



Meeting Compliance Requirements in a Competitive Marketplace

There is a growing awareness that a significant threat to corporate assets comes from management and employees within the organization rather than from third parties. Every organization faces the risk of fraud committed by knowledgeable and capable employees who utilize their authorized access to the IT assets for manipulating internal systems. As a result of high-profile, high-impact corporate fraud, several laws have been enacted in order to protect the organization's customers and share holders. These regulations pose significant challenges for organizations since most of their systems were developed and deployed before these regulations were enacted.

Privacy Regulations- HIPAA & GLBA: The Audit Trail Challenge

The HIPAA Security Rule requires healthcare organizations to "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." (Section 164.312). The Gramm-Leach-Bliley Act (GLBA) makes similar requirements regarding tracking access to financial information.

This requirement is challenging, especially for organizations that rely on legacy systems. Unlike network devices and infrastructure systems, there is typically no application access logging mechanism in the mainframe environment. 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 that companies create and maintain effective internal controls to track financial processes. As financial reporting relies on information collecting from various systems, such as purchasing, payroll, inventory, human resources and more, 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 auditing 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

How to protect sensitive information from unauthorized manipulation and disclosure by insiders has become a major concern for banks and other financial organizations worldwide. Insider threat can range from manipulating financial statements to misappropriating assets to selling customer private information, and more. Beyond fraud, there can also be noncompliant transactions in the form of errors or intentional overrides.

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. 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 insider threat 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 in today's regulations. Continuous recording of end-user activity takes place at the application level (versus network level) and across every 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 rule 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, requiring no change to application code or system infrastructure, no installation of software/hardware on hosts or clients and presenting no risk to system performance.

The screenshot shows the Intellinx Administrator interface. The main window displays a 'Business Event Report' table with columns for Started, Userid, Patientid, PatientName, SSN, Action, IPAddress, and DeviceName. A detailed view of a specific event is shown on the right, including fields for Action, First Name, Last Name, Gender, Birth Date, Address, City, State, and Telephone. Callouts from the left and right sides of the screenshot point to various data points in the table and the detailed view, each with a question: 'Who?' (Userid), 'Did What?' (Action), 'When?' (Started), 'To Which Data?' (Patientid), 'From Where?' (IPAddress), and 'How?' (DeviceName).

Started	Userid	Patientid	PatientName	SSN	Action	IPAddress	DeviceName
2004-09-20 18:59:21.807	jerryj	300593	Brown,Sam	230063193	Patient File Update	192.168.1.103	SCOTCP10
2004-09-20 18:59:17.527	jerryj	300593	Brown,Sam	681670644	Pat. Birth Date View	192.168.1.103	SCOTCP10
2004-09-20 15:30:39.437	divick	300531	Conrad,Mary		Replaying user: SCOTCP10 Started: 2004-09-20 15:30:39.437		IP07
2004-09-20 15:30:38.527	janmv	300582	Backster,Lester				IP08
2004-09-20 15:30:18.537	janmv	300582	Backster,Lester				IP08
2004-09-20 15:29:27.407	divick	300719	Gill,Greta				IP07
2004-09-20 15:29:09.17	bartm	300918	Sand,Jeffy				IP08
2004-09-20 15:28:20.113	divick	300599	Hertz,Levy				IP07
2004-09-20 15:28:04.797	janmv	300632	Lemke,Joe				IP07
2004-09-20 15:27:57.111	divick	300569	Expon,Mike				IP07
2004-09-20 15:27:40.48	divick	300569	Expon,Mike				IP07
2004-09-20 15:27:36.86	divick	300569	Expon,Mike				IP07
2004-09-20 15:17:12.59	lyva	300608	Rust,Carol				IP08
2004-09-20 15:07:26.043	lyva	300569	Expon,Mike				IP06
2004-09-20 15:07:23.017	lyva	300569	Expon,Mike				IP06
2004-09-20 15:07:19.59	lyva	300540	Mango,Mile				IP06
2004-09-20 14:48:28.51	ort	300520	Locke,Donna				IP04
2004-09-20 14:47:50.67	ort	300520	Locke,Donna				IP04
2004-09-20 14:47:43.55	ort	300520	Locke,Donna				IP04
2004-09-20 14:14:15.707	ort	300593	Brown,Sam				IP03

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. emerged from Sabratec Ltd., a leading provider of legacy integration solutions founded in 1997. In 2003, Sabratec began developing the Intellinx technology leveraging its deep knowledge of integration technologies and addressing the growing need of its customers to protect their information assets from the dangers of insider threat. Following the acquisition of Sabratec Ltd. by Software AG in January 2005, the Intellinx division, which was not part of this acquisition, was recreated as an independent company, Intellinx Limited. The Intellinx Research & Development Center is based in Israel. The Intellinx subsidiary in New York City handles marketing and support for the North American region. Intellinx is recognized by leading analyst firms including Gartner and IDC as an innovative leader in the area of insider threat solutions. Gartner listed Intellinx as a "cool vendor" in 2 categories in 2006: 'Security & Privacy' and 'Application Development'.



Intellinx Software Inc.
 156 William St., Suite 806, New York
 NY 10038, USA
 Tel: 212 513 0977 Fax: 212 513 0979

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