

A Breakthrough in Insider Threat Detection & Prevention

Surveys show that approximately two-thirds of fraud and identity-theft cases are perpetrated by company employees and other trusted insiders. The 2006 report of the Association of Certified Fraud Examiners estimates that US companies lose, on average, 5% of their annual revenues to internal fraud. The Australian Institute of Criminology estimates that the national cost of fraud in Australia to be almost \$6 billion; 70% of these losses are the direct result of insiders!

So it is not surprising that corporate officers are expected to safeguard their businesses against insider threats to control exposure to these risks.

Intellinx presents a first-of-kind, cross-platform surveillance system for unparalleled visibility of end-user activity in corporate applications across the enterprise.

Get Proactive about Insider Threat

The Intellinx Solution provides a critical infrastructure for combating internal fraud and information leakage, enabling proactive response to inappropriate insider behaviour rather than dealing with these matters, "after-the-fact." With complete recording, monitoring and analysis of user activities over multiple platforms, security officers can now act on suspicious behavior as it occurs and use the intelligence stored by Intellinx to prevent future abuse.

Hold Insiders Accountable

Intellinx provides complete visibility of end-user activity with **visual replay** of every screen, keystroke and flow of screens regardless of the host application. It enables security officers to know who did what, to which account, from where, how often and when. Intellinx records all activities; whether that is an account query by a clerk or the actions of privileged IT operators. It **can not be by-passed** regardless of permission level - all user activity is recorded.

Investigate Suspicious Behaviour

Intellinx captures very detailed field-level **audit trail** of user activity which is combined with an extensive **cross-platform search** capability. Search parameters are flexible, for example, an investigator could quickly discover every user that accessed a specific account number within a set timeframe over a number of distinct applications across the enterprise; and then the investigation could zoom-in on specific user sessions and visually replay every action taken screen by screen. Investigations can be performed immediately following a suspicious activity or after-the-event by examining historical data recordings.

Respond Now

Intellinx will generate **real-time alerts** to instantly draw attention to suspicious behaviour so an immediate and timely response can be undertaken to mitigate damage. Configurable rules track user behaviour patterns at the application level and generate alerts on irregularities in real-time. It allows auditors to immediately zoom-in on suspect users. For example, an alert could be automatically generated when a user queries customer accounts by customer name (rather than account number) more than 5 times in an hour, when the average for such query is twice an hour.

Prevent and Pre-empt the Next Crime

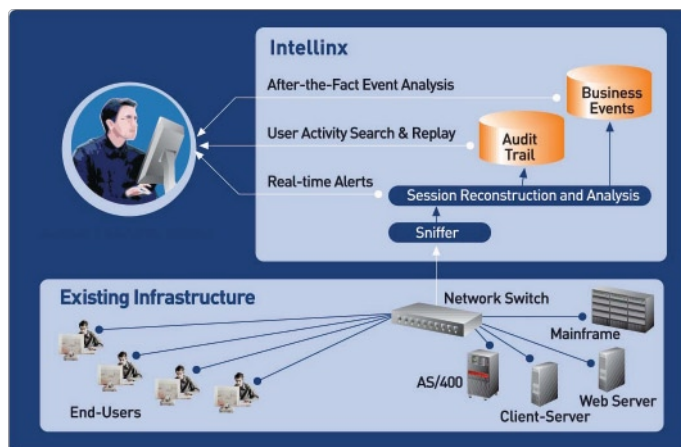
Crime is not random. It follows behavioural and operational patterns and its perpetrators fit certain profiles. Intellinx allows you to perform after-the-fact analysis of user behaviour by **applying new rules to historical recordings**. New fraud detection knowledge can be applied to recorded information. Combined with the organisation's internal resources, Intellinx can be utilised to foresee, predict and preempt crime in the future.

Out-of-the-Box Business Value

Intellinx is generally installed as a scalable appliance that is ready to deploy as a 'black-box' technology. Immediately following installation (which typically takes just a few hours), Intellinx begins capturing all cross-enterprise user activity and is then available for auditors to perform detailed investigations. Security officers will thereafter be able to search all user screens in which specific values appeared in any application across the enterprise. Intellinx implementations are so rapid that organisations will gain immediate benefit of its security capabilities out-of-the-box. Deploying an Intellinx appliance in your organisation does not require time-consuming integration with existing business systems or applications. This is why Intellinx offers exceptional business value; Validation is immediate.

No Risk Implementation

- Intellinx's patent-pending technology intercepts communication between end-users and corporate servers by sensing and capturing all data transiting network switches. Therefore, Intellinx does not impact performance of hosts or networks.
- There is no need to install any software or hardware on the host or network clients.
- Intellinx tracks user activity on any application in most major platforms, including mainframe, iSeries, Client/ Server, Web (Intranet) and more.
- Organisations benefit from quick installation process (several hours), with no risk to ongoing IT operations.
- Intellinx architecture is scalable and has proven to be a cost-effective implementation for any sized organisation.
- Recordings are stored in highly condensed format, allowing an organisation to monitor tens of thousands of end-users without major impact on disk space.
- Recording files are ciphered and digitally signed to ensure their integrity as court admissible evidence.



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 centre is based in Israel.

Advent One is the Australian and New Zealand distributor of Intellinx and is responsible for local marketing and support.

Intellinx is recognised 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 two of its 2006 'Cool Vendor' research reports: 'Security & Privacy' and 'Application Development.'



Advent One Pty Ltd

Aust. & NZ distributor of Intellinx
Level 10, IBM Centre, 60 City Road
Southbank, Victoria 3006. Australia
Tel: +61 (0)3 9626 5900 Fax: +61 (0)3 9626 5999
www.adventone.com/intellinx
email: info@adventone.com

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
email: info@intellinx-sw.com

The Intellinx Difference

Unparalleled Visibility of End-User Activity

Complete visibility into end-user activity is provided with visual replay of every screen, keystroke and flow of application screens across most major platforms. All activities are visible, including update and read-only actions.

Complete Audit Trail

Intellinx records all user activity, not just events detected as suspicious in real-time. This is crucial for making end-users accountable for their actions. Regardless of whether appropriate rules are in-place at the time of an event, post-event replay enables forensic investigation at a later time.

Cross Platform Search including Legacy

Intellinx provides a unique solution for tracking user activity across all major platforms including legacy systems. It allows you to search specific values displayed on any user screen across multiple platforms from one simple query screen. The Intellinx rules track cross-platform business processes. For example, a business process tracked by Intellinx may begin on a mainframe, continue in a client-server application and end on the web.

User Behavior Tracking at the Application Level

Intellinx is the only solution on the market that analyses user activity at the application level (not at the network level). Intellinx rules track all user keystrokes and the flow of screens accessed by the user, detecting the relevant business process including each field value accessed or updated. This information is correlated in real-time with the activity of other end-users, previous activities and other types of information.