Privileged User Monitoring for SOX Compliance

Failed login, 6:45 a.m.
Privilege escalation, 12:28 p.m.
Financial data access, 5:48 p.m.
Financial data breach, 11:32 p.m.

Know what's happening to all your critical data. When and where it happens.
Privileged User Monitoring for SOX Compliance

Many enterprises are facing the SOX compliance challenge of monitoring all of the data activity of their most privileged users. This paper highlights several of these challenges and how they can be addressed by a comprehensive database activity auditing solution.

Sarbanes-Oxley (SOX) IT controls address the integrity of databases that store sensitive financial and business information. In particular, new SOX requirements have shifted the focus from merely understanding who has access to information to continuous monitoring of database activity. These requirements target high risk database activities—privileged user behavior, direct access to sensitive data stores, user privilege escalation, failed login and failed database operations, and so on. Finally, while database applications like DB2, Oracle, SQL Server, and Sybase rightly attract most of the attention, the problem invariably extends to other sensitive data stores—file server-resident financial, legal, strategic, and spreadsheet documents being the foremost examples.

SOX Section 404 demands that companies (a) evaluate the adequacy of internal controls as they relate to financial reporting, (b) institute new controls as necessary, and (c) perform and report an assessment of these controls on an annual basis. In short, Section 404 says, "Management must ensure that appropriate internal controls for financial reporting are in place." Furthermore, Section 404 requires not only that corporate and IT officers immediately put in place internal controls to protect the integrity of financial data (and, by implication, all systems that access that data), but also that the organization must be able to demonstrate that appropriate controls are in place.

At first glance it is quite obvious that the full access credentials accorded to DBAs and system administrators creates a significant vulnerability for an enterprise’s data simply because these privileged users have access to all or a significant fraction of your data.

However, privileged users are normally highly valued and trusted individuals who are indispensable to the day-to-day workings of your data environment, and they generally do not respond well to being told by an IT auditor that they are a threat that must be monitored. In reality, with most enterprises working to enforce segregation of duties, most DBAs and System Administrators expect their activity to be monitored and have no issue with this simply because they don’t intend to do anything wrong. The problem with this approach is that it is of critical importance for DBAs to have access to database log facilities, so curtailing their privileges effectively curtails their productivity and makes their job more difficult.

This is precisely the challenge that enterprises are facing with the SOX section 404 mandate to monitor the activity, particularly database activity, of their DBAs and other privileged users. The problem arises because it makes no sense to monitor a DBA with full privileges by using the log facilities within the database applications, because their privileges will allow them to cover their tracks by deleting or otherwise altering the logs. So many enterprises are resorting to curtailing their DBAs’ privileges to prevent them from having any access to the log facilities. The problem with this approach is that DBAs use the database log facilities as a debug tool in order to do their job, so curtailing their privileges effectively curtails their productivity and makes their job more difficult.

Corporate officers, IT auditors, and database administrators find a variety of challenges in the requirement to audit all privileged user activity, which typically ranges over a variety of platforms, applications, and data stores. This paper provides detailed analysis of a number of the issues associated with privileged user monitoring.

SOX-Mandated Database Activity Monitoring

From a data administrator’s viewpoint, SOX-related monitoring requirements are quite broad, but they can be distilled under five key headings:
Monitoring database access by privileged users—DBAs and system administrators, for example

As the title of this paper implies, privileged user monitoring is the primary objective of most SOX database auditing projects. Additional requirements generally relate to specific activities initiated by privileged users or, potentially, users masquerading as privileged users for malicious purposes.

Enterprises must audit all activity by administrators and other privileged user IDs, and, perhaps more importantly, must be able to retrieve, examine, analyze, and report on this piece of the audit trail.

Enterprises working to comply with this requirement have found that in practice it can be difficult to implement due to a variety of problems:

- The very users they are monitoring typically have full administrator credentials and can cover their tracks by modifying or deleting the logs being used to monitor them.
- Privileged user credentials can be restricted to prevent log access, but this results in lowered productivity or creates an adversarial relationship with unhappy DBAs.
- Many enterprises employ databases from several different database vendors, which require individual expertise on each database’s log capabilities and makes log consolidation into useful reports a near impossibility.

A comprehensive database activity auditing solution must address all of these problems.

Monitoring changes in privileges

Not all users utilize privileged credentials all the time. Many times users will use privileged credentials on an as-needed basis to perform specific tasks. It is imperative to track when these privilege escalation events occur and maintain and regularly view reports of this activity in order to verify the legitimacy of these events.

In order to attest to the integrity of sensitive data, it is imperative to know what is happening in the user community. Have new users been defined, or an existing user de-provisioned? Have a user’s privileges been escalated or revoked? A complete database activity auditing solution will provide the necessary visibility in to these types of transactions without requiring auditors to search through seemingly endless database log files.

Monitoring access failures

Enterprises must know when login attempts fail, and also when data access attempts are unsuccessful. Failed access events are an indication that something is not right. Application data access attempts, in particular, should never fail.

There are various definitions of invalid logical access attempts. These two are most common:

- unsuccessful attempt to access a resource
- invalid or failed login

An effective database activity monitoring solution must be capable of capturing both classes of failed access operation.

Monitoring schema changes

To ensure data integrity, you must be able to track changes to compliance-related data structures. Monitoring, logging, and reporting on data structure changes not only permits you to satisfy routine auditing requirements, but also to identify anomalous, unscheduled activity.

Monitoring direct data access

Another common requirement is to track any direct access to sensitive system and data tables. Since direct access operations are uncommon in procedural applications, it is important to capture an audit trail of such activities. Alternative tracking techniques, including triggers and local agents, are expensive and do not scale.

Furthermore, a complete database activity auditing solution will capture the necessary detail in the audit trail to not only show that a direct SQL event occurred, but also who initiated the event (what user ID), what source IP address originated the event, and precisely what content was affected by the event (database, tables, columns, and rows).
In fact, an ideal database activity auditing solution will permit the exact reconstruction of any SQL transaction associated with any of the events stored in its audit trail repository.

**Additional Key SOX Activity Auditing Challenges**

Database managers, auditors, and security officers bear the burden of satisfying regulatory and internal audit demands for SOX compliance. Numerous trouble spots persist, in addition to privileged user monitoring. Key challenges include:

- **Consistent monitoring across all databases** – Large enterprises often deploy database products from multiple vendors—DB2, Oracle, SQL Server, Sybase, and so on. Until recently, monitoring access activity across varied databases in a consistent, comprehensive, and normalized way has been effectively impossible. Failed response codes, for example, differ from one product to another, or even from version to version.

- **Inadequate database logs, resulting in non-compliance** – Both native logging (database and/or server) and log consolidation tools—ignoring their well-documented performance penalties—invariably fall short of SOX auditing requirements. These solutions yield paradoxical results: both log data overload and de facto non-compliance, the worst of all worlds.

- **Inadequate data management and reporting** – SOX compliance includes the demonstrable, repeatable ability to reconstruct event flows by finding and extracting one or more critical events from the current or archived audit trail. Writing filtering tools for this purpose is very difficult. Furthermore, identifying the key events is just the first of many tasks, which may include storing such events for rapid on-line examination (typically for 60-90 days), generating scheduled reports for auditors and other stakeholders, supporting audit trail search operations, and certifying audit log security.

- **Inadequate analytics and alerting** – The spirit of SOX adherence also includes identifying and tracking access events that signal potential fraud or other data misuse. For example, it may be necessary to detect and alert on out-lie r events such as N-time failed logins, large return sets, or statistically rare data access operations. Alerts may also require integration with other security event management tools. Today’s database tools lack the analytics to support a meaningful alert detection and response system.

- **Segregation of duties requirement** – A special challenge arises when collecting and maintaining audit trail and report data on privileged users (DBAs, for example)—data that is typically stored on systems managed by these same privileged users. Native database logging and agent-based solutions exhibit this deficiency, which stands in direct violation of both SOX and common sense. The segregation of duties standard dictates that privileged user monitoring data be stored outside the control of the user or users being monitored.

**Intelligent Database Activity Auditing for the Enterprise**

Fortunately there is an approach that can enable your organization to build comprehensive and secure database activity audit trails and reports, while allowing your users to maintain their current privilege levels. Database auditing appliances like Tizor Mantra™ are powerful tools for Privileged User Monitoring and Audit (PUMA) initiatives and provide the necessary visibility into privileged user database activity without requiring DBA credentials to be restricted. A dedicated database activity auditing appliance will enable you to monitor and build detailed compliance reports for:

- All privileged user database activity
- Privilege escalation events
- Failed logins and other logical database access failures
- Database schema changes
- Direct SQL access events
Additionally, a dedicated high-performance database auditing appliance will transparently build an activity audit trail without impacting the performance of your applications and without the performance penalty associated with turning on the native fine-grained logging facilities within the database applications themselves.

The most effective database activity auditing solutions do not sit in-line with the database traffic. Instead, they passively monitor all database activity by utilizing a mirror or SPAN port off of an Ethernet switch or by utilizing a regenerative tap to capture the traffic directly from the Ethernet segment that it travels on. Figure 1 illustrates passive network deployment:

**Figure 1: Mantra and the Corporate Data Infrastructure**

There are several important benefits of this approach:

- Requires no changes to your databases or application environment.
- Enables enterprises to implement true segregation of duties by providing granular privileged user monitoring and creating a secure audit trail without forcing you to restrict the credentials of your DBAs.
- Simultaneously monitors multiple heterogeneous database platforms and generates unified activity audit reports for your entire data environment.
- Dedicated high-performance network appliance hardware scales to meet the database activity auditing needs of even the largest global data centers

In order to provide full coverage for all database traffic, the database auditing appliance must also be able to perform *local auditing*, whereby the appliance is able to monitor local console activity initiated directly on the database server itself.

Furthermore, as indicated in the diagram above, SOX compliance is not restricted to database environments. A complete SOX activity auditing solution will also be able to monitor data activity on file servers and mainframe environments.

**How does a database activity auditing appliance meet these requirements?**

There are several functions that an appropriate database activity auditing solution must perform in order to satisfy the requirements of SOX section 404. In the following sections each of these functions will be discussed and recommendations of how to integrate this capability into your organization will be provided.
Mantra™ SOX Activity Auditing Solution

Tizor has developed Mantra, a high-performance appliance for data auditing and protection that meets the challenges of SOX 404 data activity auditing and enables the most comprehensive data center coverage. Mantra’s scalable architecture ensures that any enterprise can benefit from real-time auditing of activity without the burden of host-based logging—all with a single management console and sophisticated enterprise architecture that can scale from the smallest to the largest data center without impacting deployed applications.

Furthermore, Mantra offers the only SOX data activity auditing solution to enable enterprises to manage and evaluate their corporate compliance posture for ALL of their critical data—whether it resides on databases, file servers, or mainframe applications.

Mantra SOX Activity Reports

Figure 2 shows a sample Mantra SOX Audit Activity Summary report. It summarizes the audited privileged user activity on production databases, including any alerts:

Figure 2: Mantra SOX Activity Auditing Summary Report
Recording detailed audit data is not enough to satisfy the requirements of SOX section 404. You must be able to find, consolidate, present, and distribute audit trail data in order to (a) prove that controls are actually in place, and (b) reconstruct access event history quickly and efficiently as part of an emergency or precautionary forensic investigation.

The Mantra SOX Activity Auditing solution offers an easy, transparent, fully packaged solution for SOX activity monitoring requirements. Its key advantages include:

- Policy-based capture of targeted privileged database activity, without requiring agents or relying on application logs. Comprehensive audit trail logs to satisfy SOX or internal audit requirements are automatically created, stored, and managed.
- Rich reporting designed to match auditors’ requirements to demonstrate SOX data activity monitoring controls.
- Automated analysis that can review activity logs on a real-time basis to help detect, alert, and stop data theft from data servers.

To help you get started, Mantra gives you the tools to test, assess, and evaluate existing policies and controls, helping you quickly identify the holes in current auditing systems.

**Mantra SOX Activity Policies**

A primary Tizor design objective is to provide a monitoring environment in which a small, definitive set of policies satisfies a substantial regulatory or contractual requirement. As we proceed, take note of the remarkable range of SOX auditing requirements that can be covered with just five well-designed policies.

The following screen capture from the Tizor Management Center policy configuration window shows the five policies used to achieve the database auditing objectives outlined in the earlier portion of this paper.

*Figure 3: SOX Compliance Policy Set*

Note that these fully functional policies ship preconfigured with each Mantra appliance.

<table>
<thead>
<tr>
<th>Policy #1</th>
<th>Audit Privileged User Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Audit all access activity by privileged users. (May require adjustment to match local privileged user IDs.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy #2</th>
<th>Audit Changes to User Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Audit any change to database user privileges.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy #3</th>
<th>Audit Failed Logins Attempts and Failed Access Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Audit invalid logical access attempts directed at any monitored data server.</td>
</tr>
</tbody>
</table>
Mantra™ SOX Activity Auditing Solution

Mantra SOX Policy-Based Activity Reporting

Mantra includes a powerful reporting facility that provides a clear picture of the overall compliance posture of any enterprise data environment.

Mantra’s reports and policies, are “technology agnostic.” This approach allows straightforward policies to capture activity across different databases (DB2, Oracle, SQL Server, and Sybase) and across different server types storing both structured and unstructured file data. As a result, Mantra’s reports provide a unified view of data access activity spanning all monitored data stores.

Figure 4: Policy Report: Privileged User Activity

The policy report in Figure 4 summarizes access activity captured by the PrivilegedUserActivity policy during the current month, including breakdowns by the data assets touched and the SQL operations performed.
Summary

At the core of SOX regulations and compliance frameworks is a deceptively simple three-part requirement that companies (a) track access to sensitive financial data, (b) report on their controls in a comprehensive way, and (c) behave responsibly when something goes wrong. A careful reading of virtually any information protection regulation reveals that if appropriate auditing technologies are applied, the underlying requirements of the regulation will be met. A simple rule of thumb for adequate auditing is to track “the five W’s”: who did what (read, write, SELECT,...), to which data asset, when, and from where.

Tizor’s Mantra SOX Activity Auditing solution provides a complete packaged solution to the problem of monitoring and auditing privileged user activity in databases—a fundamental SOX requirement. The Mantra auditing and alerting platform is policy-based and captures only targeted activities without impacting the performance of production databases and applications. Mantra also provides an enterprise-level solution that encompasses a variety of database products and versions (including DB2, Oracle, SQL Server, and Sybase) using a single interface and a consistent set of auditing, reporting, and analytic tools. Mantra can substantially automate SOX auditing demands, minimizing the costs and operational difficulties previously associated with achieving compliance.

Mantra’s distinctive benefits include:

- **Transparent implementation** – Non-intrusive, network deployment.
- **Single, enterprise-wide solution** – A single investment covers multiple regulations and multiple data asset types.
- **Policy templates and English-like policy definition language** – SOX policy sets and templates that can be quickly customized for your site.
- **Intelligent analytics** – Behavioral Fingerprinting® technology detects anomalous user activity in real time, helping you detect and stop non-compliant activity directed at critical data stores.
- **Rich reporting** – Provides a wide variety of summary and detail reports, greatly simplifying the tasks of (a) demonstrating compliance, and (b) sharing information with diverse stakeholders—officers, auditors, assessors, and administrators.

Tizor Mantra is the most complete, easy-to-deploy, and cost-effective SOX activity auditing solution on the market today.

About Tizor

Tizor is the leading provider of data auditing and security solutions for the data center. Tizor’s Mantra data security appliances are the industry’s first enterprise solutions capable of monitoring critical data activity across databases, file servers, and mainframe applications. Mantra solutions enable the highest level of compliance assurance, data security and privacy by providing a complete life-cycle of intelligent data auditing capabilities including audit reporting, theft detection, alerting, and data protection. Founded by former Bell Labs researchers and headquartered in Maynard, Massachusetts, Tizor is venture financed and led by industry veterans in networking, security, and software and systems management. More information on Tizor can be found at www.tizor.com.

© 2006 Tizor