Fundamental ransomware prevention solution for servers
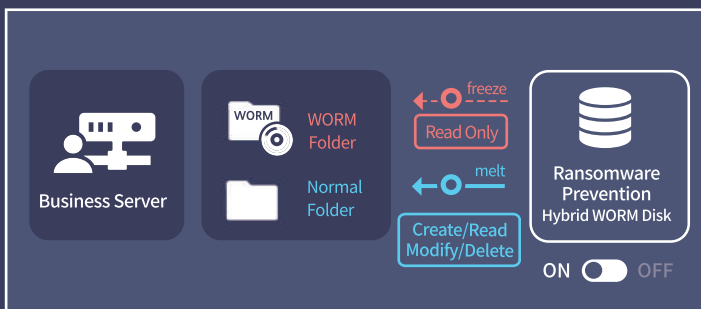
FILINGBOX MEGA

Title Video | Database | Sales history | Proposal

Product brocher | Modeling source | Contract | Promotion Video

UI kit | Video | Patient X-RAY

Q&A 1 How does FilingBox MEGA provide 100% protection from ransomware?

Conventional disks or network storage are directly controlled by a server's OS. If malware or ransomware is able to go around Anti-virus programs on your servers, then all your data can be locked. FilingBox MEGA is the ransomware prevention storage software installed on a physically separated network storage. It provides two commands that a server manager is able to change a normal folder into the WORM(Write Once Read Many) folder or the WORM folder into a normal folder on that storage. Under the WORM folder, files and subfolders within that folder cannot be modified. To change the WORM folder back into a normal folder, OTP(One Time Password) code is required.

US and PCT Patent Pending

Business Server | WORM Folder | Normal Folder | freeze → Read Only | melt → Create/Read Modify/Delete | Ransomware Prevention Hybrid WORM Disk | ON ○ OFF

Q&A 2 Can ransomware infect the data on the Linux and Windows servers?

Yes, it can. Ransomware is becoming popular in attacking servers as they operate on the network. Ransomware has been attacking servers in government agencies, medical organizations, and educational organizations more often than individual PCs. Server administrators need a new type of storage to protect the data from ransomware attacks.

Q&A 3 Can I try FIlingBox MEGA or see the demo video?

If you apply for the demo on our homepage, you can get the free live demo environment on the cloud. We offer and will install a free trial on the internal network for public organizations or medical facilities where networks are partitioned. Also, you can watch the demo video how FlingBox MEGA protects the data on the server if you search for "FilingBox MEGA" on Youtube.

▶ FilingBox

Ransomware Issue

Why can't anti-virus software installed on servers provide 100% protection against ransomware?
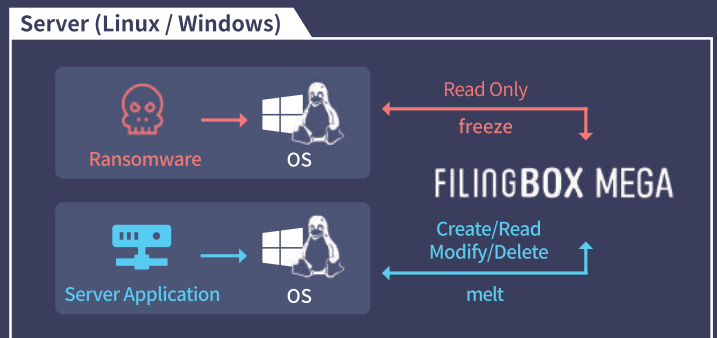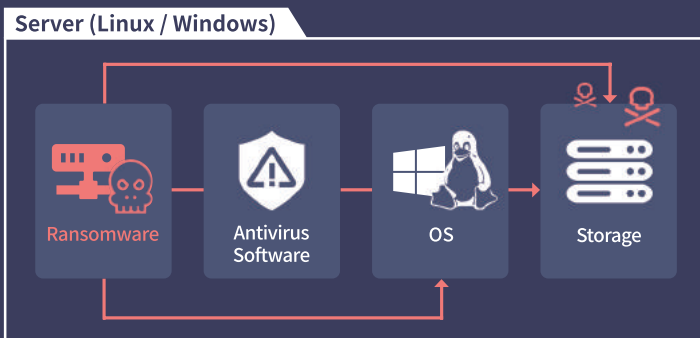
Anti-Virus is only available to block the ransomware which was uncovered earlier. It cannot stop new ransomware because new ransomware come out every day, and no one can know the pattern of new ransomware. Also, behavioral detection ransomware prevention software cannot protect the data on servers 100%. Recent ransomware goes around behavioral detection software by delaying encryption or random access encryption instead of massive encrypting attack.

Besides, some of the ransomware can stop the anti-virus or behavioral detection prevention software first and then encrypt the data. In case of the ransomware having FDE(Full Disk Encryption) or MBR(Master Boot Record) attack, the full encryption of the entire hard disk rather than just files themselves, it can bypass any prevention software.

How is FilingBox MEGA different from regular disk or conventional WORM storage?

Conventional storage including hard disk, network storage, and USB storage, create and modify the data followed by the server's operating system and any application. So if ransomware gets installed on the server, all the data on the server is encrypted. To prevent this, use WORM(Write Once Read Many) storage which provides a file with a read-only attribute since a new file is created in the beginning. It protects the data completely from ransomware, but it does not allow the storage to be reused.

On the contrary, FIlingBox Mega enables a server admin to set a folder as WORM folder. By using 'Freeze' command, an admin can set a specific folder as the WORM folder which all applications cannot modify and delete. If an admin wants to change or delete it, it requires 'Melt' command for that folder with the OTP(One-time password) code.
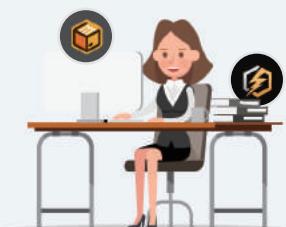
Server (Linux / Windows)

Ransomware → Antivirus Software → OS → Storage

Server (Linux / Windows)

Ransomware → OS — Read Only freeze — **FILINGBOX MEGA**

Server Application → OS — Create/Read Modify/Delete melt

Unique features Of FilingBox MEGA - Which Is Ransomware Prevention Storage For Servers

Fundamentally prevents all encryption attacks by providing the ransomware prevention WORM folder for Linux and Windows server

Switch the WORM folder into a normal folder with OTP code to be able to reuse the storage

Change the data on the existing storage as the WORM folder by connecting existing storage to FilingBox MEGA

If FilingBox MEGA is Ransomware Prevention File Server for Servers, **is there any product for companies or individuals?**

There is **FilingBox MINI** for small size companies and professionals and **FilingBox Enterprise** for government agencies and enterprises

FILINGBOX MINI　　**FILINGBOX ENTERPRISE**

If you want to try FilingBox product, request a free live demo at FilingBox.com.