E22	I.	-6		
EL	L	23	u	I E

ByStorm Software

www.bystorm.com

877-BYSTORM

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 Marketing share from being copied.

1. Start FileSure Defend

わ FileSure Defe	nd				
<u>File Options W</u> orkstations <u>H</u> elp					
Heal-time monito	r Managed machi	ne status			
Current file acti	vity for : DUAL24		 Note: Selecting a differe 	ent machine will clear the file activity window. 🚺	
Time	Username	Operation	File		
L					
L					
L					
L					
Common tasks	Rule management	Analysis, Repor	s and Alerts		
🗾 🖉 Audi	t folder moves		Audit access to files	Stop file theft	
Catch Dragg	those Accidental F Jers.	older	Who is reading patient data or customer lists?	Protect what is important while still allowing people to use it.	
Run	a report	0.	Search audit logs	🔰 Set up an e-mail alert	
Get Fil delive	Get File Activity Reports Find exactly what activity Get an e-mail when something delivered directly to your inbox. you're looking for. Get an e-mail when something				
Lock Protect acces	: <mark>file</mark> ct a file from any us s.	er	Record user activity GotDisgruntled Employees?	Manage workstations Manage workstations throughout your enterprise.	
ByStorm	ByStorm Software				

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

Common tasks Rule management Analysis, Reports an Local rules Master rules (read-only) Auditing Rule - Trial Rule for Local Machine - Audit Access Auditing Rule - watch exe writes and deletes Auditing Rule - Watch File Accesses Auditing Rule - Watch Folder Moves Deny Rule - Block virus Deny Rule - New Rule	nd Alerts to Microsoft Office Files	Quick audit Quick audit Audit access Block access Event log monitoring Edit Rule Delete rule Close
FileSure - Defend Rule Rule name: New Rule File name filters File name filters Second Se	User name filters	Operations to Deny Select All Access checks Read access Write access Delete access Status changes Create Delete Rename Security Changes File read File write
File size filters Other Options Program name filters Group name Rule applies to Image: Files Image: Files Image: Hard drives Image: Files Image: Files Image: Network drives Image: Folders Image: Folders Image: Removable drives Image: Folders Image: Folders Image: CD/DVD drives Image: Workstations Image: Driveless (VSS) Comment: Image: Comment drives Image: Comment drives	me filters Machine name filters Time slot Send e-mail on rule match Send to: Only apply rule after a threshold has been Activate rule when the threshold of 20 regimetic matches within 60 File Sure - Defend Rule Rule name: Protect Important Files File name filters	filters Signature filters reached. minutes is reached. OK Cancel

- 3. Enter 'Protect Important Files' for the Rule name
- 4. Click the "Add" button in the 'File name filters' section:

5. Type in the UNC of the shared folder you want to protect.

🏠 Edit File Filter	
Please enter file or folder name filter:	0
\\BYSTORM01\\Marketing*.*	✓ Browse
 Include matching Files in Filter Exclude Files in Filter 	✓ OK Sancel

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.]

🏠 Add User Filter	
Please enter user name filter:	0
 Include matching Users in Filter 	
C Exclude Users in Filter	UK 🛛 UK

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

File size filters Other Options Program name filters	Group name filters	Machine name filters	Time slot filters
			Add
			Edit
			Remove
Comment:			🖌 ок

12. Type '*\explorer.exe' and click OK

わ Add Program Filter			
Please enter program na	me filter:	6	
*\explorer.exe		•	
 Include matching Exclude Programs 	Programs in Filter s in Filter	🖌 OK 🛛 Cancel	

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:

 Auditing Rule - Watch Folder Moves Auditing Rule - Watch temp
Deny Rule - Block virus
🗾 🖬 Deny Bule - New Bule
🚺 🔲 Deny Rule - Protect Important Files
ByStorm Software

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 '\\ByStorm01\Marketing\' 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'

	View	•	
	Sort By	•	
	Refresh		
$\left(\right)$	Paste		
	Paste Shortcut		
	Undo Copy	trl+Z	
	Play DreamScene		
	New	•	
5	Personalize		
Dest	tination Folder Access De	ed 🗧	X
	You need permissi	n to perform this action	
_		pricingnightmare.xls Type: Microsoft Office Excel 97-2003 Worksheet	
		Size: 25.5 KB	
		Date modified: 12/23/2008 4:08 PM	
	- PPPP		
		Try Again Cancel	

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:

3/29 1:57 PM 3/29 1:57 PM 3/29 1:57 PM 3/29 1:57 PM	BYTE-AS-YELLO BYTE-AS-YELLO BYTE-AS-YELLO BYTE-AS-YELLO	Folder deleted Folder deleted Folder deleted Folder deleted	C:\wINDOWS\assembly\tmp\C1AN4HQ7 C:\wINDOWS\assembly\tmp\41YJG5U7 C:\wINDOWS\assembly\tmp\STMB01YF C:\wINDOWS\assembly\tmp\GXEVCTAR	
Common tasks Audit Catch to Dragg	Rule management t folder moves those Accidental F ers.	Analysis, Report	ts and Alets Audit access to files Who is reading patient data of customer lists?	Stop file theft Protect what is important while still allowing people to use it.
Run a Get Fil deliver Lock Protect access	a report le Activity Reports red directly to your file st a file from any us s.	inbox. er	Search audit logs Find exactly what activity you're looking for. Record user activity GotDisgruntled Employees?	Set up an e-mail alert Get an e-mail when something important happens. Manage workstations Manage workstations throughout your enterprise.
ByStorm	Software			Close

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.