Auditing complex file operations

ANSWERING TODAY'S COMPLIANCE CHALLENGES THROUGH ADVANCED FILE MONITORING TECHNOLOGY

Security-sensitive data needs to be protected, in order to prevent, identify and investigate data breaches. Nowadays, as companies rely more and more on IT systems for storing and processing such information, and with the escalation of cybercrime and the security risks associated with managing such data, this need becomes a vital necessity enforced by laws, regulations and security standards. This enforcement requires companies to implement processes designed to protect data, identify data breaches and deliver accountability for security incidents threatening data protection. Since data resides in files, an important part of these processes involve creation and enforcement of corporate policies that regulate and monitor access to files.

Data protection regulations and security standards are of paramount importance, because losing security-sensitive data in an electronic environment is as dangerous, or even more dangerous, than losing an ID card or a credit card on a sidewalk. When data breaches occur, there are usually multiple records being lost, putting a large number of persons at risk. Personally identifiable information, healthcare records, financial records, credit card information, and other types of security-sensitive information can be used by cybercriminals to commit felonies from behind their desktops, causing damage to many victims, with relatively lower risk and significantly higher benefits than your average street felon.

Companies who manipulate such data in IT environments must be responsible for protecting it, and regulatory compliance enforces minimum controls designed to protect the data, identify data breaches, and deliver accountability for the related security incidents.

Upon closer examination of the most important data protection regulations and standards, we are able to observe a common pattern around most requirements, especially those regarding how access to data should be performed and audited. Data, stored in files or databases, is at the core of all these acts, and its protection is their ultimate goal. At the same time, access to this data is strictly regulated and auditing requirements are there to make sure that the requirements are met.

Common requirements where advanced file monitoring technology makes a difference

Principle of least privilege: Access to security-sensitive data should be granted on need-to-know basis

PCI DSS Requirement 7;
HIPAA Privacy Rule;
SOX section 404;
J-SOX privacy safeguards;
EU Data Protection Directive (Legitimate purpose)
Italy's Garanteprivacy art. 154
ISO/IEC 27001:2013, Section A.9

US Federal Information Security Management Act (NIST SP 800-53 AR 4 Privacy monitoring and auditing);
US Department of Defense Instruction 8500.2, ECAN-1;
Singapore Personal Data Protection Act, the protection obligation;
Australia Privacy Act - Privacy Principle 11

Challenge	How can advanced file monitoring solutions help?
Restricting access data relies on authentication and access management features in the operating systems. Once the necessary access is established and implemented for all users, companies need to continuously monitor the effectiveness of the implementation and make sure that there are no policy breaches.	Advanced file monitoring solutions deliver alerting on data movement and reviewable information on data access, which allows compliance and security managers to: - Confirm access to files is <u>really</u> used on a need to know basis; - React when data travels to unsafe locations, where it can be accessed by unauthorized users;

Example showing the value of advanced file monitoring technology

Bob is an accountant and has access by business need-to-know to the list of POS transactions and their details. This access is regulated via NTFS and share permissions on the file server. Bob has read-only access to that folder. Bob carelessly copies the file containing the transactions to his local machine, in a folder that he shared with fellow employees who should not have access to the POS transactions log. This requirement is no longer fulfilled.

System logs and basic file monitoring solutions	Advanced file monitoring solutions
Monitoring the use of authentication mechanisms and the object access events will only show that: - Bob logged onto the file server; - Bob read a file he is supposed to read every day. There will be no trace of the obvious breach of the principle of least privilege.	Advanced file monitoring solutions would: - Log that Bob has accessed a file on the file server; - Log and alert that Bob has copied that file to his local machine, including the destination folder; - Log all subsequent access to that file on Bob's machine.

Common requirements where advanced file monitoring technology makes a difference

Data access auditing: All access to security sensitive data needs to be audited

Challenge	How can advanced file monitoring solutions help?
Security-sensitive information resides in files or databases, and simply using the system audit trail to identify logons to computers holding such information is not enough in many cases. - Logging onto a computer, does not mean that cardholder information was accessed. - Multiple users may use the same computer system and, based on logons alone, it is impossible to tell who really accessed cardholder information, and in what way. This means that using logons only makes it difficult or impossible to provide accountability for actions that put cardholder information in danger, or lead to data breaches.	Advanced file monitoring technology goes beyond monitoring logons, and take a look at who access data and in what way. Such technology can make the difference between: - Someone who read a file on the screen; - Someone who read a file to copy it to USB, network location, cloud-sync folder, etc. - Someone who modified a file; - Someone who renamed or archived a file; The audit trail generated by such a solution delivers accurate information, narrowed down to the scope of this requirement.

Example showing the value of advanced file monitoring technology

Jane and Peter work on the main accounting server every day. They both logon either interactively or via the network. Both work with files containing cardholder information as part of their job. On a certain date, both users logon to the machine. Jane logs on interactively, opens a document containing cardholder information and clicks on "Enable editing" when prompted. Then, she realizes that she opened the wrong file, so she closes it. Peter logs on via the networks and accesses the same file. He makes some edits and then uploads it via the browser to a cloud storage website.

System logs and basic file monitoring solutions	Advanced file monitoring solutions
Monitoring the use of authentication mechanisms and object access events will: - Identify that Jane logged on interactively; - Record an object access event for the file, with WRITE access for Jane (which signals her intention to edit a document, but not the actual editing) - Identify that Peter has logged on via the network; - Record and object access event with WRITE access for Peter signaling his intention to write to that file. Although Jane has not written anything in the file, she is listed as writing to that file, just as Peter. Then, there will be no indication about the fact that Peter has taken the file out of the premises. Not all access is audited in this case, leading to a breach of this requirement.	Advanced file monitoring solutions would: - Log a read event for Jane when she opened the file; - Log a read event for Peter when he opened the file; - Log a write event for Peter as he edited the document - Log and alert on the fact that the file had left the premises The audit trail is able to reconstruct **all** access to data instead of access to a machine, as well as identify the exact type of access which occurred.

Common requirements where advanced file monitoring technology makes a difference

Privileged user monitoring: All actions of privileged users need to be audited

Challenge	How can advanced file monitoring solutions help?
All actions taken by privileged users also refers to privileged access to data, as well as changes to file security (ACL), file attributes or moving files around. Advanced file monitoring solutions can track privileged access to files as well as administrative actions taken on files, such as access granted to user accounts, movement of files to locations with different security settings, etc.	Advanced file monitoring solutions can identify file related activity of users with administrative privileges and tag it appropriately. This helps during the review process to make sure that - File access privileges were not abused; - File access privileges were not misused;

Common challenges when meeting data access auditing requirements for compliance

Security sensitive data is stored in files, and moves across local networks and the internet. At the same time, manipulating such information is required as part of everyday activities. All these make protecting the data very challenging. When implementing data access monitoring procedures for regulatory compliance, companies use software solutions designed to audit basic file operations such as read, write and attributes changed. However these solutions do not cover for advanced file operations such as file copy or file archived, even though these operations are commonly used as part of security incidents leading to data loss. There is a big difference between someone reading a file to output to screen, and reading a file in order to copy to an unsecure location. Although such solutions are considered appropriate in the industry, they do not answer critical questions when it comes to providing accountability for incidents, or drawing the line between business-required use, and policy violations or privilege abuse. Since data is not static, it is also important to track how data moves, particularly when it holds security-sensitive information.

In environments where impersonated access is used to manipulate files, or when multiple users access the same resources, it is often impossible to understand where the risk lies, where the policy breach is or who is responsible. Hence, in such cases, investigations last longer and cost more, as well as the penalties, if data breaches occur.

Major regulations and standards

There are many security frameworks, regulations and standards that have data protection at core. The below list only contains the most important ones:

Major regulations and standards

Standard/ regulation	Relevant requirements for file monitoring
PCI DSS (The Payment Card Industry Data Security Standard) The PCI DSS is a security standard aimed at protecting the cardholder information and is targeted at merchants who process electronic payment transactions. PCI DSS requires implementation of a continuous process, consisting of training employees, deploying security solutions, monitoring the state of compliance and performing internal and external audits	Requirement 7: Restrict access to cardholder data by business need to know Requirement 10.2.1 Implement automated audit trails for all system components to reconstruct the following events: All individual access to cardholder information Requirement 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) Requirement 11.5 deploy a change-detection mechanism (for example, file -integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; File related activity: Requirement 10.2.2 Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges - we identify access to files and flag users who have administrative privileges. Enforcement: Requirement 12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.
HIPAA (Health Insurance Portability and Accountability Act) HIPAA is a law enacted by the US Congress and enforces a national standard for handling electronic healthcare transactions. One of the important goals of HIPAA is to protect electronic protected health information (ePHI) Further defined as guidelines by NIST SP800-66	Title II: Preventing Health Care Fraud and Abuse Privacy rule: Regulates the proper ways of accessing and disclosing ePHI. Administrative requirements enforce implementation of data protection policies; Security rule: The goals of the Security rule are to protect against any reasonably anticipated threats and hazards to the security or integrity of ePHI; and protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

Major regulations and standards	
SOX (Sarbanes–Oxley Act) SOX is an United States Federal Law meant to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures. Similar regulations were issued in Canada, Germany, India, Australia, France, Japan, Italy, South Africa, Israel and Turkey.	Section 302 requires implementation of disclosure controls that regulate how information is disclosed. Section 404 requires implementation and assessment of internal controls meant to protect information.
GLBA (Gramm-Leach-Bliley Act) Enacted by the US Congress, GLBA regulates how financial institutions and companies deal with private information	The Financial Privacy Rule: requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The Safeguards Rule: requires that financial institutions implement security programs to protect the private information.

Conclusion

Monitoring file activity is vital for data protection and compliance, but at the same time, it is a challenging task. Analyzing logs or monitoring basic file operations does not deliver true insight into what is happening with your files. Employee education is a good starting point and is always helpful in reducing the data loss risks, however, corporate data protection policies need to be

enforced by proper monitoring processes in order to be effective. Advanced file monitoring technology can deliver functionality like:

- *Accurately report on basic and complex file operations;*
- *Deliver accountability for file operations;*
- *Detect impersonated file access and the activity of users with administrative privileges;*
- *Identify file misuse that can lead to policy breaches or non-compliance*
- *Detect suspicious file activity*
- *Filterable statistical trends for file activity;*
- *Real-time alerting and advanced reporting;*

Such functionality can make the difference in preventing or investigating data loss incidents and can also integrate with existing SIEM solutions, in order to maintain single-point of reporting for compliance and data security processes.

TEMASOFT FileMonitor

About TEMASOFT FileMonitor

TEMASOFT FileMonitor is a real-time file access monitoring and change detection tool that delivers unique functionality. It relies on advanced technology built around a file system driver that performs low-level detection of file activity, and an in-memory correlation engine that looks at how data is manipulated by various processes. All these allow TEMASOFT FileMonitor to deliver accurate detection of complex file operations and all the corresponding information about who, when, where and how. For more information, please visit www.filemonitor.net

About TEMASOFT

TEMASOFT is a provider of network security solutions with over 15years experience in the field. TEMASOFT is a Microsoft Gold ISV Partner since 2006.
For more information, please visit www.temasoft.com