What do you need to audit and why?

Expect what you inspect

Don't let it be you!

Just take a few minutes to look at the most recent security breaches and it becomes quickly apparent that there's a common theme. In nearly all cases breaches occur due to an insider gaining inappropriate levels of access, either through negligence or abuse, without proper checks and measures being in place. Far too often the need to audit and monitor what privileged users are doing is not recognised as a 'NEED' and is often cited as a 'nice to have'. There is still a very high percentage of enterprises that simply don't have the means to proactively monitor privileged user activity and don't have appropriate measures in place to audit when changes are made, permissions are modified or when critical data is handled.

Far too much of the security strategy appears to be grounded in goodwill and trust across their employees and it's not until after an event it becomes apparent just how necessary a proactive approach to auditing is. Whether through negligence, lack of training or just abuse, the reality is that people are nearly always the weakest link in the IT security strategy. It's ultimately people that grant access to a confidential file, alter a password policy, copy a file or leak data - so failing to audit these activities leaves yourself open to abuse.

Ultimately – we believe, in IT security terms, you can only expect what you inspect. More specifically, if you don't have a proactive and sensible approach auditing and monitoring you can can't guarantee that at some point that your systems or data won't be breached. We're not suggesting that auditing offers a magic bullet here - though it undeniably helps identify issues and keep them internal before they create headlines. It's an essential part of a sensible balanced security plan...

Do you need Lepide?

Let's agree on a few basic assumptions; firstly that data integrity is critical to the modern business, and if your confidential data were to end up in the wrong hands the consequences could be significant. Secondly, we're assuming that you're operating in an IT environment where it's likely you have multiple system administrators and/or privileged IT users. Thirdly, we assume you agree that the speed in which an organisation is able to identify a security breach or potential security weakness directly correlates with the effectiveness of the response. The remainder of this document offers a series of sample [common sense] security questions to help you determine whether your current approach to auditing and monitoring is 'security ready.'
Do YOU need Lepide?
Let's find out...

Who has the ability to make changes to your Active Directory and at what level?

Let's start at the core – Active Directory. If your Active Directory integrity is compromised your business is compromised. From a security standpoint ensuring who know who has what which rights to your Active Directory is of paramount importance. The implications of a rogue or negligent administrator within your Active Directory can't be understated. We believe it's essential to operate a 'least privilege' approach to Active Directory administration and to achieve this you need to ensure you know exactly who has which permissions in the first place. How quickly could you tell who has which permissions and how they got them?

Question	Time taken with Lepide	Time taken with Native Auditing	How long would it take you?
Who has which types of permissions in your Active Directory?	< 1 min.	> 25 mins.	
How was the permission granted?	< 1 min.	> 15 mins.	
When was the permission granted?	< 1 min.	> 15 mins.	

How proactive is your method of tracking critical system changes?

Having an automated and proactive approach to auditing changes should be at the core of all organisations IT security plan. If administrators are making malicious changes you surely need to know immediately ? If a permission was changed that would allow access to a system to containing business critical information how long would it be before you'd know? We think it's critical that all organisations should have real time alerts and advanced reports showing exactly WHO, WHAT, WHERE and WHEN any [specified] change is made to your Active Directory, Group Policy, Exchange, SQL and SharePoint environments. Simply put, when it comes to auditing for security - you can only expect what you inspect. Here are a few questions to determine if your current approach to auditing is proactive enough.

Question	Time taken with Lepide	Time taken with Native Auditing	How long would it take you?
Who, what, where and when was a user deleted?	< 5 secs real time alert < 1 min. full report	No real time alert > 15 mins. manual log correlation	
Who added 10 new members to a privileged security group?	< 5 secs real time alert < 1 min. full report	No real time alert > 25 mins. manual log correlation	
Who, what where and when critical group policy setting was changed?	< 5 secs real time alert < 1 min. full report	No real time alert > 25 mins. manual log correlation	
A non owner of a mailbox deleted or modified or viewed a specific folder or email in a critical mailbox?	< 5 secs real time alert < 1 min. full report	No real time alert > 25 mins. manual log correlation	
How quickly could you identify the before and after values of a critical change?	< 5 secs real time alert < 1 min. full report	No real time alert > 25 mins. manual log correlation	

How do you ensure the right people have the right levels of access to your data?

One of the biggest challenges faced by IT security teams today is ensuring you appropriately provide the right levels of access to the right users to your [confidential] data. To address this, you need to ensure you have a proactive, quick and reliable means to provide meaningful reports to show you who has access to what and how and when access was granted. How confident are you that your data is being accessed appropriately and responsibly? How quickly can you answer these simple questions?

Question	Time taken with Lepide	Time taken with Native Auditing	How long does it take you?
Who has which permissions to a specific file or folder?	< 1 min. detailed report	> 25 mins.	
What was the origin of the permissions?	< 1 min. detailed report	> 25 mins.	

How would you know if a file/folder permissions was added or modified?

Aside from state in time reporting on permissions perhaps the most time consuming part of the process in ensuring a least privilege approach is keeping track of permissions being added, deleted or modified. And we're all familiar with just how easy it is for permissions to sprawl out of control and the potential consequences. How proactive is your approach?

Question	Time taken with Lepide	Time taken with Native Auditing	How long would it take you?
If a permission was deleted to a critical folder how long would it take you to find out?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 15 mins. manual log correlation	
If a permission was added then removed an hour later how long would it take you to find out?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 15 mins. manual log correlation	

How do you keep track of what your users are doing with your most critical files and folders?

If we agree that data is at the heart of the modern business, then logically we must concur that keeping track of how your users are interacting with your data is critical. To ensure information security and mitigate the risk of data leakage you need to ensure you have appropriate measures to PROACTIVELY track and alert when users are deleting, creating, copying, moving or modifying files and folders. How quickly could you answer these questions? Quick enough?

Question	Time taken with Lepide	Time taken with Native Auditing	How long would it take you?
Someone has deleted a critical file. Who did it and when did they do it?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 15 mins. manual log correlation	
A folder was renamed, the moved to another subfolder then copied? Who did it, when did they do it? What did they rename it from?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 15 mins. manual log correlation	

How do maintain identity management integrity and security?

A key part of maintaining a secure environment is ensuring you have a tight identity management policy in place. Achieving this requires both the initial configuration of your environment and continuous and proactive monitoring to ensuring it remains in the intended state. You need to track if changes are made to your password polices, identify users that aren't adhering to password procedures and keep your environment free from inactive or dormant user accounts. It is also critical you proactively check issues such as privileged password sharing or persistent account lockout issues to help prevent the risks of privilege compromise or abuse. How proactive is your current approach to these risks?

Question	Time taken with Lepide	Time taken with Native Auditing	How long would it take you?
How quickly would be able to identify account lockout issues?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 20 mins. reactive only	
How quickly would be able to identify a change made to a password policy?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 20 mins. reactive only	
How quickly would you be able to identify if a privileged account was being shared?	< 5 secs. real time alert < 1 min. detailed report	No real time alert > 20 mins. reactive only	
How quickly can you identify inactive users?	< 1 min. detailed report	> 20 mins. reactive only	

Contact Details

Product Experts

USA/Canada: +1-800-814-0578
UK/Europe: +44 (0)-845-594-3766
Rest of the World: +91 (0)-991-004-9028

sales@lepide.com

Technical Gurus

USA/Canada: +1-800-814-0578
UK/Europe: +44 (0)-800-088-5478
Rest of the World: +91 (0)-991-085-4291

support@lepide.com

Lepide