Storage Protection to Safeguard Data from Malware

FilingBox MEGA Product Introduction

FILINGCLOUD

FILINGCLOUD

01

Product
Overview

02

Key
Features

03

Achievements
& References

04

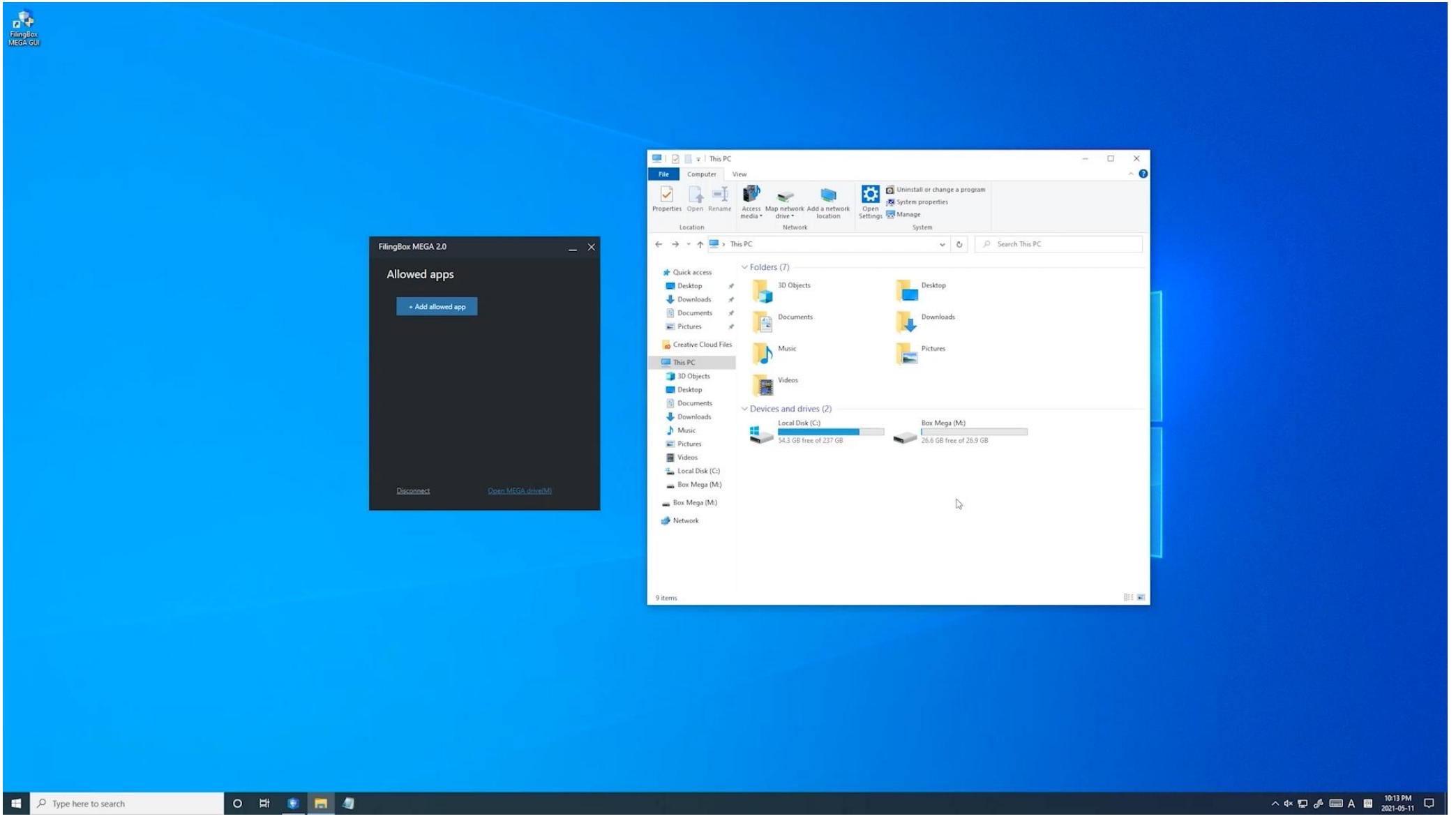
Company
Introduction

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)

01 Product Overview

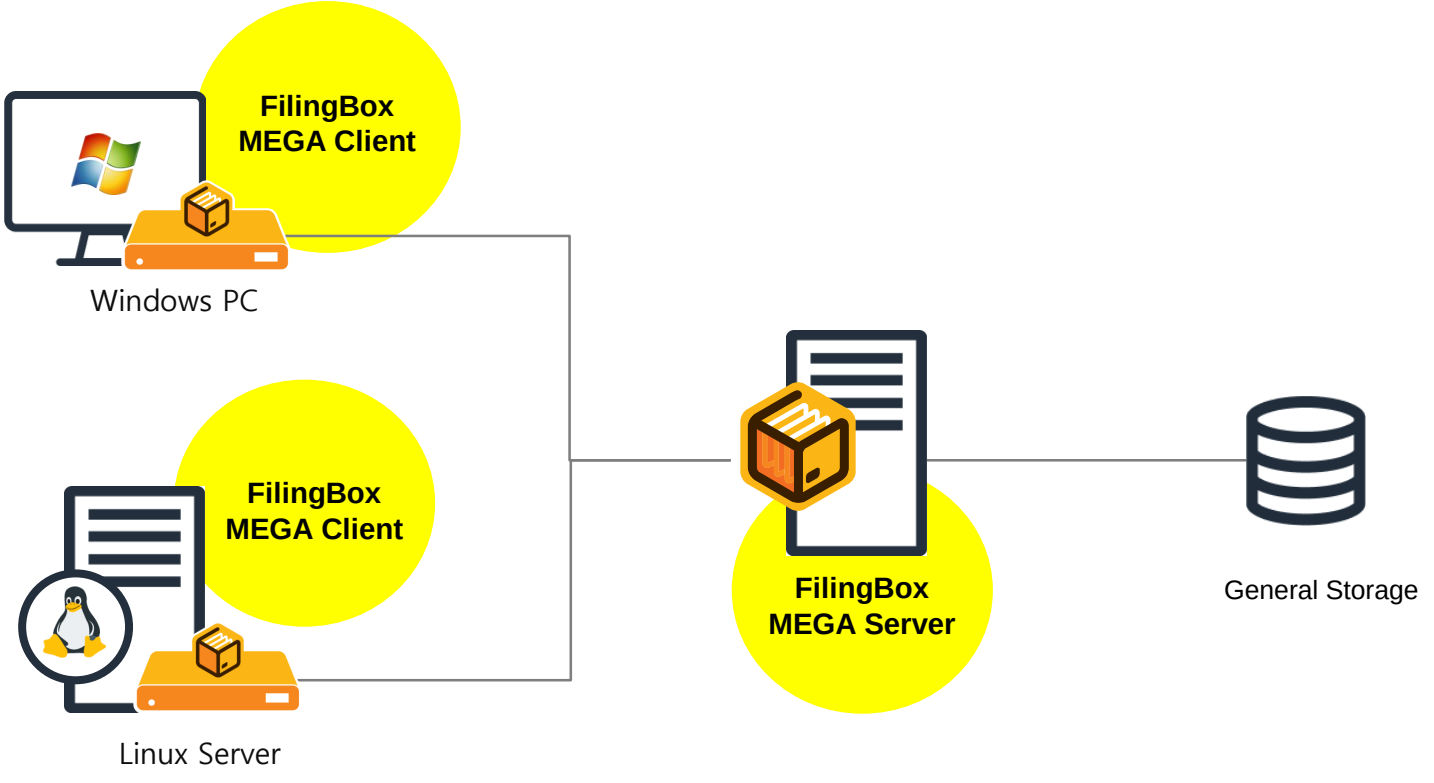


https://youtu.be/VByVeKEYorE

https://youtu.be/zNMKlIyJ4uU

FilingBox MEGA Architecture

FilingBox Mega is an application-level storage protection solution consisting of a Mega Server and Mega Client. The Mega Server is installed on a server device connected to storage and provides secure storage volumes to client devices. The Mega Client is installed on Windows or Linux devices that require access to the secure storage volumes. After user authentication, the client can access the secure storage volume (Mega Drive).



FILINGCLOUD

01

Product
Overview

02

Key
Features

03

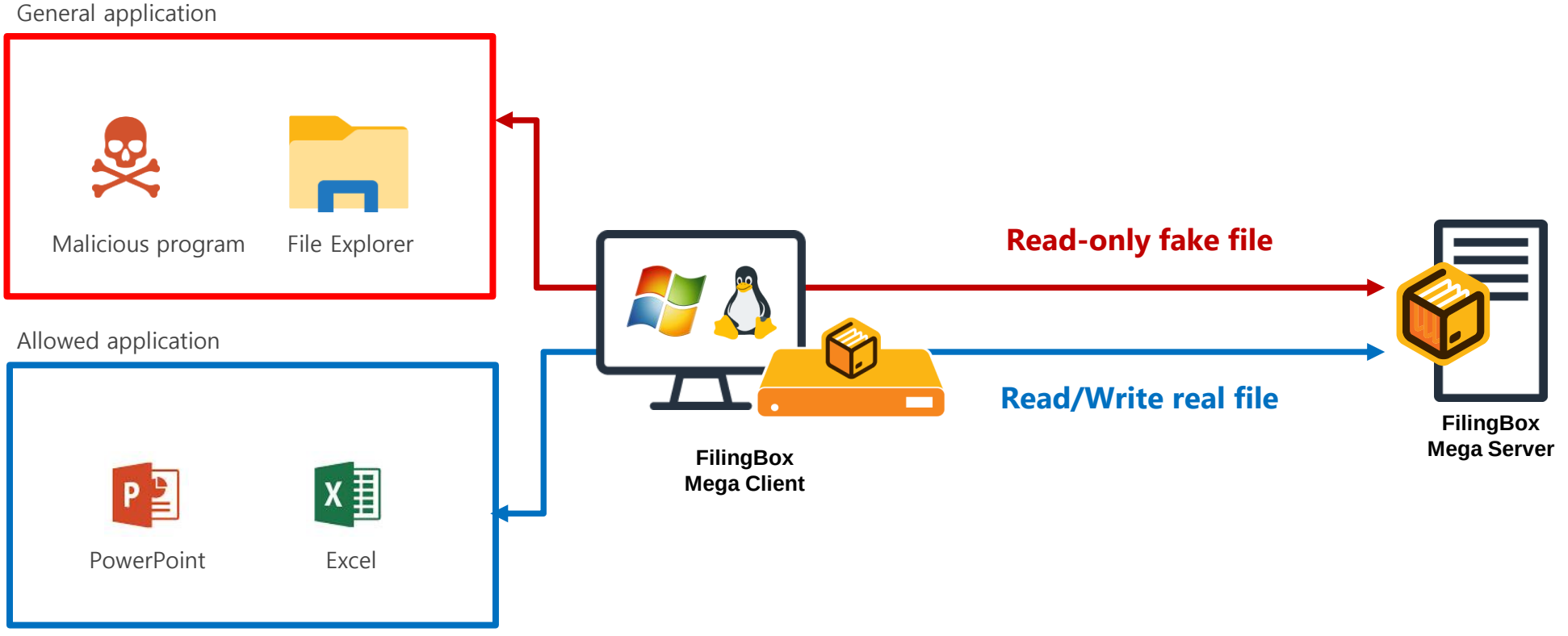
Achievements
& References

04

Company
Introduction

Feature 1 – Protects Data Even If Administrator Privileges Are Compromised by Advanced Cyberattacks

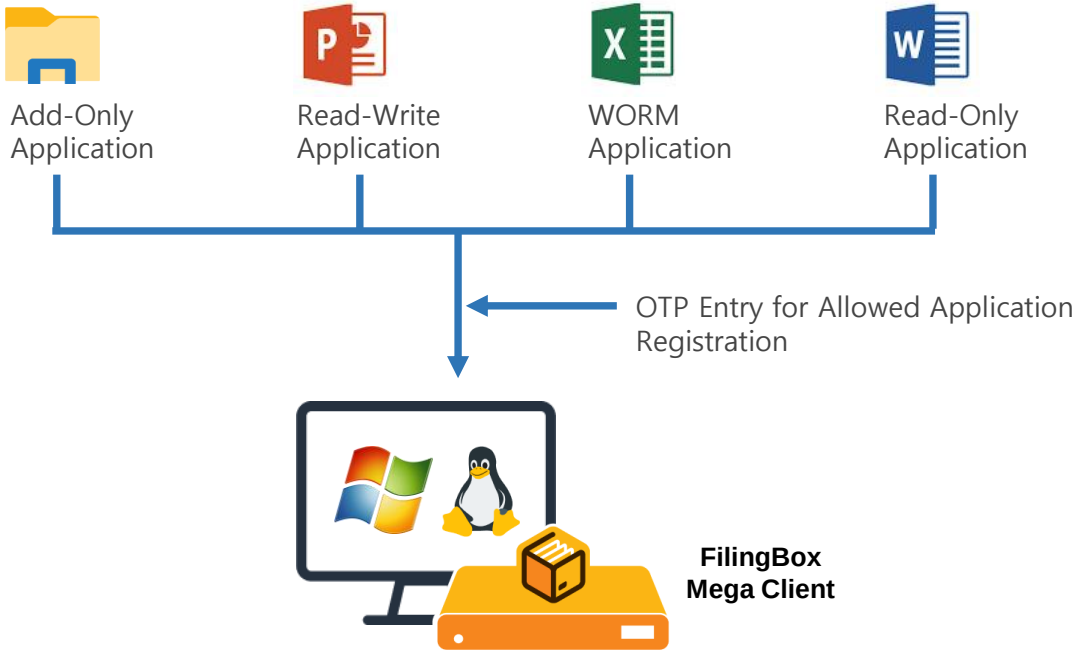
Even if administrator privileges are stolen by advanced cyberattacks such as Remote Code Execution (RCE) or zero-day exploits, data stored in FilingBox Mega will not be stolen or encrypted. The Mega Server includes an inspection module that identifies applications attempting to access the data on the Mega Drive. Pre-registered, allowed applications are provided with real files that have read/write permissions, while unregistered or ordinary applications are given read-only fake files. Therefore, even if an attacker compromises an administrator account and privileges, ordinary applications cannot encrypt or exfiltrate the data inside the FilingBox Mega drive.

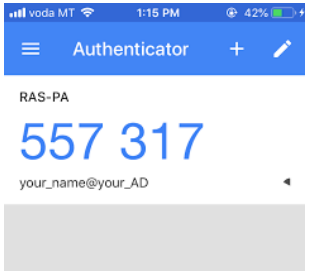


Feature 2 – Allowed Application Registration and Permission Settings Using OTP

FilingBox Mega provides an OTP (One-Time Password) based application registration and permission setting feature to securely control which applications can access the storage. This OTP authentication ensures that even if an attacker compromises an administrator account, new application registration or permission changes cannot be performed without the OTP, keeping stored data safe.

When registering ordinary applications running on a PC or server as allowed applications on the Mega Drive, administrators can assign permissions such as Read-Write, Read-Only, Add-Only, or Read-Write Versioning. For example, Read-Only allows viewing only, with no modification or deletion; Add-Only allows only new file creation; and Read-Write Versioning permits modification and deletion while preserving previous versions to enhance data safety.

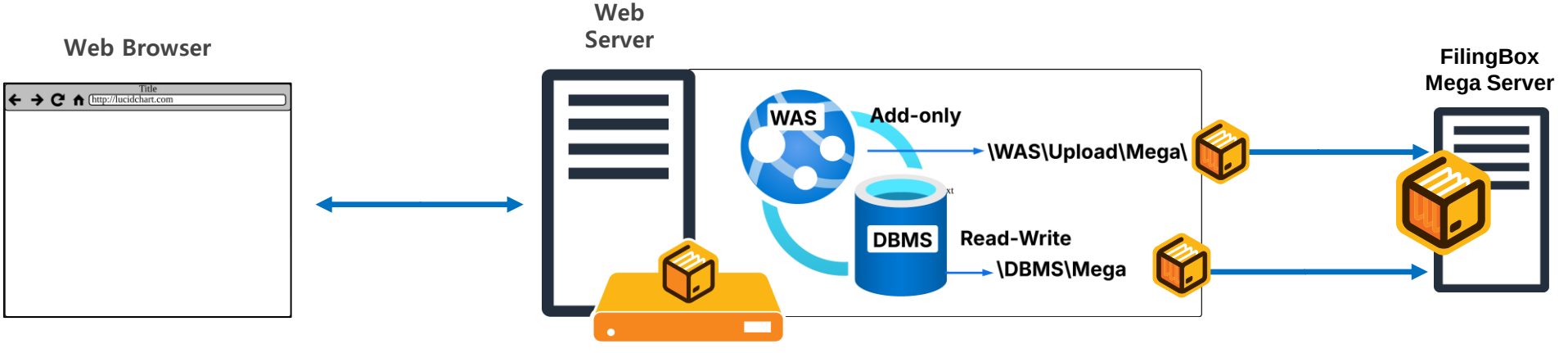




Feature 3 – Protects Active Data of Critical Server Applications

FilingBox Mega protects data actively used by server applications running on Linux servers, such as DBMS and WAS. Even if an attacker compromises the server's administrator account, only pre-registered server applications can access data on the Mega Drive. For example, in a web service composed of a DBMS and WAS, the Mega Drive can be configured to protect DBMS data files in operation and business files uploaded via the WAS.

Administrators can register the DBMS server application with Read-Write permissions and set files uploaded through the WAS to Add-Only, allowing granular security policies per application. This application-based access control protects actively used, up-to-date data directly, fundamentally differing from traditional backup/restore methods that required recovering to a specific point in time and accepting potential data loss.



FILINGCLOUD

01

Product
Overview

02

Key
Features

03

Achievements
& References

04

Company
Introduction

03 Achievements & References

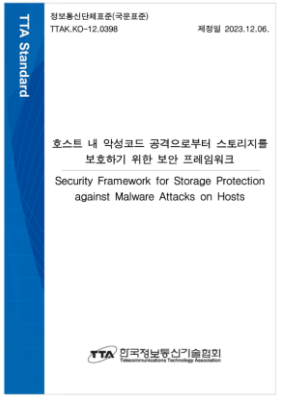
Awards

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

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.

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

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.nspam, 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

- 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