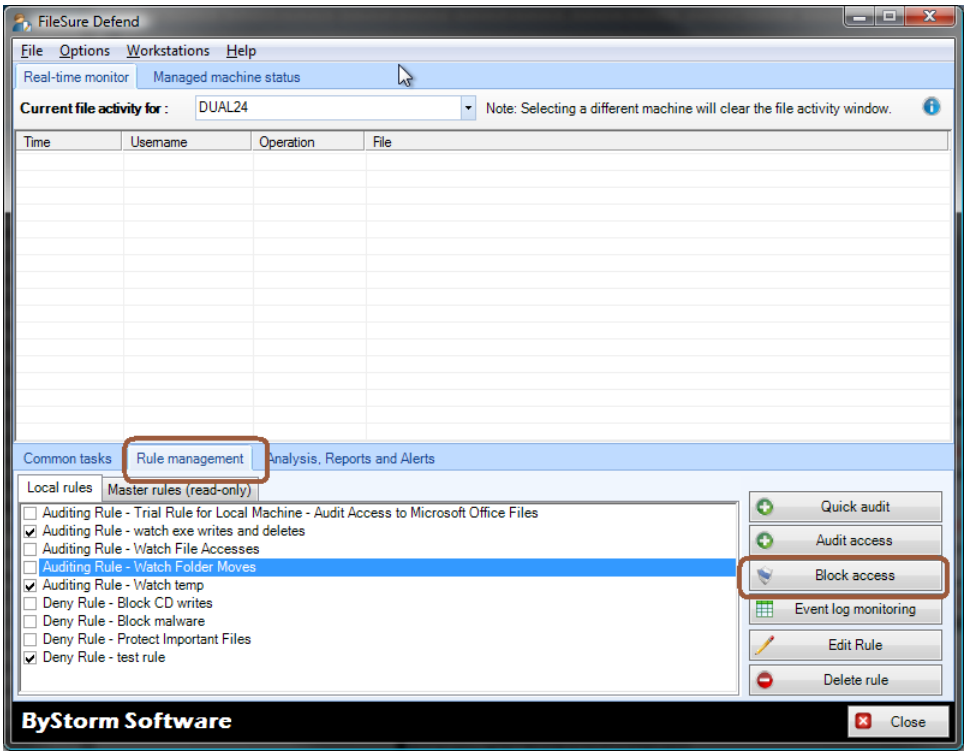
While the most popular and easiest way to steal data is to use a USB drive, another method is to burn a CD/DVD. Again, this might be intentional theft, or it might be good intentions gone wrong . . .

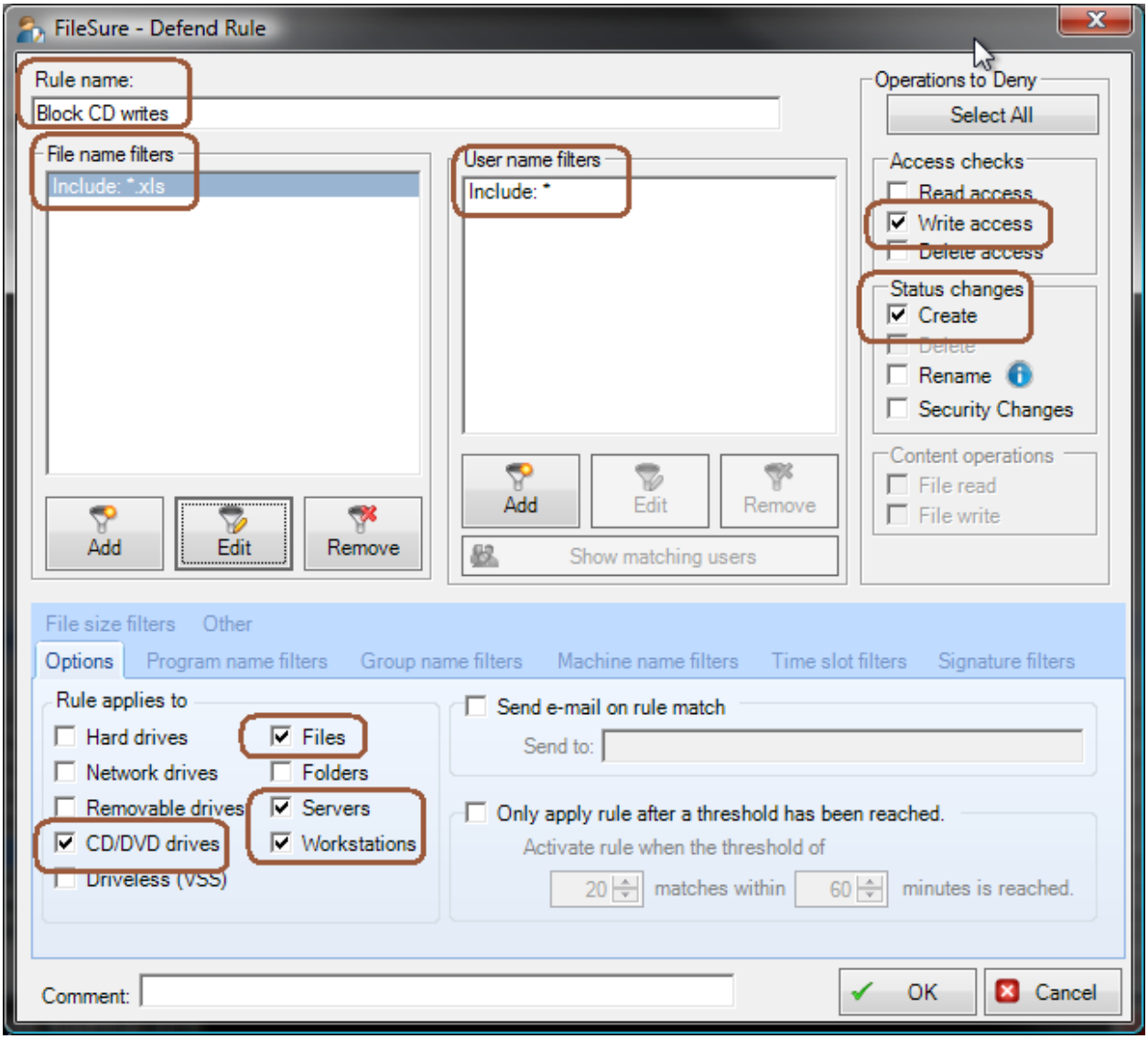
What doesn't (always) work: Like USB drives, CD burning can be turned off via Windows Group Policy. However, you may not use Windows Group Policy, or you might be worried about data theft by users who aren't normally restricted by Group Policy (e.g. Administrators). You also might want users to be able to burn some content to CD—just not the sensitive stuff. For all those scenarios, you'll need FileSure Defend.

How we do it: In most situations, just defining a FileSure rule to block file creates on the CD/DVD drive will be enough. For maximum security, designating what programs can access your sensitive files will also be necessary.

Step 1: On the main FileSure console, click the "Rule management" tab and then click the "Block Access" button:



Refer to the picture below for the next several steps:



Step 2: Name the Rule “Block CD Writes”

Step 3: Click “Add” under file name filters and “include” .xls; Click “Add” under user name filters and designate all (“*”)

Step 4: Under Operations to Deny, check Write access, Create

Step 5: On the “Options” tab under “Rule applies to . . . “ choose CD/DVD drives, files, and have it run on servers and workstations

Step 6: Click OK

Step 7: Find the “Block CD Writes” rule on the rules list and enable it.

This simple rule will probably handle 95% of theft via CD/DVDs (customized for whatever file types concern you); however, CD/DVDs are a bit different than USB drives since there isn’t a ‘file system’ on

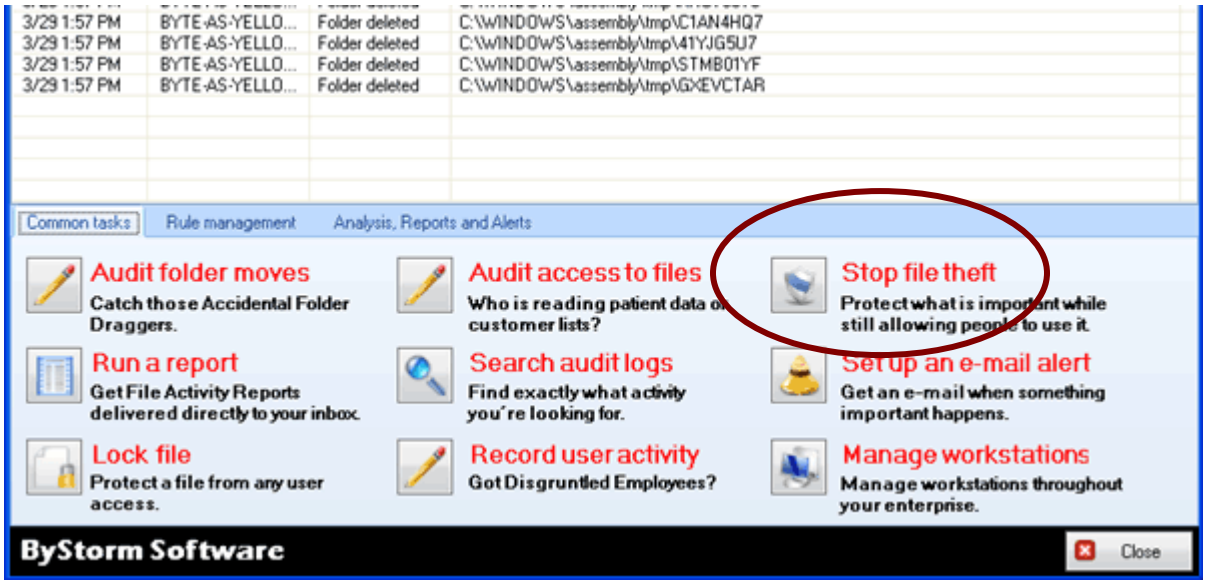
the CD/DVD until after it's burned. So if the user was to burn a CD with another program (e.g. Nero), that writes the entire CD at once, FileSure isn't going to catch it.

To block that scenario, it would be tempting to use FileSure's 'Program Name' filter to block the CD/DVD burning program explicitly (which will work), but I like to recommend that you opt for a 'white-list' approach instead of a 'black-list,' in other words . . . exclude ALL programs from reading the protected files EXCEPT the one that is allowed to.

You can use the "Stop File Theft" wizard to achieve this very quickly.

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).