing system and storage for external data transfer.

Mirae Asset Life Insurance – Implemented a secure file server system for collaboration.

Korea Investment Partners – Deployed a secure file sharing system for ransomware defense and data protection.

M Capital (formerly Hyosung Capital) – Built a business data backup system in response to ransomware threats.

Enterprise

CMB Daejeon Broadcasting – Introduced a file sharing system to prevent ransomware attacks.

Samyoung Soonhwa – Provided a file sharing service based on Microsoft Azure.

A-Sung Korea – Established a secure file sharing system for ransomware protection.

Woowon Technology – Implemented a file sharing system to enhance data security and prevent ransomware.

Public Sector

Statistics Korea – Built a centralized document management system for national census data.

Korea Railroad Corporation (KORAIL) – Established a secure file server to protect important data on user PCs of the next-generation procurement system and prevent ransomware.

Korea National Oil Corporation – Built a PC data backup and sharing system for ransomware response.

Korea Iron & Steel Association – Implemented an integrated document management system.

Andong City Hall, Gyeongbuk Province – Deployed a secure web hard drive system to prevent ransomware.

Danyang County Office, Chungbuk Province – Built a PC data backup system for ransomware response.

Jindo County Office, Jeonnam Province – Established a cloud-based file sharing system for internal staff collaboration.

Boeun County Office, Chungnam Province – Introduced a secure web hard drive system to prevent damage or leakage of administrative data from employee PCs.

Chilgok County Office, Gyeongbuk Province – Built a file sharing system for ransomware defense and team collaboration.

Namdong District Office, Incheon – Established a centralized file management system.

Daedeok District Office, Daejeon – Built a PC data backup system for ransomware response.

Buk District Office, Gwangju – Built a cloud storage system aimed at preventing ransomware.

Chungbuk Education Research & Information Institute – Introduced a file sharing and collaboration system to advance the “Chungbuk Communication Messenger.”

KCL (Korea Conformity Laboratories) – Built a file sharing system for ransomware preparedness.

National Center for the Rights of the Child – Established a secure file sharing system (formerly Central Adoption Services).

FILINGCLOUD

04 Contact

FILINGCLOUD

- Company : FilingCloud
- Website : www.filingbox.com
- General Inquiry : support@filingbox.com

Korea Office

- Address : 130 Digital-ro, Suite 1311,Gumchon-gu Seoul 08589
- Telephone : +82-2-6925-1305
- Business Inquiry : Sales@filingbox.com

Thank you