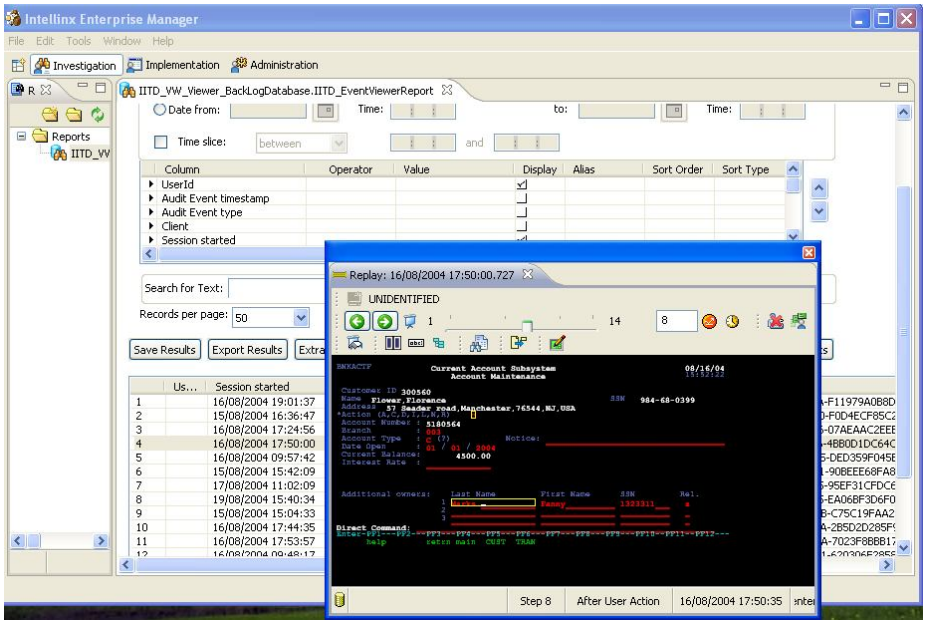
Intellinx – инновационное решение для предотвращения злоупотреблений и мошенничества

В последнее время все больше организаций финансовой сферы осознают, что наиболее значимые угрозы, влияющие на конфиденциальность, целостность и доступность критически важной информации, исходит не извне (хакеры, информационные террористы и т.п.), а изнутри, со стороны их собственных сотрудников. Недобросовестные пользователи часто используют в корыстных целях знания, навыки и привилегии, которыми обладают в силу выполнения служебных обязанностей. Различные способы внутреннего мошенничества могут заключаться в махинациях с финансовыми документами, присвоении средств, продаже конфиденциальной информации об организации и клиентах и т.п., что влечёт за собой финансовый, репутационный и другие ущербы. Они же могут быть причинены организации не столько злонамеренными, сколько ошибочными действиями сотрудников.

Решение – мониторинг действий пользователей

Intellinx предоставляет беспрецедентную возможность контроля работы сотрудников и клиентов с используемыми информационными системами. Каждый просмотренный пользователем экран и каждое нажатие клавиши регистрируются и анализируются в режиме реального времени.

Действия технического персонала (программистов, администраторов) контролируются так же, как и действия конечных пользователей – сотрудники службы ИБ могут, в том числе, отслеживать доступ к информации с помощью системных средств. Опираясь на предопределенные правила, Intellinx преобразует собранные данные в индикаторы активности, позволяя организации выявить злонамеренные или ошибочные действия, расследовать подозрительные операции путем повторного воспроизведения (replay) конкретных сеансов работы пользователей и клиентов.



Соответствие требованиям законодательства и регуляторов

Вследствие участившихся случаев мошенничеств и злоупотреблений были приняты различные законы, подзаконные акты и стандарты:

- СТО БР ИББС-1.0-2008
- ФЗ-152
- PCI DSS
- Sarbanes-Oxley
- Basel II

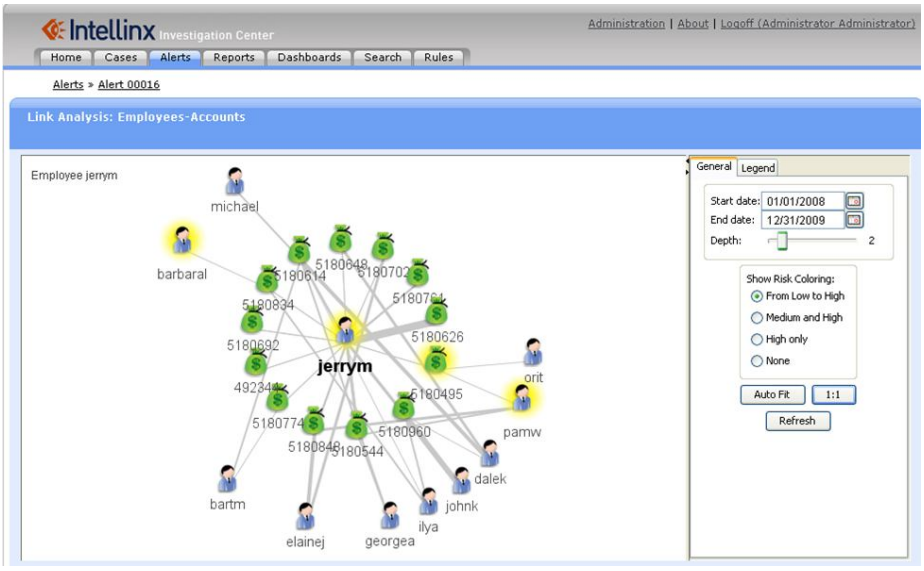
Все эти документы, содержат требования о всеобъемлющем мониторинге действий сотрудников и клиентов в регламентируемой области, в том числе получение и накопление информации о том, какие операции, кем, откуда и с какими данными производились.

В некоторых случаях, согласно предъявляемым требованиям, необходимо регистрировать действия сотрудников в специальном электронном журнале, доступном для просмотра, чтения и анализа администраторам безопасности, аудиторам и т.д.

Intellinx обеспечивает полное соответствие требованиям по мониторингу и хранению свидетельств аудита

В каких областях применяется Intellinx

- Внутреннее мошенничество
- Внешнее мошенничество
- Нарушения в ведении бизнеса и системные сбои
- Соответствие требованиям по защите персональных данных
- Соответствие требованиям Sarbanes-Oxley
- Отслеживание действий привилегированных пользователей (администраторов систем)
- Отслеживание разделения обязанностей
- Управление изменениями
- Противодействие отмыванию денег
- Обнаружение мошенничества при интернет – банкинге
- Отслеживание активности системных администраторов и других привилегированных пользователей



- Мониторинг доступности и времени отклика в критичных процессах

- Добавление контролей уровня приложений
- Анализ путей исполнения бизнес-процессов конечными пользователями
- Поддержка служб ServiceDesk

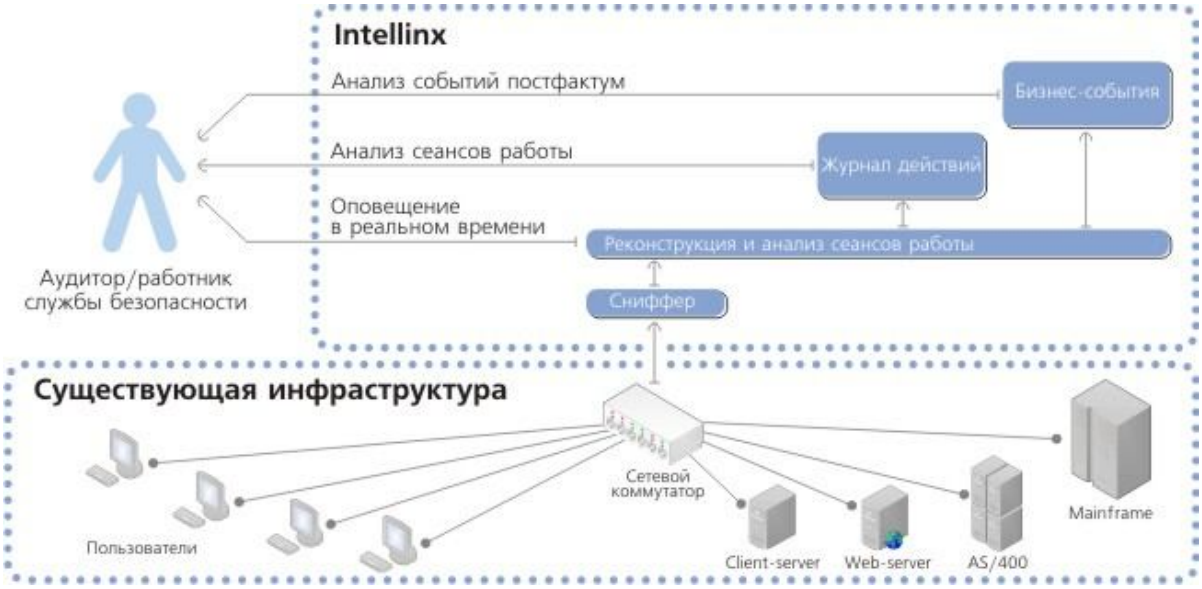
Как Intellinx обеспечивает полный контроль

- Регистрация и запись всех пройденных в процессе работы экранов, web-страниц и отправленных/принятых структурированных сообщений между системами без вмешательства в программное или аппаратное обеспечение на серверах и рабочих местах.
- «Проигрывание» пройденных экранов и действий, выполненных любым пользователем в любое время с возможностью поиска определенных экранов, полей и данных. Например, найти и "проиграть" пользовательские сеансы, в которых просматривали или изменяли данные конкретного банковского счета;
- Предопределенные бизнес-правила выявляют неправомерные действия пользователей и оповещают о них в реальном времени. Например, отслеживание банковских служащих, выполняющих операцию «Поиск и просмотр счета клиента по имени клиента» более 20 раз в течение часа, тогда как средняя частота выполнения такого запроса не более двух раз в час.
- Возможность применения новых бизнес-правил, для обнаружения фактов мошенничества в прошлом, путем их применения к сохраненным в базе данных записям сеансов.
- Графический интерфейс для моделирования бизнес-процессов на основе анализа элементов информационной системы;
- Настраиваемая структура объектов контроля, позволяющая описать и контролировать любые действия в информационных системах – от входа в АБС во внерабочие часы до корректности закрытия операционного дня
- Сохранение в собственной базе данных информации о фактах, мерах, бизнес-сущностях возможностью поиска, просмотра и анализа взаимосвязей.

Технология Intellinx

- Запатентованная технология перехвата сообщений между клиентами и серверами путем прослушивания сетевых потоков. Таким образом, Intellinx никак не влияет на производительность серверов и рабочих станций.
- Отсутствие необходимости устанавливать какое-либо программное обеспечение или оборудование на сервере и клиенте.
- Быстрая установка (несколько часов) без негативного влияния на нормальное функционирование ИТ-систем.
- Информация записывается в сжатой форме, что позволяет сохранять данные о работе тысяч пользователей, не требуя большого дискового пространства.
- Данные записываются в закодированном и защищенном от изменений формате, позволяя использовать их в суде[1] в качестве доказательств.

[1] Судебная практика за пределами РФ



Intellinx «из коробки»

Сразу же после установки Intellinx, не требуя дополнительной конфигурации или определения бизнес-правил, начинает отслеживать работу пользователей. Intellinx фиксирует действия пользователей и автоматически распознает экраны, поля и сообщения. Записанные данные могут быть просмотрены и проанализированы.

Почему Intellinx ?

Intellinx может контролировать любые традиционные приложения - как собственной разработки, так и стандартные - вне зависимости от языка программирования или интерфейса. Многие другие решения для мониторинга ограничены форматами данных конкретных систем.

Встраивание функций мониторинга непосредственно в используемые приложения требует огромных затрат, поскольку изменения должны быть внесены в каждую программу, применяемую конечными пользователями, вновь созданный код должен пройти полное тестирование после чего необходимо произвести обновление всех приложений.

Мониторинг в режиме реального времени

В противовес другим решениям мониторинга, основанным на анализе информации в базах данных (лог-файлах) и действующих «постфактум», Intellinx контролирует действия пользователей в режиме реального времени, предоставляя, таким образом, более полные, точные и реальные сведения. Более того, другие решения, основанные на анализе данных, не могут отразить полную картину работы пользователей, так как многие операции (например, просмотр информации) не фиксируются в журналах БД и логах, но могут быть частью мошеннических действий.

Видимость (обзор) действий пользователей

Полная видимость – визуальное проигрывание любой пользовательской сессии в масштабах организации – экран за экраном, нажатие за нажатием как будто вы стоите за плечом сотрудника.

Отслеживание поведения пользователей

Настраиваемые правила позволяют выделить шаблоны поведения пользователя при использовании бизнес-приложений, и генерировать предупреждения об их нарушении в реальном времени.

Свидетельства аудита

Детальные свидетельства аудита автоматически создаются и сохраняются для всех действий пользователей в мониторируемых приложениях в масштабах организации.

Расследование и судебная экспертиза

Поскольку вся деятельность пользователей сохраняется, каждый экран и каждое поле в любой форме является доступным на любой момент времени в прошлом, может быть проанализировано и использовано как доказательство для внутреннего расследования потенциального мошенничества.

Адаптируемость к изменениям в мониторируемых приложениях

В случае, если формы в мониторируемом приложении изменяются, привязка полей данных к содержимому экрана перестает действовать, но она может быть изменена в любой момент после обнаружения изменений. Поскольку во время мониторинга сохраняется полное представление экрана, оно может быть проанализировано позже в любой момент, и поля данных могут быть переопределены.

Отсутствие накладных расходов на производительность

Нулевые накладные расходы на сервера, сетевую инфраструктуру[2] и клиентские рабочие места.

Стоимость администрирования и сопровождения

Требуется администрировать и сопровождать только сервера Intellinx. Нет дополнительных затрат на основные сервера и рабочие места в организации.

Контроль действий пользователя

Intellinx сам по себе не вмешивается в действия пользователей, но может инициировать процессы в других информационных системах, например, приостановку доступа пользователя, осуществляющего подозрительные действия

Надежность

Процесс мониторинга не зависит от работы серверов и рабочих станций, таким образом, с одной стороны, не существует способа заблокировать слежение на рабочей станции или сервере, и с другой стороны – любые неполадки с Intellinx не влияют на информационные системы организации.

Простота внедрения

В отличие от других решений, требующих дорогостоящего и долгого внедрения, для установки Intellinx не нужно написания нового кода, изменения существующих

[2] За исключением передачи трафика между компонентами Intellinx при распределенной установке

приложений или установки программного или аппаратного обеспечения на клиентах или сервере. Необходимо просто подсоединить сервер Intellinx к сети и, используя базовую функциональность («из упаковки») и немедленно получить требуемые результаты. В дальнейшем развитие функциональности Intellinx производится путем разработки бизнес-правил внутри системы, и может выполняться как силами специалистов организации, так и бизнес-консультантами.

Об Intellinx

Технология Intellinx была создана компанией Sabratec Ltd. - лидером в области продуктов для интеграции систем.

По мнению ведущих мировых аналитиков (Gartner, IDC), Intellinx Ltd. является передовой компанией в области разработки решений для мониторинга действий пользователей интерактивных систем. Gartner внес Intellinx в список наиболее новаторских (Cool vendor) продуктов в 2006 году в двух категориях: «Защита и безопасность» (Security & Privacy) и «Разработка приложений» (Application Development).

На данный момент продукты Intellinx установлены более чем у 80 заказчиков в разных странах мира, таких как Bank Leumi (Израиль), Equifax (США), GE Money Bank, Delaware Criminal Justice System (США), Post Authority Bank (Израиль), Leumi Card (Израиль), Department of Home Affairs (Южная Африка), Uniqa Insurance (Венгрия), VolksBank (Венгрия) и многих других.

Несколько крупных российских банков уже выбрали для себя Intellinx в качестве основной системы для борьбы с мошенничеством и обеспечения соответствия предъявляемым требованиям по мониторингу и хранению свидетельств аудита.