



of technology and business
innovation
2000 - 2010

intelscape

inteliware



Связующее защитное ПО для электронного сделок

ЗАДАЧА:

■ Для многих современных организаций электронный бизнес является составной частью рабочей модели. Однако в настоящее время электронный бизнес встречает на пути своего развития множество сложностей и препятствий. Махинации с кредитными карточками, распознавание личности пользователя, операции повышенного уровня риска и атаки извне – лишь некоторые угрозы, которые могут привести к потере огромных доходов. Онлайн-компании нуждаются в надежных инструментах определения этих угроз в режиме реального времени и их незамедлительного устранения.

РЕШЕНИЕ:

■ Связующее ПО, встроенное в Inteliscape, служит защитной оболочкой для приложений вашего предприятия в Интернете. С его помощью организация получает возможность вести измерение, управление и контроль самого приложения и поведения пользователей.

Используя собственный фильтр предварительной обработки от FMT, связующее ПО анализирует запрос навигатора до и после входа в приложение. Это позволяет организации пользоваться доступом ко всем данным каждого запроса (включая IP-адрес, информацию о навигаторе и более). В сочетании с другой информацией (просмотр географического положения, "черные" списки и предыдущее поведение клиента) предлагаемая нами система борьбы с мошенничеством принимает незамедлительное решение в режиме реального времени. Например, она может отказать в праве доступа к приложению, отправить сообщение, запросить дополнительное подтверждение, завести учетную запись о попытке несанкционированного доступа, изменить брендинговые или рекламные элементы или просто дать разрешение на проведение операции. Если онлайн-пользователю предоставляется доступ к электронному приложению, ответные действия все еще могут модифицироваться в зависимости от контекстных действий.

С помощью перекрестного обращения к данным внешнего интерфейса, система принимает эффективные решения относительно права доступа пользователя к определенным приложениям и режимам его использования.

Это возможно благодаря связующей программной прослойке, устраняющей вынужденное беспокойство клиентов, необходимость применения дополнительного интерфейса или внесения изменений в коды программных приложений!

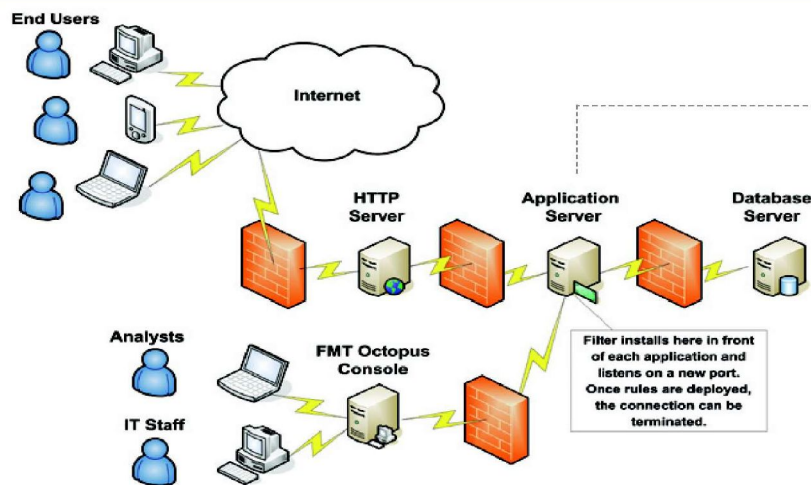
Опираясь на механизм графических настроек, эта программа предотвращения махинаций дополняет или защищает программное обеспечение. Модификации легко подключаются и отключаются без остановки сервера! При этом используются предписанные правила, внесенные в тот же программный сервер, на котором установлена система защиты от мошенничества. На базе инфраструктуры происходит исполнение команд по всему предприятию без привлечения дополнительного оборудования или серверов. В итоге, отпадает потребность в дополнительных устройствах, кроме консоли, на которой установлено само приложение.

В рамках ориентированной на сервис архитектуры наша система защиты позволяет в режиме реального времени следить за рабочими процессами на платформе встроенной функции отправки запросов в формате XML. Таким образом, организация может извлечь большую пользу:

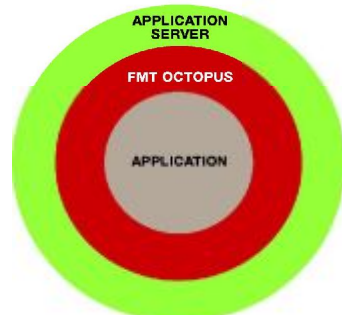
- Применение правил обеспечения безопасности
- Управление ПО
- Наблюдение за рабочими процессами
- Устранение отслеживания отказов
- Отслеживание статистики, выставления счетов и обработки спорных операций

Организации в сфере электронного бизнеса могут:

- Поддерживать функциональность программы
- Снижать риски и случаи мошенничества
- Совершенствовать онлайн-безопасность
- Улучшать маркетинг
- Вести наблюдение за работой ПО
- Повышать оперативность



The rules engine has a simple drag-and-drop interface so there's no need to learn a programming language. Simply move a rule (such as an SMS alert) onto the canvas, connect it to your application and you're done. Full training for certified users takes just three days.



Дополнительные преимущества:

- Установка всего за несколько часов
- Контекстная персонализация пользовательских привычек
- Контроль и усиление сторонних приложений без изменения кодов
- Независимая от разработчика интеграционная платформа снижает технологическую очередность

Функциональные возможности

<ul style="list-style-type: none"> ▪ Динамичное изменение вида и функционирования чужих статичных приложений 	<ul style="list-style-type: none"> ▪ Проверка данных между навигаторами и приложениями в ходе тестирования
<ul style="list-style-type: none"> ▪ Определение попытки кражи информации и организованной атаки 	<ul style="list-style-type: none"> ▪ Проверка ответственных за проведение операций с высоким уровнем риска
<ul style="list-style-type: none"> ▪ Отслеживание пользователей из единого центра 	<ul style="list-style-type: none"> ▪ Внедрение скоростных правил и определение IP-адресов
<ul style="list-style-type: none"> ▪ Предотвращение совместного использования идентификационных параметров 	<ul style="list-style-type: none"> ▪ Проверка IP-адресов на совпадение с данными списка подозрительных серверов
<ul style="list-style-type: none"> ▪ Отправка сообщений и смс 	<ul style="list-style-type: none"> ▪ Сокращение очереди нерешенных дел
<ul style="list-style-type: none"> ▪ Получение сообщений и смс 	<ul style="list-style-type: none"> ▪ Перенос данных в хранилища
<ul style="list-style-type: none"> ▪ Динамичное добавление рекламы 	<ul style="list-style-type: none"> ▪ Интегрирование чужих приложений обработки данных
<ul style="list-style-type: none"> ▪ Ведение "черных" списков и проверка имен 	<ul style="list-style-type: none"> ▪ Распознавание устройств
<ul style="list-style-type: none"> ▪ Определение необычного поведения 	<ul style="list-style-type: none"> ▪ Ведение функциональной статистики
<ul style="list-style-type: none"> ▪ Сбор данных для отражения угроз нарушения защиты и мошенничества 	<ul style="list-style-type: none"> ▪ Настройка приложений чужой разработки
<ul style="list-style-type: none"> ▪ Определение географического положения 	