

InfoWatch Data Control – легкое решение проблемы утечки данных из компании!

Информационные активы компании – постоянная мишень для атак. Потеря конфиденциальных данных и, в частности, персональных данных клиентов может нанести урон деловой репутации и прямой финансовый ущерб компании.

Проблема контроля за распространением конфиденциальной информации стара как мир. Раньше задача предотвращения утечек конфиденциальных данных из информационных систем решалась в основном тремя способами:

- разграничением прав доступа к различным ресурсам,
- ограничением доступа к портам и внешним устройствам на уровне «разрешить/запретить доступ»,
- шифрованием данных.

Однако описанные выше методы обеспечивают защиту информации только в местах ее хранения и не дают возможности контролировать обработку и перемещение конфиденциальных данных.

Сегодня существуют специализированные технологии и решения, которые защищают конфиденциальные данные от внутренних угроз и позволяют контролировать данные как в процессе их хранения, так и в процессе их обработки и передачи по различным каналам. При этом под внутренними угрозами понимаются как умышленные нарушения, так и непреднамеренные действия сотрудников в рамках своих прав доступа к данным.

Такие решения получили название DLP-систем (DLP – Data Leakage Prevention).

Современное DLP-решение – это система, которая позволяет предотвратить утечку именно конфиденциальных данных. При этом информация, которая не подпадает под гриф «конфиденциально», должна свободно передаваться по любым электронным каналам, не нарушая привычного хода бизнеса.

Сегодня на рынке существует довольно много продуктов, позволяющих выявлять и предотвращать утечки конфиденциальной информации. Однако лишь немногие из них действительно являются DLP-системами. Еще меньше решений, которые ориентированы не на крупных заказчиков, а на небольшие и средние компании. Таким решением является новая разработка InfoWatch Data Control.

InfoWatch Data Control – это интегрированный продукт для комплексной защиты конфиденциальных данных компании среднего и малого бизнеса. Решение представляет собой **программно-аппаратное устройство, которое выполняет мониторинг и фильтрацию данных, передаваемых за пределы компании по электронной почте, через веб или интернет-пейджеры.**

Решение предназначено для компаний, работающих с персональными данными (медицина, банки и т.п.), а также обладающих ценной технологической информацией, потеря которой может ударить по конкурентоспособности (ИТ, фармацевтика и т.п.). InfoWatch Data Control позволяет минимизировать юридические риски, связанные с утечкой информации и соблюдением требований законода-

тельства, а также предотвратить финансовые потери (недополученная прибыль и т.п.).

Активная защита

InfoWatch Data Control осуществляет не только мониторинг данных, выходящих за пределы компании, и их категоризацию, но и предотвращает утечку критических данных, заблокировав перемещение тех из них, которые признаны конфиденциальными.

Уникальные технологии фильтрации

В основе решения заложен принцип **гибридного анализа информации** – интеграция передовых технологий детектирования критичной информации в различных документах и текстах, как то: **лингвистический и морфологический анализ, цифровые отпечатки и детектор объектов.** Метод морфологического анализа позволяет защищать документы на

Простота и удобство использования

Настройка различных компонент InfoWatch Data Control, таких как системы перехвата или модуль анализа, может быть осуществлена в рамках единой консоли. Данная консоль также позволяет в режиме реального времени отслеживать все перехватываемые системой события.

Решение поставляется с набором предустановленных настроек, что позволяет ввести его в эксплуатацию сразу же после подключения.

Перехват и фильтрация трафика

InfoWatch Data Control осуществляет перехват и фильтрацию исходящей из компании информации по следующим каналам: электронная почта, Интернет (веб-почта, форумы, чаты и т.д.), ICQ и другие веб-пейджеры.

Одно из главных требований, предъявляе-



любом этапе их жизненного цикла. Применяемые алгоритмы не требуют какой-либо предварительной обработки внутренней документации компании для того, чтобы в дальнейшем она могла быть выявлена системой контроля за утечкой данных, и не нарушают существующий документооборот. Решение позволяет анализировать даже небольшие объемы информации, например сообщения ICQ.

Простота настройки и сопровождения

Решение в виде программно-аппаратного комплекса позволяет максимально упростить как процесс настройки и интеграции продукта в инфраструктуру компании, так и его дальнейшее обслуживание. Все компоненты решения сосредоточены на одном сервере, с сокращением количества параметров, настройка которых требует специализированных знаний. Поэтому администрирование решения не требует усилий отдельного ИТ-специалиста.

InfoWatch Data Control может поставляться и как отдельное программное решение, которое может быть установлено на любой сервер, соответствующий рекомендованным характеристикам.

мых к DLP-системам, – возможность активной защиты, т.е. система должна не только фиксировать утечку конфиденциальной информации, но и давать возможность ее предотвратить. Поэтому InfoWatch Data Control для всех контролируемых каналов поддерживает схемы интеграции «в разрыв», когда решение устанавливается непосредственно на канал передачи данных, что позволяет блокировать несанкционированную пересылку информации.

Анализ и принятие решения

Для того чтобы не допустить утечки конфиденциальных данных, система защиты должна проанализировать перехваченные данные, определить, являются ли они конфиденциальными, и принять решение, пропускать их дальше или нет. При этом качество и точность фильтрации являются одними из наиболее критических показателей.

Уникальные технологии гибридного анализа, используемые в продукте InfoWatch Data Control, позволяют комбинировать различные методы анализа перехваченных данных, обеспечивая тем самым максимальную степень защиты конфиденциальных данных.

InfoWatch Data Control в процессе анализа проверяет как формальные атрибуты перехваченного объекта (размер, тип вложения и т.п.), так и его содержимое. На основании правил автоматической обработки система выносит вердикт о конфиденциальности перехваченных данных и принимает решение, блокировать данные или нет.

Детектирование и распаковка

Одной из важных задач, которые приходится решать в процессе анализа перехваченных объектов, является определение типа пересылаемого контента и корректное извлечение текста из перехваченных объектов.

Пример:

Сотрудник одного банка, в котором было установлено решение InfoWatch, контролирующее веб-почту, пересылал в другой банк списки надежных заемщиков. Для того чтобы обмануть систему, он пытался «спрятать» пересылаемую информацию, меняя исходное расширение файла на «трз». Однако решение InfoWatch обнаружило несоответствие между действительным типом файла и его расширением. Таким образом, был выявлен инсайдер.

InfoWatch Data Control поддерживает работу со следующими типами файлов:

- мультимедиа и графические форматы – TIFF, JPEG, GIF, PNG, EMF, WMF, MP3, WAV, AVI, WMV;
- форматы баз данных – MS Access (MDB);
- детектирование и распаковка архивов – ZIP, RARZIP, BZIP2, TAR, ARJ, LHA;
- текстовые объекты – MS Office 97–2007 (MS Word, MS Excel, MS PowerPoint), MS Outlook TNEF, RTF, PDF, TXT, HTML, XML.

Контентный анализ текста

Помимо анализа по формальным атрибутам (отправитель, получатель, тип вложения и т.п.), InfoWatch Data Control позволяет выполнять анализ содержимого перехваченных данных – контентный анализ текста, извлеченного из перехваченных объектов.

Контентный анализ выполняется на основе заранее созданной базы контентной фильтрации (БКФ). БКФ не только описывает категории информации, циркулирующей в компании, но и учитывает различные атрибуты её конфиденциальности, в т.ч. специфику деятельности компании, ее требования к безопасности. В итоге тексту присваиваются те или иные категории (различные степени конфиденциальности либо отсутствие конфиденциальности), соответствующие его тематике и содержанию.

Хранение и ретроспективный анализ

Немаловажную роль в защите конфиденциальной информации играет пост-анализ. В отличие от многих конкурентных решений, вся информация, прошедшая через InfoWatch Data Control, хранится в едином унифицированном виде в универсальном хранилище InfoWatch Storage. В случае необходимости вся собранная информация доступна офицеру информационной безопасности для анализа. Поиск данных возможен по:

- формальным признакам перехваченных объектов (перехватчик, отправитель/получатель, дата/время отправки и т.д.);
- атрибутам, добавленным в процессе обработки объекта (вердикт, теги и т.д.);
- содержимому перехваченных объектов (полнотекстовый поиск).