

Storage Protection to Safeguard Data from Malware

FilingBox GLGA

Product Introduction



FILINGCLOUD

01

Product
Overview

02

Key
Features

03

Achievements
& References

04

Company
Introduction

Folder-Level Storage Protection

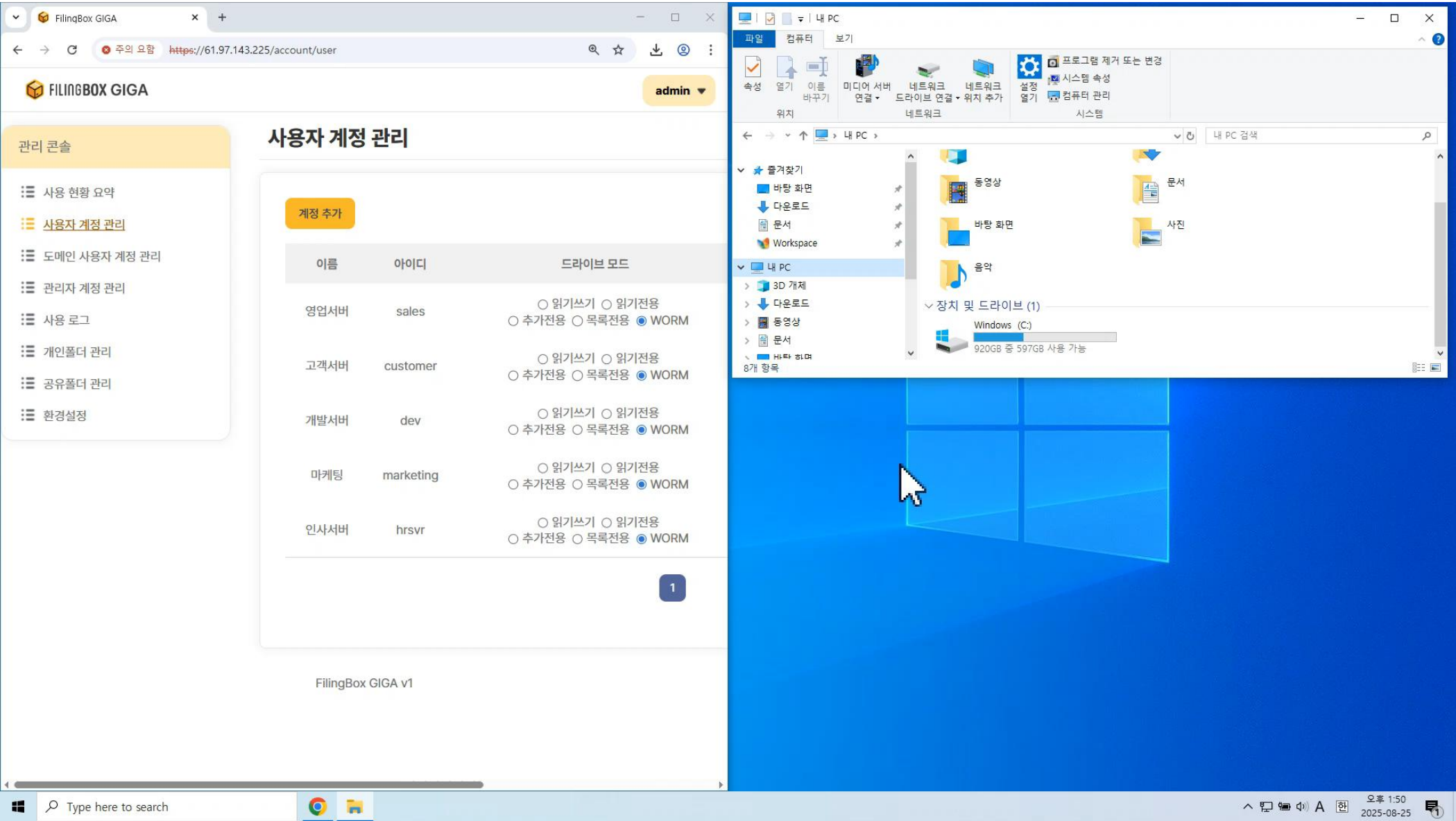


FILINGBOX GIGA

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.1223, GS Certification)

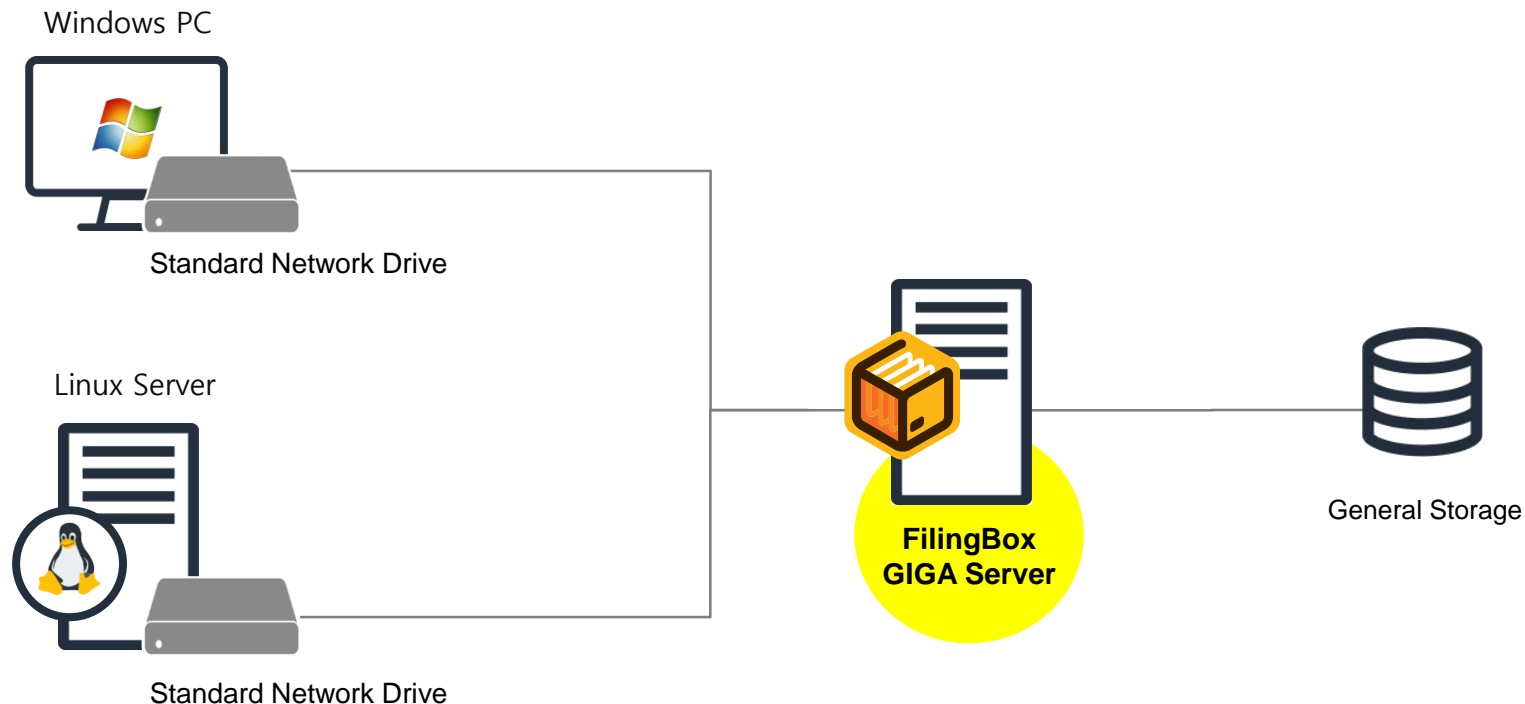
01 Product Overview



<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.



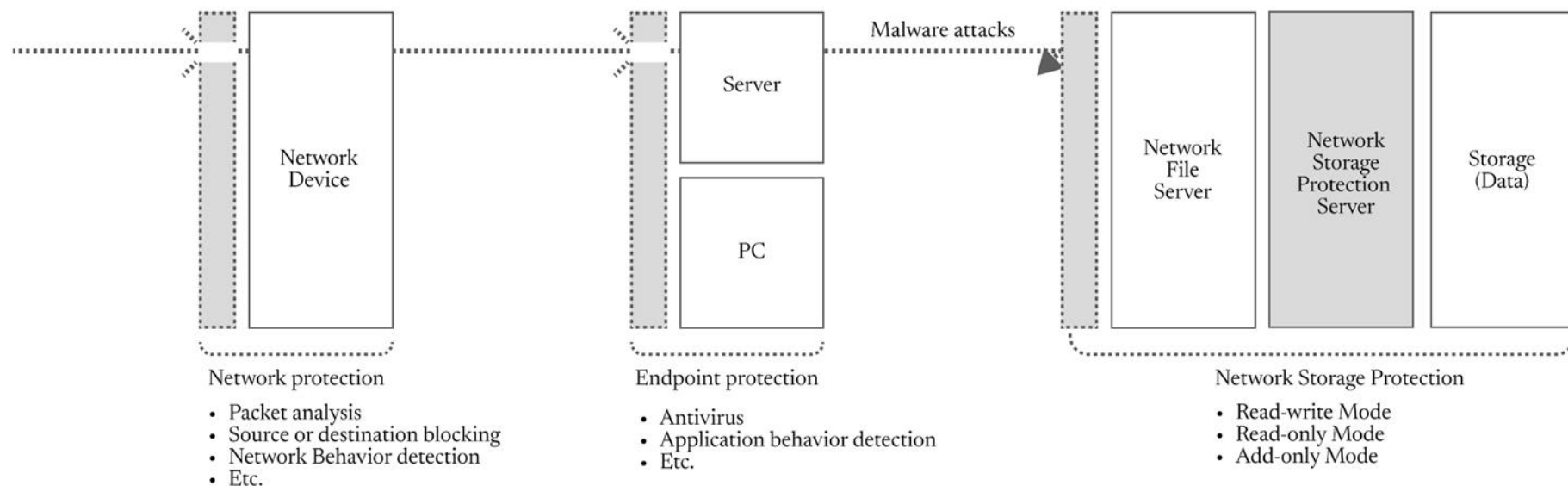
International Network Storage Protection Standard – ITU X.nspam

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.



01

Product
Overview

02

Key
Features

03

Achievements
& References

04

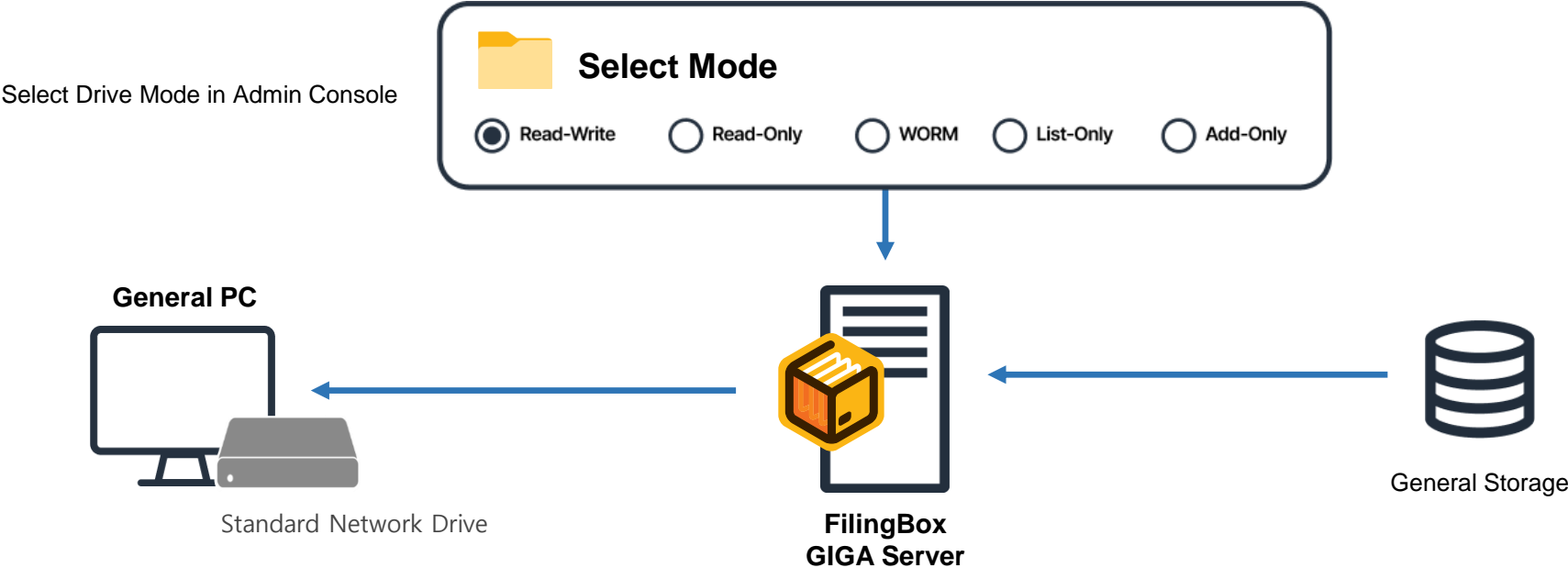
Company
Introduction

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.

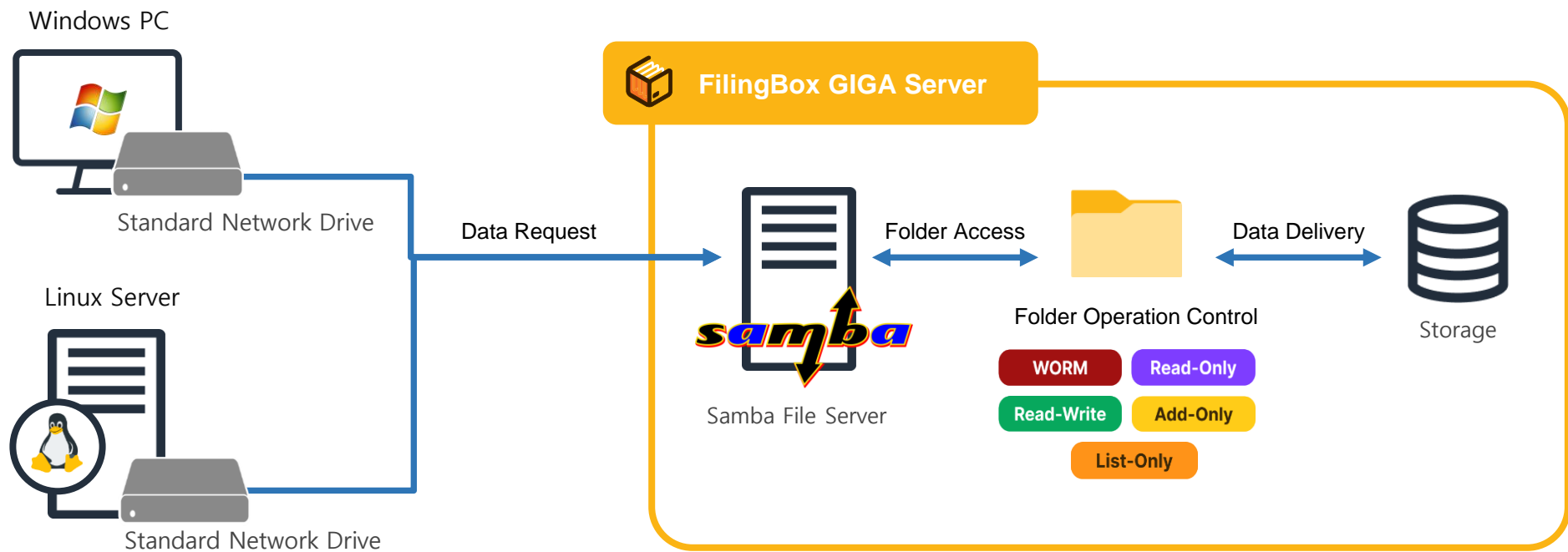
In addition, operation modes are configured out-of-band via the FilingBox GIGA administrator console, not from the network drive itself, which prevents attackers from altering them. When an administrator designates modes such as Read-Only, WORM, or Add-Only, the data cannot be encrypted or deleted even 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.



Feature 2 – Standard Network File Server Supporting Five Operation Modes

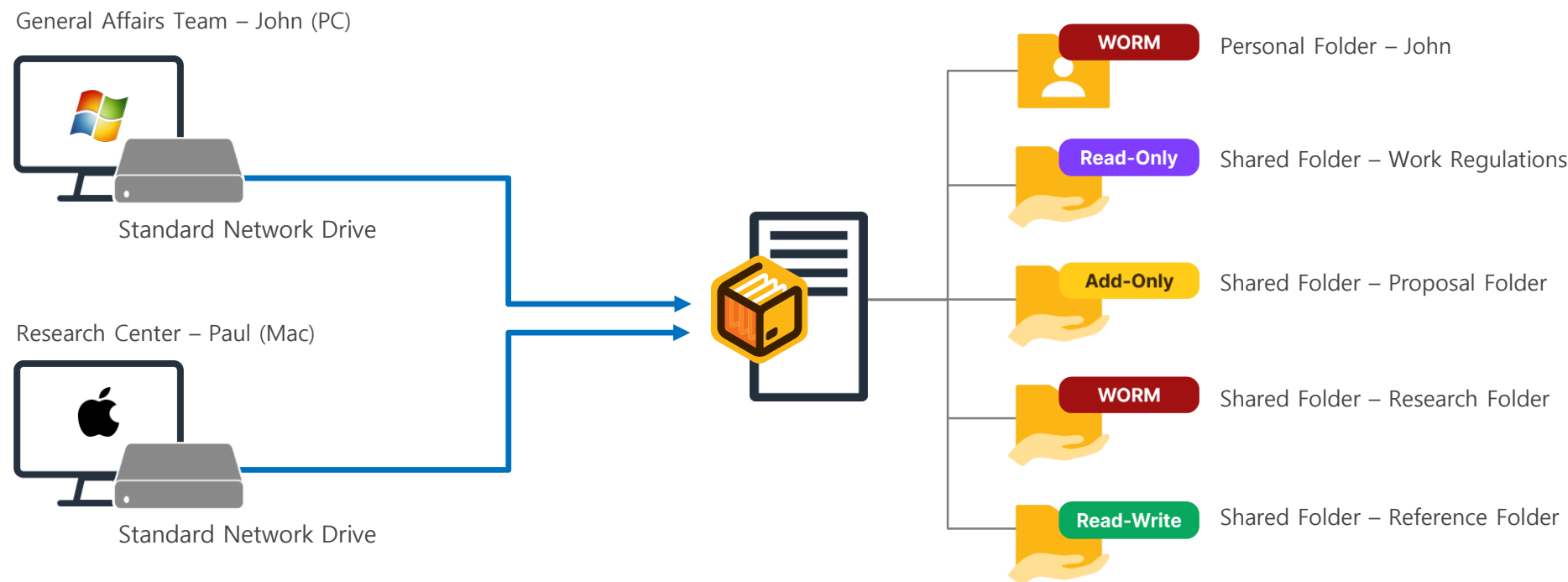
FilingBox GIGA allows network drives provided to PCs or servers to be configured in five operation modes: Read-Write, Read-Only, WORM (Write Once Read Many), Add-Only, and List-Only. Administrators can assign modes per drive, enabling flexible operation according to data usage and required security levels.

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.

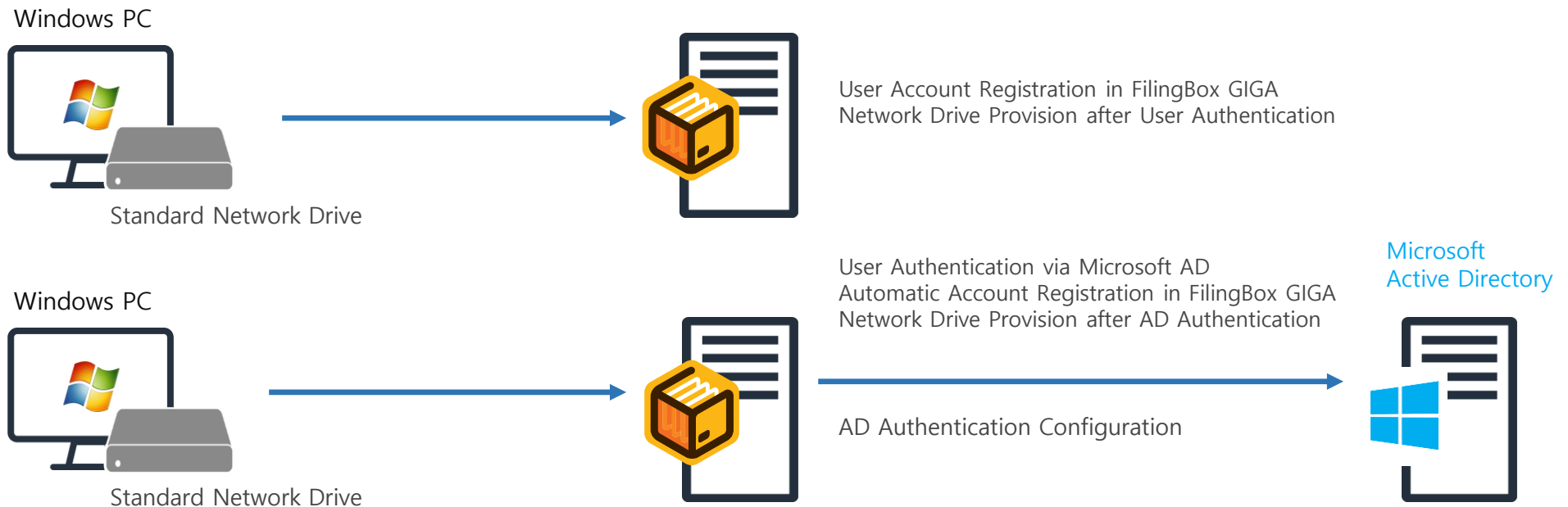


02 Key Features

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.

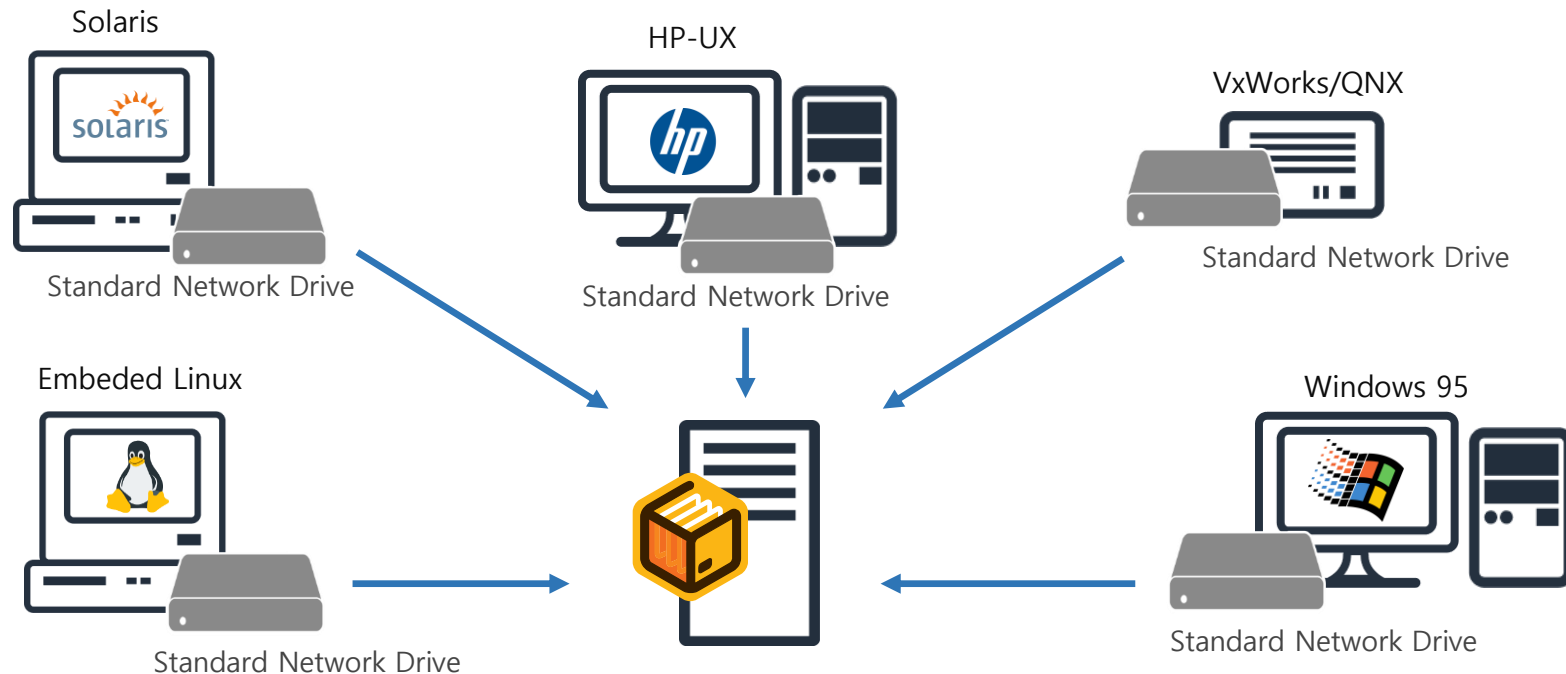


02 Key Features

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.



01

Product
Overview

02

Key
Features

03

Achievements
& References

04

Company
Introduction

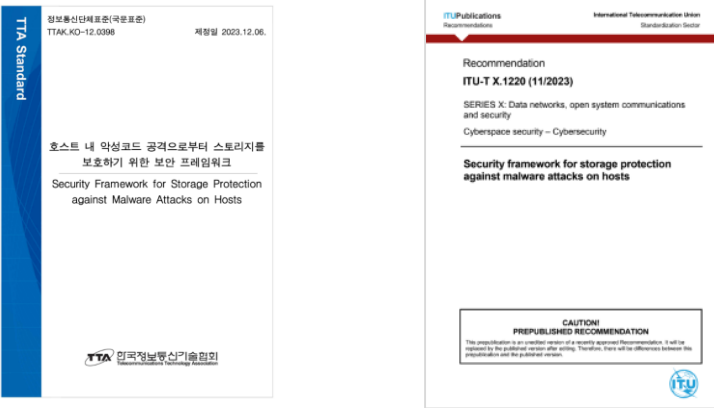
03 Achievements & References

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



Certificates



03 Achievements & References

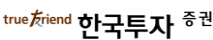
Finance



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.

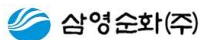


M Capital (formerly Hyosung Capital) – Built a business data backup system in response to ransomware threats.

Enterprise



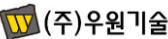
CMB Daejeon Broadcasting – Introduced a file sharing system to prevent ransomware attacks.



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



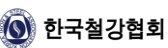
Statistics Korea – Built a centralized document management system for national census data.



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.1223, 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**



FILINGBOX MEGA

Protects data on Linux and Windows servers.

**Folder-Level
Storage Protection**



FILINGBOX GIGA

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

**User-Action-Level
Storage Protection**



FILINGBOX ENTERPRISE

Protects and manages data for enterprises and public institutions.

04 Company Introduction



- 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