All Gain – No Pain

Avoiding the *PAIN* inherent with native-Windows file auditing while *GAIN*ing Data Loss Protection

ByStorm Software, LLC
6315-B FM 1488 #264
Magnolia, Texas 77354
USA
www.bystorm.com
info@bystorm.com
+1.877.BYSTORM (297.8676)

So you want to audit what files different users are accessing without having to tolerate the pains associated with native-Windows file auditing?

Most administrators avoid native-Windows file auditing due to the massive CPU consumption and volumes of log events it generates. Furthermore, attempting to set audit and access permissions (SACLs and DACLs) just the way you want them on all of your file shares, folders, and files, is a never ending project for which there simply is no time. Even if it could be completed once, there would always be gaps resulting from the daily changes made to support the business that unknowingly undermine what you have painstakingly established.

There is a better way! And “the better way” can also do more than just audit, or log, which users accessed what files, who changed them, who deleted them, who copied what and where. What about keeping your critical data safe? How do you control which users and processes can access the data in the first place? How do you ensure the integrity of your data and stop unwanted changes to sensitive data/files? File integrity is paramount for just about every governing regulation and is part of every company security policy.

And what about protecting your data from escaping? Maybe you have patient data, credit card data, personal information, or company intellectual property that could damage your competitive posture or your brand equity if it got out!

Read this short paper to learn how you can GAIN simple to use Windows file auditing and data loss protection without having to endure the PAIN you have known previously!

FileSure
Audit. Protect. Comply.

Be Sure that you are….

- …auditing all file accesses
- …protecting your sensitive data
- …complying with regulations and policies

By ByStorm Software.

ByStorm, ByStorm Software, and FileSure are trademarks of ByStorm Software, LLC, in the U.S. and other countries. All other product and company names are trademarks or registered trademarks of their respective owners. The information contained in this document is subject to change without notice. ByStorm Software makes no warranty of any kind with regard to this material, included, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. ByStorm Software shall not be liable for errors contained herein or for incidental, consequential, or other indirect damages in connection with the furnishing, performance, or use of this material.

TABLE OF CONTENTS

PAIN – native-Windows File Auditing 4
Excessive CPU utilization 4
Massive log event volumes 4
System-level objects 4
Security Audit Settings - SACLs 5
Limited Visibility 5
PAIN – native-Windows File Access Controls 6
Access Control Granularity - DACLs 6
Privileged users unstoppable 6
What about sometimes? 7
Inheritance, changes, and exceptions 7
Webmail Gap 7
Rogue application authority misuse 8
What program(s) are accessing the data? 8
GAIN – Right-sized and flexible file access auditing 9
GAIN – Protect your data with user and process access controls 9
GAIN – Comply with regulations and policies – Alerting and Reporting! . 10
GAIN – 3 minute installation 14
About ByStorm Software 14

PAIN – native-Windows File Auditing

Excessive CPU utilization

Native-Windows file auditing can quickly become extremely CPU intensive! With just one simple wrong SACL (System Access Control List – aka security audit policy) inherited across a large share you can CRUSH your server performance. Most system administrators have had previous bad experiences with native-Windows file auditing and have therefore chosen not to utilize it except in very unique situations. This means that file access activity is only being logged, if at all, for a fraction of the data within organizations and usually only the most sensitive shares/folders/files. Obviously this is not desirable, but is a reality of the Windows world we live in. But it doesn't have to be this way! ☺

Massive log event volumes

Native-Windows file auditing often produces dozens of events in the security event log for only a single action in reality. Just about everything every user does involves use of the file system in some way. Sometimes it is the user directly accessing a file, but most times it is an application, or process, on behalf of the user, accessing the file. Regardless, the volume of events that this produces across the entire IT infrastructure is just massive and can often be measured in Terabytes of log data that must be collected and stored. What's worse is that most local logs are configured to be relatively small and wrap quickly resulting in lost security event data so turning on settings that cause this to happen frequently is obviously not a good idea!

Some administrators leverage backup applications at regular intervals to take snapshots of the log data to try and store the data before it wraps. This can directly impact performance on busy systems during production hours though. But doing this off hours means that the logs could have wrapped hundreds of times between backups. So SACLs must be minimal in order to gather only the most critical data while avoiding a wrap.

Some organizations have purchased expensive log management solutions that move the massive amounts of log data to a central store, but this consumes network bandwidth and processing capacity as well, not to mention storage. Then, once all that log data is collected, attempting to search through the massive amounts of log data is cumbersome. Running a single report can take hours because it has to search through all of the data in order to filter down to what is actually desired. It would seem that utilizing a solution that more precisely audits what file activity is occurring would solve a lot of problems, don't you think?! ☺

System-level objects

Many regulations require that system-level object auditing be enabled. Actually, it isn't just changes to the operating system that most regulations want logged, it is any change to application configurations. The problem with 'system objects' is that they are stored in the Windows folder and the 'Program files' folder which are probably the two largest folders on the machine, but since a 'system object' can actually be placed ANYWHERE, you would be forced to audit the entire computer and since you can't say 'only watch system objects' with the native tools, you end up watching all files…even though that's not what you actually need.

Security Audit Settings - SACLs

If you have ever looked at the security event log, you know how painful it can be if you enable all of the possible auditing.   Many of these events provide no added value but are unavoidable. Setting your security audit settings (System Access Control Lists – SACLs) to enable 'just the security auditing you desire' is a huge challenge and is never ending. Even after you get your settings exactly as you desire, when a new share is brought online without the same settings you could easily have a gap introduced.

And what if one of your administrators changes the SACL on a sub folder? When you set things up you had the inheritance box checked and the sub folders inherited what you wanted them to. But when a sub-folder SACL is later changed, totally unbeknownst to you, which is what will happen, guaranteed, you have a gap and are not auditing what you think you are auditing! Also, by pushing down inherited SACLs to sub-folders you may very well be overwriting a SACL on a sub-folder that you don't actually want changed.

What's more challenging is that SACL changes are rarely audited and therefore impossible to track down, which means you are unable to see who changed a SACL and what they changed it to; or worse yet, a malicious administrator could turn off SACL change auditing and do whatever they want and then turn back on auditing after they finish.

So when it comes to your SACLs, it is simply not possible to know absolutely everything about every file in your organization. It is also simply not possible to keep users from moving these files to new shares or onto their own workstations where the SACLs may not be set the way you want them resulting in unpredictable security auditing!

There are many challenges with native-Windows security auditing! I wonder if there is a better way? ☺

Limited Visibility

Due to the above mentioned challenges, windows file auditing is rarely, if ever, utilized to its full extent. Actually, it is only utilized in very specific cases where there simply is no choice. This creates so many problems for IT when it comes to daily operational problem solving, security, and compliance. Even for simple issues such as which folder did a file accidentally get dropped into? Did the file get deleted? Who copied or moved a file, and when? What about proactively knowing that a block copy of a large number of files has occurred? Wouldn't it be nice to know within a few seconds that something like this had occurred?

PAIN – native-Windows File Access Controls

Access Control Granularity - DACLs

A DACL is a Discretionary Access Control List and it contains a list of Access Control Entries. Each of these entries can allow or deny a user a certain right to a file or folder. These lists could get complicated if they were actually used. Since the model is so granular, administrators usually set broad rights on an entire share and then attempt to use group membership to control access.

A major unintended consequence of this extreme granularity is that people use of other systems to "get around the access rights limitations" and by copying protected data onto protected shares to unprotected shares. If a user needs access to a file they don't normally have access to in order do their job, they often have their boss, who has access to the data, email it, change the DACL, or copy/move the file to an unprotected/public location. This is extremely common and totally undermines the security model. For example, if a marketing manager needs access to some internal sales figures to produce a report, they just contact the sales Director, who then would just e-mail the figures, or worse yet, the whole file, or maybe they would change the DACL thereby granting the Marketing manager direct access, or even worse, maybe they just copy the protected data to a temp share with no access controls whatsoever. This happens a lot and RARELY do people remember to go back and remove what they did, nor do they have the time to do so.

Thus there are competing challenges at work. Non-IT personnel just want to be able to get their work done on time. While of course they care about security, they don't want the security model to get in the way of getting things done. On the other hand, IT Administrators are trying to find the right balance of security to mitigate security risks while allowing the business to operate. There is never perfect alignment.

Privileged users unstoppable

Fortunately, administrators have permissions to deliver on projects and to make the changes the business wants and needs. Unfortunately, administrators have the keys to the kingdom. Auditors are often frustrated with the inability to track and control what administrators have done, have seen, or could do or see.

Anyone in the administrators groups can touch or do just about anything. Even if they don't have access, administrators have the knowledge and the authority to get around native-Windows security. If denied access to a file, all they have to do is "take ownership" of the file and then they are guaranteed to have authority to do whatever they want to it. They can also use the administrative share to obtain access.

If they so choose, they can change access permissions and audit settings, go and do what they want to do, and then reset the settings back to what the company security policy says they should be. In most cases, organizations never know this has occurred because they only do occasional "point in time" security checks, or snapshots, and they have no idea what has happened between the snapshots.

Company executives are often totally unaware that their data is viewable by all users in the administrators group. What about the case where executives are preparing for a layoff? Or maybe they are working on an announcement that will impact the stock price in some way. Administrators need elevated permissions to manage the infrastructure, but they don't need permission to access all sensitive data!

Another common challenge for IT management is the inability to prove that their personnel have not been accessing what they are not supposed to. Many of the regulations to which organizations must comply require for IT to prove that sensitive data has not been accessed by their most privileged users. This is certainly easier said than done! That is, with native-Windows security of course! ☺

What about sometimes?

If a user has "write" authority for a folder, they can change anything in it. Of course, access can be denied for specific files in the folder if the DACL for that file is set up appropriately. But this is next to impossible to manage/maintain across an entire organization.

There is no real way, with native-Windows security, to allow a user to have create/write access to a folder, yet somehow limit this authority in some way. For example, if the user is scanning in evidence for a court case, in order to do their job, they must be able to create new files and write to the folder. But what is to stop them from altering the stored image or text in some way? If they have the permission to write, they have the permission. Wouldn't it be nice to allow the user to write to the folder only when the scanning application is actually the application doing the writing? Imagine being able to make decisions for file access based on the application/process that the user is using. Makes you think doesn't it!! ☺

Inheritance, changes, and exceptions

Just like with SACLs, DACLs are typically inherited from parent folders. At any time, these and can also be manually pushed down to all sub-folders and files at any given point in time. However, there are almost always exceptions that administrators must account for, for various business reasons, when it comes to sub-folder access and specific file access. There is no real way for all administrators to know precisely what the other administrators know and why they made DACL changes/exceptions. It is just too complicated and fast paced and there are just too many files and folders. By forcing inheritance, which logically seems to be a good thing to ensure consistency, they could be making a grave mistake and accidentally violating the company security policy.

What's worse is a disgruntled administrator, or potentially a criminally minded administrator. You never know what is actually set and why when it comes to DACLs….so why rely exclusively on such a model? Good question! Maybe there is a better way! ☺

Webmail Gap

Your user's browsers all run under the security context of that user. If that user has permission to read a file, then so does webmail and thus it can be attached to to webmail emails and sent outside of your organization. The existing Windows security model does not enable you to make file access decisions based on the process/application that the user is utilizing. Wouldn't it be great to give the user's access to all the data they need to have access to but only allow certain processes they are utilizing to interact with that data? For example, if Microsoft Word was the only application that could open (read) a file ending in ".doc" or ".docx" then it would be impossible for internet explorer, or FireFox, or Chrome to open that file for read, which is precisely what happens when your webmail application attempts to attach a file.

Rogue application authority misuse

The same is true for rogue applications. Your users can unknowingly become infected if they visit a website that exploits browser vulnerabilities and installs rogue applications or zero-day viruses/worms and your anti-virus systems will not catch this! Another common issue is the downloading and installing of assorted applications that the user intends to be installed, yet it is infected with something malicious. And there is of course the risk of a file download via webmail that bypasses perimeter security solutions. And worse yet, there is the potential for some other internal action, such as the inserting of an infected USB key drive that they received at a trade show.

The ultimate problem is that any application or process running on the user's machine runs with the security context of that user. Thus it has access permissions to any data to which the user has access permissions. Anti-virus systems are able to detect what they already know about and have signatures to watch for. But that leaves a significant gap in your organization. Wouldn't it be great to be able to control not only which users and groups have access permissions, but better yet, what access permission they have based on the application they are utilizing, whether knowingly or unknowingly? Or even better than this, wouldn't it be great to only allow specific white-listed applications to actually write anything!?? ☺

What program(s) are accessing the data?

End-user access to data on network file shares is actually a "remote access" to the data on file shares. The file server has no way of knowing what program or process is actually making the read, write, create, delete request. The file server simply knows the user account that is making the request and will make the decision to allow/deny the request based solely on the DACLs on the file share.

In just about every industry there are industry-specific programs used to design a product or deliver a service. These programs must have access to the data so it is the users that are given the permissions since the programs run under the user's security context. For example, if an engineer has permission to access a file share containing CAD designs, potentially worth millions, in order to do their engineering work, then they have access to the CAD designs to attach to webmail and send it outside the organization. Wouldn't it be great to limit access to certain types of data based on the application that is accessing that data? ☺

GAIN – Right-sized and flexible file access auditing

We have discussed many challenges when it comes to file access auditing and much of this is probably not news to you. What is likely news to you, is that there is a way to audit file activity to the extent that you want to audit, without having to manage SACLs.

ByStorm FileSure is a rules-based Windows file system management solution that will audit precisely what you want audited at a fraction of the CPU utilization that native-Windows auditing uses and with a fraction of the events that native-Windows file auditing produces. The audited events can be written to the Windows security event log or to the ByStorm application log, or both. You can consolidate these events, alert on them, and report on them at any time. You also have the flexibility to change auditing policy from a single central location.

What makes ByStorm FileSure unique is that it allows you to set rules to audit precisely what you want audited. Maybe you want to audit all access to the payroll share, or all access to patient data, or all accesses to the cardholder network where credit card data might exist, and you never have to be concerned with SACLs or changes to permissions that you might discover after the fact.

NAS – Another GAIN

Many NAS (Network Attached Storage) devices emulate the Windows file system or have some proprietary file system on them. This creates additional challenges when it comes to file access auditing. Even if you were to set your SACLs how you want them and are auditing on Windows servers what you want, how then are you going to manage SACLs on these systems where they don't exist? Tthese systems cannot discern what application, or process, on a remote system is actually attempting to access the data. All the file system on the NAS knows is who is making the request, what they are trying to do (Read, write, create, delete, etc.). Without auditing enabled on the *originating system or workstation*, it is impossible to record what application/process is, in effect, actually interacting with the file. With ByStorm FileSure you are not only able to audit on Windows file servers but also you are able to audit at the workstation itself, which is a huge plus when it comes to NAS devices.

GAIN – Protect your data with user and process access controls

Since data loss prevention products are typically expensive and difficult to use, most administrators don't believe that such capabilities are even available to them. With ByStorm FileSure this is now possible.

Blocking access to data, blocking the copying of data, allowing the changing of data when and where you want and only for certain users can be next to impossible. FileSure achieves this by extending its reach to workstations and laptops and allowing you to restrict access to a file by application. For example, you can configure FileSure to allow only Microsoft Excel to read spreadsheet files. As simple as this approach may seem, with this one rule, you can use FileSure to stop virtually all digital data loss of Microsoft Excel files. This blocks webmail attach of spreadsheets because the browser is not Microsoft Excel. This blocks a worm, which would be an executable other than Microsoft Excel, from opening the spreadsheet in an attempt to copy it or alter it.

With FileSure you can not only control access to the data but you can also control where the data can be written, by who or what process, and even limit it to certain times of the day or days of the week. With FileSure you have **complete control** of where your data goes with no discernable impact on performance.

GAIN – Comply with regulations and policies – Alerting and Reporting!

Regulations have been created to protect data in some way for some very good reasons but it all boils down to file auditing and file access control. Ensuring data integrity is paramount to all compliance initiatives. Knowing who is accessing/changing files, what they did, and when they did it, are all critical for organizations to ensure that policies are being adhered to and furthermore that they remain compliant with industry and governmental regulations.

With FileSure you not only have record of all of these accesses, but also can know in near real time via the built in alerting that can be based on particular activity being detected, or maybe on certain volumes of activity, or thresholds being crossed. FileSure can send emails to alert you based on a variety or criteria.

Reporting is critical for compliance too and so many products have difficult to use and uncustomizable reporting. Not only is FileSure reporting customizable, but also you can automate report generation to be on the scheduled interval you desire.

Here are some examples of the reports provided out of the box:

USER ACTIVITY REPORTS	
Name	**Description**
After-hours activity	This “detail” report shows file activity that occurs after hours and on weekends; nice for knowing who is doing what when everyone else is gone. The report is grouped by user.
Number of deleted files	This “at a glance” report sorted by user name allows you to quickly find how many files a certain user has deleted. This report is more useful for trend analysis than it is for abnormal behavior detection.
Number of files opened for read access	This “at a glance” report sorted by user name allows you to quickly find how many files a certain user has opened for reading. This report is more useful for trend analysis than it is for abnormal behavior detection.
Number of files opened for write access	This “at a glance” report sorted by user name allows you to quickly find how many files a certain user has opened for writing. This report is more useful for trend analysis than it is for abnormal behavior detection.
Delete access denied	This “detail” report shows all the attempts to delete a file that were denied either by FileSure Defend OR native-Windows security; it is useful for detecting users attempting to delete files that they shouldn’t be.
Files copied	This “detail” report shows all the files that have been copied by common means (Windows Explorer, XCopy or the Copy command). The report is not limited to a certain device and will report all file copies. Since this report uses a process name, it is most useful when reporting on workstation file activity.
Files created	This “detail” report shows all the files that have been created by each user. This report is useful for see what sort of information users are storing on the server. The report is grouped by user.
Files deleted	This “detail” report shows all the files that each user has deleted. Monitoring file deletion is useful for detecting inappropriate activity by a user. This report is perfect for sending to department managers.
Files renamed	This “detail” report shows all the files that each user has renamed. Monitoring file renames is useful for detecting inappropriate activity by a user. This report is perfect for sending to department managers.
Files possibly sent with web mail	This “detail” report shows all the files that have been read by Internet Explorer and FireFox. The reading of a file by an internet browser often indicates that the file is being sent via web mail. Since this report uses a process name, it is most useful when reporting on workstation file access activity.
	This “detail” report shows all the files that have been read by Internet Explorer and FireFox and all files written to a removable drive. The reading of a file in an internet browser often indicates

Potential File theft	that the file is being sent via web mail. Since this report uses a process name, it is most useful when reporting on workstation file access activity.
Files written to a removable drive	This “detail” report shows all the files that have been written to a removable drive. Writing files to a removable drive often indicates that someone is taking some work home which is moving it outside the security measures that are in place in the office. Additionally, this is one of the more methods for data loss/theft.
Folders deleted	This “detail” report shows all the folders that have been deleted by each user. This report is useful for monitoring the folder deletions of a suspect employee.
Folders renamed	This “detail” report shows all the folders that have been renamed by each user. This report is useful for monitoring the folder renames of a suspect employee.
Folders moved	This “detail” report shows all the folders that have been moved by each user. This report is useful with the “accidental dragger” problem, which is when someone drags a folder to another location by accident.
Read access denied	This “detail” report shows all the attempts to read a file that were denied either by FileSure Defend OR native-Windows security; it is useful for detecting users attempting to read files that they shouldn’t be accessing.
Root folders moves	This “detail” report shows the root folders that have been moved. Moving root folder should rarely occur and can cause great pain when they do. This report identifies what user moved the folder and when.
File security changed	This “detail” report shows all the security changes that have occurred. Changing file security can open a security breach and allow unintended users access to otherwise secure data; it’s important to be aware of these changes and who made them.
Touched files	This “detail” report shows all files that have been read, written to, deleted, moved or had its security changed. It can be a very large report and is only useful to make auditors happy.
Write access denied	This “detail” report shows all the attempts to write to a file that were denied either by FileSure Defend OR native-Windows security; it is useful for detecting users attempting to write to files that they shouldn’t be accessing.

FILE ACCESS SUMMARY REPORTS

Name	Description
Number of files created	Typically file servers chug along just fine, but then someone, somewhere decides to copy their entire music library to their home share…all 30 thousand songs. This “at a glance” report will help you find people doing bulk copies TO the server. This report is sorted by the number of files created.

Number of files deleted	This “at a glance” report will help you find people doing bulk deletes from the server, which probably shouldn’t happen very often. This report is sorted by the number of files deleted.
Number of files opened for read access	If you need to migrate a server, this is a handy “at a glance” report to show you who is still using the old server. This report is sorted by the number of files opened for read access.
Number of files opened for write access	This “at a glance” report will help you find people doing bulk writes to a server, since bulk operations are typically automated, a program writing to bunches of files is rarely a good thing. This report is sorted by the number of files opened for write access.
Files deleted	This “detail” report is useful to review all the files that have been deleted from a file server. This is a nice report to e-mail to department managers. The report is ordered by file path so managers can search for a deletion of a specific file.
Folders deleted	This “detail” report is useful for reviewing what folders are being deleted. Folder deletions shouldn’t occur that often and should be investigated. The report is ordered by folder path so a specific folder deletion can be found easily.
Time of file deletions	This “detail” report is useful for watching for file deletions during suspicious times, for example file deletions after hours. Evil doers like try to hide what they are doing, so they tend to do them when they believe that no one is watching. The report is ordered by time.
Time of folder deletions	This “detail” report is useful for watching for folder deletions during suspicious times, for example folder deletions after hours. Evil doers like try to hide what they are doing, so they tend to do them when they think no one is watching. The report is ordered by time.

FileSure Configuration Changes and Exceptions Reports

Name	Description
FileSure log errors	This “detail” report is useful for IT personnel to monitor FileSure for problems; a perfect choice for e-mailing an IT administrator.
FileSure log information	This “detail” report is useful for security administrator to watch for changes to the overall FileSure system. The entries of this report are typically configuration changes performed by a user; a perfect choice for e-mailing the security administrator.
FileSure log complete	This “detail” report is useful when the security administrator and the IT administrator are the same person. This report will show both FileSure errors and FileSure configuration changes.
FileSure rule change report	This “detail” report shows all the changes that have occurred to the FileSure rules. This report is useful for watching what changes are being made to the file security and auditing system; perfect for a security administrator.
FileSure log errors	This “detail” report is useful for IT personnel to monitor FileSure for problems; a perfect choice for e-mailing an IT administrator.

GAIN – 3 minute installation

FileSure installs quickly, doesn't require setting up an external database server, and is pre-configured to audit Microsoft Office files anywhere on the server. Really? Yes!

No external database technology needed!

Aside from the obvious plus of not having to manage an external database, here are some other pluses of our highly compressed, encrypted, and unalterable data store files:

About FileSure Encrypted Data Management	
Feature	**Description**
Performance	By optimizing for insertion of data, we achieve significantly better performance than an external database. For you, it means events aren't lost, even under heavy load.
Storage savings	Our compact data format is extremely efficient. FileSure's data store is massively compressed getting about 5 million records per GB, so it's unlikely that you will ever need to purge or restore the data store.
Easy backup	Audit data is simply stored as files in the file system. Your current file-based backups will handle FileSure data perfectly.
Easy archival	Each system's data is stored in a separate file, and we start a new file each month. You can offload old data simply by removing a file while having the ability to restore at any time - without any need to stop FileSure and miss important events! Try to do that with an external database!
Security	You don't have to worry about some other user (or DBA!) modifying your audit data with an accidental query. There's no additional security model to learn, establish, or audit. FileSure even includes reports so you can see what changes were made to FileSure itself! FileSure Data stores are not only tightly compressed, but also encrypted with powerful BlowFish Encryption protecting it from people wishing to hide what they are doing.

About ByStorm Software

ByStorm Software, founded in 2003 with over 100 customers today, provides IT organizations with low footprint, yet comprehensive file auditing, data loss protection, and compliance enabling alerting and reporting for the Microsoft Windows platform. ByStorm Software is committed to ensuring that our solutions install and begin providing value within minutes and that our customers are empowered to meet PCI, HIPAA, NERC/CIP, NIST, SOX, and other security and compliance mandates.