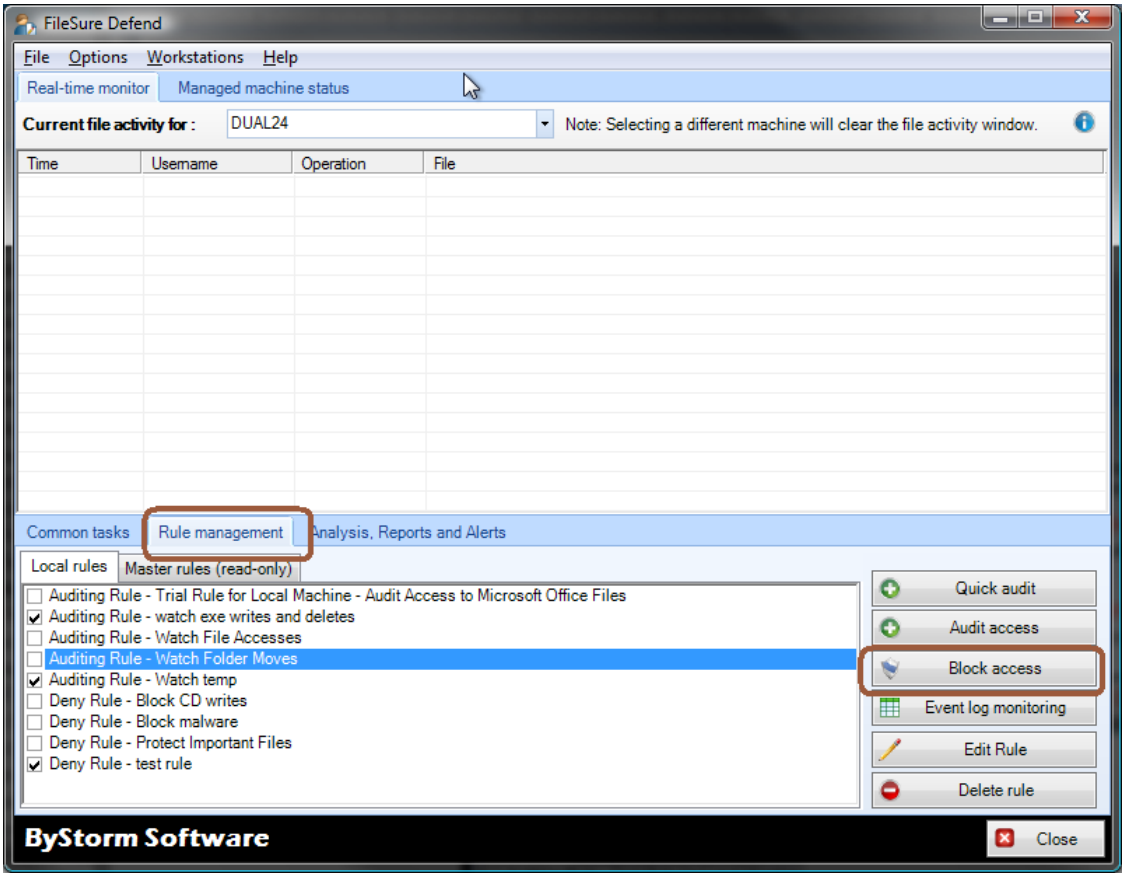
The USB Switchblade attack is a very scary thing. In 30 seconds alone with a computer a hacker can steal any sensitive data on it. One method uses the Windows AutoRun feature to run a program that silently infects the computer and steals data by running as a background task (this same attack works with CD/DVD drives.) Blocking this sort of attack by disabling the components involved (Autorun, external drives in general) is very cumbersome and not very secure.

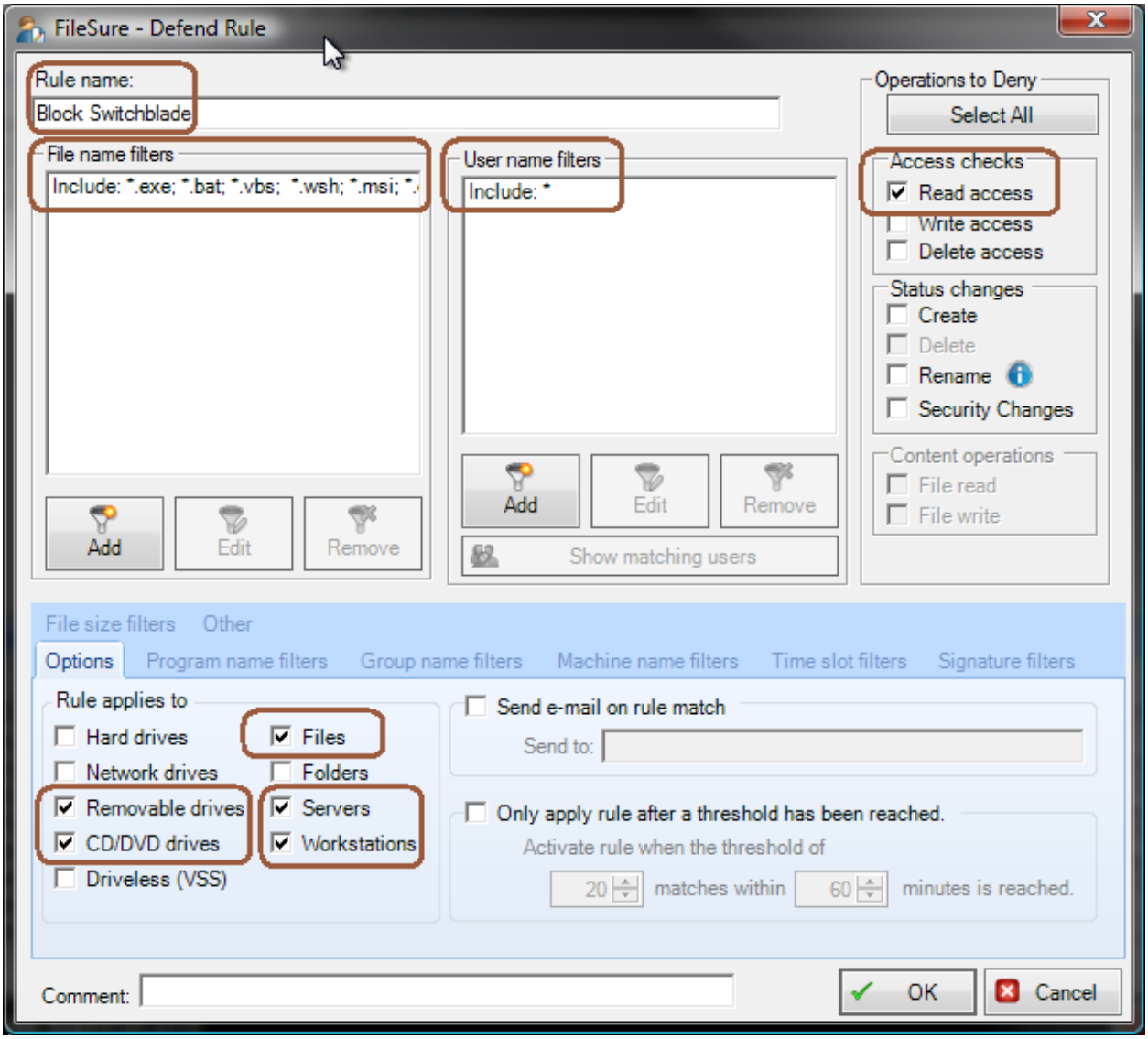
Thankfully, blocking a Switchblade attack is a simple with FileSure Defend. We're going to use FileSure Defend to block reading of code from removable drives and CD\DVDs and since we're not going to allow code to be read, it can't be used to attack the computer. But, users can still use their USB drives, and we didn't have to disable Autorun in Windows.

Here's how:

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



That will bring up a define Defend rule dialog that will look like this:



Refer to the above picture for the next several steps.

Step 2: Name the rule by typing ‘Block Switchblade’ in the ‘Rule name’ area.

Step 3: Add a file name filter. Click the ‘Add’ button in the ‘File name filters’ area.

Step 4: Enter the filter of ‘*.exe; *.bat; *.vbs; *.wsh; *.msi; *.cmd; *.inf’ indicating that this rule will only apply to files with those extensions. Blocking *.inf will block Windows ‘Autorun’ feature and if the hacker is somehow able to get control of the keyboard, blocking all the other types will prevent running the attack directly from the USB drive. (Note: this may not be a complete list of extensions to block, but as of writing it’s a pretty good list)

Step 7: Add a user name filter for all users. Click the ‘Add’ button in the ‘User name filters’ area:

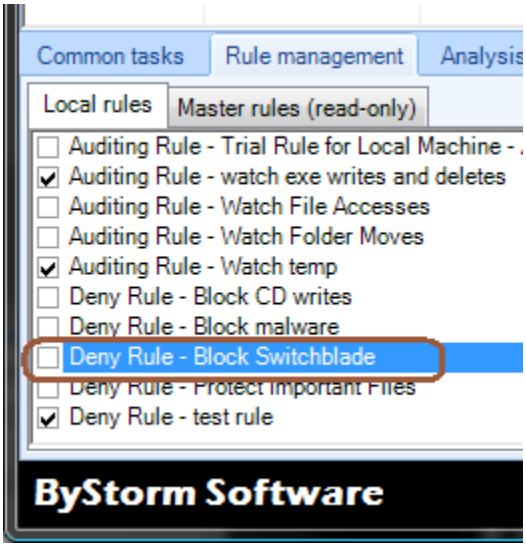
Step 8: Enter the filter of '*' for all users, make sure that the 'Include matching Users in Filter' is checked and click 'OK'

Step 9: Select the operations we want to block, which is Open for Read.

Step 10: On the 'Options' tab in the 'Rule applies to' area, ensure that 'Removable drives', 'CD/DVD Drives', 'Files', 'Servers' and 'Workstations' is checked.

Step 11: Click 'OK' to close the dialog.

Step 12: Find the new 'Block Switchblade' rule in the 'Local rules' list



Step 13: Click the checkbox next to the rule and accept the 'Please verify' message.

Step 14: Sit back and relax, knowing your environment is safe from switchblade hackers.