Storage Protection to Safeguard Data from Malware

FilingBox GIGA Product Introduction

FILINGCLOUD

01

Product Overview

02

Key Features

03

Achievements & References

04

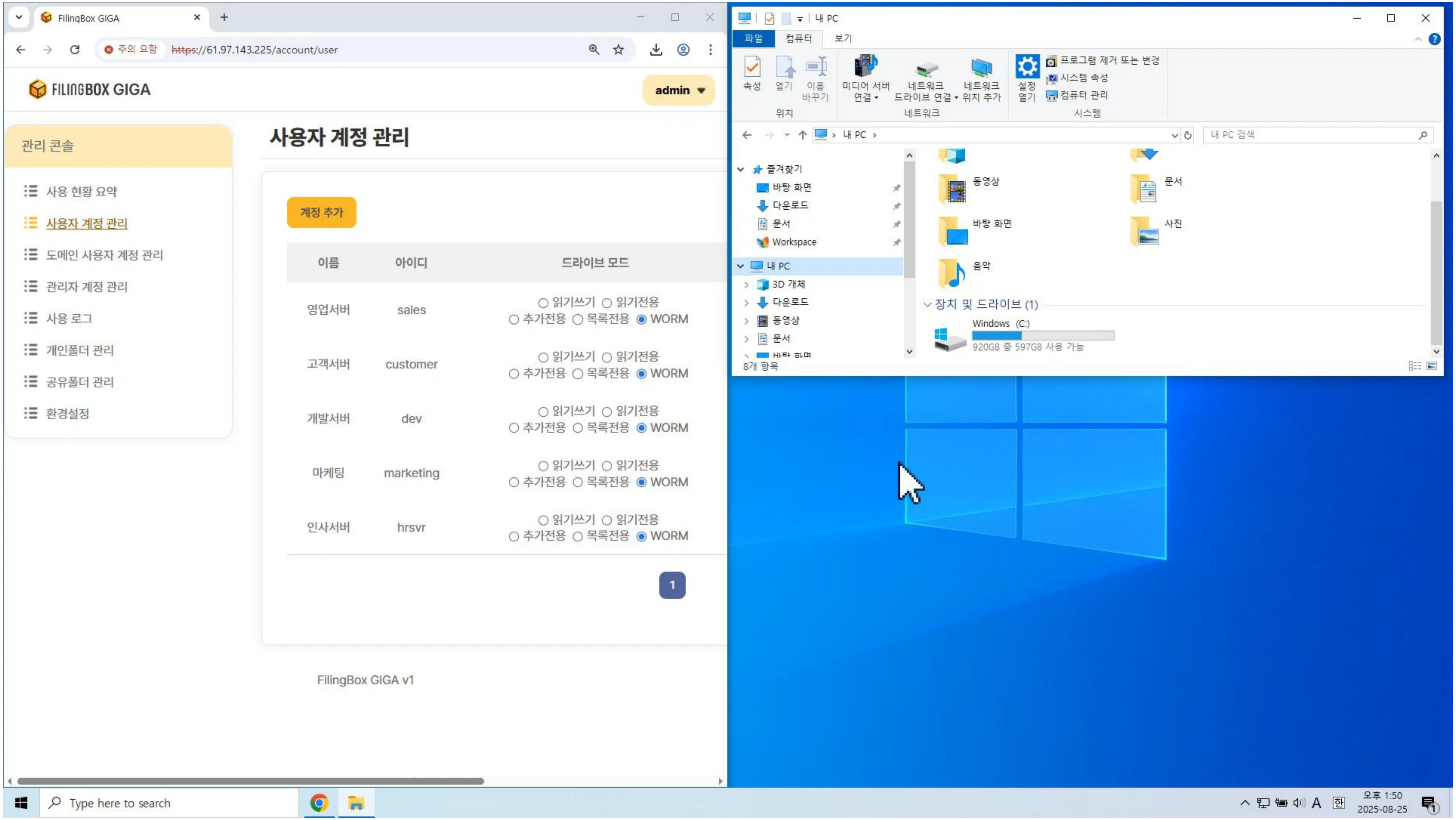
Company Introduction

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 operation 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)

01 Product Overview



FilingBox GIGA

주의 요함 ~~https~~://61.97.143.225/account/user

FILINGBOX GIGA

admin

관리 콘솔

- 사용 현황 요약
- 사용자 계정 관리
- 도메인 사용자 계정 관리
- 관리자 계정 관리
- 사용 로그
- 개인폴더 관리
- 공유폴더 관리
- 환경설정

사용자 계정 관리

계정 추가

이름	아이디	드라이브 모드
영업서버	sales	○ 읽기쓰기 ○ 읽기전용 ○ 추가전용 ○ 목록전용 ● WORM
고객서버	customer	○ 읽기쓰기 ○ 읽기전용 ○ 추가전용 ○ 목록전용 ● WORM
개발서버	dev	○ 읽기쓰기 ○ 읽기전용 ○ 추가전용 ○ 목록전용 ● WORM
마케팅	marketing	○ 읽기쓰기 ○ 읽기전용 ○ 추가전용 ○ 목록전용 ● WORM
인사서버	hrsvr	○ 읽기쓰기 ○ 읽기전용 ○ 추가전용 ○ 목록전용 ● WORM

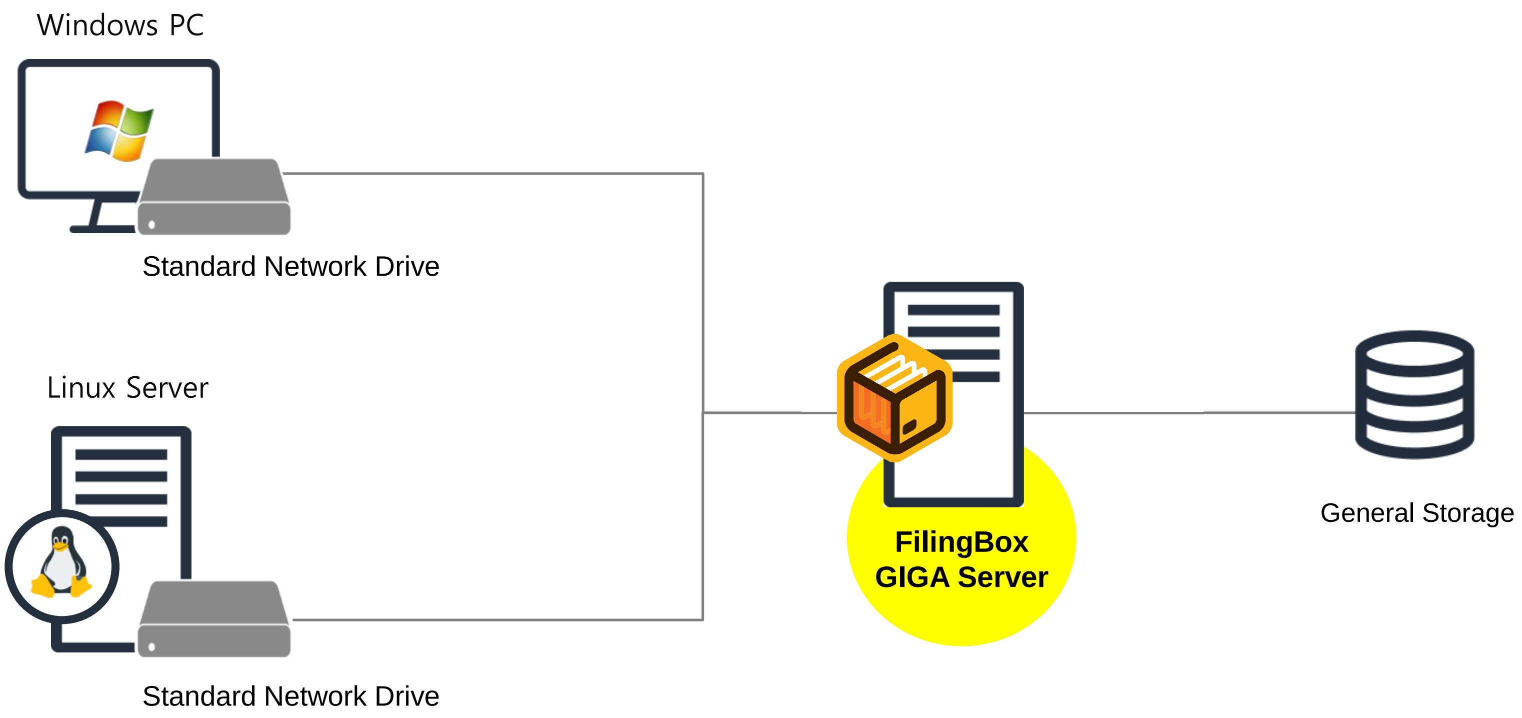
1

FilingBox GIGA v1

https://youtu.be/KVwNii9AY3k

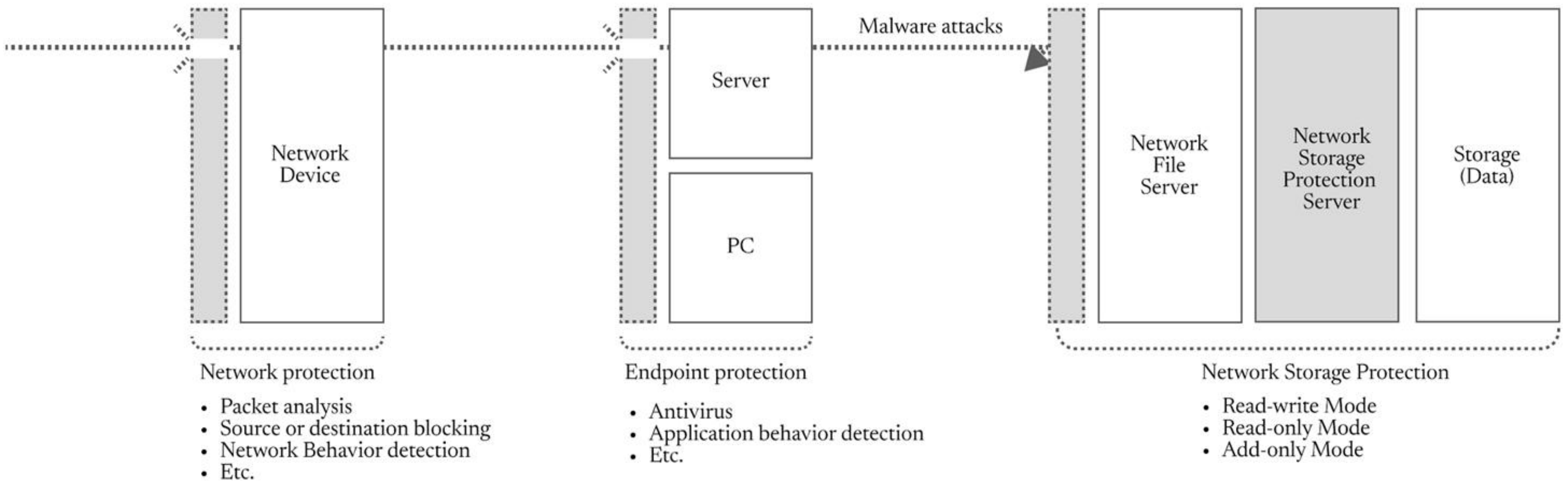
FilingBox GIGA Architecture

FilingBox GIGA is a folder-level storage protection solution that embeds data protection functions into a standard Samba file server. The GIGA server utilizes a standard Samba file server, so there is no need to install separate client software on client devices. Users can connect network drives from various client devices, including Windows, Linux, iOS, and Android, and configure operation modes on the connected network drives to protect the data within them. The available operation modes are Read/Write, Read-Only, Add-Only, WORM (Write Once Read Many), and List-Only.



International Network Storage Protection Standard – ITU X.nspam

FilingBox GIGA is a network file server that applies the X.nspam (Network Storage Protection against Malware) standard technology established by the International Telecommunication Union (ITU).
When malware or malicious code bypasses existing Network Protection or Endpoint Protection systems and executes, all data on the network drives connected to PCs or servers can be encrypted or stolen.
However, FilingBox GIGA adds a storage protection layer between the network file server and the storage, allowing operation modes (such as Read-Only, WORM, Add-Only, etc.) to be configured for network drives.
This ensures that even if an attack bypasses existing security layers, the data within the network drives remains safely protected.



Network protection

- Packet analysis
- Source or destination blocking
- Network Behavior detection
- Etc.

Endpoint protection

- Antivirus
- Application behavior detection
- Etc.

Network Storage Protection

- Read-write Mode
- Read-only Mode
- Add-only Mode

FILINGCLOUD

01

Product Overview

02

Key Features

03

Achievements & References

04

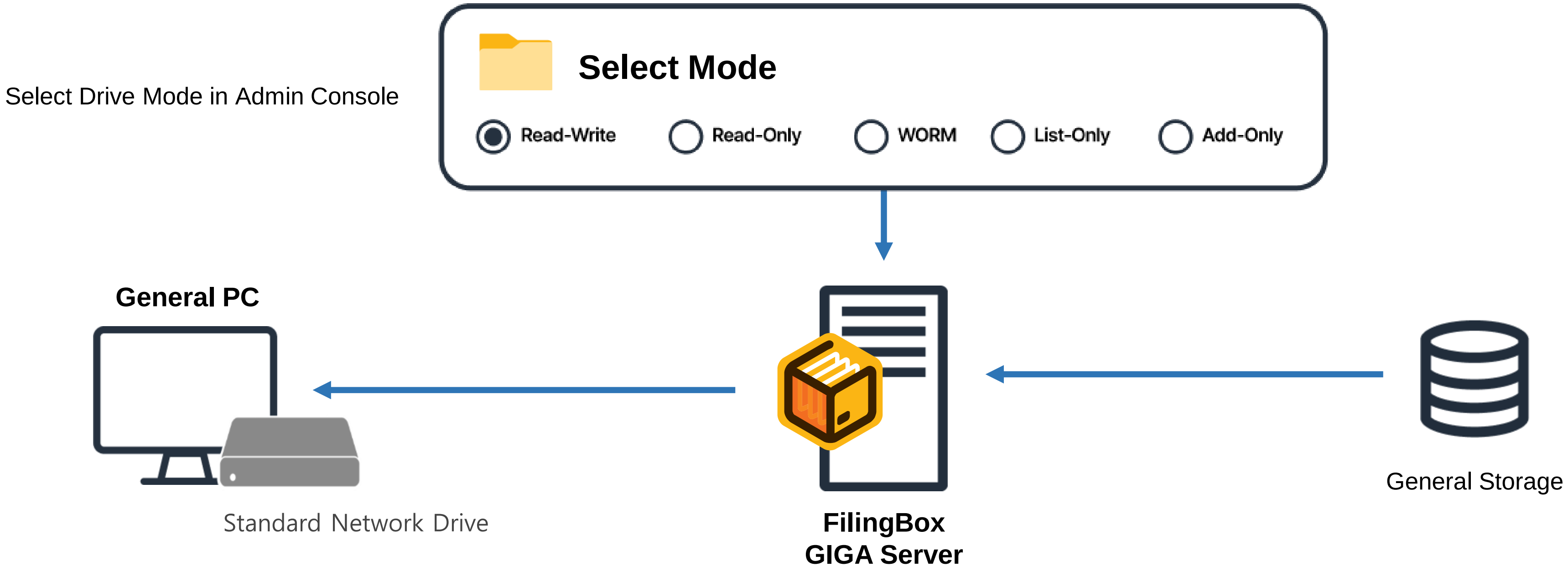
Company Introduction

02 Key Features

Feature 1 – Protects Data Even When Administrator Privileges on a PC or Server Are Compromised by Advanced Cyberattacks

Even if advanced cyberattacks such as Remote Code Execution (RCE) or Zero-day Exploits occur and administrator privileges are compromised, the data stored in FilingBox GIGA remains securely protected. FilingBox GIGA combines storage protection with a standard network file server—providing network drives to PCs or servers, while directly controlling their operation modes from within FilingBox GIGA.

In addition, operation modes are configured out-of-band via the FilingBox GIGA administrator console, not from the network drive itself, which prevents attackers from altering them. When an administrator designates modes such as Read-Only, WORM, or Add-Only, the data cannot be encrypted or deleted even if administrator privileges on the PC or server are compromised. In other words, FilingBox GIGA securely protects network drive data even during an active attack.



Select Drive Mode in Admin Console

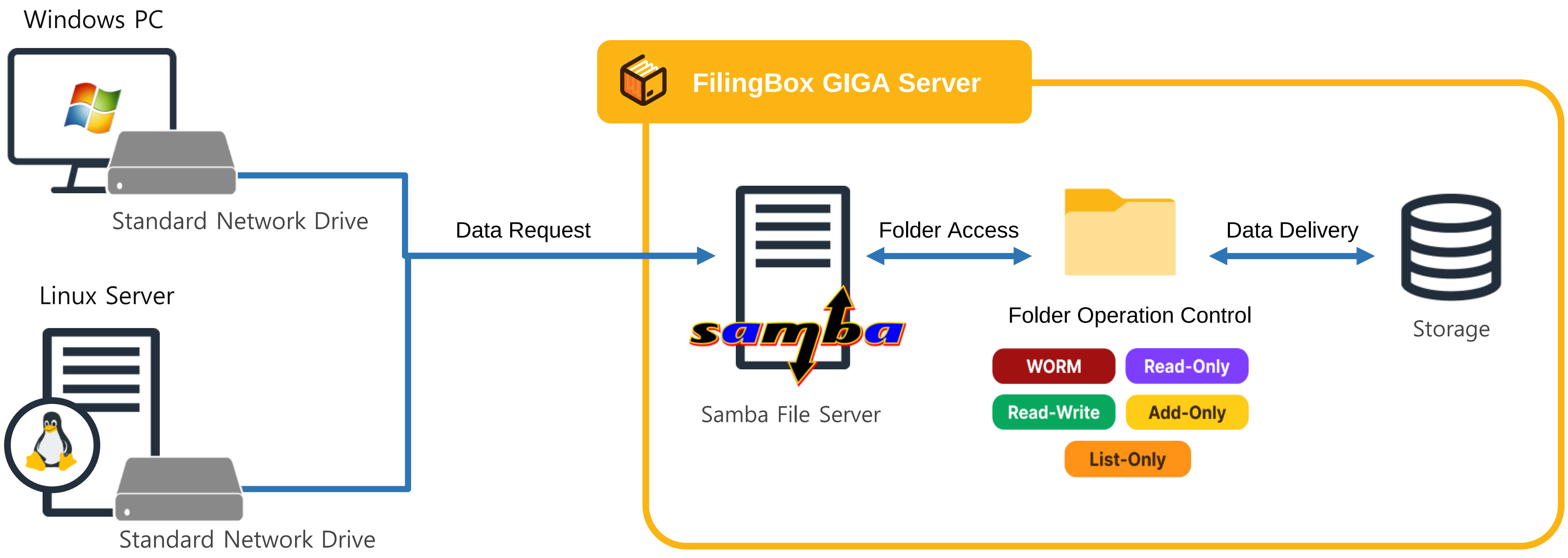
Select Mode

● Read-Write ○ Read-Only ○ WORM ○ List-Only ○ Add-Only

Feature 2 – Standard Network File Server Supporting Five Operation Modes

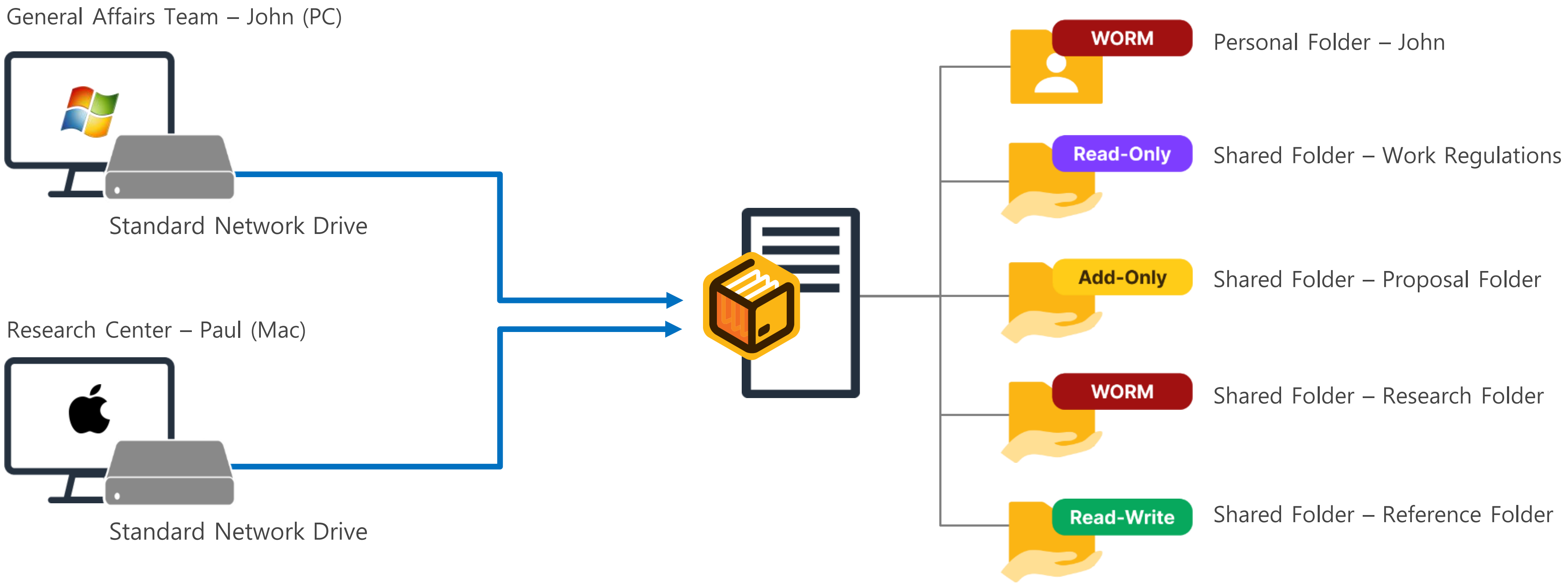
FilingBox GIGA allows network drives provided to PCs or servers to be configured in five operation modes: Read-Write, Read-Only, WORM (Write Once Read Many), Add-Only, and List-Only. Administrators can assign modes per drive, enabling flexible operation according to data usage and required security levels.

For example, frequently updated documents can be set to Read-Write, public notices to Read-Only, and research data can be protected using the WORM mode. Likewise, incoming records for an approval system can be stored in Add-Only mode, while List-Only mode restricts access to viewing filenames only. Through these five operation modes, FilingBox GIGA effectively safeguards network drive data against a wide range of threats.



Feature 3 – File Server Supporting Operation Modes from Personal to Group Folders

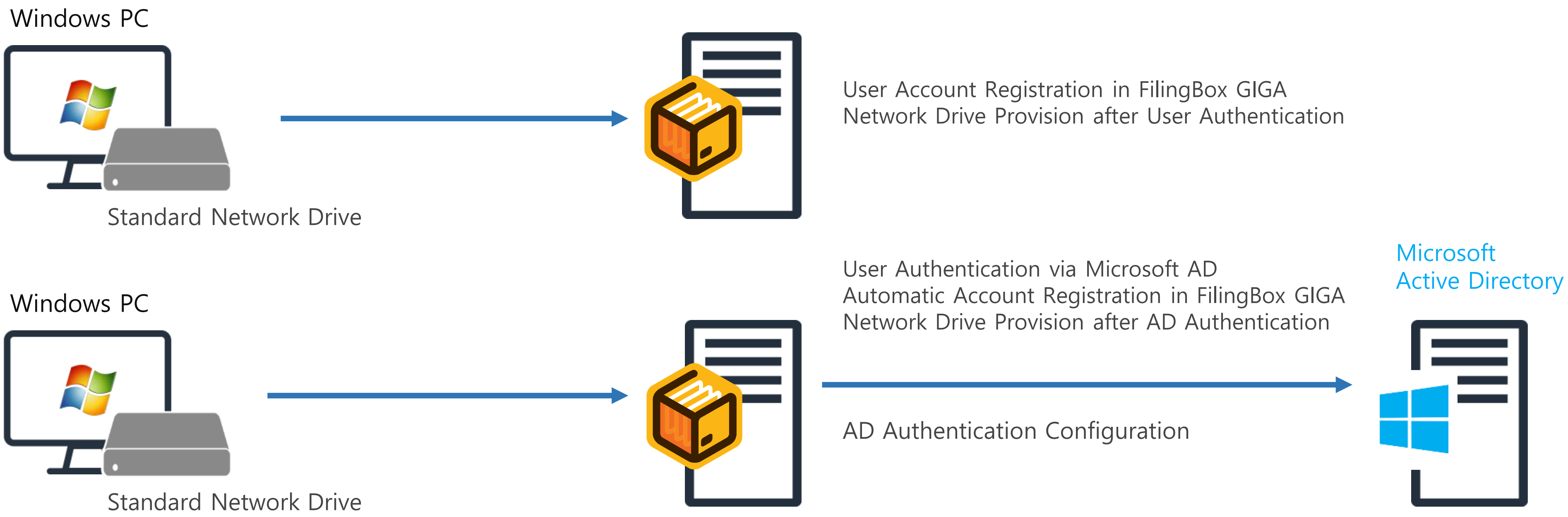
FilingBox GIGA automatically creates a personal folder each time an administrator adds a new user account, allowing a specific operation mode to be assigned per folder so that individual work data can be protected according to its purpose. When the administrator creates group folders, each can also be configured with its own operation mode, enabling secure management of shared team data. For example, setting a group folder to **WORM** mode ensures that files cannot be modified or deleted once created, maintaining data integrity and transparency during collaboration. Therefore, even if some users’ PCs or servers are compromised, shared files remain safe. Through this flexible structure, FilingBox GIGA provides a file server environment that applies appropriate protection policies for both individual and group-level data, matching diverse operational and security needs.


General Affairs Team – John (PC)
Standard Network Drive
Research Center – Paul (Mac)
Standard Network Drive
WORM
Personal Folder – John
Read-Only
Shared Folder – Work Regulations
Add-Only
Shared Folder – Proposal Folder
WORM
Shared Folder – Research Folder
Read-Write
Shared Folder – Reference Folder

Feature 4 – Supporting Authentication from File Server Accounts to Active Directory (AD)

FilingBox GIGA allows administrators to manually create user accounts and provide each user with a network drive. This enables small organizations or environments without a centralized account system to easily issue accounts and operate a secure file server.

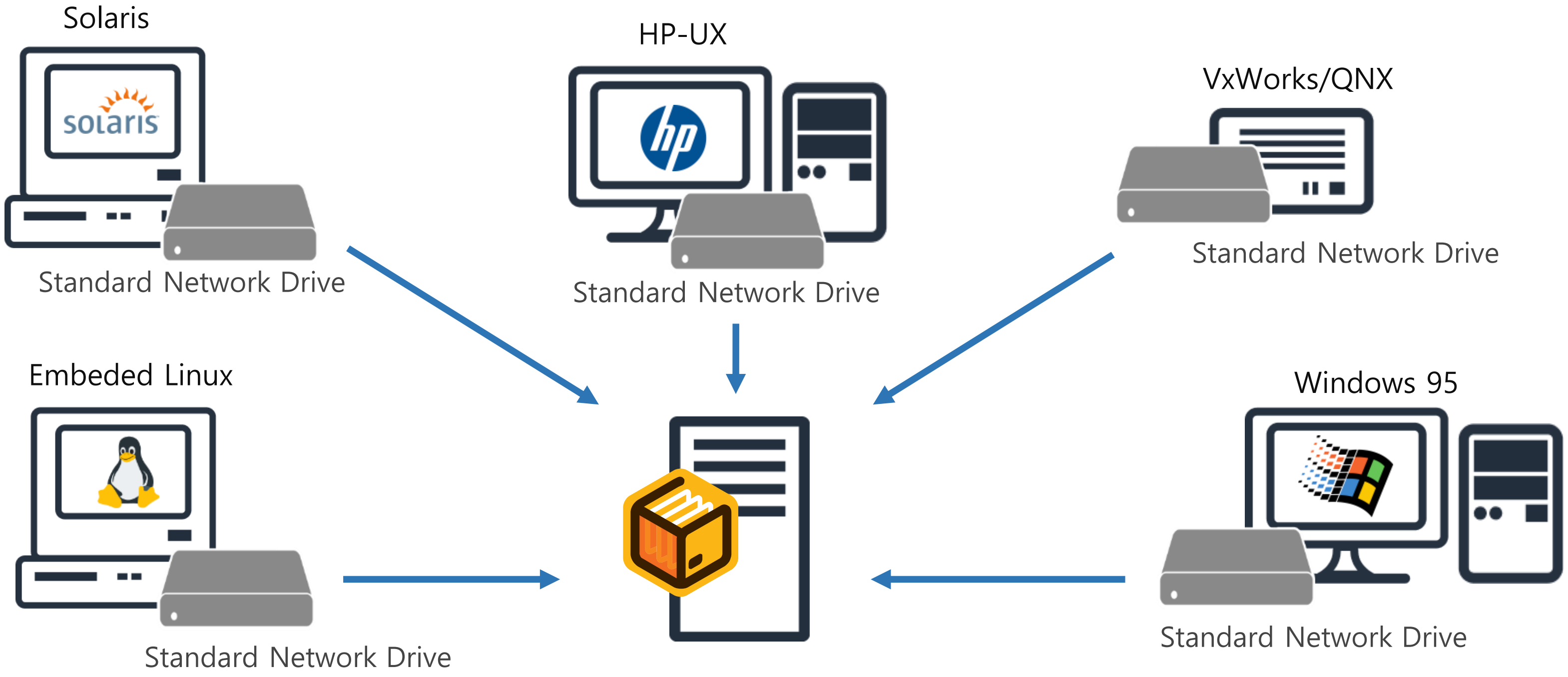
For organizations already using Microsoft Active Directory (AD), FilingBox GIGA administrator can simply enable AD authentication in the authentication settings. Once configured, users can automatically create and access their network drives through AD credentials—without any separate account registration. This approach allows companies and institutions that use AD to adopt and expand GIGA seamlessly, ensuring smooth integration with their existing infrastructure.


Windows PC
Standard Network Drive
User Account Registration in FilingBox GIGA
Network Drive Provision after User Authentication
Windows PC
Standard Network Drive
User Authentication via Microsoft AD
Automatic Account Registration in FilingBox GIGA
Network Drive Provision after AD Authentication
AD Authentication Configuration
Microsoft
Active Directory

Feature 5 – Data Protection for Legacy Servers and EMR Devices Using Standard Network Drives

Since FilingBox GIGA is based on the standard Samba (SMB) network drive protocol, it can reliably store and protect data across a wide range of operating systems, including Windows, macOS, Linux, iOS, and Android. This enables not only modern systems but also legacy servers and lightweight IoT or EMR devices to securely store files without any additional software installation.

In particular, when a web server is connected to FilingBox GIGA's WORM network drive, even if the web server is compromised, user-uploaded data remains tamper-proof and undeletable. Likewise, for services that periodically generate data—such as database backups or CCTV recordings—connecting via the Add-Only mode allows new data to be continuously accumulated while preventing existing data from being modified or accessed, ensuring stable and secure backup data protection.



FILINGCLOUD

01

Product Overview

02

Key Features

03

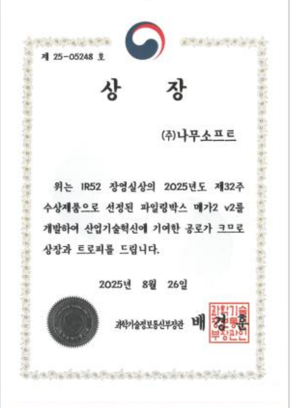
Achievements & References

04

Company Introduction

03 Achievements & References

Awards



제 25-05248 호

상 장

(주)나무소프트

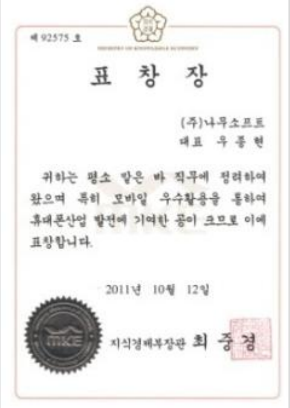
위는 IR52 장영실상의 2025년도 제32주 수상제품으로 선정된 파일링박스 메가2 v2를 개발하여 산업기술혁신에 기여한 공로가 크므로 상장과 트로피를 드립니다.

2025년 8월 26일

과학기술정보통신부장관 배 경 훈

과학기술정보통신부장관인

IR52 Jang Yeong-sil Award



제 92575 호

표 창 장

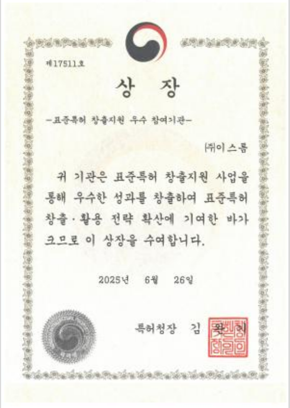
(주)나무소프트
대표 우 종 현

귀하는 평소 맡은 바 직무에 정려하여 왔으며 특히 모바일 우수활용을 통하여 휴대폰산업 발전에 기여한 공이 크므로 이에 표창합니다.

2011년 10월 12일

지식경제부장관 최 중 경

The Minister's Award



제17511호

상 장

-표준특허 창출지원 우수 참여기관-

(주)이스톰

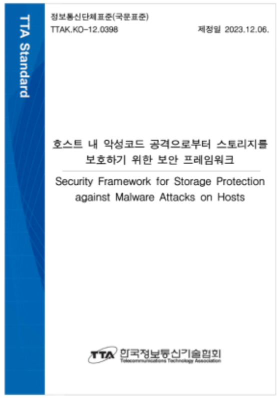
귀 기관은 표준특허 창출지원 사업을 통해 우수한 성과를 창출하여 표준특허 창출·활용 전략 확산에 기여한 바가 크므로 이 상장을 수여합니다.

2025년 6월 26일

특허청장 김 완 기

The Commissioner's Award

Standard Technologies



TTA Standard

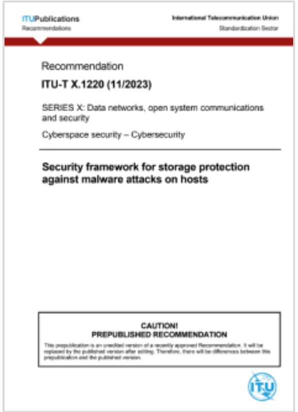
정보통신단체표준(국문표준)
TTAK.KO-12.0398 제정일 2023.12.06.

호스트 내 악성코드 공격으로부터 스토리지를 보호하기 위한 보안 프레임워크

Security Framework for Storage Protection against Malware Attacks on Hosts

TTA 한국정보통신기술협회
Telecommunications Technology Association

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



ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1220 (11/2023)

SERIES X: Data networks, open system communications and security

Cyberspace security – Cybersecurity

Security framework for storage protection against malware attacks on hosts

CAUTION!
PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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

Presentations

AI for Good

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

ITUEvents

Cyber Drill Asia-Pacific 2025

02-05 September 2025
Ulaanbaatar, Mongolia

#Cybersecurity
itu.int/cyberdrills

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

GOOD Software

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.

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).

01

Product
Overview

02

Key
Features

03

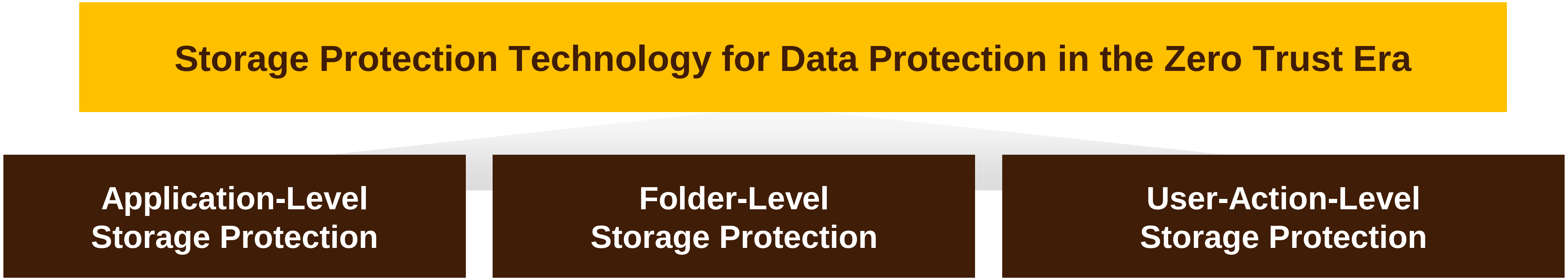
Achievements
& References

04

Company
Introduction

Storage Protection 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

Protects data on Linux and Windows servers.

FILINGBOX GIGA

Protects data on NAS systems, professional environments, and AI/OT/IoT devices.

FILINGBOX ENTERPRISE

Protects and manages data for enterprises and public institutions.

04 Company Introduction

FILINGCLOUD

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

Request Implementation

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

Thank you