

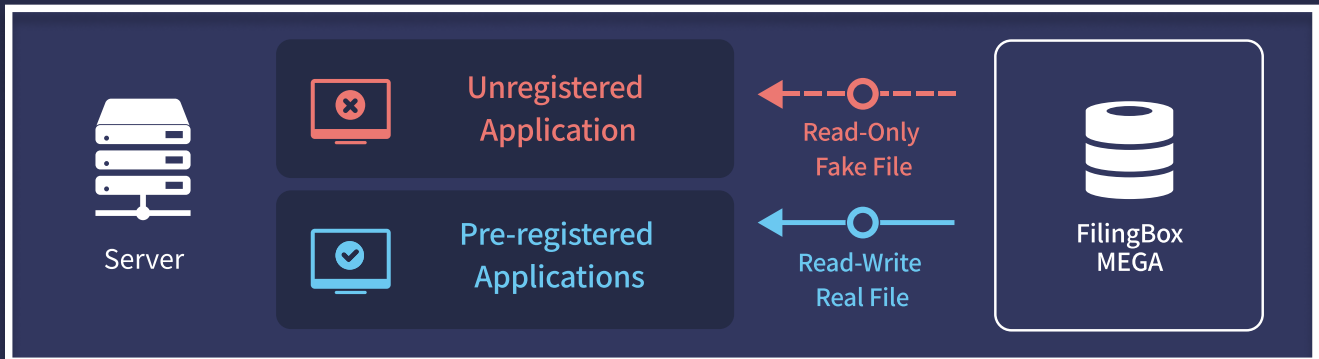
# Malware In-Advance Prevention Storage for Linux and Windows Servers

# FILINGBOX MEGA



## FilingBox MEGA

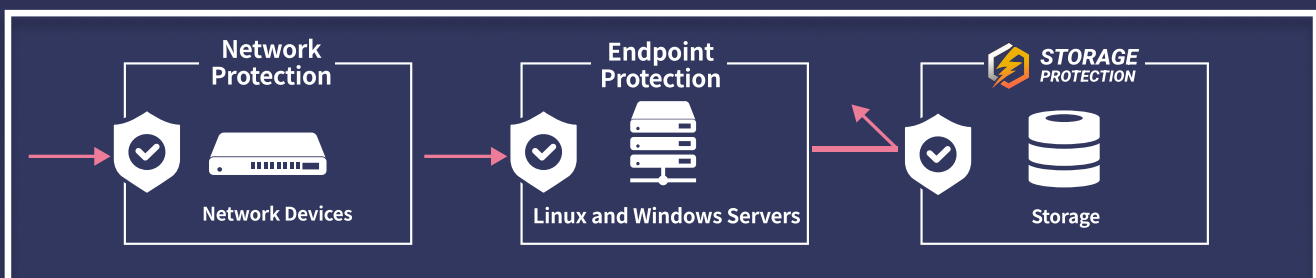
FilingBox MEGA is a storage protection solution that proactively prevents ransomware and data theft malware attacks on servers. FilingBox MEGA is equipped with an application inspection module, and when data requests come through the network drive, it inspects the application on the requesting server. It provides real files with read/write attributes to pre-registered applications, while all other applications receive fake files with read-only attributes, ensuring the data is safely protected. This way, even if the root account of the server is compromised, the data remains secure.



Registered Patents in Korea, the United States, Japan, China, and Europe

## Data protection technology recommended by international standard X.1220 and validated by international CC certification.

Storage protection technology safeguards data within storage from ransomware and data theft malware attacks. Similar to traditional network protection and endpoint protection technologies that include inspection modules, storage protection technology adds an inspection module to the storage, allowing only pre-registered applications to read and modify data. This technology is recommended by the ITU-T, the international standardization organization under the UN, as X.1220 and has obtained international CC (Common Criteria) certification in accordance with the CCRA (Common Criteria Recognition Arrangement).



# FilingBox MEGA Features

Storage protection for servers that proactively prevents ransomware and data theft attacks.

## Various Installation Packages



FilingBox MEGA supports various Linux, including Rocky, RHEL, Debian, and Ubuntu. Additionally, the client supports Windows as well.

## Read/Write Capable Application



FilingBox MEGA allows only the applications pre-registered by the administrator to create, read, modify, and delete data.

## Data Theft Prevention



FilingBox MEGA provides read-only fake files in response to file requests from unregistered applications, preventing data theft.

## Read-Only Application



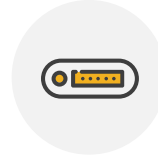
FilingBox MEGA can be configured to allow registered applications to read files only, thereby protecting existing data.

## Add-Only Application



FilingBox MEGA can be configured to allow registered applications to create new files only, thereby protecting existing data.

## Safe Application Registration



To register an application in FilingBox MEGA, an OTP code is required, and only authorized administrators can perform the application registration.

## FilingBox MEGA Usage Examples

FilingBox MEGA works effectively in Linux and Windows server environments. Protect the data of your critical servers using FilingBox MEGA.



**Application Server Administrator**

Protection of User Uploaded Files and Database Backup Files



**Backup Server Administrator**

Protection of Backup Data on Windows and Linux Servers



**Secure USB Administrator**

Prevention of Data Theft by Malware After Secure USB Connection



**Network Segregation Administrator**

Data Protection for PCs in a Network-Segregated Environment

If FilingBox MEGA is a malware prevention storage solution for servers, is there a product available for experts or enterprises?



For experts, there is FilingBox GIGA, and for enterprises, there is FilingBox Enterprise.



FILINGBOX  
**GIGA**



FILINGBOX  
**ENTERPRISE**

If you want to try FilingBox products, please request a demo at [filingbox.com](https://filingbox.com).