FileSure	Sure How to protect, alert and report on chang	
ByStorm Software	www.bystorm.com	877-BYSTORM

This 'How-to' will show how to configure FileSure-Defend to protect your website from change--except to certain users or at certain times. We will generate an e-mail alert when a change was blocked, and set up an automatic daily report showing all the changes that were attempted.

1. Start FileSure, switch to the 'Rules management' tab and click the 'Block access' button:

🐴 FileSure Defe	nd					- • •
<u>F</u> ile <u>O</u> ptions	Workstations <u>H</u> el	р				
Real-time monitor	r 👘 Managed machi	ne status				
Current file activ	vity for : DUAL24		 Note: Selecting a different machin 	e will clear	the file -	activity window. 🛛 🕕
Time	Username	Operation	File			
Common tasks	Bule management	Analysis, Repo	its and Alerts			
Local rules M	aster rules (read-onlu)					
Auditing Rule	 Monitor AutoCAD_file 	es		*	0	Quick audit
Auditing Rule	- Trial Rule for Local	Machine - Audit A	ccess to Microsoft Office Files		0	Audit access
Auditing Rule	- watch exe writes and	d deletes		Ξ	~	Block access
Auditing Rule	Auditing Rule - Watch File Accesses					DIOCK access
Auditing Rule	- Watch rolder moves - Watch temp	i				Event log monitoring
Deny Rule - Bl	lock CD writes				1	Edit Rule
Deny Rule - Bl	lock Maiware			-	0	Delete rule
ByStorm	ByStorm Software Software					

2. This will bring up the 'Defend Rule' screen (next page). We are going to configure an example rule involving only allowing access to the webmaster and only at a certain time of the week. You can tweak the criteria to fit your needs.

わ FileSure - Defend Rule	
Rule name: Protect web site from changes	Operations to Deny Select All
File name filters	ser name filters hclude: * xclude: *\WebMaster Access checks □ Read access ✓ Write access ✓ Delete access Status changes ✓ Create □ Delete □ Delete ○ Rename ○ Security Changes ✓ Content operations □ File read □ File write
File size filters Other Options Program name filters Group name filters	ilters Machine name filters Time slot filters Signature filters
Rule applies to Hard drives Network drives Removable drives CD/DVD drives Driveless (VSS) 	Send e-mail on rule match Send to: Only apply rule after a threshold has been reached. Activate rule when the threshold of 20 matches within 60
Comment:	🗸 OK 🛚 🛛 Cancel

- a. Change the Rule Name to be 'Protect web site from changes'
- b. Check all the 'Operations to Deny' except for Read Access. This is telling FileSure not to allow any changes, but to let users read the files.
- c. In the 'Rule applies to' section, check only 'Hard drives', 'Files' and 'Servers'.
- d. Use the 'Add' button in the 'File name filters' area to enter a filter that points to your website on the hard dive. In my example, I'm protecting 'C:\inetpub\live corp\web*'. The '*' at the end means the rule applies to ALL files in that folder and any subfolder.
- e. Use the 'Add' button in the 'User name filters' area to enter a user name filter of '*'; this will cause the rule to be applied to all users.
- f. Use the 'Add' button in the 'User name filters' area to enter a user name filter of '*\WebMaster', this time click the 'Exclude' option instead of the default 'Include'. This will exclude the user 'WebMaster' from the rule.
- g. Click the 'Time slot filters' tab and select every time slot except for Saturday morning from 8AM to 12PM. [Note: if you click on the day, all time slots for that day will be selected]. This tells FileSure to enforce this rule all the time, except for Saturday mornings...say for scheduled maintenance.

わ FileSure - Defend Rule		.			
Rule name:	Rule name:				
Protect web site from changes		Select All			
File name filters Include: C:\Inetpub\Live Corp Web*	User name filters Include: * Exclude: *\WebMaster	Access checks Read access Write access Delete access			
		Status changes Create Delete Rename () Security Changes			
Add Remove	Add Performance Remov	/e Content operations // File read			
File size filters Other Options Program name filters Group na	me filters Machine name filters	ne slot filters			
Sunday					
Monday					
Tuesday					
Wednesday					
I hursday					
Saturday					
12AM 4AM	8414 12PM 4F	M 8PM 12AM			
Comment:		🖌 OK 🛛 Cancel			

h. Click the 'Other' tab and enter '77 for the 'Alert ID' filter. We're going to use the alert ID to trigger our e-mail alerts.

わ FileSure - Defend Rule		
Rule name: Protect web site from changes		Operations to Deny Select All
File name filters Include: C:\Inetpub\Live Corp Web*	User name filters Include: * Exclude: *\WebMaster	Access checks Access Read access Write access Content access Content access Content access Content access Content access
Add Edit Remove	Add Edit Remove Show matching users	 File read File write
File size filters Other Options Program name filters Group name	e filters Machine name filters Time slo	t filters Signature filters
Audit noise reduction Avoid Audit Storms Advanced rename options Allow renames with same file extension Denv changes "to" chosen extension(s) 	Advanced alerting support Generate an Event Log record on rule None Alert ID: 77 🕂 6	
Comment:		🗸 OK 🛛 🛛 Cancel

- i. Click 'OK' to close the rule.
- 3. Find the newly created rule and enable it by clicking the checkbox next to the rule name

Common tasks Rule management Analysis, Reports and Alerts
Local rules Master rules (read-only)
Deny Rule - Block CD writes
Deny Rule - Block malware
Deny Rule - Block Switchblade
Deny Rule - Protect Important Files
Deny Rule - Protect Microsoft Office Excel 97-2003 Worksheet files pt. 1
Deny Rule - Protect Microsoft Office Excel 97-2003 Worksheet files pt. 2
Deny Rule - Protect Microsoft Office PowerPoint Presentation files pt. 1
Dony Rule Protoct Microsoft Office PowerPoint Presentation files pt. 2
Deny Rule - Protect web site from changes
Deny Rule - test rule
ByStorm Software
bystorm software

At this point, FileSure is protecting your website from changes and recording any attempts in the auditing data store. Now, let's see if we can't use that data for an alert and a daily report.

4. Select the 'Analysis, Reports and Alerts' tab and click the 'Scheduled repots' button.

🐴 FileSure Defe	nd		-			
<u>File</u> Options	<u>File Options W</u> orkstations <u>H</u> elp					
Real-time monito	Managed machin	ne status				
Current file acti	vity for : DUAL24			 Note: Selecting a 	differen	t machine will clear the file activity window. 🛛 🕕
Time	Usemame	Operation	File	3		
Common tasks	Rule management	Analysis,	Reports and Alerts			
Analysis			Reports			Alerts
Ever	nts recorded today:	13	Total sc	heduled reports:	3	Total alerts: 4
Opera	tions denied today:	5	Active sc	heduled reports:	3	Active alerts: 2
			F	Report recipients:	1	Machines monitored: 1
						Machines managed: 2
	🔍 View	Data		Reports		
				(
	Search fo	or Frends		Scheduled repo	orts	O Manage alerts
ByStorm	ByStorm Software					

5. This will bring up the 'Schedule Reports' where you need to click the 'New' button. Note the 'Scheduled job execution time' as this is the time that the reports will run everyday.

Schedule Reports				• ×
Report Jobs:			9	Q. (1)
Drag a column header here to group	by that col	umn.		
Job Name:	Enabled	Report Name:	Send To:	
New Job	V	User Activity Report Touched files	gene@bystorm.com	
Auto-generated report for 214,335,828	1	User Activity Report: Folders moved	gene@bystorm.com	
Auto-generated report for 43,349,093	V	User Activity Report: Touched files	gene@bystorm.com	
O New / Edit 🔕 Be	amove	SMTP Settings Scheduled	job execution time 02:00 PM	Glose

6. This will bring up the 'Edit Job' screen. This is where we will configure the scheduled report. Change the following things:

🔊 Edit Job	
Job Name	Attempted web site changes
Report Report name	User Activity Report: Write access denies
	Sorted by users doing the activity, report shows what files denied the user write access. Data is dependent on auditing rules active during designated time period.
Date Range:	Quick Range Previous day Previous 30 Day(s)
Filters	
	Run this report against all managed computers.
	DUAL24 XP2PROVM XPPROVM
User Name Filters*:	O Acrobat File (PDF) O Excel File O XML O CSV O HTML
Delivery Mail to*:	gene@bystorm.com
Save to folder: Schedule	Browse
* Separa	Image: Monday Image: Tuesday Image: Wednesday Image: Thursday Image: Friday Image: Saturday Image: Saturday Image: Saturday Image: Saturday Image: Saturday Image: Saturday Image: Saturday <

- a. Enter 'Attempted web site changes' for the 'Job Name'
- b. Select the 'User Activity Report: Write access denied' in the 'Report name' drop down.
- c. For the 'Date Range', select the 'Quick Range' of 'Previous day'
- d. In the 'Mail to' area, enter the e-mail address of who should get the report.
- e. In the 'Schedule' area, select the additional options of 'Saturday' and 'Sunday'

7. Click OK to close the screen and save the report job. Click 'Close' on the 'Schedule Reports' screen. If haven't already configured your SMTP settings, you will be prompted to do so.



8. Now we have a daily report scheduled, but we want to know about the change attempts as they are happening. For that, we need to set up an Alert. Back on the main screen, select the 'Common tasks' and click the 'Set up an e-mail alert' button.

🐴 FileSure Defe	end			
<u>File</u> Options	Workstations Hel	р		
Real-time monite	or Managed machin	ne status		
Current file acti	vity for : DUAL24		 Note: Selecting a different mac 	hine will clear the file activity window. 🛛 🌀
Time	Usemame	Operation	File	
Common tasks	Rule management	Analysis, Report	s and Alerts	
Audi	/ it folder moves	ß	Audit access to files	Stop file theft
Catch Dragg	those Accidental F ers.	older	Who is reading patient data or customer lists?	Protect what is important while still allowing people to use it
Run	a report	Ø,	Search auditlogs	Set up an e-mail alert
delive	red directly to your	inbox.	you're looking for.	important happens.
Lock	file	19	Record user activity	Manage workstations
Protection acces	ct a file from any us s.	er 🗾	Got Disgruntled Employees?	Manage workstations throughout your enterprise.
ByStorm	Software			🛛 Close

9. This will bring up the 'Define Alert' screen which is where we will configure the alert, but before we can do that we need to set up a summary. Click the 'Manage Summaries' button.

わ Define Al	ert	ALC: NO.	a la la como de	X
Summary:	Extension Summary by User		Manage Sun	nmaries 💫
			Sample	Summary Data
	Count	userName	extension	-
	▶ 76	BYSTORMSOFTWARE\allengb	exe	
	58	BYSTORMSOFTWARE\allengb	4.4	
_	10	BISTORMSOFTWARE\allengb	awg	-
	Monitor all machines			6
	DUAL24			~
Machines:	XPPROVM			
			1	-
- 1	1			
	Send e-mail when count exce	eeds: 10 🗢 Do not send e	e-mails more than every:	30 🜩 minutes.
Mail to:				
Subject*:	[
	[
Body*:				
_	*Use right-click to enter a va	ariable. [Note]: the body text wil	Il repeat once for every item ov	er the threshold.
	To:			
	Subject:			
Preview				
Treview.				
	Enabled		🗸 OK	Cancel
Preview:	✓ Enabled		🗸 ОК	Cancel

10. This will bring up the 'Manage summaries' screen which shows all the current summaries. On this screen, click the 'New' button.

Manage	Summaries		
Summari	es:		W 4
Drag a co	ulumn header here to group by	that column.	
Enabled	Record Age	Summary Name	
V	1 days 0 hours 0 minutes	Extension Summary by User	
17	1 days 0 hours 0 minutes	Drive type usage by user	
1	1 days 0 hours 0 minutes	Program summary	
177	1 days 0 hours 0 minutes	Root Folder Moves	
1	0 days 0 hours 5 minutes	Auto-generated summary for alert: 214,335,828	
23	0 days 0 hours 10 minutes	Hidden File Access	
4	0 days 1 hours 0 minutes	Summary for rule: watch exe writes and deletes	
17	0 days 0 hours 5 minutes	Auto-generated summary for alert: 43,349,093	
10	0 days 1 hours 0 minutes	Test summary	
	\checkmark		
O New	Edit	e	

11. This will bring up the 'Define Summary' screen. Here is how to configure the summary:

 \sim

🗞 Define Summary	
Name Watching for website writes.	✓ Enabled
Oldest Record Age: 0 🚔 days 1 🚖 hours 0 🚔 minutes	
select count(extension), extension from AuditRecords where extension <> "" and eventTime OldestRecordAge group by Upper(extension);	•>
SQL	
Query:	
Test Summary Query Dublish this summary as a desktop/scree	ensaver alert
Sample	e Summary Data
Visit the Summary Section of the ByStorm User Forum.	🛛 Cancel

- a. Enter 'Watching for website writes' for the 'Name'
- b. Enter '1' in the hour section 'Oldest Record Age'. This tells FileSure that we only want to look in the past hour for events. We do this so we don't continue to send out alerts for old events.
- c. Click either the little 'world' button or the 'Visit the summary section of the ByStorm User Forum' link. This will open a browser to the ByStorm Forum:



d. Select the 'Detailed summary by Alert ID' link

Detailed summary by Alert ID

(a) newtopic (b) postreply ByStorm Software Forum Index -> Alert summaries								
View previous topic :: View next								
Author	Message							
ByStormAdmin Site Admin	D Posted: 09 Nov 2009 09:33 am Post subject: Detailed summary by Alert ID							
	This summary is useful for alerting on a rule match.							
Joined: 10 Aug 2004	Change the 'alertID = 10' in the SQL below to match what is defined in the rule.							
Posts: 46	select 1 count, fileName, userName from AuditRecords where alertID = 10 and eventTime > OldestRecordAge							
Back to top	🚨 profile) (😹 pm) (🎯 email)							

- e. Copy the circled area into the clipboard. Here is the actual text: '*select 1 count, fileName, userName from AuditRecords where alertID = 10 and eventTime > OldestRecordAge*'.
- f. Paste the text into the SQL Query area of the alert and change the '10' to '77' to match the alert ID we put on the rule.

ᡖ Define	Summary	
Name:	Watching for website writes.	🔽 Enabled
Oldest R	ecord Age: 0 🚖 days 1 🚖 hours 0 🖨 minutes	
	select 1 count, fileName, userName from AuditRecords where alertID = 77 and eventTime > Oldest	RecordAge

12. Click 'OK' to close the summary screen and click 'Close' on the 'Manage Summaries', this will take you back to the 'Define Alert' screen. Define your alert like this:

ᡖ Define Al	ert								
Summay:	Watching for website writes.		•	Manage Summaries					
<u> </u>									
	Count	fileName	userName						
	Monitor all machines				0				
	DUAL24				*				
Machines:	XPPROVM								
					-				
	Conditional address of the second		De unit construction and	Harr average 20 [1]					
	Send e-mail when count exceed:		Do not send e-mails more	than every: 30 🚍	minutes.				
Mail to:	genecobystonn.com								
Subject*	Website change denied!								
(<%userName%> was denied the ability to change <%fileName%>								
Body*:									
	*Use right-click to enter a variable	e. [Note]: the	e body text will repeat once	for every item over the th	reshold.				
	To: gene@bystorm.com								
	Subject Website change denied								
Preview									
	Enabled			🗸 ОК 🛛	Cancel				

- a. Pick the newly created 'Watching for website writes' summary from the drop down.
- b. Enter '1' for the 'Send e-mail when count exceeds'
- c. Enter '30' for the 'Do not send e-mails more than every'
- d. Enter the email address you want the alert to be sent to
- e. Enter 'Website change denied!' for the 'Subject'
- f. For the body enter:

```
<%userName%> was denied the ability to change <%fileName%>.
```

g. Click 'OK' to close the 'Define Alert' screen

Now we have an alert configured to send an alert when someone is blocked from changing a file on our website.

To recap: We have set FileSure-Defend to block writing, deleting, renaming or changing security on any file on our web site except when those changes are made by the user 'WebMaster' or during our scheduled maintenance time of Saturday morning.

We have scheduled a report to be sent everyday listing all blocked changes.

We have set up an alert to tell us when someone has attempted to change the website, right as it happens.