РЕШЕНИЯ INFOWATCH
ДЛЯ РАЗЛИЧНЫХ ОТРАСЛЕЙ ЭКОНОМИКИ

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

InfoWatch Traffic Monitor Enterprise – это комплексное решение, которое предназначено для защиты корпоративной информации крупных организаций с учетом отраслевой специфики.

БАНКИ

- Предотвращение утечки персональных данных клиентов
- Снижение рисков юридического преследования из-за противоправных действий сотрудников
- Обеспечение соответствия требованиям регуляторов
- Защита планов развития и запуска продуктов
- Контроль использования корпоративных ресурсов
- Автоматическая категоризация информационных потоков и построение маршрутов распространения информации

НЕФТЕГАЗОВАЯ ОТРАСЛЬ

- Защита операционных данных, связанных с нефте/газодобычей
- Защита планов разработки месторождений от конкурентной разведки и промышленного шпионажа
- Консолидация в едином хранилище информации, собираемой с множества географически-распределенных площадок
- Снижение репутационных рисков, связанных с возможными утечками информации о контрагентах, клиентах, партнерах и потребителях, а также о чрезвычайных ситуациях на производстве

ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

- Защита конфиденциальной информации и персональных данных от утечки и нецелевого использования
- Построение маршрутов распространения информации для оптимизации процессов
- Контроль нецелевого использования служебных информационных систем
- Выявление нелояльных и неэффективных сотрудников

ТЕЛЕКОММУНИКАЦИИ

- Минимизация риска утечки персональных данных абонентов
- Выполнение требований отраслевых регуляторов и закона о персональных данных
- Защита конфиденциальной информации от конкурентной разведки и промышленного шпионажа
- Построение маршрутов распространения информации для оптимизации бизнес-процессов
- Управление репутационными и юридическими рисками, связанными с неосторожными и противоправными действиями сотрудников

КОРПОРАЦИИ

- Автоматическая категоризация информационных потоков и построение маршрутов распространения информации
- Защита интеллектуальной собственности
- Выявление нелояльных сотрудников
- Инструмент для проведения расследований инцидентов
- Защита персональных данных клиентов
- Обеспечение соответствия требованиям регуляторов
- Защита информации от утечки и несанкционированного обращения

Райффайзенбанк

За полгода промышленной эксплуатации с помощью InfoWatch Traffic Monitor были выявлены 369 инцидентов нарушения информационной безопасности.

Возрождение Банк

Компания Infowatch — зарекомендовавший себя производитель, с успешным опытом внедрения решений в крупнейших банках России.

Банк Москвы

Наша организация методом проб нашла свои решения, которые устраивают именно нас, — они РАБОТАЮТ для нас. Это решения компании Infowatch.

ЛУКОЙЛ Нефтяная компания

InfoWatch Traffic Monitor Enterprise, внедренный компанией, обеспечивает полноценный контроль над информационными потоками с различными сценариями реакции на нарушения политики безопасности.

РЕШЕНИЯ INFOWATCH УЖЕ ИСПОЛЬЗУЮТ:

НЕФТЕГАЗОВАЯ ОТРАСЛЬ

Транснефть · TVEL · ЛУКОЙЛ Нефтяная компания · Газпром · TATNEFT · Сургутнефтегаз Открытое акционерное общество

ЭНЕРГЕТИКА

РусГидро · РусГидро Энерго Ресурс · e.on

ГОСУДАРСТВЕННЫЕ СТРУКТУРЫ

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

ПРОИЗВОДСТВО

SUKHOI · GAZ GROUP · Открытое акционерное общество Магнитогорский металлургический комбинат · УГМК

БАНКИ

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

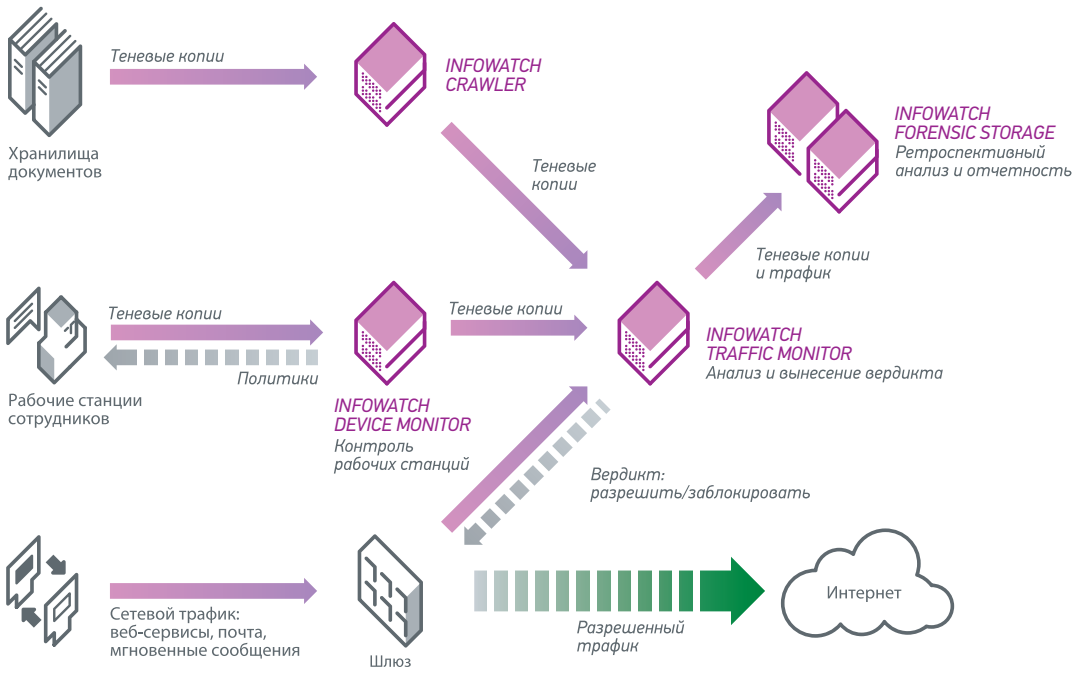
ТЕЛЕКОММУНИКАЦИИ

Билайн · МТС · МегаФон

INFOWATCH TRAFFIC MONITOR ENTERPRISE

ПРОДУКТ СОСТОИТ ИЗ НЕСКОЛЬКИХ МОДУЛЕЙ

- *InfoWatch Traffic Monitor* – модуль, осуществляющий контроль сетевых каналов передачи данных
- *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.
- *InfoWatch Crawler* – модуль для контроля информации в общедоступных сетевых хранилищах и системах документооборота. Осуществляет сканирование и применение политик к информации, хранящейся «в покое».
- *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 расследования инцидента и в ходе судебных разбирательств.



Программные агенты *Device Monitor*, установленные на рабочих станциях, контролируют действия сотрудников. 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*.

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 ведикт, 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*.

ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

INFOWATCH TRAFFIC MONITOR ENTERPRISE ОСУЩЕСТВЛЯЕТ

- Мониторинг и анализ данных, отправляемых за пределы организации через почтовые системы, web, системы обмена сообщениями, распечатываемые и копируемые на съёмные носители
- Автоматическую классификацию передаваемой информации
- Предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае обнаружения нарушения политики безопасности
- Безопасное хранение данных для анализа и проведения расследований

МОНИТОРИНГ ИНФОРМАЦИИ

- 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 agent, GTalk и другие)
- Контроль использования устройств и портов на рабочих станциях
- Теневое копирование распечатываемых и копируемых на съемные носители документов

АНАЛИЗ И ПРИНЯТИЕ РЕШЕНИЯ

- Комбинированный контентный анализ с помощью нескольких технологий: цифровые отпечатки, детектор объектов и лингвистический анализ для точного выявления конфиденциальных данных
- Специализированные Базы контентной фильтрации для компаний различных отраслей: энергетических и финансовых учреждений, телекоммуникационных операторов, страховых компаний, гос. структур
- Распознавание всех популярных форматов хранения данных, извлечение текстовой информации из отсканированных документов
- Автоматическое принятие решения о разрешении или блокировке передачи данных

ХРАНЕНИЕ И ОТЧЕТНОСТЬ

- Сохранение полного архива всех информационных потоков
- Встроенная графическая система отчетности: более 60 шаблонов с возможностью создания собственных
- Возможность задания зон ответственности сотрудников службы информационной безопасности для разграничения доступа к хранящейся информации
- Выгрузка хранимой информации, как в исходном виде, так и с результатами анализа
- Полнотекстовый поиск по содержимому перехваченных сообщений и вложений
- Возможность мониторинга активности сотрудников в режиме «реального времени»

НАДЕЖНОСТЬ И ОТКАЗОУСТОЙЧИВОСТЬ

Оба компонента решения - *InfoWatch Device Monitor* и *InfoWatch Traffic Monitor* поддерживают 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.

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Точное детектирование конфиденциальных данных и специализированные отраслевые решения
- Идентификация сотрудников-нарушителей
- Автоматическая классификация информации
- Сохранение информации и результатов анализа в едином архиве на неограниченный срок
- Возможность сбора юридически значимой доказательной базы для расследования инцидентов
- Отказоустойчивость и высокая производительность (до 400 Мбит/с)
- Модульность и гибкая схема интеграции в IT-инфраструктуру

КОНЦЕПЦИЯ ЭФФЕКТИВНОГО ВНЕДРЕНИЯ И ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ

PRE-DLP	DLP	POST-DLP
• Аудит состояния информационной безопасности в компании	*• Внедрение технических средств DLP*	*• Получение криминалистически правильных цифровых доказательств правонарушения*
• Категоризация информационных ресурсов	*• Настройка технических средств в соответствии с разработанными регламентами*	*• Юридическое сопровождение внутренних расследований*
• Разработка регламентирующей документации	*• Техническое сопровождение DLP системы*	*• Юридическое преследование злоумышленников*

В РЕЗУЛЬТАТЕ PRE-DLP КОМПАНИЯ ПОЛУЧАЕТ

- Оценку текущего состояния режима коммерческой тайны и порядка обращения с информацией, содержащей коммерческую тайну
- Установленный режим коммерческой тайны, который полностью соответствует законодательству
- Юридически грамотно составленное «Положение о коммерческой тайне» и сопутствующие документы:
  - позволяют минимизировать правовые риски Компании в случае наступления инцидентов ИБ
  - обеспечивают возможность юридического преследования виновного лица

НА ЭТАПЕ ЭКСПЛУАТАЦИИ DLP-СИСТЕМЫ

На основе регламентирующих документов созданных на этапе Pre-DLP, производится тонкая настройка правил обработки информационных потоков. Это обеспечивает соответствие настроек технического средства DLP регламентам, принятым в компании. Благодаря этому подходу и наличию централизованного архива InfoWatch Forensic Storage компания получает:

- Предотвращение неправомерного доступа к конфиденциальной информации
- Выявление «инсайдеров», лиц, занимающихся промышленным шпионажем, халатности персонала при работе с конфиденциальной информацией
- Инструменты анализа и бизнес-разведки (BI – Business Intelligence) в целях контроля деятельности персонала и определения степени их лояльности компании
- Автоматический сбор цифровых доказательств в распределенных сетевых корпоративных средах с учётом правовых особенностей Государства
- Оперативное отслеживание состояния информационной безопасности с помощью отчетности
- Неограниченный объем хранения собранных данных

В СОСТАВЕ УСЛУГИ POST-DLP КОМПАНИЯ ПОЛУЧАЕТ

- Поддержку, в случае наступления инцидента информационной безопасности
- Юридическое сопровождение внутрикорпоративных расследований инцидентов
- Организацию юридического преследования злоумышленников:
  - Криминалистически правильную фиксацию и снятие копий энергозависимых данных на внешний цифровой носитель информации
  - Корректное изъятие компьютерных носителей информации, их упаковка и опечатывание
  - Пакет документации об инциденте, оформленный в соответствии с нормативно-правовыми актами РФ
  - Юридически грамотно составленное заявление в правоохранительные органы об инциденте ИБ, следствием чего будет являться возбуждение уголовного дела, дальнейшее привлечение злоумышленника к ответственности и компенсация нанесенного ущерба
  - Представление интересов Компании при производстве «внешних» расследований

Данный подход предоставляет возможность для юридического преследования лица, виновных в утечке конфиденциальной информации, а также позволяет защитить коммерческую тайну и иную конфиденциальную информации компании.

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Свяжитесь с нами, чтобы запросить демонстрацию или заказать пилотный проект:

+7 (495) 22-900-22
sales@infowatch.ru, www.infowatch.ru