White Paper

7 Questions to Assess Data Security in the Enterprise

netwrix

Table of Contents

Executive Overview

The enterprise IT organization is moving at a pace like never before. With IT's focus to reduce expenses, increase revenue (when possible), and most importantly—mitigate risk, IT is looking for new technologies to help achieve those goals. Use of the cloud, virtualization, data protection, and threat management are now commonplace and extend the scope of reach for IT organizations. With each new technology and solution, IT executives must maintain a focus on how each can assist with increasing regulatory compliance, operational efficiency, and system security.

With this constant state of looking forward toward the use and security of new technologies, IT organizations often overlook the core technologies that act as the foundation of IT operations. The most fundamental of these is a server farm. Server farms represent the very foundation for housing everything from a simple spreadsheet to complex databases hosting email, accounting data, or patient health records. Users with access to every piece of sensitive data imaginable within your organization utilize server farms daily as part of routine tasks.

In short, your organization lives and breathes on top of server farms and the file system security they employ.

The challenge for IT organizations is how to stay on top of an ever-changing landscape of permission assignments and access in an environment where file system security no longer gets the lion's share of IT organizations' time, and yet 71 percent of end users say that they have access to company data they should not be able to see[1].

The answer lies in automating the auditing of server farm security. By doing so, the organization creates visibility into two key aspects of file system security:

- **State of Security** – With 88% of insider threats involving the misuse of assigned privileges[2], auditing who has (or had) access to files containing sensitive information is critical and represents your organization's overall potential risk. This is accomplished by looking at present and past security assignments and ownership within the file system security.

- **Use of Privileges** – Auditing user access to file storage further hones the potential risk down to a subset of all users who have (or had) access. And given that 54 percent of those users with access they believe they shouldn't characterize that access as frequent or very frequent1, auditing user access becomes critical.

[1] Ponemon, Corporate Data: A Protected Asset or a Ticking Time Bomb, 2014

[2]Verizon 2014 Data Breach Investigations Report

Executive Overview

This visibility reduces the potential risk of data breaches by ensuring proper security controls are in place, while also monitoring for improper access as an additional security layer.

The visibility necessarily requires more than just a simple annual review; with 46% of IT organizations making changes daily or weekly that impact security , the dynamic nature of security permissions demands constant monitoring, thus requiring automation. An automated auditing solution can continually gather, monitor, alert, and report on file system security, ensuring every part of your environment remains secure and compliant, lowering your organizational risk while improving your security stance.

Next Steps

The remainder of this paper demonstrates how file system security can be assessed and addressed with auditing by asking just seven questions. It is intended as a reference for those who are implementing and managing the security of your organization daily. It also can be used as a gauge for the IT executive to test the abilities of the IT security staff to see if they are able to answer the security questions without the need for an auditing solution.

[3]Netwrix 2014 State of IT Changes Report

netwrix

Typical Audit Questions which Help to Maintain Security in the Enterprise

Despite the advent of cloud-based storage and collaborative solutions, such as Microsoft SharePoint, one of the most used solutions today remains the Windows file system. Today, organizations large and small continue to use Windows to centrally store and share most of an organization's most sensitive data.

Enterprises serious about the state of file server security best assess their current risk by thinking about questions an auditor would ask, deriving those questions by looking at file server security from three perspectives: permissions, ownership, and access. Two of these three perspectives (permissions and ownership) provide organizations with a sense of the potential risk their current security configuration allows, with the third (access) yielding insight into risk incurred through contact with sensitive information.

Permissions to files and folders are a two-part mix of assignments within a Windows file system and the user and group accounts in those assignments that reside in Active Directory (AD). Determining exactly who is impacted by permission assignments involves utilizing both sources of information.

Ownership becomes important because of the risk introduced. While a user may not have any permissions to a given file or folder, should they be the owner of that same file or folder, they retain the right to change the permission assignment anytime – which includes giving themselves permissions to access the file or folder in question.

Lastly, **access** demonstrates the actual risk incurred. If fifty users have permissions to an Excel spreadsheet with social security numbers but only one has actually accessed it, your risk is limited to what that one person did. So it's important to understand the actual use of the permissions assigned.

PERMISSIONS

1.Who Has Which File/Folder Permissions?

The question of "who has access" has its' roots in the scenario where a specific data set is of significance to a compliance mandate, a data breach inquiry, or general security concerns. Knowing who has access is the first step is determining whether security is well-established and well-maintained, meeting compliance objectives and/or security policies.

At the surface, this appears to be an easily answered question with the security properties of a given file or folder providing the details needed. However, Windows file system permissions are a complicated mix of explicit assignments to files and folders, inheritance from permissions higher in the folder tree, assignments to users and groups, and group memberships, making this a somewhat taxing task.

Answering the Question

[Difficulty Level: Moderate]

It's possible to provide a proper answer to this question, but IT teams will need to gather a number of sets of permissions (both explicit and inherited) to both users and groups, and then logically expand the memberships of any related groups (presumably either via a manual search in AD or via script), keeping in mind that groups can be nested, requiring the continual logical expansion of group memberships until you have a final list of every user included.

Alternatively, Netwrix Auditor simplifies the collection, computation, and de-complication of permissions, pulling the needed information from both the file system and Active Directory, providing a report showing the net result of who has permissions, whether from group memberships, explicit assignments, or inheritance.

NETWRIX\bhelwig	Traverse folder/execute file List folder/read data Read attributes Read extended attributes Read permissions
NETWRIX\blloyd	Traverse folder/execute file List folder/read data Read attributes Read extended attributes Read permissions

[2] Thycotic 2014 Black Hat Hacker Survey

2. Are Any Files/Folders Exposed to Everyone?

IT departments often focus on tactical daily objectives and see permissions management as an unnecessary distraction, finding it easier to simply grant access to everyone, ignoring any risks it may create.

While functionally this question is merely a subset of the previous, its answer potentially represents the greatest risk and exposure to company data.

Answering the Question

The process is similar to that of the previous question but dramatically simplified. No longer is there a need to look for every user account or the need to traverse nested group memberships. In this case, simply looking for when the dynamic group Everyone has been assigned permissions is sufficient.

Netwrix Auditor provides the same level of detail, focused in on the Everyone group by specifying that group in the same report.

Path Folder: \\pdc\Users\Administrator\Documents\Shared documents\Accounting & Finance

Account	Permissions
Everyone	Traverse folder / execute file List folder/ read data Read attributes Read attributes Create files data Create folders / append data Write attributes Write attributes Delete subfolders and files Read permissions Change permissions Take ouunership

3.What Permissions Does "Username" Have on a Server or File Share?

This is the direct opposite of the previous questions, which focused first on the resource (i.e. a file or folder) and then sought to determine who could access it. In this case, the focus is on an individual IT user and building a list of every file and folder they have permissions to access, along with the associated permissions.

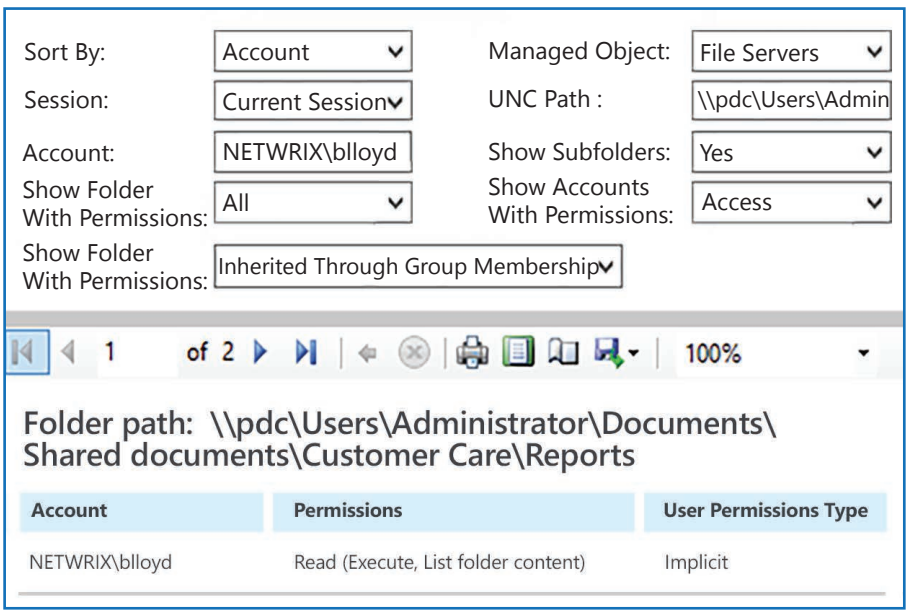
In reality, this question may be expanded by an auditor to more than one server or file share, or even to additional systems, because their focus is to understand exactly where an individual in question may have had the ability to access sensitive or business-critical data.

Answering the Question

[Difficulty Level: High]

The sheer amount of manual work needed to collect every permissions assignment from every file and folder, mixed with the need to expand every associated group (including nested groups) within AD to ensure nested group affiliations don't go undiscovered, and the cross-reference of all this information only results in obtaining detail about a single user's permissions.

Netwrix Auditor automates these manual tasks, collecting every assignment, scouring AD for every group and traversing any nested group membership until reaching the associated users, correlating the data and building the permissions list necessary to provide a simple answer to what is actually a complex question.



4.Who Had Which File/Folder Permissions in the Past?

The true nature of an organization's security is not simply reflected by looking at its' present state; it's properly reflected by looking at it as a constantly moving target, requiring auditors to inquire about changes since the last time you were audited. That's why this question is so important and seeks to uncover who may have had permissions - even if only for a minutes, hours, or days - at some time in the past.

This already difficult task is only exacerbated by the necessity to perform the complex work spelled out in the first question. In essence, the answer to this question will also comprise the state of inherited permissions, and the state of groups and their memberships – all at the point in time in question.

The reference point to the past will likely need to be a range instead of a specific point in time, in order to ensure states of permissions are not overlooked. For example, if an organization were subject to a security audit, the question might be to ascertain who had permissions anytime in the last year.

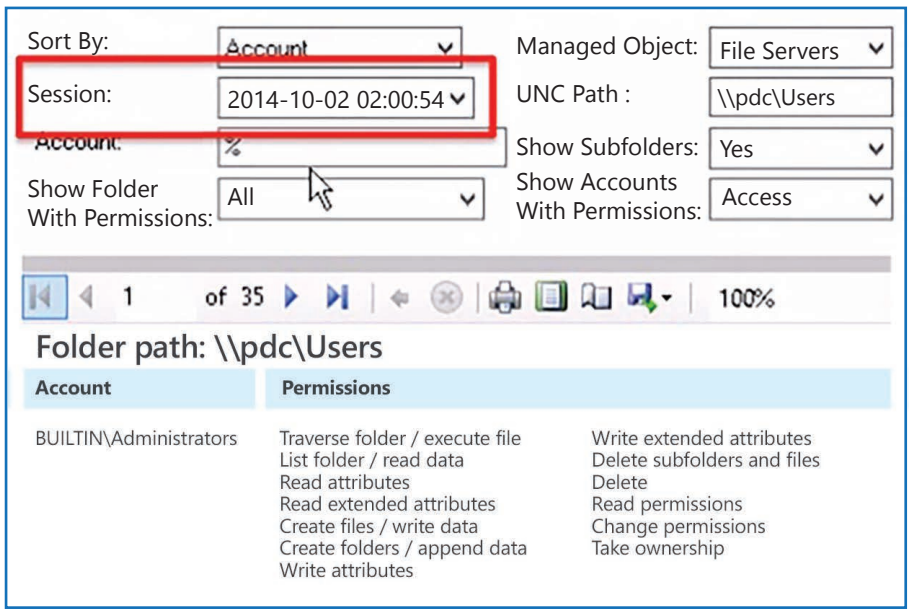
Answering the Question

[Difficulty Level: Severe]

Only those organizations implementing change control or change management solutions may have an ability to answer a question about a past security configuration. Even with those solutions in place, a record of changes to permissions likely exists, while it is highly unlikely a record of the state of permissions has been maintained. Reconstruction of permissions to a specific point in time may be possible if an initial point of reference exist to apply the recorded changes to.

4.Who Had Which File/Folder Permissions in the Past?

Because Netwrix Auditor maintains its own snapshots of permissions at pre-configured intervals, it has the ability to provide state-in-time reporting at any point in the past it has been recording permissions. By selecting the snapshot (which corresponds to a date and time), auditors can easily see what the permission state was, providing them with the detail needed to answer this question.



5.What Permissions Have Changed Recently?

The only constant in IT is, of course, change. This is one of the primary reasons auditors ask the previous question, seeking to understand what permissions looked like in the past. Additionally, this question is often raised when attempting to find the root cause of a problem. A simple permissions change can impact tens, hundreds, or thousands of users.

Knowing what's changed has similar ties to knowing what permissions were in the past, in that they both require some record-keeping. In this case, the record isn't of the state of permissions, but the changes to permissions.

Answering The Question

[Difficulty Level: Moderate]

Native Windows auditing can supply a record of permission changes to the file system, but is more positioned on its own as a solution to find one-off changes. To build a report of everything that has changed within a given timeframe, an expectation of manual work will be needed, perhaps involving some advanced use of Excel or scripting.

Besides keeping track of the constant state of file system permissions, Netwrix Auditor's primary function is to monitor, track, and audit changes to critical systems, including Windows file systems. So viewing recently changed permissions is not only a simple task, it's native to Netwrix Auditor. In addition, should the question be asked as part of determining the root cause of a problem, Netwrix Auditor also provides the ability to revert unwanted or problematic changes.

Action	Object Type	What Changed	Where	Who Accessed	When Changed
Modified	File	\Users\Administrator\ Documents\Shared documents\ Operations \Legal.txt	pdc	NETWRIX\ administrator	2/25/2015 3:31:49 AM
Attributes changed from "Archive" to "ReadOnly, Archive"					
Added	File	\Users\Administrator\ Documents\Shared documents\ Operations \546 - Copy.txt	pdc	NETWRIX\ administrator	2/25/2015 3:34:37 AM
Added	Folder	\Users\Administrator\ Documents\Shared documents\ Accounting &Finance\Invoices	pdc	NETWRIX\ administrator	2/25/2015 7:46:17 AM
Removed	File	\Users\Administrator\ Documents\Shared documents\ Marketing \White Papers\NewWP.pdf	pdc	NETWRIX\ administrator	2/25/2015 7:57:13 AM

OWNERSHIP

6.Who Is the File/Folder Owner?

From a security perspective, ownership to files and folders, if left unchecked, has the same net effect as a known vulnerability that goes unpatched. If a user has no permissions to a file or folder, but is the owner, they can easily assign themselves permissions, granting access. This is the key reason why this question must be asked when considering the state of your file system security.

Like permissions, the process of determining ownership has the same complexities around inheritance, and nested group memberships, making this more than just a simple exercise.

Answering The Question

[Difficulty Level: low]

Determining ownership is rather easy process requiring Windows PowerShell commands. All you have to do to determine the owner of a file is call the Get-Acl cmdlet, passing Get-Acl the path to the file in question. In turn, Get-Acl will report back information.

Netwrix Auditor keeps track of ownership, making the identification of owners a simple task of running a report and targeting the files or folders in question.

Owner: BUILTIN\Administrators

UNC Path
\\pdc\Users\Administrator\Documents\Shared documents\Accounting&Finance
\\pdc\Users\Administrator\Documents\Shared documents\Accounting&Finance\Invoices
\\pdc\Users\Administrator\Documents\Shared documents\Accounting&Finance\Invoices\sdfsdfsdf.txt
\\pdc\Users\Administrator\Documents\Shared documents\Accounting&Finance\Reports
\\pdc\Users\Administrator\Documents\Shared documents\Accounting&Finance\Reports\BS_2011.xlsx

ACCESS

7.Who Has Accessed a File Within a Specific Period?

Access helps to quantify an organization's risk. For example, in answering this question, should it be determined that no one has accessed a file containing sensitive information, the risk is quantified (and will likely be subsequently mitigated through modifying the permissions to that file).

Organizations can determine access more easily than permissions, since access only involves users and not groups. Additionally, Windows auditing provide a solid foundation around providing details.

Answering The Question

[Difficulty Level: Moderate]

Even with file system auditing set up, and Windows Event Logs containing the detail necessary to answer this question, the challenge for organizations revolves around two basic issues. The first is the audit log data is not presented in an intelligible format and could require multiple log entries to equate to a single action by a user. The second is the timeframe in which you want to determine access. Simple inquiries involving a single day's access can be addressed manually, with longer durations requiring advanced exporting and data mining to deliver an answer.

Additionally, many organizations do not archive log data for extended periods of time, limiting how far back in time access can be determined.

Netwrix Auditor takes related log entries form a single action and intelligently combines them into a single entry, simplifying the process of quickly understanding whether a file was access and what was done to it. Additionally, Netwrix Auditor maintains its own database, allowing for independent retention times from that of log data, ensuring you have the ability to answer the question, regardless of the timeframe.

Action	Object Type	What Changed	Where	Who Accessed	When Changed
Modified	File	\Users\Administrator\ Documents\Shared documents\ Operations \Legal.txt	pdc	NETWRIX\ administrator	2/25/2015 3:31:49 AM
Attributes changed from "Archive" to "ReadOnly, Archive"					
Added	File	\Users\Administrator\ Documents\Shared documents\ Operations \546 - Copy.txt	pdc	NETWRIX\ administrator	2/25/2015 3:34:37 AM
Added	Folder	\Users\Administrator\ Documents\Shared documents\ Accounting &Finance\Invoices	pdc	NETWRIX\ administrator	2/25/2015 7:46:17 AM
Removed	File	\Users\Administrator\ Documents\Shared documents\ Marketing \White Papers\NewWP.pdf	pdc	NETWRIX\ administrator	2/25/2015 7:57:13 AM

Going Beyond File System Permissions

Looking beyond the 7 questions to identify risk within a Windows file system, it's important to note how many of the answers rely on the configuration of Active Directory. Specifically, those security concerns that depend on group memberships.

In the same way permissions or ownership in the Windows file system changes over time, so do group membership within Active Directory, making it critical to expand the scope of an audit to include Active Directory as part of the conversation.

About Netwrix Corporation

Netwrix Corporation's core competency is in change auditing of critical systems across the entire IT infrastructure. With the broadest platform coverage available in the industry, innovative technology and strategic roadmap aiming to support different platforms, devices and applications, Netwrix offers award-winning auditing solutions and superior customer service at affordable prices. Founded in 2006, Netwrix has evolved as #1 for change auditing as evidenced by thousands of satisfied customers worldwide. The company is headquartered in Irvine, CA, with regional offices in New Jersey, Ohio, Georgia and the UK. Netwrix is ranked No. 73 on the Inc. 5000 list of the Top 100 Software Companies and an overall 831 on the Inc. 5000 list of America's Fastest Growing Private Companies in 2013.

Netwrix Corporation, 300 Spectrum Center Drive, Suite 820 Irvine, CA 92618, US

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-308-3023