Employees need access to files to work—you need to ensure those files stay safe and on premises.

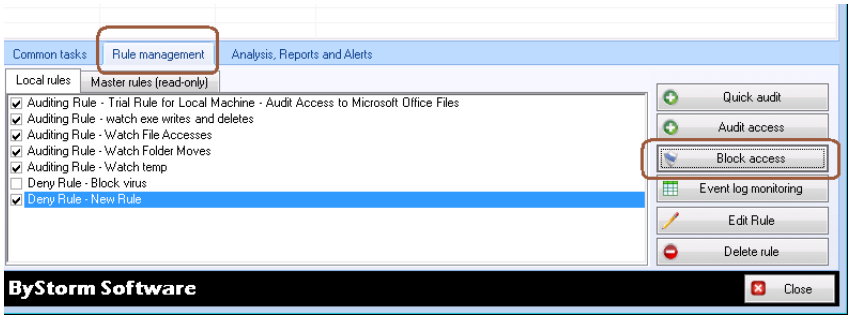
FileSure handles this problem by its unique ability to block access by program type. How?

- A file that cannot be accessed by Windows Explorer cannot be moved or copied to any other folder/drive. This stops about 95% of intentional or accidental data loss/theft, and is a good way to protect files in a certain folder. This involves denying Windows Explorer access to files in that folder.
- A file that can ONLY be accessed by the program in which it normally runs cannot be accessed to be moved or copied (or otherwise altered) by any external program. This is the safest route. It involves making a "white list" of programs authorized to open protected file types, and then blocking all others.
- In BOTH these scenarios, authorized users still have full access to open and edit files in the applications in which they are meant to run.

To protect a folder from theft while still allowing authorized file access:

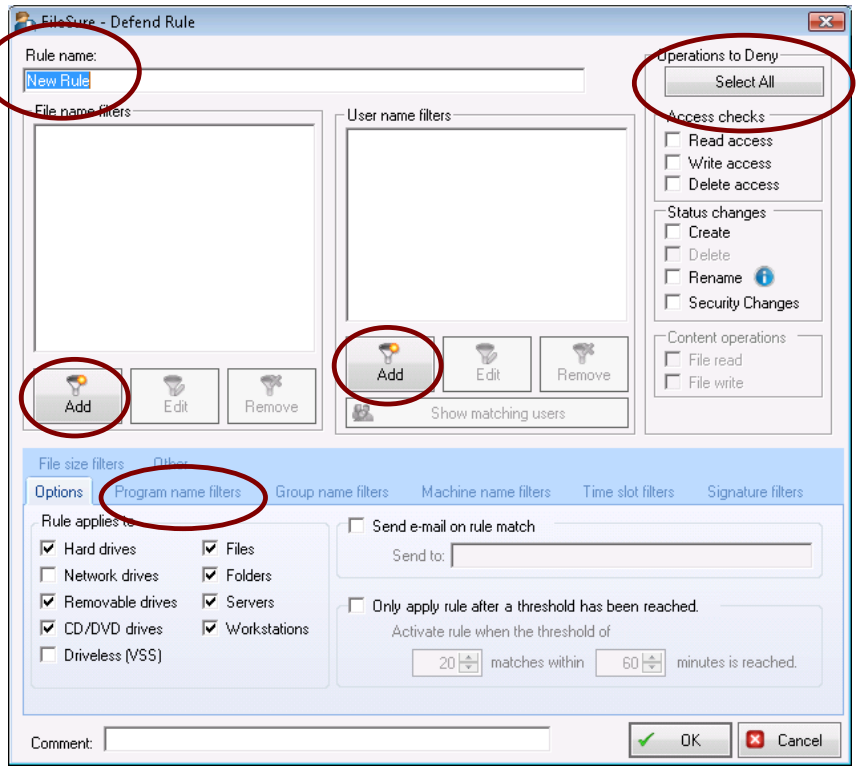
Since we need an example, we're going to keep files in the 'C:\Important Doc' folder from being copied.

1. Start FileSure Defend
2. Click the "Rules management" tab and then click "Block access"

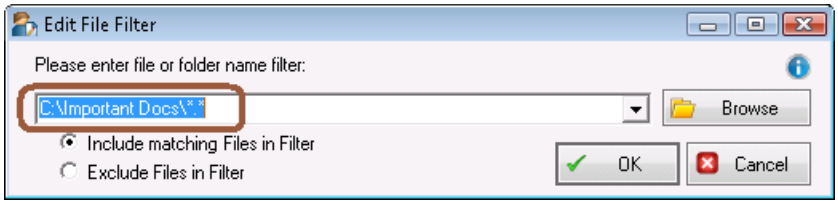


The next few steps refer to the circled areas in the following figure.

3. Name the rule “Protect Important Files” in the Rule name box.

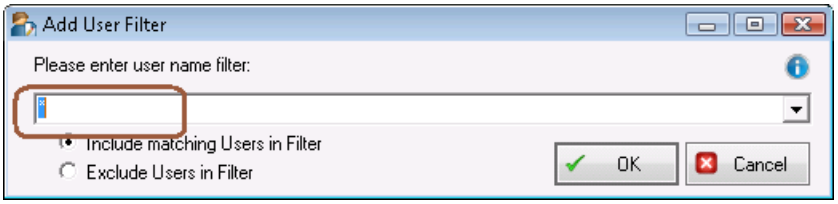


3. Click the “Add” button in the ‘File name filters’ section and type in ‘C:\Important Docs*.*’. **[Note: In a non-test environment, this path would likely be a UNC to a network share, for example: ‘\\Server\Share*.xls’]**

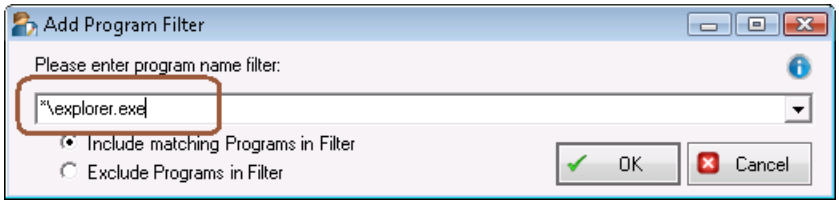


4. Click the ‘Add’ button in the ‘User name filters’ section and accept the default of ‘*’ meaning all users.

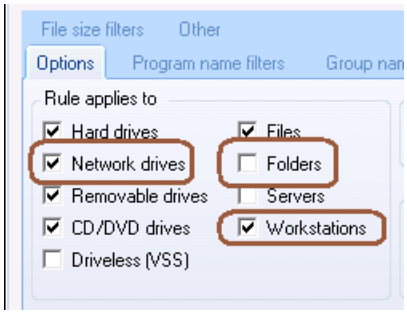
Comment [GA1]: This is redundant



5. In the “Operations to Deny’ section click the ‘Select All’ button to deny all operations.
6. Click the ‘Program name filters’ tab and click the ‘Add’ button and type ‘*\explorer.exe’ and click OK

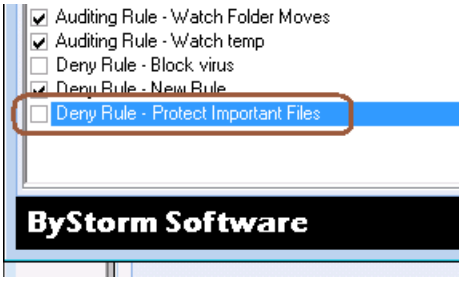


7. Click the ‘Options’ tab and check ‘Network drives’, uncheck ‘Folders’, uncheck ‘Servers’ and check ‘Workstations’



8. **Click ‘OK’ to close the ‘Add rule’ dialog.**

9. Find the ‘Protect Important Files’ rule on the rules list and check the box next to the rule. You will then verify that you want to turn on the rule.

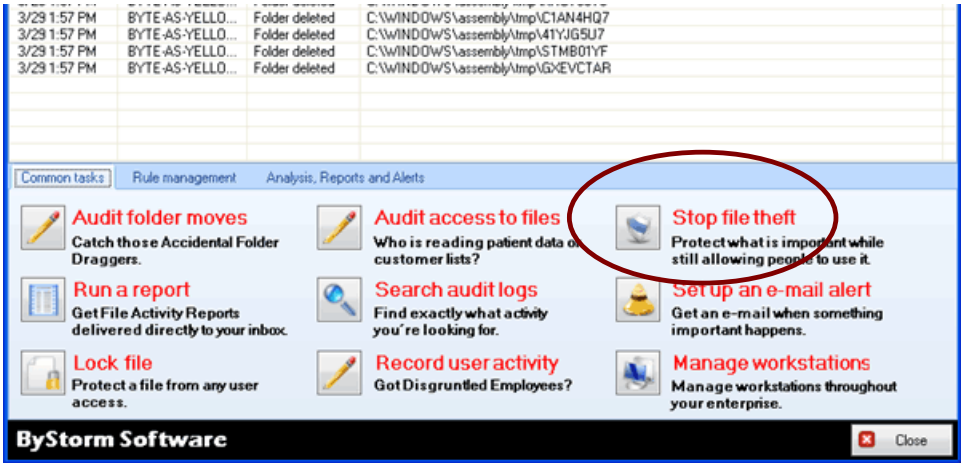


A t this point FileSure Defend will block Windows Explorer from reading files in ‘C:\Important Doc’ and if Explorer can’t read the files, it can’t copy them. You may now try to drag and drop, copy and paste, or otherwise remove the files. They won’t move, but they will open in their intended programs.

While this will handle 95% of data theft, ***a better approach is to use FileSure Defend to protect files by blocking ALL applications except an explicate list ('white list') of programs.***

To protect all files of chosen types from theft while allowing authorized access:

Use the 'Stop File Theft' wizard on the 'Common tasks' area tab:



This wizard will build 2 rules:

Rule #1 blocks all access to the named file type with the exception of the program listed as its default program, and

Rule #2 prevents said type being written to a removable drive. You simply designate the file type (such as .doc, .xls, etc) and the wizard does the rest

You will see the new rule listed on the rules list and already turned on and running. Select the rule and click **Edit Rule** if you need to add more programs to the list of "exceptions," or other adjustments. .

[Note: Known issue correction: You will need to click Edit Rule and check the 'Create' checkbox in the 'Operations to Deny' area. The wizard correctly blocks write to removable media but misses blocking file creates. This is a know issue and has been corrected.]

For added security, a rule blocking file type changes for your protected file types is recommended. Example: if you have protected .xls files, create a new "block access" rule for files *.xls, all users, and click "renames" under file operations. If you then go to "other" at the bottom tabs, you can choose to allow renames within the same file type (so budget.xls can become budget1.xls, but NOT budget.123).