InfoWatch Traffic Monitor Enterprise

Контроль и классификация информационных потоков

В современных организациях информационный обмен производится с помощью разнообразного программного обеспечения. Корпоративная почтовая система, web-доступ к рабочему почтовому ящику, системы мгновенных сообщений, Skype, съёмные устройства хранения – популярные технические средства, позволяющие передавать информацию между сотрудниками и контрагентами.

Традиционные организационные меры, запрещающие использование определённого программного обеспечения, закрывающие доступ к съёмным носителям или ограничивающие использование собственных ноутбуков и мобильных устройств, становятся неэффективными в современном мире. Наличие формальной политики безопасности и тренинги сотрудников не гарантируют исполнение политики, так как в большинстве случаев в компаниях нет точного понимания, какие конкретно документы или сведения не подлежат распространению.

По оценкам экспертов только около 20% конфиденциальных данных структурировано, 10% изменяется ежедневно, а вновь созданные документы составляют примерно 10% всей конфиденциальной информации компании. Дополнительные сложности создаёт непрерывный рост объёмов информации, обрабатываемой современными организациями ежедневно. В результате риск намеренной или непреднамеренной утечки только растёт.

В сегодняшних условиях эффективными становятся не запретительные меры, а всесторонний контроль над информационными потоками и их обработка в соответствии с политикой информационной безопасности.

Специально для компаний, заинтересованных в защите своих конфиденциальных данных, компания InfoWatch разработала комплексное решение для контроля информационных потоков – InfoWatch Traffic Monitor Enterprise. Решение позволяет компаниям определить, кто использует конфиденциальную информацию, как она передается и кто имеет к ней доступ. Система автоматически выполняет классификацию передаваемой информации, позволяет оценить степень её защищённости и динамически отслеживать риски утечек чувствительной информации.

Средние затраты на устранение последствий одного инцидента разглашения данных в 2011 году составили около 5,5 млн. долл. США

Ponemon Institute,
Cost of a Data Breach Study 2012

ЗАО «Райффайзенбанк», один из самых надежных банков России, использует InfoWatch Traffic Monitor для обеспечения необходимого банку уровня безопасности конфиденциальных данных. За полгода промышленной эксплуатации с помощью InfoWatch Traffic Monitor были выявлены 369 инцидентов нарушения информационной безопасности.

Райффайзен БАНК

InfoWatch Traffic Monitor Enterprise для защиты корпоративной информации

InfoWatch Traffic Monitor Enterprise – комплексное модульное решение по защите информации от внутренних угроз, которое позволяет контролировать различные каналы утечки данных. Решение состоит из следующих модулей:

InfoWatch Traffic Monitor - защита периметра сети

- InfoWatch Traffic Monitor for Web - для контроля данных, передаваемых с помощью web-почты, блогов, форумов и других Интернет-ресурсов.
- InfoWatch Traffic Monitor for HTTPS - для контроля данных, передаваемых с помощью зашифрованного Интернет-протокола.
- InfoWatch Traffic Monitor for Mail - для контроля информации, проходящей через корпоративную почтовую систему.
- InfoWatch Traffic Monitor for IM для контроля систем обмена мгновенными сообщениями, работающими по протоколу OSCAR (ICQ, Miranda и др.), включая перехват файлов и sms.

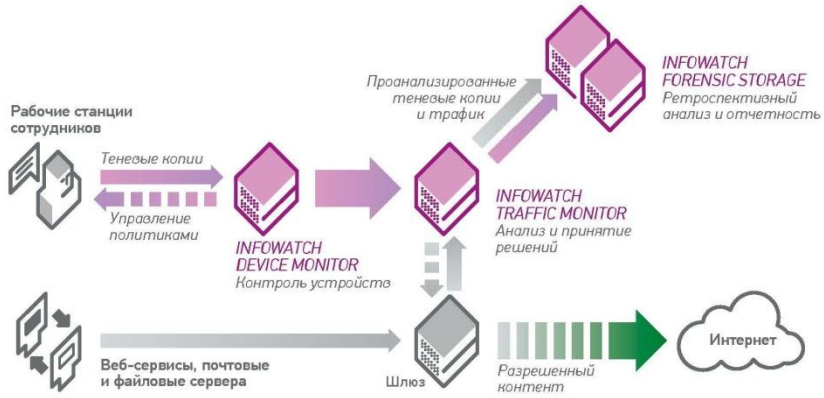
InfoWatch Device Monitor - защита рабочих станций

- InfoWatch Device Monitor for Devices – для контроля доступа и копирования информации на съёмные носители. Контролирует устройства, подключаемые по портам COM, LPT, USB (всего 26 различных типов устройств).
- InfoWatch Device Monitor for Print – для контроля печати документов посредством сетевых и локальных принтеров.
- InfoWatch Device Monitor for Skype – для контроля мгновенных сообщений и передачи файлов и sms-сообщений посредством приложения Skype.

InfoWatch Forensic Storage - централизованное архивирование

Архив всей перехваченной информации для дальнейшего проведения расследований нарушений политики безопасности и составления аналитических отчетов.

Взаимодействие элементов системы показано на схеме:



InfoWatch Traffic Monitor Enterprise осуществляет:

- Мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых на локальные и сетевые принтеры и копируемых на различные съёмные устройства.
- 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

Кому предназначено решение?

Операторам персональных данных для обеспечения соответствия требованиям нормативных актов, в частности ФЗ-152 «О персональных данных»:

- финансовые учреждения
- медицинские организации
- телекоммуникационные операторы
- страховые компании
- государственные структуры

Компаниям, обладающим интеллектуальной собственностью или ноу-хау для защиты от потери информации, которая может нанести урон финансовым показателям. Например, относящимся к наукоемким отраслям:

- фармацевтика
- энергетика
- производство
- разработка ПО

ОАО «ВымпелКом» (торговая марка Билайн) – один из ведущих российских телекоммуникационных операторов. Использование InfoWatch Traffic Monitor Enterprise помогает Билайн не только обеспечить безопасность конфиденциальных данных, но и соответствовать требованиям нормативных актов Федеральной службы по финансовым рынкам (ФСФР), что положительно сказывается на взаимодействии компании с инвесторами и партнерами.

Функциональные возможности

Работа системы логически состоит из этапов перехвата, анализа и принятия решения, и, наконец, архивирования информации. Данные, хранящиеся в архиве, могут быть использованы для ретроспективного анализа при расследовании инцидентов.

Перехват трафика

С помощью модуля для защиты периметра корпоративной сети осуществляется перехват трафика, отправляемого по протоколам SMTP (корпоративная почта), HTTP (Web), HTTPS[1] (защищенный Web-канал), протоколам систем обмена сообщениями (ICQ и др.).

Модуль для защиты рабочих станций включает в себя агент, который устанавливается на рабочие станции сотрудников и создает теневые копии документов при выполнении операций копировании, печати, общении сотрудников посредством Skype. Затем теневые копии передаются для анализа на сервер InfoWatch Traffic Monitor.

Анализ и принятие решения

Для принятия решения о блокировке передачи информации или дальнейшей её транспортировке система определяет, нарушает ли данный факт передачи корпоративную политику безопасности. Выполняется контентный анализ передаваемых данных, идентификация отправителей и получателей.

Для определения отправителей и получателей используется механизм единой идентификации. Применяется справочник сотрудников с контактными данными, идентифицирующими их в рамках различного информационного обмена: рабочий и домашний e-mail, ICQ UIN, Skype name, Live Journal ID и т.п. Первоначально справочник импортируется из Microsoft Active Directory и в дальнейшем пополняется автоматически системой при перехвате соответствующей информации. Это позволяет осуществить привязку инцидентов к конкретным сотрудникам вне зависимости от протокола передачи данных.

Перед выполнением контентного анализа производится извлечение текстовой информации из переданных сообщений, документов, графических изображений. Система определяет формат файла вне зависимости от его расширения и извлекает все вложенные документы (например, из архивов или файлов Microsoft Office). В извлеченном тексте производится поиск признаков конфиденциальной информации. Комбинирование нескольких технологий анализа позволяет делать это максимально эффективно. Детектор цифровых отпечатков выявляет цитаты заранее заданных эталонных документов. Детектор текстовых объектов находит структурированные последовательности символов, например, номера паспортов, кредитных карточек. Модуль лингвистического анализа автоматически определяет тематику и степень конфиденциальности анализируемого фрагмента информации на основании встречающихся в нем терминов и их сочетаний.

Комбинированные технологии контентного анализа для точного выявления конфиденциальной информации

Выявление конфиденциальной информации является одной из самых сложных задач для систем защиты данных. InfoWatch Traffic Monitor Enterprise включает в себя интеллектуальную систему контентного анализа, комбинирующую несколько технологий и позволяющую выполнять классификацию информации с высокой точностью.

Совместно используются следующие технологии:

- Лингвистический анализ
- Детектор объектов
- Цифровые отпечатки

Благодаря наличию технологии Лингвистического анализа решение защищает даже вновь созданные документы. Подобным документам, как правило, еще не присвоен уровень конфиденциальности и для них не создан цифровой опечаток. Технология адаптирована для 16 языков и для различных отраслей экономики.

Совместное применение нескольких технологий позволяет эффективно использовать достоинства каждой из них и защищать информацию в течение всего жизненного цикла.

[1] *В интеграции с решениями партнеров.*

На финальном этапе анализа данных принимается решение о дальнейшем движении информации – оно либо блокируется, либо разрешается. Правила позволяют определять поведение системы не только в зависимости от результатов анализа, но и на основе формальных атрибутов – канал передачи данных, время передачи, размер и формат файла и тому подобное. Кроме блокировки передачи информации, возможно, задавать дополнительные действия:

- не сохранять в архив
- отметить специальным тэгом
- уведомить нарушителя/офицера

Хранение и ретроспективный анализ данных

Перехваченные данные сохраняются в централизованном архиве InfoWatch Forensic Storage. Архитектура архива ориентирована на работу с информационными потоками крупной организации:

- 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.
- Возможность ограничения просмотра содержимого перехваченной информации, что позволяет соблюсти право на тайну переписки.

Для организации ретроспективного поиска:

- Поиск по широкому спектру критериев: свойствам перехваченных сообщений (получатель, отправитель, дата, время отправки) и результатам анализа информации.
- Полнотекстовый поиск по содержимому перехваченных сообщений и вложений.
- Выгрузка хранимой информации, как в исходном виде, так и с результатами анализа.
- Графическая система отчетности для построения контентных маршрутов, определения наиболее нелояльных сотрудников и статистического анализа.
- Более 60 предустановленных отчетов и возможность создания собственных отчетов.
- Возможность мониторинга активности сотрудников в режиме «реального времени».
- Удобная навигация – настраиваемая система фильтров и каталогов.

InfoWatch Forensic Storage позволяет отследить маршруты движения информации, случаи нецелевого использования корпоративных ресурсов, определить отправителя, получателя данных и представляет собой надежную доказательную базу для расследования инцидентов, поиска утечек конфиденциальной информации.

Извлечение текста из изображений

Многие документы в организациях распространяются в отсканированном виде. Зачастую такими документами являются отсканированные договора, протоколы совещаний. Для того чтобы эти документы могли быть проанализированы средствами контентного анализа ко всей графической информации применяется технология распознавания текста в изображениях OCR (optical character recognition).

ООО «ЛУКОЙЛ-ИНФОРМ» осуществляет информационно-технологическое обеспечением деятельности Группы «ЛУКОЙЛ».

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

Установка и администрирование

Установка InfoWatch Traffic Monitor Enterprise полностью автоматизирована и оказывает минимальное влияние на инфраструктуру компании.

Поддерживается два режима работы системы – копии трафика и блокирующий.

Режим копии трафика не оказывает влияния на бизнес процессы организации и позволяется выполнить первоначальную классификацию информации и настройку системы в соответствии с корпоративной политикой безопасности. В режиме копии трафика решение получает трафик от TAP или SPAN устройств.

Блокирующий режим позволяет предотвращать утечки информации. В этом случае система перехватывает реальный трафик сотрудников организации, получая его от прокси-серверов, поддерживающих протокол ICAP, и от корпоративной почтовой системы. Компонент InfoWatch TMG Plugin используется для интеграции с Microsoft Forefront TMG.

Модуль для защиты рабочих станций устанавливается на рабочие станции сотрудников с помощью средств централизованного управления установкой или с помощью собственного механизма удаленной установки. В него встроена защита от деинсталляции, намеренного вывода из строя и удаления созданных теневых копий документов.

В решение встроен модуль самодиагностики, который следит за состоянием множества параметров системы и в случае превышения допустимых значений оповещает офицеров безопасности и выполняет действия, направленные на стабилизацию состояния.

Производительность и отказоустойчивость

Оба компонента решения - InfoWatch Device Monitor и InfoWatch Traffic Monitor поддерживают схему кластеризации, что позволяет повысить масштабируемость и отказоустойчивость решения.

Максимальная пропускная способность модуля защиты периметра корпоративной сети в схеме кластера составляет - 400 Мбит/с. Максимальная пропускная способность одного плеча кластера составляет 200 Мбит/с.

Производительность модуля защиты рабочих станций ограничивается только возможностями аппаратного обеспечения. При увеличении количества пользователей или повышении интенсивности их работы достаточно добавить дополнительные сервера с производительностью, пропорциональной увеличению обрабатываемого потока данных.

Интеграционные возможности

Для того чтобы встраивание системы в развитую инфраструктуру происходило максимально эффективно InfoWatch Traffic Monitor Enterprise предлагает совместные решения с производителями других программных продуктов:

Прокси-сервера с поддержкой протокола ICAP
Совместное решение с Aladdin eSafe, BlueCoat ProxySG, Cisco IronPort S-Series для перехвата HTTPS-траффика.

Системы документооборота
Интеграция с Oracle IRM для «запечатывания» конфиденциальной информации.

Системы защиты рабочих станций
Интеграция с Device Lock и Lumension Device Conrol для клиентов, которые уже используют эти решения.

Системы обмена сообщениями
Интеграция с Microsoft Lync Server 2010 – средством коммуникации, передачи сообщений, документов, аудио и видео звонков.

Решения для различных отраслей экономики

Специфика деятельности организации определяет, какая именно информация подлежит защите. Например, для финансовых организаций наибольший интерес имеет защита платежной информации, для конструкторского бюро опасность представляет утечка чертежей проектируемых объектов, для компании нефтегазовой отрасли – координат месторождений. Чтобы защита была эффективной, технологии анализа информации должны учитывать специфику деятельности организации. InfoWatch Traffic Monitor Enterprise предоставляет разные наборы правил обработки информации для различных отраслей экономики. Специализированные Базы контентной фильтрации, иерархические справочники категорий, на основании которых выполняется лингвистический анализ, разработаны для следующих отраслей:

- Финансовая (банки, финансовые организации)
- Нефтегазовая
- Телеком
- Страхование
- Разработка программного обеспечения

Что дает InfoWatch Traffic Monitor Enterprise бизнесу?

- Полный контроль над обращением корпоративной информации.
- Предотвращение финансовых или репутационных потерь, связанных с утечкой информации.
- Уверенность в том, что ценная информация не "утекает наружу".
- Соответствие требованиям законодательства.
- Управление рисками, связанными с утечкой данных.
- Мониторинг деятельности сотрудников.
- Обучение сотрудников в области ИБ, улучшение корпоративной культуры.

Решения InfoWatch уже используют более 150 крупнейших компаний России из различных отраслей экономики, в том числе банки, крупнейшие телекоммуникационные операторы, компании нефтегазовой отрасли:

Почему именно InfoWatch Traffic Monitor Enterprise?

Автоматическая классификация передаваемой информации. Сразу после установки решения, вся передаваемая информация начинает подвергаться автоматической классификации. Нет необходимости снимать цифровые отпечатки или выполнять другие трудоемкие действия. Отраслевые Базы контентной фильтрации позволять провести точную классификацию с учетом специфики деятельности организации.

Точное детектирование конфиденциальных данных. Совместное использование нескольких технологий контентного анализа позволяет эффективно использовать достоинства каждой из них и защищать информацию в течение всего жизненного цикла**.**

Идентификация сотрудников-нарушителей. Любое зафиксированное событие будет привязано к карточке отправителя и получателя данных вне зависимости от канала передачи данных. Это достигается благодаря системе Единой идентификации, синхронизации с Microsoft Active Directory и автоматическому пополнению карточек контактной информацией.

Централизованный архив. Сохранение всей информации в архиве позволяет отследить маршруты движения информации, случаи нецелевого использования корпоративных ресурсов, и представляет собой надежную доказательную базу для расследования инцидентов, поиска утечек конфиденциальной информации.

Графическая система отчетности. Позволяет наглядно оценки уровень соответствия организации политикам информационной безопасности, построить графическое представление контентных маршрутов.

Модульность и гибкая схема интеграции в IT-инфраструктуру. Разнообразные схемы внедрения и совместные решения с другими производителями программного обеспечения позволяют гибко интегрировать решение в существующую инфраструктуру организации. Модульное решение позволяет поэтапно расширять функциональность без необходимости переустановки системы.

Высокая производительность и отказоустойчивость. Решение рассчитано на крупные организации с распределенной структурой и большими объемами анализируемого трафика, имеет средства кластеризации и балансировки нагрузки.

Контроль необходимых каналов передачи данных. Комбинированное решение для защиты периметра сети и рабочих станций позволяет контролировать все необходимые каналы передачи данных без излишней дополнительной нагрузки на узлы сети.

Лицензирование InfoWatch Traffic Monitor Enterprise

Централизованное архивирование	InfoWatch Traffic Monitor Forensic Storage Linguistic Analysis with InfoWatch Traffic Monitor Forensic Storage Fingerprints with InfoWatch Traffic Monitor Forensic Storage Templates Analyser with InfoWatch Traffic Monitor Forensic Storage
Защита периметра сети	InfoWatch Traffic Monitor for Web InfoWatch Traffic Monitor for HTTPS InfoWatch Traffic Monitor for Mail InfoWatch Traffic Monitor for IM
Защита рабочих станций	InfoWatch Device Monitor InfoWatch Device Lock Adapter

Системные требования

	Аппаратное обеспечение	Программное обеспечение
Защита периметра сети **InfoWatch Traffic Monitor**	Сервер: HP DL360 G6 CPU: Intel Xeon x86 3GHz, 2 CPU с 4 ядрами RAM 2 GB HD 160GB	Red Hat Enterprise Linux Server R6 x64 МСВСфера 5.2 Сервер
Защита рабочих станций **InfoWatch Device Monitor** **Device Monitor Server**	CPU: Intel Pentium 4 2GHz или выше RAM 1 GB HD 100GB	Windows Server 2003 Service Pack 2, Windows Server 2008 R2 Oracle, MS SQL Server, PostgreSQL, MS SQL Express .NET Framework 3.0
Device Monitor Client	CPU: Intel Pentium 4 2GHz или выше RAM 512 MB	Microsoft Windows 2000 Professional SP 4 (ограниченная поддержка) Windows XP SP3, Windows Vista, Windows 7
Централизованное архивирование **InfoWatch Traffic Monitor Forensic Storage**	Server: HP DL360 G6 CPU: Intel Xeon x86 2.4GHz или выше RAM 4 GB RAID level 1 или выше (200GB)	Oracle RDBMS 11gR2 (11.2.0.1) (входит в комплект поставки и не требует дополнительного лицензирования)
Консоль управления	CPU: Pentium 4, 3GHz RAM: 1 GB	Microsoft Windows XP SP3, Microsoft Windows 7

О компании InfoWatch

Группа компаний InfoWatch объединяет несколько организаций, работающих в области информационной безопасности, защиты корпоративной информации, лингвистического анализа – InfoWatch, Kribrum, EgoSecure. Портфель продуктов ГК InfoWatch включает решения для крупных корпоративных заказчиков: флагманский продукт по защите от утечек InfoWatch Traffic Monitor Enterprise, облачный сервис мониторинга высказываний в Интернете – InfoWatch KRIBRUM. А также решения для малого и среднего бизнеса: защита от утечек - InfoWatch Traffic Monitor Standard, система для защиты рабочих станций InfoWatch EgoSecure.

Несколько фактов о компании:

- Основана «Лабораторией Касперского» в 2003 году.
- Является лидером российского DLP-рынка, более 50% рынка России и стран СНГ.
- Имеет партнерскую сеть в России, СНГ и дальнем зарубежье.
- Активно развивает технологические партнёрства с другими производителями продуктов по информационной безопасности.

Преимущества технической поддержки InfoWatch:

- Выделенная команда разработчиков, которая оперативно работает с обращениями в техническую поддержку.
- База Знаний, в которой содержится вся необходимая документация и инструкции.
- Учёт пожеланий клиентов, при формировании требований к улучшению продуктов.
- Несколько каналов коммуникации: выделенная телефонная линия, электронная почта, веб форма на сайте InfoWatch

