

Lumigent® Entegra™

Data Auditing for Risk Management



The Need For Data Auditing

Enterprises have never been more dependent on their data. For most, data is the lifeblood of the organization. When data is compromised, business is at risk. Consequences of improper data use include, but are not limited to, damage to brand and reputation, loss of value in stock purchase price, customer attrition, fines, even lawsuits.

Enterprises that manage the inherent risks associated with the access and use of data mitigate their exposure for business loss and assure data integrity.

Demands for accountability

More accountability to assure the integrity, security, and privacy of data is demanded by stakeholders including customers, partners, auditors, and regulators. Demonstrating accountability has become a boardroom issue for corporations, the burden of which is reaching beyond the offices of the CEO and CFO to the CIO and the IT organization as a whole.

Regulatory compliance

Sarbanes-Oxley, 21CFR11, HIPAA, Basel II, and other regulations don't mandate specific technology requirements, but they do have broad implications for IT as most, if not all, critical business information resides in databases. These databases require control and monitoring as they store the organization's most sensitive data.

Human error and fraud

By many accounts the source of 70% of data corruption comes from internal users as a result of human error or intentional fraud. Consider the following scenarios. An employee keys an incorrect selling price into the database that feeds the price list of a national retailer. The incorrect price is published before the error is discovered and, as a result, the company must honor the advertised price. In scenario two, an employee steals money from her employer by setting up a fictitious employee ID and payroll, which deposits directly into her own bank account. The consequences of either scenario can be dire - and very public. Data misuse, loss, or corruption from human error or fraud can be a disastrous event resulting in financial losses, damage to reputation, even lost customers.

Existing security measures and policies

Investments in IT security have largely been focused on preventive security measures such as firewalls and intrusion detection or application controls. Without auditing at the data level there can be no certainty that these controls are effective and working as intended. In addition, these measures have no ability to monitor internal users who have privileged and direct access to the database.

It is the comprehensive, continuous audit trail that mitigates the business risks associated with data use, and meets the challenges associated with regulatory compliance by employing best practices for management of data.

Privileged users

Most organizations have numerous preventive controls associated with the use of applications that drive data. But, once information is in the database, it is subject to additional changes—authorized and otherwise. Privileged users, such as DBAs, developers, even managers, have ongoing and direct access to sensitive data, making it imperative to implement monitoring controls at the database level.

It is clear, that with so many threats to the organization and its data, combined with added pressures for compliance and accountability, organizations can no longer operate without an effective system to monitor and audit the access and use of data. It is the comprehensive, continuous audit trail that mitigates the business risks associated with data use, and meets the challenges associated with regulatory compliance by employing best practices for management of data.

Lumigent Entegra — Data Auditing for Risk Management

Entegra is an enterprise database auditing solution that is essential to an organization's ability to mitigate the inherent risks associated with data use and regulatory compliance. By continuously monitoring and reporting database activity, Entegra provides a permanent record of who did what to which data, when.

Built for data auditing

Entegra is architected specifically for data auditing. Entegra unlocks the rich data found in the transaction or redo logs and augments it with other information from the database to build a complete picture of database activity. This approach to data auditing is superior to others as it provides the only true record of database activity to meet demands for integrity and accountability. In contrast, native tools and other approaches only capture a “snapshot” of transaction history, leaving the validity of audit information open for question.

Ensures data integrity with an unimpeachable audit trail

Entegra provides continuous monitoring and auditing of data use—including before and after values of data changes, which are critical to assessment and correction. By capturing this permanent, unimpeachable audit trail of database activity, executives can confidently attest to data integrity. This is especially important given the personal accountability of CEOs and CFOs in the current regulatory environment.

No “backdoors”

A major vulnerability and area of risk comes from internal users with direct or privileged access to the database. DBAs, developers, and other IT staff members can make changes directly to the database, bypassing preventive measures such as application and access controls that may be in place. In addition, other internal users, such as senior managers, may have privileged access that allows them to bypass controls that apply to other users. While it is tempting to “trust your employees”, the current regulatory environment and best operational practices dictate that all access to critical data systems must be audited in order to validate claims of data integrity. And, in the event of suspected wrongdoing, organizations now have proof beyond circumstantial evidence and employees are protected from false accusations.

Mitigates risk with alerts of key activity

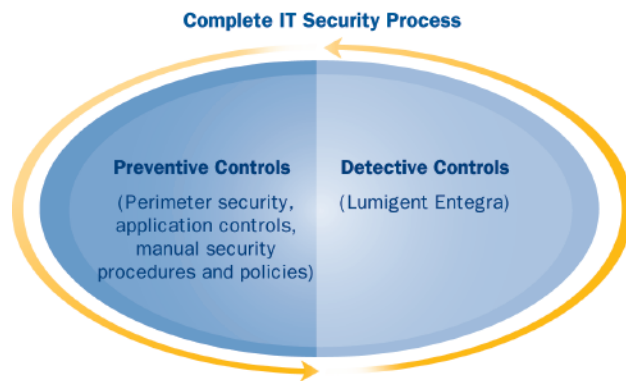
Human error is one of the biggest risks to data integrity and may go undetected until the damage is done. And, most fraud is perpetuated for months before it is realized. With Entegra’s alert capability, organizations can mitigate these risks by being aware of key events when they occur. Further, once fraudulent activity is identified, the organization has a complete history of what happened in order to assess and repair the damage, quickly.

Architected for performance

Chief among a DBA’s concerns is database performance optimization because of the business implications of poor system performance which range from lost productivity to lost customers. Recognizing this, Entegra was architected with performance in mind. Relative to native tools and traditional auditing methods, Entegra mitigates performance impact to production systems by using the database logs in combination with low impact agents to collect audit data.

Strengthens security measures — ensuring preventive controls work

Prevention of data misuse, intentional or otherwise, is critical. Security investments continue to be one of the fastest growing components of IT budgets. These measures include perimeter security (such as firewalls and intrusion detection) and application controls. These *preventive controls* are important and necessary but without *detective controls* to monitor their effectiveness, the organization is left vulnerable. Entegra augments security measures to form a complete IT security framework — thereby strengthening your total security investment. By monitoring activity at the source — the database — Entegra helps assure security measures are working as intended.



Derives business value from audit data — reporting & analysis

Having a comprehensive record of database activity is critical, but by itself does not provide the organization with the true value of an enterprise data auditing system. The data that Entegra captures from all audited databases is consolidated and stored in one or more centralized repositories. A rich reporting system, which enables the management, scheduling, and viewing of reports, gives management and administrators the ability to query and share information about collected data. A set of more than 30 insightful reports are included.

24x7 service

With Entegra, you benefit from a team of leading professionals skilled in assessment, implementation, and maintenance. With experience helping organizations solve the most critical data management challenges, our team has the know-how to help facilitate the most complex data auditing challenges.

Native Tools & Other Approaches

Organizations must consider several requirements when evaluating enterprise auditing solutions. While native database tools and traditional methods (i.e. triggers and application modification) have been available for several years, they fall short of today's requirements for enterprise data auditing. Simply put, they are not scalable to the enterprise, are unmanageable, and are not reliable. They impair database performance, produce a false sense of security by failing to capture all database activity, are costly and difficult to maintain, and fail to meet basic principles of auditing best practices such as segregation of duties.

Comparison of Approaches to Data Auditing

	ENTEGRA	NATIVE DATABASE TOOLS	TRIGGERS	APPLICATION MODIFICATION	NETWORK SNIFFER-BASED AUDITING
Unimpeachable audit trail	✓				
Audits privileged users	✓				
Built-in segregation of duties	✓				
Central repository with consolidated audit data	✓				
Scalable architecture	✓				
Schedulable, automated reporting	✓				

Summary

The risks associated with the use of data, combined with today's regulatory environment, require organizations to employ a continuous data monitoring and auditing system. The business risks (and personal exposure for senior executives) are simply too great to rely on preventive security measures or incomplete technical solutions that leave the organization vulnerable.

Entegra is built for data auditing. Entegra's unique, log-reading technology offers a superior approach to data auditing, providing organizations with an unimpeachable audit record. Entegra extends beyond collecting audit data to deliver business value through its reporting capabilities that leverage an information-rich, centralized repository of audit data. Entegra meets the requirements of enterprises that need a single cross-platform solution that provides a rich, enterprise-class auditing capability with minimal performance overhead on critical production systems. And, with Entegra comes the experience of professionals skilled in delivering comprehensive data auditing solutions that meet the most critical demands for data integrity and accountability.

Lumigent Technologies, Inc. is the leader in enterprise data auditing solutions for organizations that need to reduce risk associated with regulatory compliance and the use of corporate data assets.

LUMIGENT

Lumigent Technologies, Inc.

289 Great Road
Acton, MA 01720 USA

Toll Free 1 866-LUMIGENT
1 866-586-4436

Phone 1 978-206-3700

E-mail info@lumigent.com

www.lumigent.com

Copyright © 2004 Lumigent Technologies, Inc. All rights reserved. Lumigent, the Lumigent logo and Entegra are registered trademarks or trademarks of Lumigent Technologies, Inc. All other names and marks are property of their respective owners.