InfoWatch Traffic Monitor Enterprise

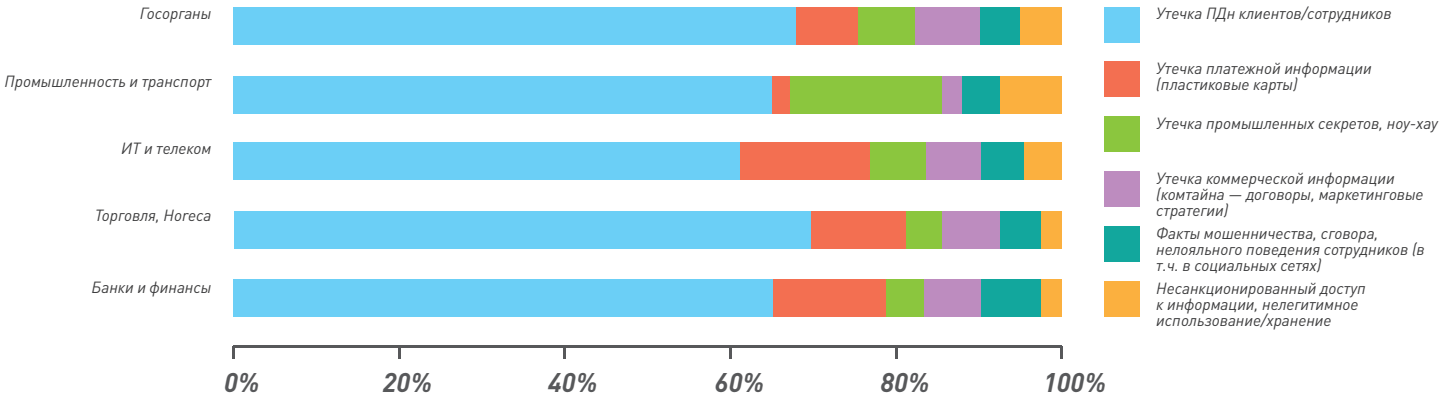
Комплексный контроль потоков движения корпоративной информации

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Вопрос контроля информации, которая представляет реальную ценность для компании, актуален для бизнеса не только с точки зрения предотвращения возможных финансовых потерь от ее утечки, но и защиты репутации, привлечения к ответственности нарушителей, выявления и сокращения количества инцидентов.

На сегодняшний день в компаниях различных сфер бизнеса количество внутренних атак превышает количество внешних. По статистике, около 80% инцидентов происходит внутри компании и организовано ее сотрудниками. Такие злоумышленники используют слабые места в бизнес-процессах компании, знают «уязвимые» места и имеют доступ к секретной информации.

Картина инцидентов по отраслям, доли



DLP-система *InfoWatch Traffic Monitor* — единственное средство информационной безопасности, которое решает исключительно бизнес-задачи:

- помогает бизнесу получить уверенность в безопасности ценных и конфиденциальных данных
- дает понимание всех внутренних и внешних потоков информации в организации
- позволяет выявить сговоры, злоумышленников, лиц, занимающихся промышленным шпионажем, а также круг причастных лиц
- помогает осуществлять бизнес-разведку с целью контроля деятельности персонала и определения степени его лояльности к компании
- формирует доказательную базу по инцидентам для дальнейшего юридического преследования нарушителей

77% всех российских утечек носят явно злонамеренный характер

Стоимость внедрения и обслуживания системы защиты корпоративной информации и данных от внутренних угроз соизмерима с объемом потерь от одного небольшого инцидента.

Главной особенностью решения InfoWatch является вовлечение бизнес-подразделений в управление безопасностью — HR-служба, владельцы информации, топ-менеджеры. Это позволяет свести к минимуму угрозы со стороны собственного персонала, минимизировать риски.

***InfoWatch Traffic Monitor Enterprise* — комплексное решение, которое охватывает организационные, технические и юридические вопросы обеспечения внутренней безопасности компании:**

ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ: *Pre-DLP*

- аудит состояния информационной безопасности в компании
- категоризация информационных ресурсов
- разработка регламентирующей документации
- внесение изменений в режим коммерческой тайны

ТЕХНИЧЕСКИЕ АСПЕКТЫ: *DLP*

- внедрение технических средств DLP
- настройка технических средств в соответствии с разработанными регламентами и отраслевой спецификой
- техническое сопровождение DLP-системы

ЮРИДИЧЕСКИЕ АСПЕКТЫ: *Post-DLP*

- юридически значимая база инцидентов
- получение криминалистически правильных цифровых доказательств правонарушения
- юридически грамотное сопровождение внутренних расследований

InfoWatch Traffic Monitor Enterprise

СОВРЕМЕННОЕ РЕШЕНИЕ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ, КОНТРОЛЯ ПОТОКОВ ДВИЖЕНИЯ ИНФОРМАЦИИ КАК В РАМКАХ КОРПОРАТИВНОЙ СЕТИ, ТАК И ЗА ЕЕ ПРЕДЕЛЫ, А ТАКЖЕ ЗАЩИТЫ ПРЕДПРИЯТИЯ ОТ ВНУТРЕННИХ УГРОЗ

Продукт состоит из нескольких модулей:

1. **InfoWatch Traffic Monitor** — модуль для контроля сетевых каналов передачи данных
2. **InfoWatch Device Monitor** — модуль для защиты рабочих станций, осуществляющий контроль печати и копирования документов на съемные носители, а также позволяющий производить контроль портов и съемных устройств
3. **InfoWatch Crawler** — модуль для контроля информации в общедоступных сетевых хранилищах и системах документооборота, осуществляет сканирование и применение политик к информации, хранящейся «в покое», а также поддерживает в актуальном состоянии эталонные документы и выгрузки
4. **InfoWatch Forensic Storage** — специализированное хранилище, содержащее архив всех информационных потоков организации, в том числе нарушения политик безопасности и факты утечек конфиденциальной информации; является юридически значимой доказательной базой при проведении внутрикорпоративного расследования инцидентов и в ходе судебных разбирательств

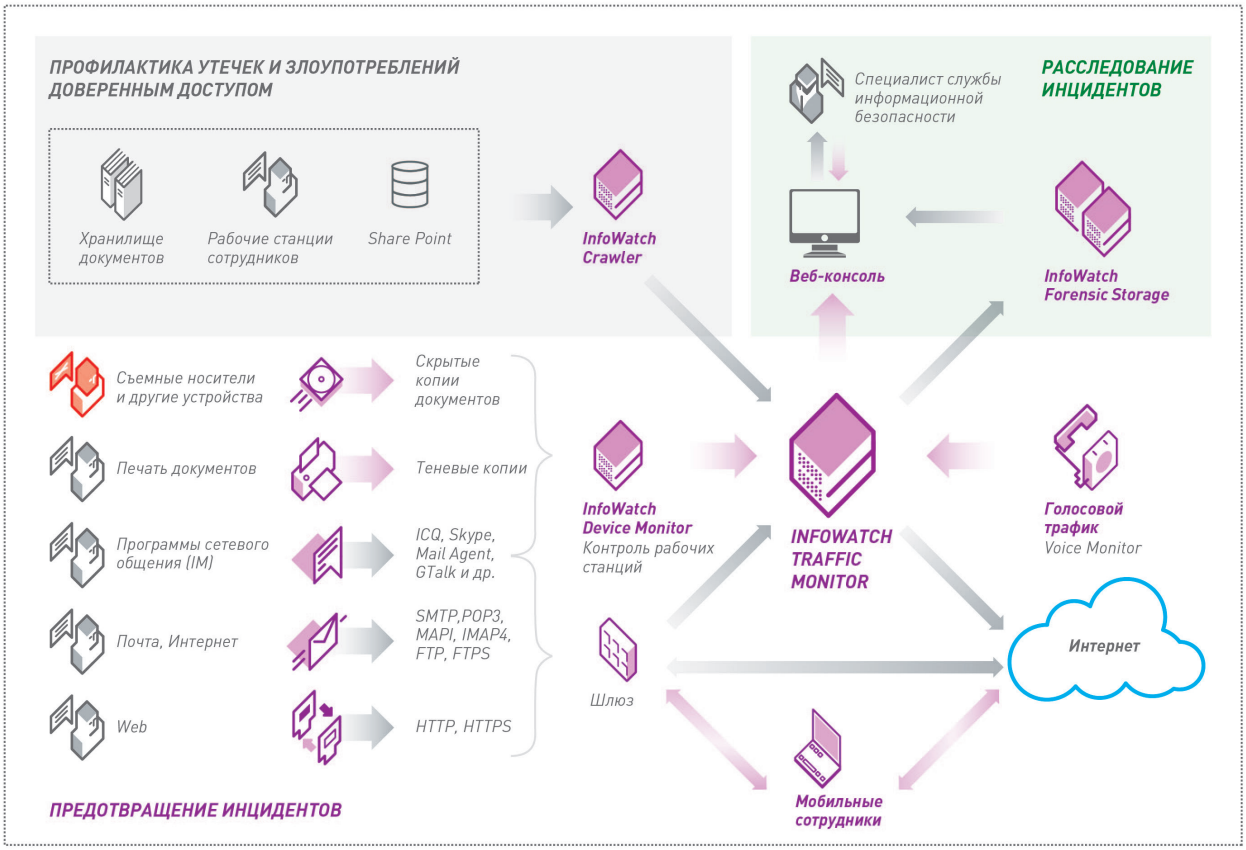
Программные агенты *Device Monitor*, установленные на рабочих станциях, контролируют локальные процессы обработки информации. При сохранении документов на съемные носители агент создает идентичную копию этого документа, а при печати — его графическую копию. Созданные документы называются теневыми копиями. Теневые копии передаются на сервер *Traffic Monitor* для дальнейшего анализа.

Передача информации через сетевые каналы передачи данных (web-сервисы, почтовые и файловые сервера, сервисы мгновенных сообщений) осуществляется через сетевой шлюз и контролируется модулем сетевого перехвата, который также передает перехваченные данные на сервер *Traffic Monitor.*

Если в потоке передаваемых данных была выявлена конфиденциальная информация и система классифицировала эту передачу как инцидент, автоматически срабатывает режим защиты, и запускается процедура реагирования на инцидент, например, происходит блокирование передачи информации, отправитель получает предупредительное сообщение, или оповещение приходит лицу, ответственному за информационную безопасность. Информация об инциденте вместе с копией перехваченного документа сохраняется в архиве.

Модуль *InfoWatch Crawler* сканирует общедоступные сетевые хранилища данных и системы документооборота и создает теневые копии найденных документов. Теневые копии передаются на сервер *Traffic Monitor* для дальнейшего анализа и применения политик.

Сервер *Traffic Monitor* выполняет анализ полученных данных и автоматически выносит вердикт, является ли операция нарушением политики безопасности. Если политика безопасности требует предотвращения передачи данных, *Traffic Monitor* осуществляет блокирование выполнения операции. Все перехваченные данные и результаты их анализа сохраняются в *InfoWatch Forensic Storage.*



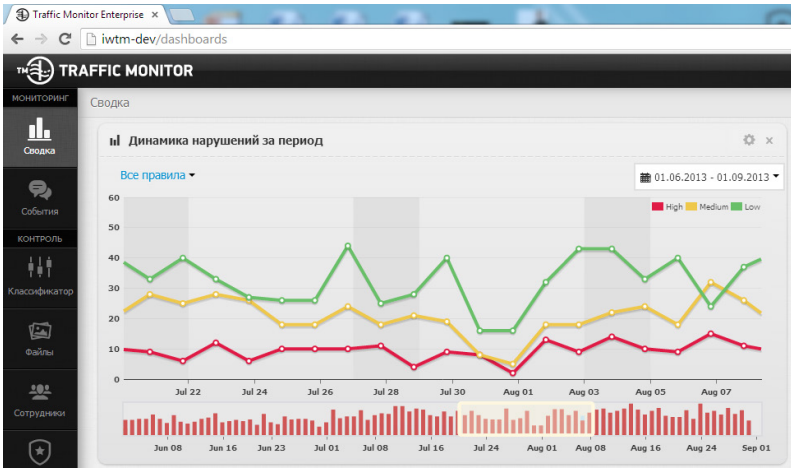
ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ
InfoWatch Traffic Monitor Enterprise

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

осуществляется через мониторинг, перехват и анализ всех информационных потоков компании, с учетом установленных политик информационной безопасности и правил. Вердикт о разрешении или блокировке передачи данных выносится автоматически благодаря технологиям, которые позволяют точно детектировать конфиденциальные данные «на лету», а также автоматически классифицировать информацию. Технологии InfoWatch позволяют распознавать документы и понимать их смысл даже при анализе небольших фрагментов текста, которые могут быть вставлены в любой документ или отправлены в неформальной переписке или через систему мгновенного обмена сообщениями.

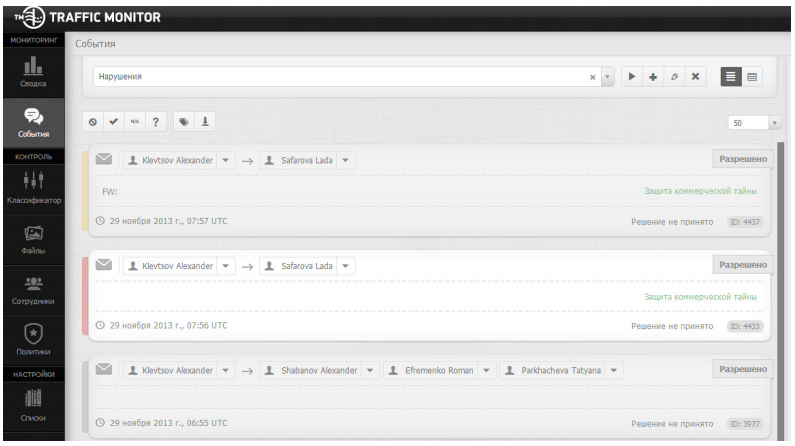
***InfoWatch Traffic Monitor* осуществляет:**

- контроль информации, передаваемой через корпоративную почтовую систему, интернет-ресурсы, средства общего доступа к файлам (SMTP, HTTP, HTTPS, FTP)
- контроль систем обмена сообщениями (ICQ, Skype, Mail.ru Агент, GTalk и другие)
- контроль голосового трафика (Skype)
- контроль использования устройств и портов на рабочих станциях
- контроль сетевых соединений на рабочих станциях
- теневое копирование распечатываемых и копируемых на съемные носители документов
- предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае нарушения политики безопасности



Контроль выгрузок из бизнес-приложений

Современные бизнес-приложения — это необходимый инструмент, который помогает организациям принимать более эффективные решения, сокращать расходы и повышать производительность труда. В них хранится огромный объем корпоративных данных, в том числе конфиденциальных. Обнаружение выгрузок таких данных из бизнес-приложений осуществляется с помощью технологии «Детектор выгрузок из баз данных», которая оперативно реагирует на передачу данных, блокирует несанкционированное распространение и позволяет использовать цифровые доказательства в случае наступления инцидента для проведения расследования или судебного разбирательства.



Контроль бумажных копий документов

InfoWatch Traffic Monitor контролирует и перехватывает задания на печать независимо от типа и модели используемого принтера, а также позволяет отслеживать количество напечатанных копий документов. Помимо контроля бумажных копий *InfoWatch Traffic Monitor* отслеживает движение отсканированных документов благодаря технологии OCR (мгновенное распознавание изображений), выявляет принадлежность скан-копии документу, содержащему конфиденциальные данные, и контролирует их перемещение внутри организации и за ее пределы.

Контроль актуальных версий документов

Продукт позволяет автоматически обновлять базу цифровых отпечатков при изменении их источника, благодаря чему детектор объектов всегда работает с актуальной базой эталонных документов.

Устранение нелегитимного хранения данных

Владельцы защищаемой информации могут самостоятельно формировать политики информационной безопасности в системе *InfoWatch Traffic Monitor.* В целях предотвращения нарушений реализована возможность уведомления руководителя о нелегитимном хранении конфиденциальных данных сотрудником. Это позволяет предотвратить как простую халатность в обращении с информацей, так и вероятную злонамеренную утечку.

ВЫЯВЛЕНИЕ НЕЛОЯЛЬНЫХ СОТРУДНИКОВ И ЗЛОУМЫШЛЕННИКОВ

Мониторинг сотрудников в «группе риска»

Благодаря встроенным инструментам взаимодействия с HR-службой, *InfoWatch Traffic Monitor* учитывает больше данных для формирования картины угроз, чем традиционные DLP-системы. Продукт позволяет настраивать и применять особые целевые политики контроля персонала, входящего в т.н. «группу риска» с созданием специальных отчетов по активности подобных сотрудников.

К примеру, HR-специалист компании может включить в «группу риска» сотрудников, находящихся на испытательном сроке или планирующих уволиться, и к ним автоматически будет применяться более строгая политика безопасности.

Нарушители — «как на ладони»

InfoWatch Traffic Monitor идентифицирует нарушителей и круг причастных лиц, ведет статистику нарушений, что позволяет предупредить наиболее опасные угрозы, включая комбинированные (внутренние и внешние нарушители, действующие в сговоре). Вся информация хранится в единой базе для дальнейшего расследования инцидентов, построения отчетов и оперативного реагирования на инцидент.

Продукт представляет информацию о нарушениях в разрезе:

- выбранного периода времени
- уровня нарушения: низкий, средний, высокий
- типов нарушенных правил: передачи, хранения и копирования

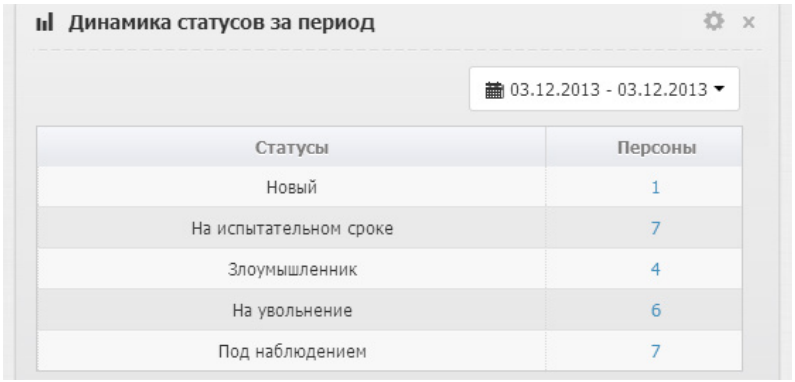
Контроль злоупотребления доступом

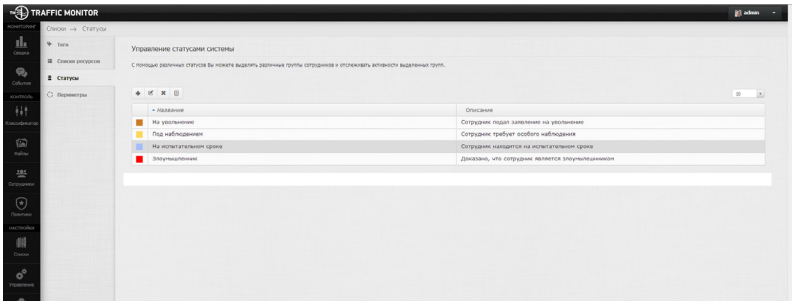
InfoWatch Traffic Monitor позволяет задать разные уровни нарушений с учетом того, кто, в каком объеме и к каким категориям данных имеет доступ. Для каждого уровня нарушения задается соответствующая реакция. Благодаря функции контроля злоупотребления доступом офицер безопасности может выявить как факты злонамеренного нарушения политик, так и случаи халатного отношения сотрудников к конфиденциальным данным.

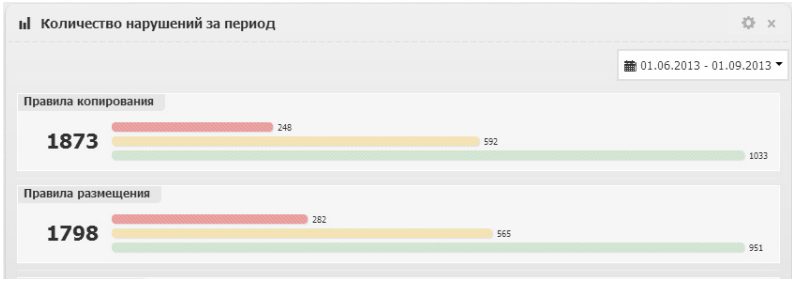
Контроль мобильных сотрудников

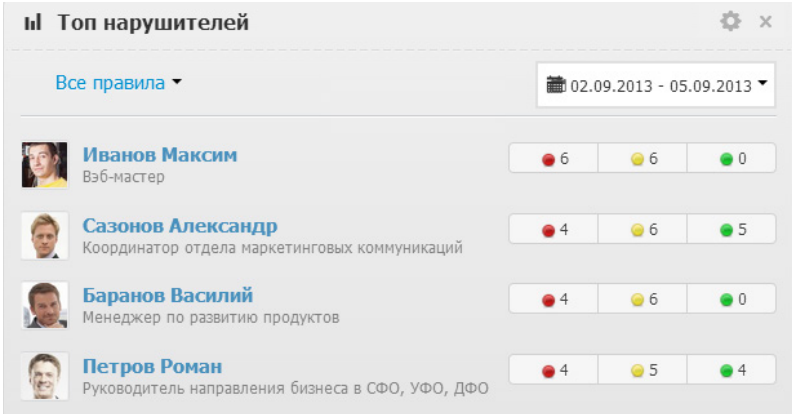
InfoWatch Traffic Monitor осуществляет:

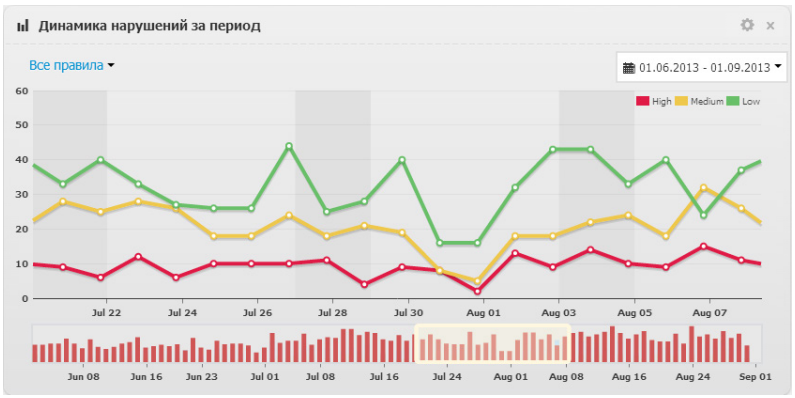
- анализ и контроль всех сообщений при работе сотрудников с корпоративной почтой через мобильные устройства под управлением iOS, Android и т.д.
- мониторинг информации на ноутбуках в периметре и за пределами компании: агентская часть продукта продолжает работать, даже когда рабочие ноутбуки вынесены за пределы компании, и передает полученную информацию в подсистему анализа при их возвращении в корпоративную сеть
- благодаря технологии контроля сетевых соединений, ноутбуки, находящиеся за периметром компании, могут выходить в Интернет только через шлюз корпоративной сети, что гарантирует контроль всего сетевого трафика











РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

InfoWatch Traffic Monitor поможет предотвратить утечку конфиденциальной информации, защитить интеллектуальную собственность, а также расследовать инциденты информационной безопасности, связанные с неправомерными действиями сотрудников, выявить сговоры, злоумышленников и причастных лиц.

InfoWatch Forensic Storage — архив всей перехваченной информации, позволяет отследить маршруты движения информации, случаи нецелевого использования корпоративных ресурсов, определить отправителя и получателя данных и представляет собой надежную доказательную базу для глубокого анализа и расследования инцидентов, связанных с утечкой конфиденциальной информации.

Преимущества:

- объем хранимой информации ограничивается лишь возможностями СУБД и аппаратной платформы, что позволяет осуществлять хранение данных за неограниченный период времени
- решение масштабируемо при увеличении объемов передаваемой информации, может использоваться в организациях с филиальной структурой
- функция зон ответственности позволяет реализовать различные модели доступа сотрудников к сохраненным данным
- реализована возможность ограничения просмотра содержимого перехваченной информации, что позволяет соблюсти право на тайну переписки
- выгрузка хранимой информации возможна как в исходном виде, так и с результатами анализа
- полнотекстовый поиск осуществляется по содержимому перехваченных сообщений и вложений
- мониторинг активности сотрудников можно осуществлять в режиме «реального времени»

DLP-система InfoWatch и уникальная методология внедрения дают компаниям необходимый набор инструментов как для проведения внутренних расследований, так и для дальнейшей правовой защиты собственных интересов.

Преимущества подхода InfoWatch к внедрению DLP-системы:

- DLP-система оказывается «заточенной» под решаемую бизнесом задачу
- вся информация в компании классифицирована с точки зрения конфиденциальности: известно что «ловить» и что защищать
- есть документация и регламенты по использованию системы в компании, а также скорректирован или введен режим коммерческой тайны
- детектирование «на лету» конфиденциальных данных, причем не только тех, что были в базе, но и любых новых писем и документов
- отслеживание маршрутов движения информации, случаев нецелевого использования корпоративных ресурсов
- детектирование и перехват инцидентов в соответствие с составленными методиками
- осуществление контроля за соблюдением разработанных и внедренных политик ИБ, при необходимости их оперативная корректировка
- подготовка доказательств для разбирательства как внутри компании, так и в суде

INFOWATCH ОБЛАДАЕТ ОБШИРНОЙ ЭКСПЕРТИЗОЙ И ОПЫТОМ РЕАЛИЗАЦИИ ПРОЕКТОВ ЛЮБОЙ СЛОЖНОСТИ

НЕФТЕГАЗОВАЯ ОТРАСЛЬ

Транснефть, TVEL, ЛУКОЙЛ, Газпром, TATNEFT, Сургутнефтегаз

ЭНЕРГЕТИКА

РусГидро, Русгидро Энерго Ресурс, e.on

ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

МЧС России, Федеральная таможенная служба, Министерство финансов РФ, Арбитражный суд Москвы

ПРОИЗВОДСТВО

SUKHOI, GAZ GROUP, Магнитогорский металлургический комбинат, УГМК

БАНКИ

Райффайзенбанк, Сбербанк, Связь Банк, Возрождение Банк, РосЕвроБанк, Банк Москвы, ВТБ, Газпромбанк

ТЕЛЕКОММУНИКАЦИИ

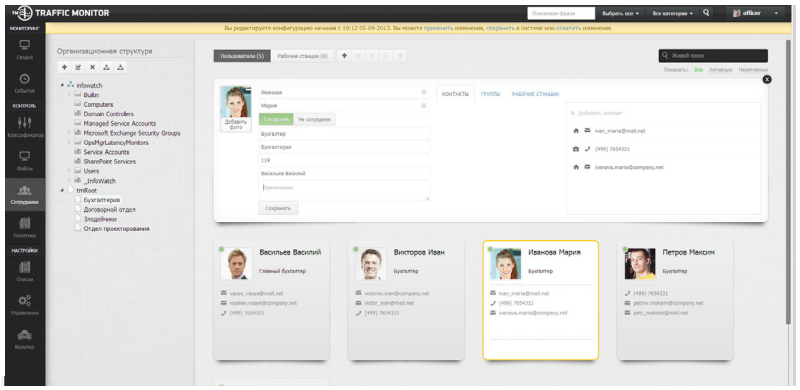
Билайн, МТС, МегаФон

InfoWatch Traffic Monitor

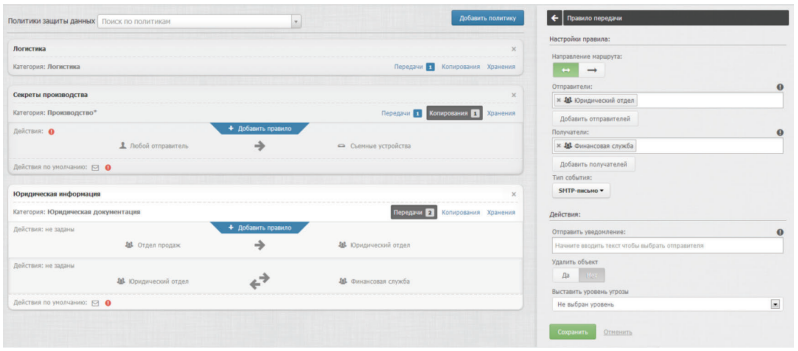
Ключевые преимущества решения

***InfoWatch Traffic Monitor* — единственное решение, которое рассчитано на крупные организации с большим объемом анализируемого трафика и территориально распределенной структурой:**

- Мощное высокопроизводительное **решение класса Enterprise**
- Точное детектирование конфиденциальных данных «на лету», **автоматическая классификация информации**
- **Удобный пользовательский web-интерфейс:** управлять системой можно с любой рабочей станции независимо от используемой операционной системы (Windows, Linux, Apple Mac OS) и браузера
- **Идентификация сотрудников-нарушителей:** карточки сотрудников и связей
- Сбор юридически значимой **доказательной базы** для расследования инцидентов
- Модульность и **гибкая схема интеграции** в ИТ-инфраструктуру
- Специализированные **отраслевые решения** (разработаны базы контентной фильтрации для компаний различных отраслей: финансовых учреждений, телекоммуникационных операторов, страховых компаний, государственных структур, энергетических компаний)



- **Высокая кастомизируемость** *InfoWatch Traffic Monitor* позволяет создавать специализированные решения под уникальные бизнес-процессы компании
- **Вовлечение всех бизнес-подразделений компании в управление безопасностью корпоративных данных** — HR-служба, юридический департамент, маркетинг, топ-менеджеры и т.д. с возможностью предоставления ролевого доступа для разных групп пользователей
- **Максимальная гибкость и управляемость:** задачи бизнеса меняются, поэтому службе ИБ необходимы надежные инструменты для адаптации политик информационной безопасности, отражающих весь спектр рисков и угроз потерь информации, защиты предприятия от внутренних угроз



- **Высокая надежность и отказоустойчивость решения:** решение *InfoWatch Traffic Monitor* поддерживает схему кластеризации, что позволяет повысить масштабируемость и отказоустойчивость решения. При увеличении количества пользователей или повышении интенсивности их работы достаточно добавить дополнительные сервера с производительностью, пропорциональной увеличению обрабатываемого потока данных. *InfoWatch Crawler* имеет встроенные средства контроля нагрузки, оказываемой на сеть организации
- **Сертификация:** НДВ 4, ИСПДн до 1 класса включительно, Газпромсерт, аккредитация ЦБ РФ, ФСБ России

INFOWATCH — ПЕРВЫЙ РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ ЗАЩИТЫ ОТ УТЕЧЕК В МАГИЧЕСКОМ КВАДРАНТЕ GARTNER

Исследовательская компания Gartner включила *InfoWatch* в «магический квадрант» Content-Aware Data Loss Prevention. *InfoWatch* — первая и пока единственная российская компания, чей продукт — *InfoWatch Traffic Monitor Enterprise* — получил столь высокую оценку международных экспертов.