

Meeting Compliance Requirements in a Competitive Marketplace

As more and more high-profile cases of corporate insider fraud come to light, there is an increased awareness of the internal threat to corporate assets coming from company employees and management - as opposed to malicious outsiders. Most companies and public service organizations are exposed to the very real threat posed by insiders who have authorized access to and are capable of manipulating internal systems for personal gain. In response, governments worldwide have enacted new regulations with the foremost intention of protecting the customers and shareholders who place their trust in the organizations serving and representing them. While beneficial, these regulations pose significant technical challenges for organizations as most of their systems were developed and deployed before these regulations were enacted.

Privacy Regulations- PCI, HIPAA & GLBA: The Audit Trail Challenge

The Payment Card Industry Data Security Standard (PCI DSS) requires organizations that deal with credit card transactions to "Implement automated audit trails for all system components to reconstruct all individual user accesses to cardholder data." The Gramm-Leach-Bliley Act (GLBA) makes similar requirements regarding tracking access to financial information and the HIPAA Security Rule poses similar requirements regarding electronic protected health information.

The requirement to maintain a detailed audit trail is challenging for organizations that rely on both legacy and modern systems. Unlike network devices and infrastructure systems, there is typically no detailed user access logging mechanism in most applications. Developing such a mechanism involves tremendous effort and cost, potentially altering thousands of programs. Mechanisms that track changes to corporate databases are not sufficient, as they track update and alteration of data but do not capture critical "read-only" access to data.

Sarbanes-Oxley Act: The Activity Monitoring Challenge

The Sarbanes-Oxley Act requires executives and auditors of publicly traded companies to validate the accuracy and integrity of their financial reporting. Section 404 of the act requires companies to create and maintain effective internal controls for tracking financial processes. As financial reporting relies on information collection from various systems and resources, (purchasing, payroll, inventory, human resources, etc.), compliance with section 404 requires development of effective controls cross-platform. This is challenging, as systems developed prior to the Sarbanes-Oxley Act typically do not have sufficient logging or control mechanisms. Database Trace Monitoring solutions provide limited visibility into user actions, tracking changes to the database but not to end-user actions, such as accessed screens. In addition, user queries cannot be traced with this type of solution, missing out on potential fraud attempts.

Basel II Accord: The Insider Threat Challenge

The Basel II Accord introduces the requirement of banks to manage operational risk as part of their overall risk management. According to Basel II, the risk the bank is exposed to affects its capital requirements. Operational risk is defined as the "direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events." The accord lists several types of operational risk including Internal Fraud, External Fraud and Business disruption and system failures. Most of the existing solutions for fraud detection focus on external fraud and do not provide an effective solution for internal fraud which requires granular visibility to internal end-user behavior. As internal fraud represents a serious operational risk, banks now have even stronger incentive to be proactive about insider threat.

Intellinx presents a breakthrough in enterprise fraud detection and prevention, providing a first-of-its-kind cross-platform surveillance system for unparalleled visibility of end-user activity in corporate applications across the enterprise.

The Intellinx Solution

Intellinx solves some of the most challenging requirements posed by current government regulations. Continuous recording of end-user activity takes place at the application level (versus network or database level) and across every major platform – from the forgotten mainframe to web. Every screen viewed and every keystroke made by end-users is recorded and analyzed in real-time, creating field-level forensic audit trails of insider access to corporate systems.

A powerful analytic engine tracks user behavior patterns in real-time, triggering instant alerts on irregularities. This allows security officers to immediately zoom-in on suspects and visually replay all actions related to suspicious events, screen-by-screen. Extensive, cross-platform search capabilities simplify the process of investigation. Post-event analysis includes the ability to apply new rules to pre-recorded information.

Intellinx is a reliable and cost-effective compliance solution, enabling organizations to implement controls to their legacy and modern systems without any change to application code or system infrastructure. The system's agent-less architecture requires no installation of software/hardware on existing hosts or clients and presents no risk to system performance.

Who?

Did What?

When?

To Which Data?

From Where?

How?

Started	Userid	PatientID	PatientName	SSN	Action	IPAddress	DeviceName
2004-09-20 18:59:21.807	jerrym	300593	Brown,San	230063193	Patient File Update	192.168.1.103	SCOTCP10
2004-09-20 18:59:17.527	jerrym	300593	Brown,San	681670644	1 sh-Busine# Visuatio	192.168.1.103	SCOTCP10
2004-09-20 15:30:39.437	devick	300531	Conrad,Mary		Replaying user: SCOTCP10 Started: 2004-09-20 15:30:39.437		EP07
2004-09-20 15:30:26.527	jamvw	300582	Backster,Lester		1 38 72		EP08
2004-09-20 16:30:18.537	jamvw	300582	Backster,Lester				EP08
2004-09-20 15:29:27.407	devick	300719	Ohl,Greta				LP07
2004-09-20 15:29:09.17	bartm	300918	Sed#Jenny				LP08
2004-09-20 15:28:30.113	devick	300589	Hertz,Levi				LP07
2004-09-20 15:28:04.797	devick	300632	Lemke,Joe				LP07
2004-09-20 15:27:57.111	devick	300569	Expon,Mike				LP07
2004-09-20 15:27:40.48	devick	300569	Expon,Mike				LP07
2004-09-20 15:27:36.86	devick	300569	Expon,Mike				LP07
2004-09-20 15:17:12.59	lyva	300608	Rust,Carol				LP08
2004-09-20 15:07:26.043	lyva	300569	Expon,Mike				LP06
2004-09-20 15:07:23.017	lyva	300569	Expon,Mike				LP06
2004-09-20 15:07:19.59	lyva	300540	Mengo,Mile				LP06
2004-09-20 14:48:26.51	orlt	300520	Locke,Donna				LP04
2004-09-20 14:47:50.67	orlt	300520	Locke,Donna				LP04
2004-09-20 14:47:43.55	orlt	300520	Locke,Donna				LP04
2004-09-20 14:14:15.707	orlt	300593	Brown,San				LP03

- Key Benefits**
- Application Activity Recording and Monitoring
 - Visual Screen-by-Screen Replay
 - Cross-Platform Detailed Forensic Audit Trail
 - Support for Mainframe, AS/400, Client/Server, Web
 - Real-Time Alerts, Post-Event Analysis
 - Cost-Effective, No Risk Implementation

About Intellinx

Intellinx Ltd. is the innovative leader in end-user behavior tracking solutions for detecting and preventing enterprise fraud and information leakage. The Intellinx solution enables large and medium size organizations to address the challenge of various types of fraud committed by legitimate end-users who are authorized to access corporate applications from within or from outside the organization. Intellinx detects fraud attempts and information leakage in real-time generating a very detailed forensic audit trail of user access to corporate applications and data. This enables organizations comply with government regulations including PCI, GLBA, FACTA Red-Flags, Sarbanes-Oxley and Basel II. The Intellinx patent-pending agent-less technology imposes no risk and no overhead on the organization's infrastructure. The Intellinx customer base includes over 90 financial, healthcare, government and telecom organizations around the world.



Intellinx Software Inc.
 560 Sylvan Ave., Englewood Cliffs,
 NJ 07632, USA
 Tel: 201 567 7737 Fax: 201 567 7745

Intellinx Ltd.
 1c Yoni Netanyahu St. P.O.B. 1035
 Or-Yehuda 60200, Israel
 Tel: +972 3 538 5555 Fax: +972 3 634 9230

www.intellinx-sw.com
 E-Mail: info@intellinx-sw.com