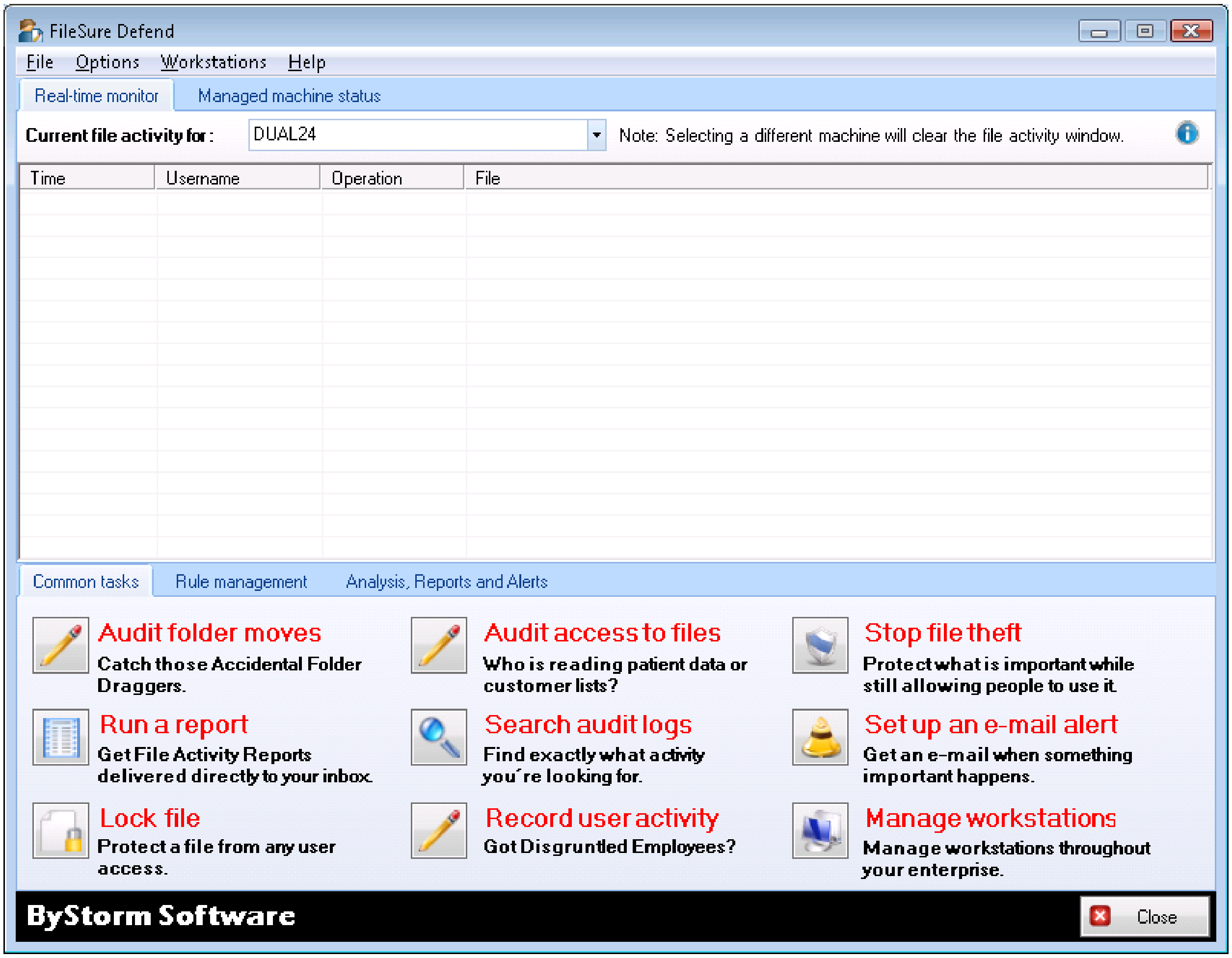
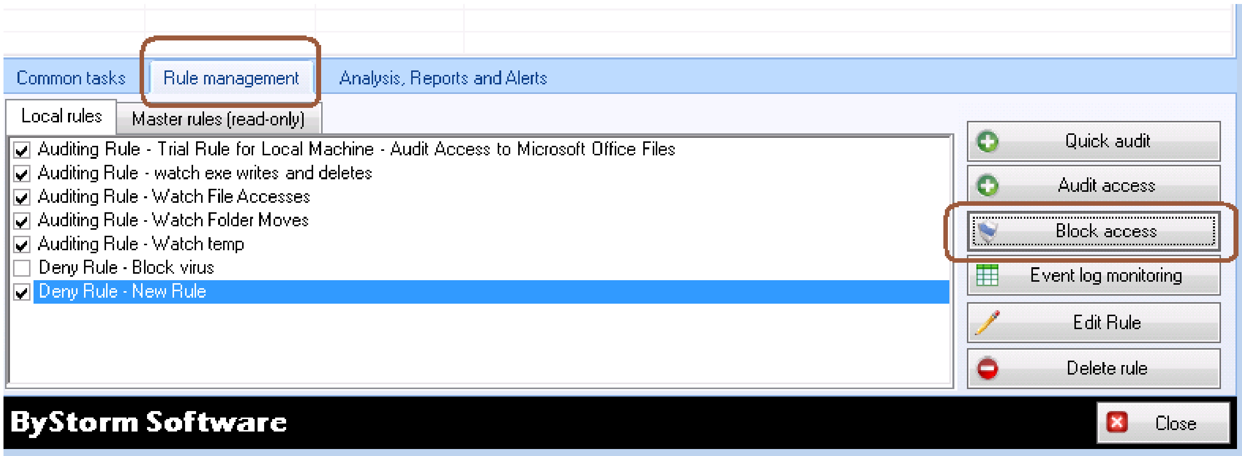
This short document shows you how to set up a FileSure Defend rule to block file copies from a certain folder.

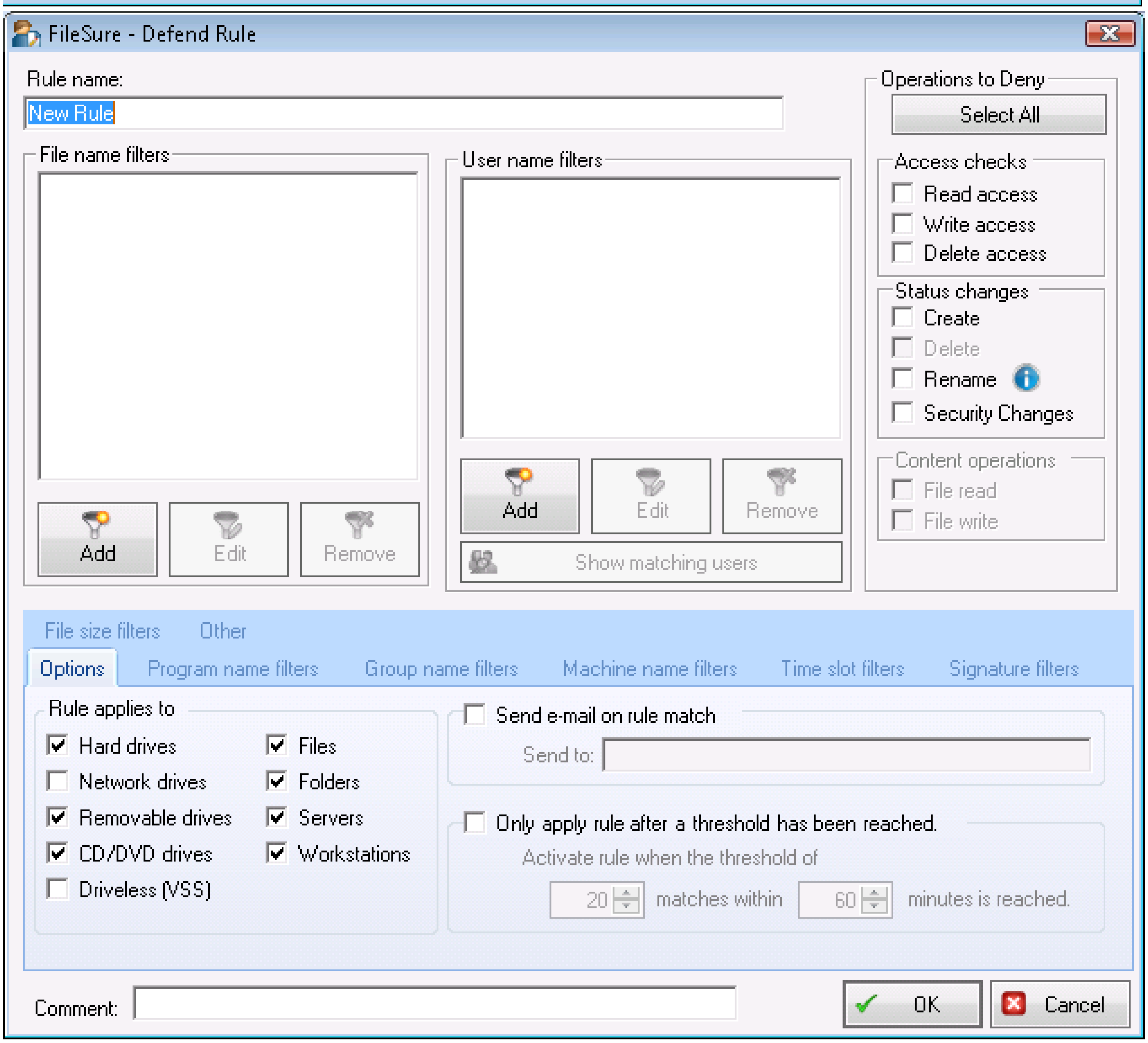
Since we need an example, we're going to keep files in the C:\Important Doc folder from being copied.

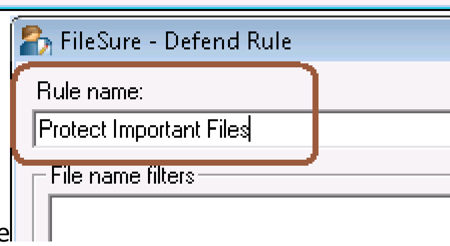
1. Start FileSure Defend



2. Click the ‘Rules management’ tab and then click the ‘Block access’ button

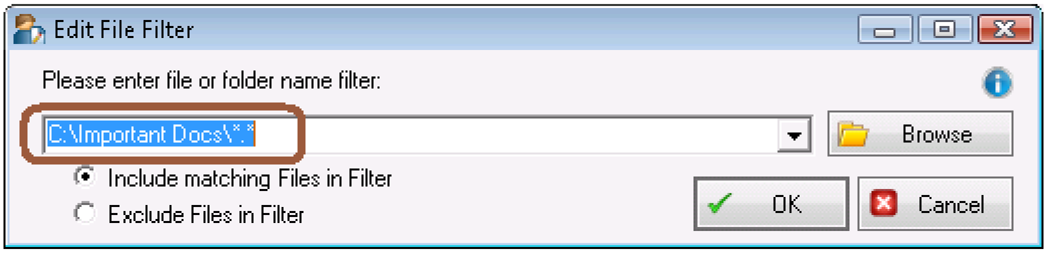




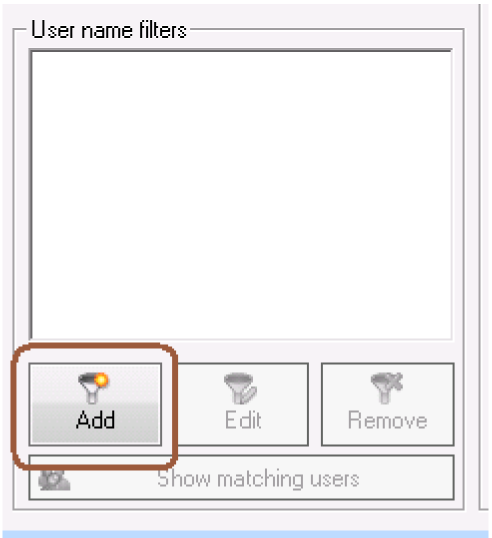


3. Enter ‘Protect Important Files’ for the Rule name
4. Click the “Add” button in the ‘File name filters’ section:

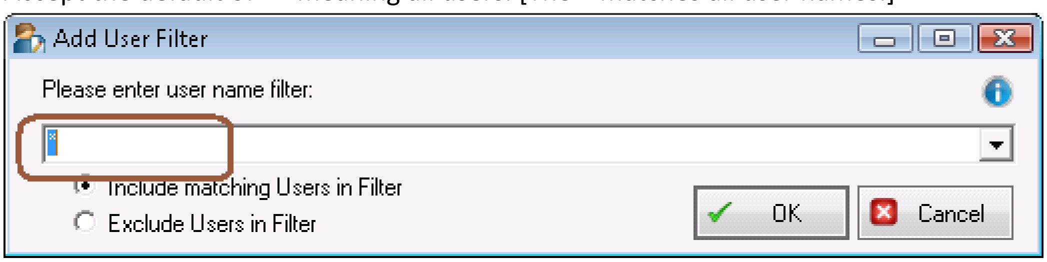
5. Type in ‘C:\Important Docs*.*’



6. Click ok.

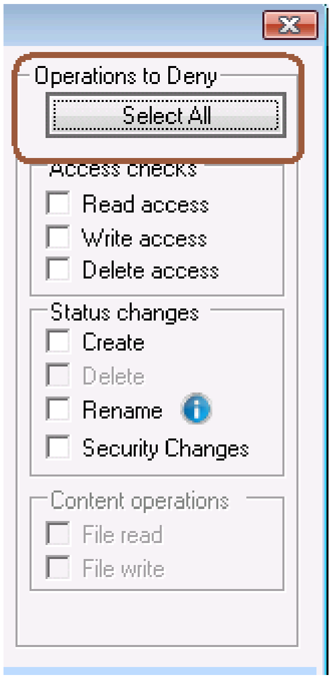


7. Click the ‘Add’ button in the ‘User name filters’ section:
8. Accept the default of ‘*’ meaning all users. [The * matches all user names.]

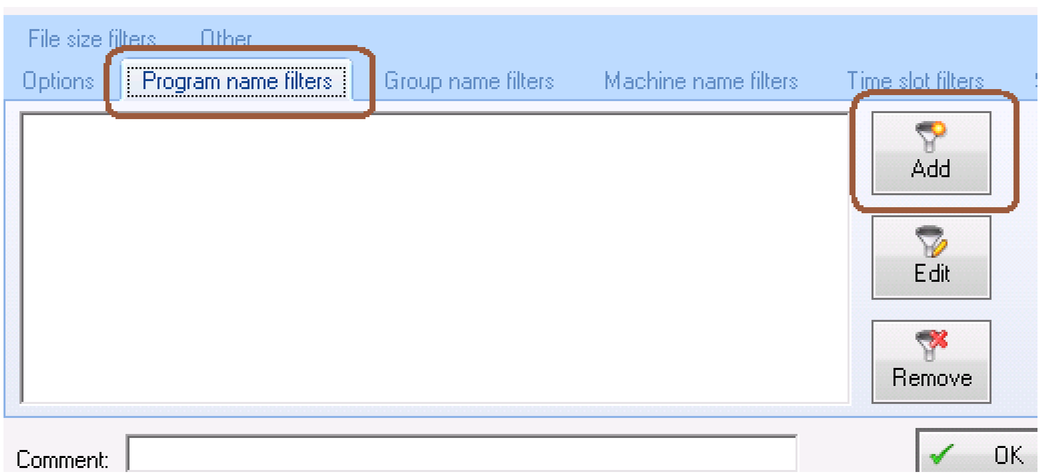


9. Click OK

10. In the “Operations to Deny’ section click the ‘Select All’ button to deny all operations.

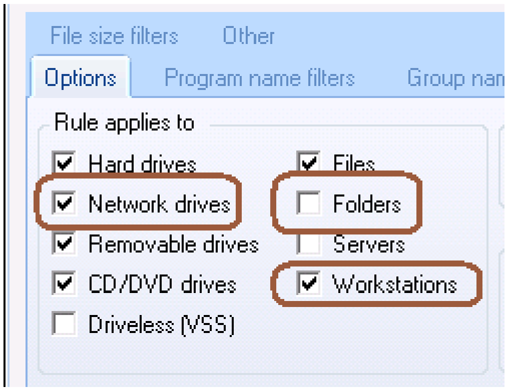


11. Click the ‘Program name filters’ tab and click the ‘Add’ button



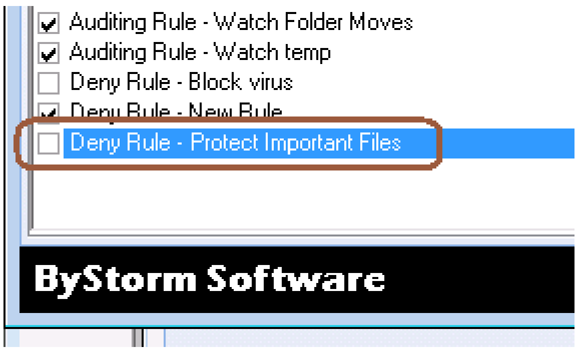
12. Type ‘*\explorer.exe’ and click OK

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

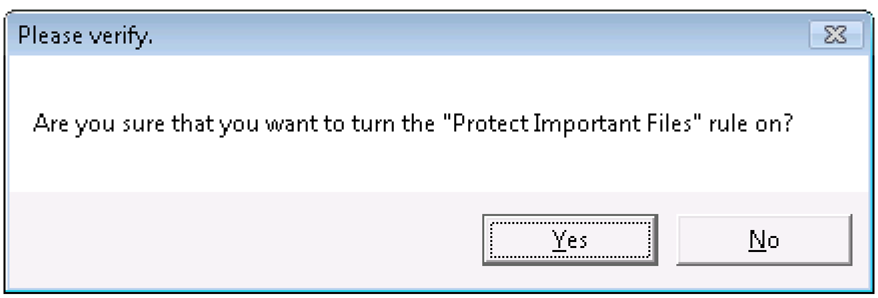


14. Click ‘OK’ to close the ‘Add rule’ dialog.

15. Find the ‘Protect Important Files’ rule:



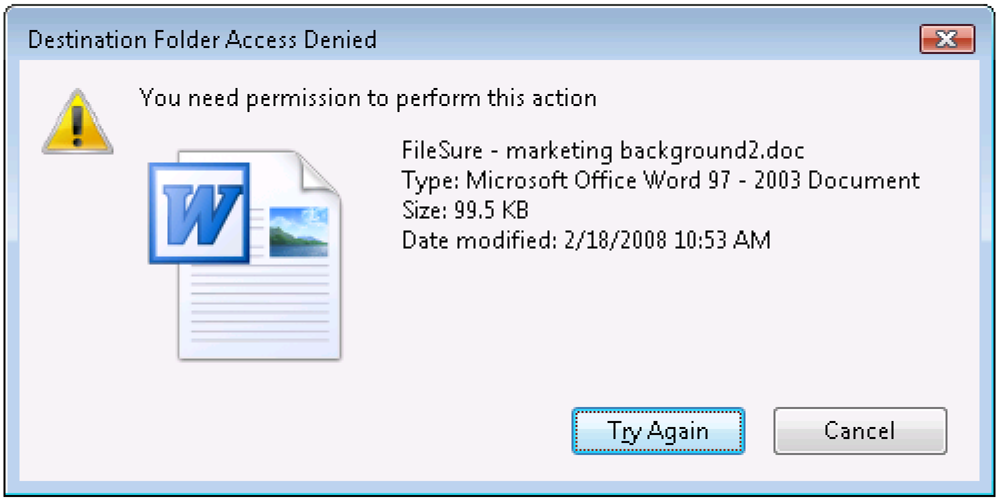
16. Check the check box next to the rule: and select ‘Yes’



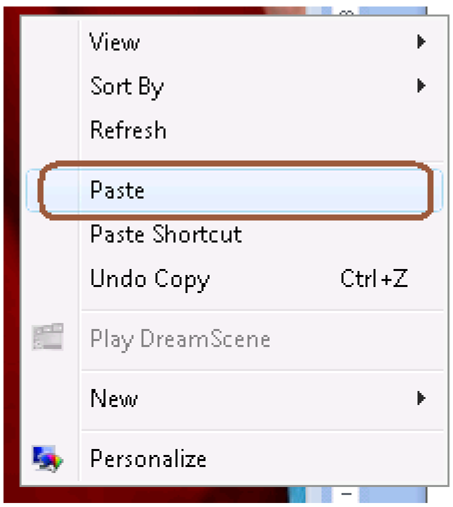
A t this point FileSure Defend will block Windows Explorer from reading files in ‘C:\Important Doc’ and if Explorer can’t read the files, it can’t copy them.

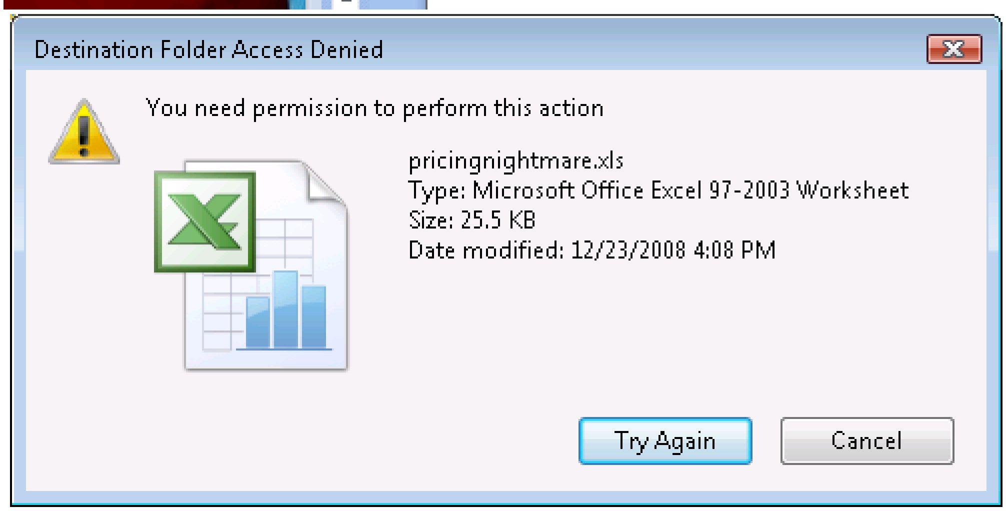
Since this is a workstation-based rule, we switch to a FileSure managed workstation and try to copy a file from the protected location.

17. Navigate to the protected share and attempt to drag and drop them to a USB drive:

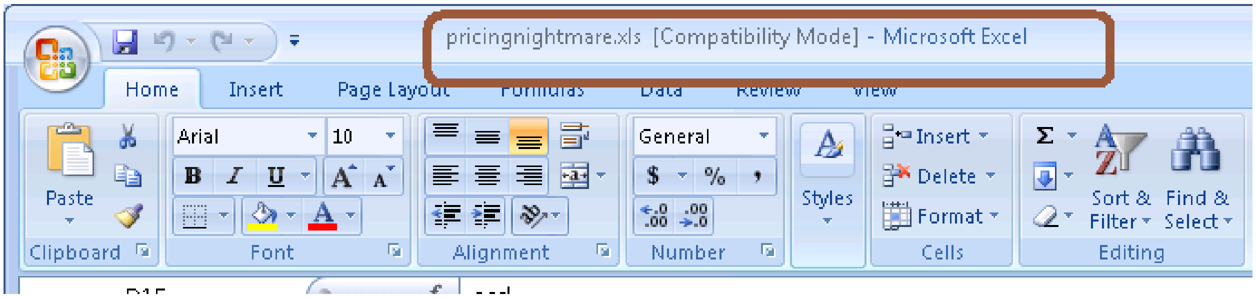


18. Right click on a protected file and select ‘Copy’ then right click on the Desktop and select ‘Paste’





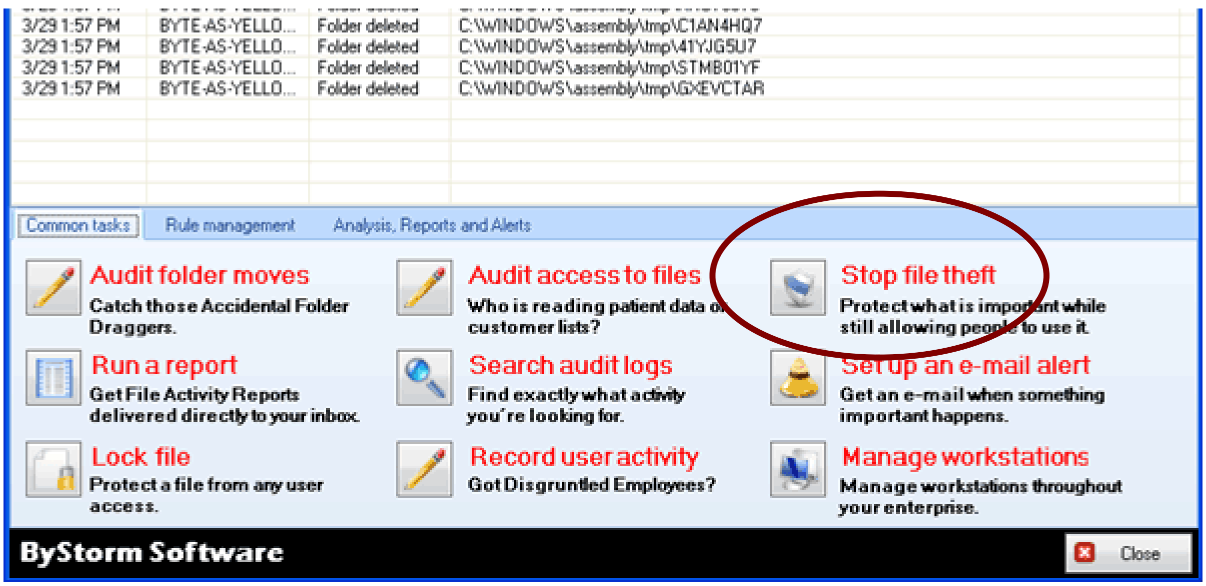
19. Since we want to stop copying but not work, double click on a protected file; in my example, I double click on pricingnightmare.xls and it opens:



This shows how FileSure Defend can protect files in an important folder from being copied by Windows Explorer. While this will handle 95% of data theft, a better approach is to use FileSure Defend to protect files everywhere by blocking ALL applications from accessing them except an explicate list ('white list') of programs. You will need to create a different "anti-theft" rule for every file type which has data in it you wish to protect. Here is how:

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:

1. To block all access to the named file type with the exception of the program listed as its default program, and

2. To prevent 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. Among other things, this will stop someone from simply doing a "save as" to a removable drive.

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: 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).

Please also remember—if you are seeking permission-based file security FileSure can also just limit file access by user. Try the “Lock File” wizard, or other rules based on user or group names.