FILINGBOX

HYBRID WORM DISK

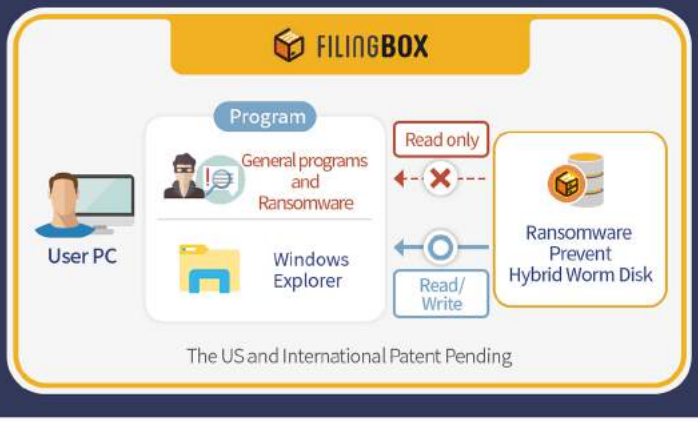
The Ultimate Ransomware Prevention Solution For Enterprise

FILINGBOX

For Enterprise

Q&A1 Why is FilingBox 100% safe from ransomware?

Conventional disks or network storage are controlled by PCs directly. If malware or ransomware manages to get around your PC's Anti-virus software, then all your data can be locked. FilingBox is a physically separated network storage device that has its control daemon, which decides whether its best to provide a file with a read-only or read-write mode. When a PC asks to send a file to FilingBox, it always sends a file within the read-only mode. So, even though ransomware runs on your PC and tries to encrypt the data, FilingBox does not allow any changes to happen to your files. Also, when users attempt to delete or modify a file on FilingBox through Windows Explorer, FilingBox enables the user to change the file.



Q&A2 Where can I watch a video that demonstrates how FilingBox prevents ransomware?

FilingBox |

If you search for FilingBox on YouTube you will be able to watch a video that shows how files within FilingBox are safely stored unencrypted, even though the PC is infected with ransomware.

Q&A3 Can I try FilingBox for enterprise?

For regular enterprises, it is possible to get a free trial of the cloud version. For public organizations or medical facilities where networks are partitioned, we personally install the free trial on the internal network. If you register for the trial through 'www.filingcloud.com', we will provide it to you for free.

Numerous companies and public organizations (i.e., Korea Local Governments, KB Kookmin Bank, KB Kookmin Card, NH Investment and Securities, Lush, etc.) are currently using FilingBox.

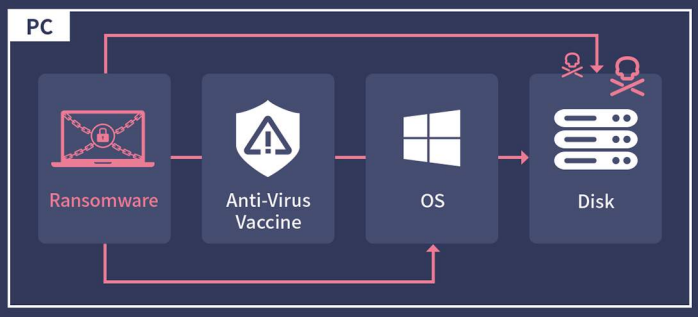
Ransomware Issue

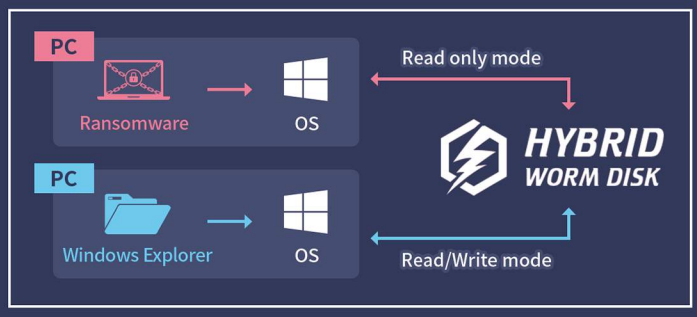
Issue 1 Why can't Anti-virus software installed on PCs prevent ransomware 100%?

Ransomware, a form of malicious software, is also a type of software that runs on the operating system just like a vaccine or any other prevention software. Since there are some cases among ransomware that stop vaccine or any additional protection software from running and encrypt files afterwards, the software-based solution can't guarantee the ransomware prevention 100%. Also, it is difficult to keep up with procuring signatures of new types of ransomware pouring out every day, and in case of abnormal behavior detection methods, it is too ambiguous to define an activity as a ransomware attack simply because it continuously reads and writes on the hard disk. If too loose, it is vulnerable against ransomware attack. If too strict, even normal programs are all blocked together. On top of that, in the event of 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't guarantee 100% prevention since they can bypass the soft-ware-based prevention method.

Issue 2 How is FilingBox different from regular disks or conventional WORM disks?

When a regular hard disk, external USB disk, or network disk is connected to a PC, any kind of program can modify or delete files within a disk. Accordingly, when ransomware runs on PC, all files are encrypted. On the other hand, a WORM(Write Once Read Many) disk, like CD-ROM and DVD, can generate a file in the beginning no matter what kind of program it is, but also provides it with read-only access so it can't be modified afterwards. This is the reason why the data on the WORM disk is safely guarded, even though the PC is infected by ransomware. However, the conventional WORM disk is way too expensive and unsuitable to store work-related data that constantly changes since it is impossible to delete or edit files once they are created. On the contrary, FilingBox runs as a conventional WORM disk for regular programs but also runs as a normal disk that allows only Windows Explorer to edit/delete files.





Unique features of FilingBox which is Ransomware Prevention Disk for Enterprises

1. Fundamentally prevent all encryption attacks by providing ransomware prevention hybrid WORM disk to PCs
2. Even document files saved on PCs are automatically backed up to the ransomware prevention disk
3. Provide an organization disk for sharing files between teams or departments as well as a personal disk per user

If FilingBox is a Ransomware Prevention File Server for Enterprises, is there any product for smaller companies or professionals?

FilingBox MINI is a lightweight version of our Ransomware Prevention File Server for smaller companies and professionals. Its a network attached disk device that has 1 terabyte disk space. Please check this site

FilingBox MINI (http://mini.filingcloud.com)

FilingBox for team and professional

FILINGBOX MINI