

Success Stories

Intellinx is currently being utilized by leading financial, government, healthcare and utilities organizations around the world. Due to the sensitive nature of the solution's implementation, typically for internal fraud detection, most Intellinx customers prefer not to have their details publicized. Following are just a few examples of how Intellinx solves critical business issues without disclosing private customer details.

International Bank Saves Over \$1 Million with Intellinx

A prominent International Bank, with branches in 20 countries and more than 100 billion dollars in assets under management, utilizes Intellinx to meet current compliance regulations for their sector.

A regulation based on the Basel II Accord requires all banks (in the country to which the bank belongs) to maintain a very detailed audit trail of user access to customer data, including all update and query activities. In the past, the Bank logged some update but no query transactions. Implementing a log for all transactions would require changes in thousands of mainframe application programs. The Bank estimated that it would take approximately 100 programmer-months to accomplish the task, with a total cost of over 1 million dollars. Instead, they chose Intellinx and achieved immediate compliance without changing a single line of code, saving over 1 million dollars.

The Bank's Senior VP and Head of Operations said "As a financial institution we need to comply with government regulations that require a full audit trail of both update transactions and queries. Intellinx allowed the Bank to comply with this regulation after a very short implementation process, saving the Bank many programmer-months that would have been, otherwise, invested in altering our online applications. The Intellinx non-invasive solution poses zero overhead on our infrastructure and requires very limited disk space."

Intellinx Halts Credit Card Information Leakage

A known Credit Card Company recently implemented Intellinx for its information leakage and internal fraud detection capabilities. The Company uses Intellinx to record user activity in internal corporate applications, thereby providing auditors with the ability to replay every screen and keystroke of every end-user. The Intellinx rules help to track end-user behavior patterns, while generating alerts on exceptions in real-time. Only several weeks after installation, Intellinx proved critical to the Company, when the system detected and alerted security personnel to an employee misusing his authorized access rights in an attempt to leak sensitive customer information. The fraud investigator visually replayed the suspect's actions allowing for full session reconstruction. This reconstruction proved that the context of accessing the data in question was not part of the employee's normal and legitimate work.

Government Agency Uses Intellinx to Deter Employee Fraud

A large Government Agency with more than 11,000 employees has selected Intellinx to capture, record and generate forensic audit trails of all user activities across all internal business applications. The solution enables them to keep perfect track of all user access to citizen-sensitive data.

By adopting a policy of openly informing all employees and contractors of the presence of Intellinx, the Agency has said they are taking "preventative measures to deter potential fraud and information leakage."

Insurance Company Detects Internal Fraud of Privileged Users

A European Insurance Company deploying Intellinx for internal fraud detection discovered that insider threat can pertain to employees with privileged access rights, as much as to those with lesser access rights.

Intellinx business rules were implemented to generate alerts in real-time regarding suspicious user behavior patterns. Those very rules helped the Company to monitor, detect and eventually put a stop to the abuse of privileged rights by a System Administrator who attempted to update information in a production database using a DB utility that cannot be traced by other means except for Intellinx.

"Intellinx has helped us to capture and reconstruct all user activity, including that of our Database and System Administrators and Programmers. These privileged users can pose a serious threat to information security by way of their technical knowledge and authorized access to internal servers and resources."