

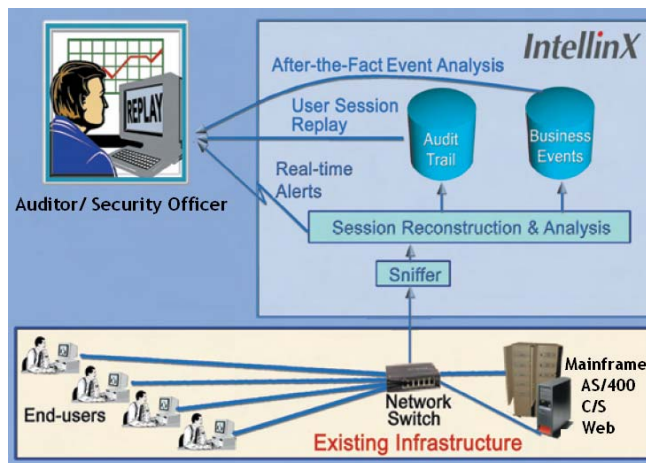
Insider Threat SOA Solution for the Enterprise

Protecting sensitive information from unauthorized manipulation and disclosure by its employees and management has become a major concern for large organizations worldwide. Intellinx offers a unique and innovative software solution for mitigating this insider threat. By continuously recording and analyzing all end-user activity in the internal business applications across the enterprise, Intellinx collects invaluable forensic evidence.

Introducing a new dimension for information security officers and internal auditors, Intellinx provides unparalleled visibility to end user activity. It allows for visual replay of user screens and keystrokes in any application, as if looking over the user's shoulder. Configurable business rules track user behavior patterns, generating alerts on exceptions in real-time, allowing the internal auditor to immediately zoom-in on specific suspects. Intellinx patent-pending technology offers agent-free solution based on sniffing network transmissions with zero foot-print and zero overhead. Integrated with the IBM SOA architecture and utilizing IBM software and hardware platforms, Intellinx provides a scalable enterprise-level solution.

The Intellinx Business Value

- Reduce fraud losses by detecting internal fraud and other malicious activity in real-time (the ACFE estimates that US companies lose on average 6% of all revenues due to internal fraud).
- Reduce the Basel 2 capital requirements by reducing internal fraud and controlling operational risk.
- Deter potential fraudulent users just by knowing that all their actions are recorded.
- Improve information security effectiveness by alerting on suspicious user behavior and providing full visibility for the security officer to all the actions of each specific suspect, as if looking over his or her shoulder.
- Improve internal audit effectiveness by enabling investigations on any event in the past by searching for example, for all the users who accessed a specific customer account number in a specific timeframe across all corporate internal applications.
- Scalable, reliable and cost-effective solution for the enterprise, integrated with the IBM SOA architecture.
- Comply with privacy regulations that require a detailed audit trail of end-user access to sensitive customer information.
- Rapid time-to-value – out-of-the-box record/replay functionality with automatic forensic audit trail generation allowing for ad-hoc investigation of user access to sensitive corporate data.



The Intellinx SOA Architecture

Aligned with the IBM SOA strategy, Intellinx is designed to provide a scalable solution for mitigating insider threat at large organizations. Intellinx records and analyzes user activity in the internal business applications running on various platforms (mainframe, iSeries, Client/Server and Web) by non-invasively sniffing network transmissions. Intellinx can also track application activity transmitted through the Enterprise Service Bus (ESB). The recorded data is analyzed in real-time tracking user behavior patterns generating instant alerts on suspicious events.

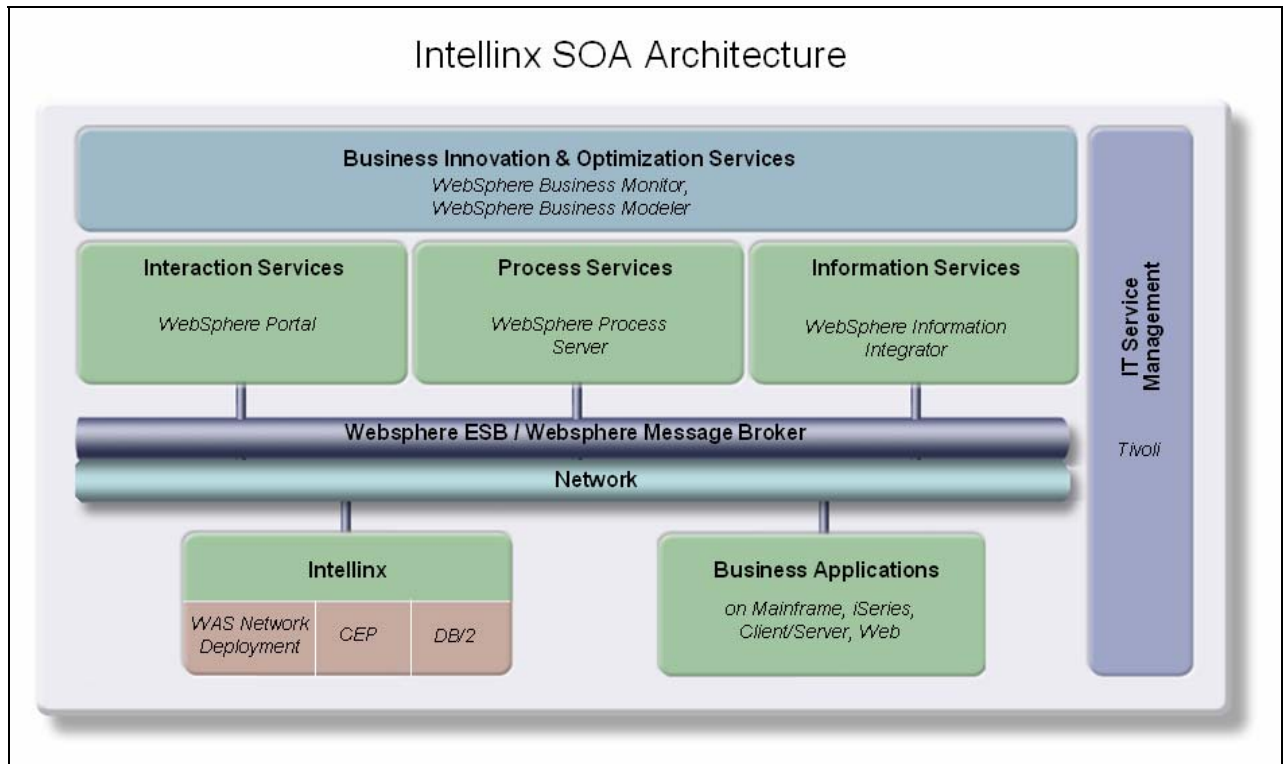
Intellinx can be used proactively through integration with Websphere Process Server (WPS). Business processes managed by WPS can be orchestrated to check with Intellinx if they are allowed to be completed upon the status of suspicious events that may have been detected by Intellinx.

The integration of Intellinx and Websphere Business Monitor provides an overall view of suspicious events (including severity levels) that have been detected by Intellinx and need to be investigated.

Intellinx utilizes 3 Websphere components as its infrastructure:

- DB/2 is utilized for storing the recorded sessions and analyzed screen content

- Websphere Application Server Network Deployment is utilized for managing loads and resources in high volume implementations
- CEP (Complex Event Processing - AMIT) is utilized for analyzing the recorded user workflow, tracking end-user behavior patterns and triggering alerts on exceptions in real-time



Intellinx was developed using Java and Eclipse and runs on various IBM hardware platforms including eServer pSeries running AIX or Linux as well as eServer xSeries running Linux.

Key Differentiators

- Full visibility into end-user actions
- Unique solution for monitoring user activity and collecting forensic data in heterogeneous platforms including IBM mainframe and iSeries
- Full integration with SOA
- Automatic generation of detailed audit trail without changing a single line of code
- Business rules can be applied after-the-fact based on the recorded data
- Non-invasive, risk free implementation
- Very Short implementation process, with immediate business value

About Intellinx

Intellinx Ltd. is the innovative leader in end-user behavior tracking solutions for safeguarding against the insider threat. Intellinx enables large organizations to address the challenge of internal fraud committed by legitimate end-users and comply with regulations such as GLBA, HIPAA, Sarbanes-Oxley and Basel 2. Intellinx patent-pending technology is non-invasive and is overhead-free.

Intellinx Ltd. emerged in January 2005 from Sabratec Ltd., a leading provider of legacy integration solutions. Sabratec products are deployed at more than 200 customers worldwide including large corporations such as GE Capital, Sabre, First National Bank, Ricoh, Swiss Re, Brazil Telecom, Telemar, RTVE, and many others. Following the acquisition of Sabratec Ltd. and its legacy integration division by Software AG, the Intellinx division was transferred to Intellinx Ltd., which emerged as an independent company.