InfoWatch Traffic Monitor Enterprise

Контроль над конфиденциальной информацией – важная задача бизнеса

Современный бизнес работает в условиях жесткой конкуренции, когда для сохранения своего положения на рынке все более важным становится успешное противодействие внутренним угрозам информационной безопасности – утечкам конфиденциальных данных. Утрата таких данных в результате кражи по заказу конкурентов или небрежности сотрудников неминуемо ведет к потере конкурентного преимущества, а, возможно, и самого бизнеса. Даже однократная утечка информации может существенно повредить репутации компании, вызвать отток клиентов и привести к санкциям со стороны регулирующих органов.

Аутсорсинговые проекты, повсеместное распространение мобильных устройств доступа к информации, совместная работа с конфиденциальными данными в офисах компании, расположенных по всему земному шару, создают дополнительные сложности для обеспечения информационной безопасности. В таких условиях традиционный подход, включающий в себя организационные меры и обеспечение сетевой безопасности, становится недостаточным.

Огромный объем информации, обрабатываемый современными компаниями ежедневно, также существенно усложняет обеспечение должного уровня информационной безопасности. В большинстве случаев в компаниях нет точного понимания, какая конкретно информация не подлежит распространению. Как показали опросы клиентов, проведенные InfoWatch, только около 20% конфиденциальных данных в компании структурировано, около 10% конфиденциальных данных изменяется ежедневно, а вновь созданные (zero-day) документы составляют примерно 10% всей конфиденциальной информации компании.

В сегодняшних условиях обеспечение информационной безопасности возможно только при условии смещения фокуса защиты в сторону самой информации.

Специально для компаний, заинтересованных в защите своих конфиденциальных данных, компания InfoWatch разработала комплексное решение для защиты от внутренних информационных угроз – InfoWatch Traffic Monitor Enterprise.

Решение позволяет компаниям полностью контролировать свои информационные потоки и точно понимать, какие данные являются конфиденциальными, где и как они хранятся или передаются и кто их использует.

В среднем, затраты на устранение последствий одной утечки в 2009 году составили около 6,75 млн.долл. США

Ponemon Institute,
Cost of a Data Breach Study 2009

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 обработаны 369 инцидентов нарушения информационной безопасности.

Райффайзен БАНК

InfoWatch Traffic Monitor Enterprise для защиты корпоративных данных

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:

- **Модуль для защиты периметра корпоративной сети – InfoWatch Traffic Monitor,** который включает в себя:
  - InfoWatch Traffic Monitor for Web для контроля данных, передаваемых с помощью web-почты, блогов, форумов и др.
  - InfoWatch Traffic Monitor for HTTPS[1] для контроля данных, передаваемых с помощью зашифрованного Интернет-протокола
  - InfoWatch Traffic Monitor for Mail для контроля информации, проходящей через корпоративную почтовую систему

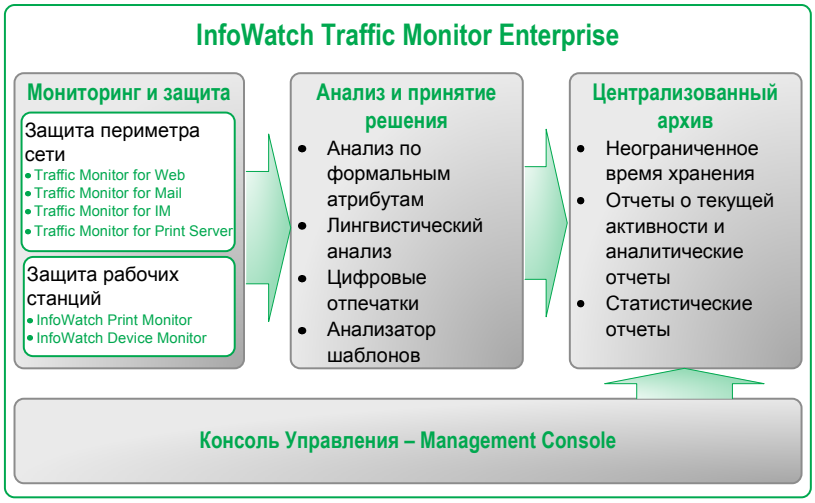
[1] *В интеграции с решениями партнеров*

- InfoWatch Traffic Monitor for IM для контроля данных, отправляемых с помощью систем обмена сообщениями, таких как ICQ и др.
- InfoWatch Traffic Monitor for Print Server для контроля печати документов посредством сетевых принт-серверов

- **Модуль для защиты рабочих станций – InfoWatch Device Monitor,** который включает в себя:
  - InfoWatch Print Monitor для контроля печати документов посредством локальных принтеров
  - InfoWatch Device Monitor для контроля доступа к устройствам ввода-вывода и контроля копирования информации на различные съемные носители
- **Модуль для централизованного архивирования и управления – InfoWatch Traffic Monitor Base**. Здесь сохраняется вся информация для дальнейшего проведения расследований нарушений политики безопасности или составления статистических отчетов и осуществляется управление решением с помощью Консоли управления (Management Console).

InfoWatch Traffic Monitor Enterprise осуществляет:

- Мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых или копируемых на различные устройства ввода-вывода
- Предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае обнаружения нарушения политики безопасности
- Анализ и хранение данных для проведения расследований



Архитектура решения

Кому предназначено решение

InfoWatch Traffic Monitor Enterprise предназначен:

- Операторам персональных данных (банки и финансовые учреждения, медицинские организации, телекоммуникационные операторы, страховые компании, промышленные предприятия, государственные структуры и др.) для обеспечения соответствия требованиям различных отраслевых стандартов, нормативных актов и законодательства, в частности ФЗ-152 «О персональных данных»
- Компаниям, обладающим ценной информацией (IT, фармацевтика, энергетика и др.) для защиты от любых видов потерь, которые могут быть связаны с публичным разглашением такой информации

Билайн – один из ведущих российских мобильных операторов, с абонентской базой около 25 млн. человек. 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). Такое соответствие положительно сказывается на взаимодействии компании с инвесторами и партнерами.

Beeline™

Функциональные возможности

Мониторинг и фильтрация трафика

Защита периметра корпоративной сети: InfoWatch Traffic Monitor

С помощью модуля для защиты периметра корпоративной сети осуществляется мониторинг и фильтрация трафика, отправляемого по протоколам SMTP (корпоративная почта), HTTP (Web), HTTPS[2] (защищенный Web-канал), протоколам систем обмена сообщениями (ICQ и др.). Модуль для защиты периметра обеспечивает также контроль печати документов посредством принт-серверов. Решение поддерживает различные схемы интеграции: «в разрыв», перехват в режиме копии (например, Cisco SPAN) и интеграцию с прокси-сервером по ICAP[3].

Защита рабочих станций: InfoWatch Device Monitor

Модуль для защиты рабочих станций включает в себя программные агенты для контроля копирования данных на съемные носители и локальной печати. Они устанавливаются на рабочие станции сотрудников и помогают предотвратить случайную или намеренную утечку данных через локальную печать, съемные устройства и порты (USB, LPT, COM и др.). Когда сотрудник копирует данные на съемные устройства или отправляет их на печать, модуль для защиты рабочих станций снимает с этих данных теневые копии, которые затем отправляет для анализа на сервер InfoWatch Traffic Monitor Enterprise. Продукт позволяет осуществлять извлечение текстовой информации из графических файлов с помощью технологий распознавания символов (optical character recognition – OCR). Благодаря интеграции с Microsoft Active Directory модуль для защиты рабочих станций можно централизованно установить на все рабочие станции корпоративной сети с помощью средств Microsoft Active Directory либо с помощью собственного механизма удаленной установки. Модуль позволяет напрямую выбирать пользователей или группы пользователей из корпоративного каталога и применять к ним политики безопасности.

Специально для клиентов, в сетях которых для контроля рабочих станций используется продукт Device Lock, InfoWatch предлагает модуль InfoWatch Device Lock Adapter. Этот модуль позволяет использовать для анализа данные, накопленные Device Lock.

Анализ и принятие решения

InfoWatch Traffic Monitor Enterprise изначально анализирует перехваченные данные (объекты) по формальным атрибутам (тип монитора, отправитель / получатель, дата и время отправки, имя / тип / размер файла и др.). Затем происходит извлечение и контентный анализ содержимого перехваченного объекта.

По результатам анализа автоматически принимается решение, как дальше следует поступить с перехваченным объектом – разрешить передачу или заблокировать. Решение принимается на основании правил и политик безопасности, которые можно гибко настраивать.

В случае нарушения политики безопасности InfoWatch Traffic Monitor Enterprise информирует офицера безопасности, предоставляя ему подробную информацию о перехваченном объекте, но без прямого доступа к содержимому. Благодаря этому не нарушается требование законодательства о защите прав сотрудников на тайну переписки. Офицер безопасности может подтвердить или изменить автоматически принятое решение.

Несколько технологий контентного анализа для более точной идентификации конфиденциальных данных

Идентификация 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 для более точной идентификации конфиденциальной информации.

Совместное использование таких технологий, как стоп-слова и регулярные выражения, анализ комплексных текстовых объектов (анализатор шаблонов), цифровые отпечатки и лингвистический анализ (включая морфологический анализ для русского, английского, немецкого, французского, итальянского, испанского и др. языков), существенно повышает надежность определения конфиденциальной информации и позволяет защитить данные в течение всего их жизненного цикла[4].

Решение защищает даже вновь созданные документы: документы, которым еще не присвоен уровень конфиденциальности, для которых не определена контентная категория и для которых не существует каких-либо родственных документов.

[2] *Интеграция с прокси-серверами посредством ICAP поставляется совместно с партнерами.*

[3] *BlueCoat,. За дополнительной информацией обращайтесь, пожалуйста, в InfoWatch.*

[4] *Подробную информацию можно получить в брошюре о компании или у представителей InfoWatch.*

Хранение и ретроспективный анализ данных

Перехваченные данные сохраняются в централизованном архиве InfoWatch Traffic Monitor Base. Время хранения данных не ограничено.

Решение позволяет полностью проследить историю всех операций сотрудников с конфиденциальными данными и предоставляет возможность мониторинга текущей активности пользователей (оперативные запросы) и составления подробных статистических отчетов.

Поиск необходимых данных возможен по:

- Формальным атрибутам перехваченного объекта (тип монитора, получатель / отправитель, дата / время отправки и др.)
- Атрибутам, добавленным в процессе контентного анализа объекта
- Содержимому перехваченного объекта (полнотекстовый поиск)

Решение позволяет составлять подробные статистические отчеты (в том числе и графические[5]) по перехваченным объектам.

По сравнению с 2008 годом в 2009 общее количество утечек данных выросло на 39%.

Глобальное исследование утечек, InfoWatch 2009

Преимущества клиентов от использования InfoWatch Traffic Monitor Enterprise

- Полный контроль над обращением конфиденциальной информации
- Соответствие требованиям законодательства
- Управление различными рисками (финансовыми, законодательными, коммерческими, репутационными), связанными с утечкой данных
- Улучшение корпоративной культуры благодаря обучению сотрудников в сфере информационной безопасности

InfoWatch Traffic Monitor Enterprise: диаграмма потоков данных

[5] *За дополнительной информацией обращайтесь, пожалуйста, в InfoWatch.*

InfoWatch Traffic Monitor Enterprise

Решение для вертикальных сегментов рынка

Чтобы ускорить процесс внедрения и позволить компаниям немедленно воспользоваться преимуществами решения по защите информации от внутренних угроз, InfoWatch Traffic Monitor Enterprise поставляется с набором предустановленных правил обработки объектов: базой контентной фильтрации, шаблонами текстовых объектов, правилами автоматического вынесения вердикта. В настоящее время эти правила специально адаптированы под потребности таких вертикальных сегментов рынка, как банковская и финансовая отрасль, нефтегазовый сектор, телекоммуникации и др.

Лукой Информ занимается информационно-технологическим обеспечением деятельности Группы «ЛУКОЙЛ». InfoWatch Traffic Monitor Enterprise, внедренный компанией, обеспечивает полноценный контроль над информационными потоками с различными сценариями реакции на нарушения политики безопасности и эффективной обработкой данных.

ЛУКОЙЛ ИНФОРМ

Преимущества решения

- **Точная идентификация конфиденциальных данных** благодаря совместному использованию различных технологий контентного анализа
- **Надежная защита периметра корпоративной сети** благодаря контролю над различными каналами утечки данных, включая копирование документов и их печать
- **Поддержка различных типов и форматов файлов**
- **Предустановленные правила обработки и база контентной фильтрации,** чтобы позволить компаниям немедленно воспользоваться всеми преимуществами решения по защите информации от внутренних угроз
- **Централизованный архив** для мониторинга текущей активности сотрудников, составления аналитических отчетов и проведения расследований
- **Гибкая схема интеграции в IT-инфрастуктуру:** интеграция «в разрыв», поддержка ICAP, перехват в режиме копии трафика (SPAN, port mirroring и др.)
- **Сертификация ФСТЭК**
- **Дополнительный уровень безопасности:** InfoWatch Traffic Monitor Enterprise может быть интегрирован с системой шифрования InfoWatch CryptoStorage Enterprise

Лицензирование InfoWatch Traffic Monitor Enterprise

Централизованное архивирование и управление	• InfoWatch Traffic Monitor Base • Linguistic Analysis with InfoWatch Traffic Monitor Base* • Fingerprints with InfoWatch Traffic Monitor Base* • Templates Analyser with InfoWatch Traffic Monitor Base*
Защита периметра сети	• InfoWatch Traffic Monitor for Web • InfoWatch Traffic Monitor for HTTPS* • InfoWatch Traffic Monitor for Mail • InfoWatch Traffic Monitor for IM • InfoWatch Traffic Monitor for Print Server
Защита рабочих станций	• InfoWatch Device Monitor • InfoWatch Device Lock Adapter

**Лицензируется дополнительно*

InfoWatch Traffic Monitor Enterprise

Системные требования

Защита периметра сети: InfoWatch Traffic Monitor

Аппаратное обеспечение

- Сервер: HP DL360 G6
- CPU: Intel Xeon x86 3GHz, 2 CPU с 4 ядрами
- RAM 2 GB
- HD 160GB

Программное обеспечение

- Red Hat Enterprise Linux Server release 5 upd 4, x86-32

Защита рабочих станций: InfoWatch Device Monitor

InfoWatch Device Monitor Server

Аппаратное обеспечение

- CPU: Intel Pentium 4 2GHz или выше
- RAM 1 GB
- HD 100GB

Software

- Windows 2003 Server Service Pack 1
- RDBMS: Oracle / MS SQL Server / PostgreSQL / MS SQL Express
- .NET Framework 3.0

InfoWatch Device Monitor Client

Аппаратное обеспечение

- CPU: Intel Pentium 4 2GHz или выше
- RAM 512 MB

Программное обеспечение

- Windows 2000 Professional SP 4 or Windows XP SP2 or Windows Vista

Централизованное архивирование и управление: InfoWatch Traffic Monitor Base

Централизованный архив

Аппаратное обеспечение

- Server: HP DL360 G6
- CPU: Intel Xeon x86 2.4GHz или выше
- RAM 4 GB
- RAID level 1 или выше (200GB)

Программное обеспечение

- Oracle RDBMS 11gR1 (11.1.0.7)

Консоль Управления (Management Console)

Аппаратное обеспечение

- CPU: Pentium 4, 3GHz
- RAM: 1 GB

Программное обеспечение

- Microsoft Windows XP Service Pack 2

Контакты:
тел.: **+7 495 22 900 22**
Российская Федерация, 123458, Москва,
проезд №607, дом 30, офис 507

www.infowatch.ru
info@infowatch.ru
sales@infowatch.ru
support@infowatch.ru