



## Enterprise Fraud Management

In today's climate fraud and the loss of confidential data are some of the most serious threats faced by many organisations. At e-Solutions, we offer a unique and innovative software solution, Intellinx, for prevention, detection and mitigation of insider threats. Intellinx also provides the audit tool required for PCI DSS compliance and an innovative AML solution by recording and analysing end-user and transactional activity.

### Business Benefits

- Reduce fraud losses by detecting fraud and other malicious activity in real-time.
- Fraudulent and curious users are deterred just by the knowledge that all their actions are being recorded. This includes queries that usually do not leave any traces in traditional logs.
- A full audit of users that have had access to credit card details is available to meet PCI DSS requirements.
- Improved internal audit effectiveness by alerting on detection of suspicious behaviour.
- Provides full visibility of all the actions of each end-user under investigation as if looking over their shoulder.
- Provides alerts on suspicious customer transactions for AML purposes.
- Enforce corporate security policies by detecting security breaches and exceptions.
- Increase productivity and improve customer satisfaction by detecting process slowdown and bottlenecks in real-time, triggering alerts on service level breaches.

### Intellinx Technology

The Intellinx solution monitors a wide range of platforms with no need to install any hardware or software on host or clients. The software intercepts communication between end-users and application servers by 'sniffing' traffic through the network switch. Recorded data is stored in a highly condensed format, allowing monitoring of thousands of end users without a major impact on disk space. Recorded files are encrypted and digitally signed so that they can be used in court as evidence if required.

### Product Features

- Record all screens displayed, end-user keystrokes and messages between applications without interfering with the host's or client's software or hardware.
- Replay of screens accessed and actions performed by each end-user as if looking over their shoulder.
- Search for end-user sessions in a specific timeframe according to screen content and headers, field names and values within screens. Search and replay, for example, all user screens displayed on a specific date in which a specific account number was accessed.
- Pattern recognition algorithms automatically identify application screens, fields, flows and messages.
- Simple tools for mapping application screens, fields and flows into meaningful business indicators and entities.
- Customisable business rules track end-user behaviour patterns in real-time, identify exceptions and triggering alerts.
- Recorded data may be archived and new rules applied on old recordings after-the-fact.



## Insider Fraud

For years, organisations have been focusing their information security efforts to protect themselves against external threats. Most organisations have built solid walls to protect their perimeters against exposure to the internet. Today, many of them are realising that for the most part these defences cannot help with a different type of threat – the insider threat.

A significant amount of fraud is either executed or assisted by staff members who have access to systems and knowledge of internal processes. However, the degree of internal knowledge makes it difficult to identify culprits.

Intellinx is the only solution on the market that non-invasively records and analyses in real time. Intellinx analyses the interaction between internal staff and business applications over different types of applications which includes legacy systems, client server applications and newer HTTP based systems. Intellinx works by 'sniffing' network traffic and as a result has no impact on existing system performance and can be installed and operational in hours.

Tracking the activity of privileged users is a tough challenge for most organisations. On one hand these users pose higher risk than regular users as they have higher authorisation level. On the other hand these users typically utilise programming and administrative tools which do not provide any audit trails in most cases.

Intellinx can monitor the activity of privileged users including System Administrators, Database Administrators, Programmers and others.

The system can track normal behaviour patterns and generate alerts on exceptions in real-time. In addition, the system enables investigators to visually replay the activity of those under investigation screen by screen.

## AML Monitoring

Intellinx can track customer behaviour patterns and transaction activity on online banking systems and messages sent in Swift and other protocols.

Based on the recorded data Intellinx rules can generate alerts and reports required by AML regulations.

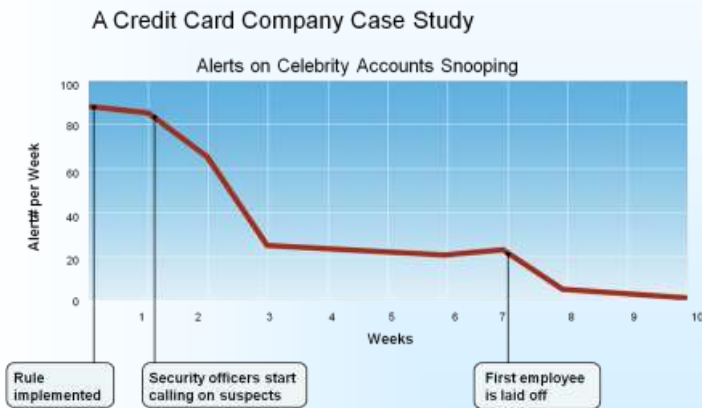
The rules are fully customisable to an organisation's specific needs. Examples where alerts and reports could be generated include:

- A foreign currency purchase that exceeds the amount that requires reporting.
- Consecutive transactions with the amount just below the amount that requires reporting.
- A cash deposit followed shortly by withdrawals of a higher than usual amount.
- A series of similar value deposits / withdrawals for the same account.
- Multiple transactions to the same target account in a given period.
- New customer (individuals, entities, securities, countries) found in a watch list (OFAC, FATF, NCCT, PEP, etc).
- Customer Profiling - to classify the account into different risk categories (high risk, low risk etc.) for the purpose of activity and transaction monitoring. The transaction risk can be linked to the product, the industry or the geographical location.





## The Deterrence Impact of Real-Time Alerts



## PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) was developed by the major credit card companies as a standard for organisations that process card payments for preventing credit card fraud, hacking and various other security vulnerabilities and threats.

Intellinx presents a breakthrough in Insider Threat Detection and Prevention providing an out of the box solution for PCI DSS requirements 10.2.1 and 10.2.2 by automatically generating a full audit trail with visual replay of user screens and keystrokes in any application on all major platforms. The audit trail includes both update and read-only actions for both regular and privileged end-users.

Introducing a paradigm shift for information security officers and internal auditors, Intellinx provides unparalleled visibility to end user activity providing additional benefits that exceed the requirements of the DSS.

Configurable fraud rules track user behaviour patterns at the application screen level, generating alerts on exceptions in real time, and allowing the internal auditor to immediately zoom in on specific suspects.

Intellinx offers an agent-less solution based on sniffing network transmissions. As a result no software needs to be installed on the user's desktop / terminal and there is no impact on system performance.

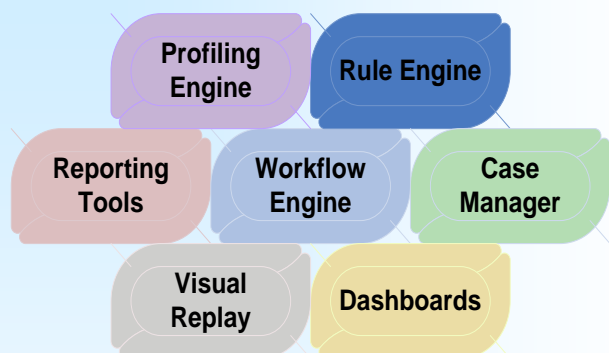
## Information Leakage

Recent new powers granted to the Information Commissioners Office (ICO) mean that companies now have to be far more accountable for any data breaches or loss. Breaches over 1,000 records can result in action such as enforcement notices to encrypt portable media and data.

A growing list of organisations have been served with enforcement notices relating to data breaches or loss. Most at risk are those organisations with call centres with large quantities of low paid workers, and high staff turnover. These environments tend to provide staff with the greatest opportunity to commit fraud as most will have access to large amounts of data.

With Intellinx in place, alerts can be sent to auditors, managers, and investigators in real time to advise on staff members viewing or amending client data, or downloading large quantities of unsecured data. Auditors would be able to replay complete user sessions with evidence potentially admissible in court.

## The Intellinx Investigation Centre



Intellinx has an optional Investigation Centre or it can be integrated with an organisation's existing case management system. The Investigation Centre provides a full control mechanism so that alerts can be prioritised and placed in workflow queues for an investigator to action. Direct access to the Intellinx database to playback the user's session is available. The Investigation Centre can also integrate with other tools to provide a single system for all fraud related activity.

### Instant Results

Intellinx works by connecting into network switches with no need for time consuming integration with any of the organisation's systems. Intellinx provides unique business value. Immediately following installation, Intellinx provides the functionality of record, replay and search with no need for time-consuming integration with any of the organisation's systems. e-Solutions can work with clients to provide more complex bespoke rule sets as required.

