

СОВМЕСТНОЕ РЕШЕНИЕ INFOWATCH TRAFFIC MONITOR И АРТИ DPRINTER

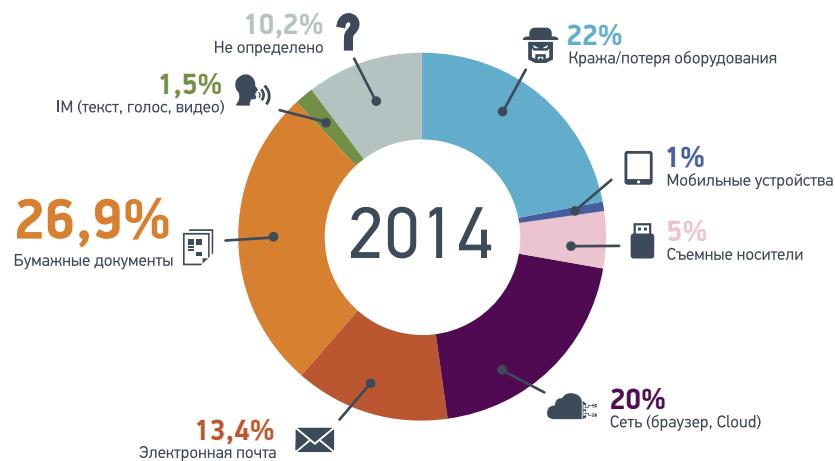
20% ВСЕХ УТЕЧЕК ИНФОРМАЦИИ ПРОИСХОДИТ ЧЕРЕЗ ПРИНТЕР

Принтеры являются необходимым инструментом корпоративной инфраструктуры. Распечатанные документы постоянно используются в документообороте любой компании, что существенно увеличивает риски случайных и злонамеренных потерь коммерческой тайны, и значительно осложняет работу офицера безопасности, пытающегося самостоятельно выявить нелояльных сотрудников, распечатывающих корпоративные секреты.

По данным аналитического центра InfoWatch, каждая пятая утечка информации была реализована с помощью обычного офисного принтера. Утечки через бумажные носители входят в четвёрку «популярных» каналов – вместе с потерей и кражей оборудования, сетевыми ресурсами и электронной почтой.

Порядка 30% непреднамеренных утечек информации происходит из-за ошибок сотрудников при печати документов – это самый большой показатель среди случайных утечек. Самые распространенные случаи: сотрудник взял из принтера чужие документы, или распечатал файл, чтобы поработать дома, а по дороге потерял папку с бумагами и т.п.

РАЗДЕЛЕНИЕ ПО КАНАЛАМ СЛУЧАЙНЫХ УТЕЧЕК



*По данным Аналитического центра InfoWatch

СЛУЧАЙ ИЗ ПРАКТИКИ

«Внутренняя переписка Удмуртского отделения Сбербанка России: подписанные заявления-анкеты заемщиков, копии паспортов, обнаружены выброшенными на одну из улиц Ижевска. В анкетах указаны сведения о наличии у человека собственности, информация о его долговых обязательствах, а также номера счетов и банковских карт. К некоторым заявлениям приложены копии документов – паспортов, трудовых книжек, справок о доходах».

Агентство «Интерфакс-Поволжье»

Подобные инциденты могут привести к серьезным последствиям, прямым финансовым и репутационным потерям. Для уменьшения данных рисков рекомендуется использовать специальные средства контроля процессов печати и исполнения политики информационной безопасности при работе с печатными документами.

INFOWATCH И АРТИ РАЗРАБОТАЛИ СОВМЕСТНОЕ РЕШЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ПРОЦЕССАМИ ПЕЧАТИ

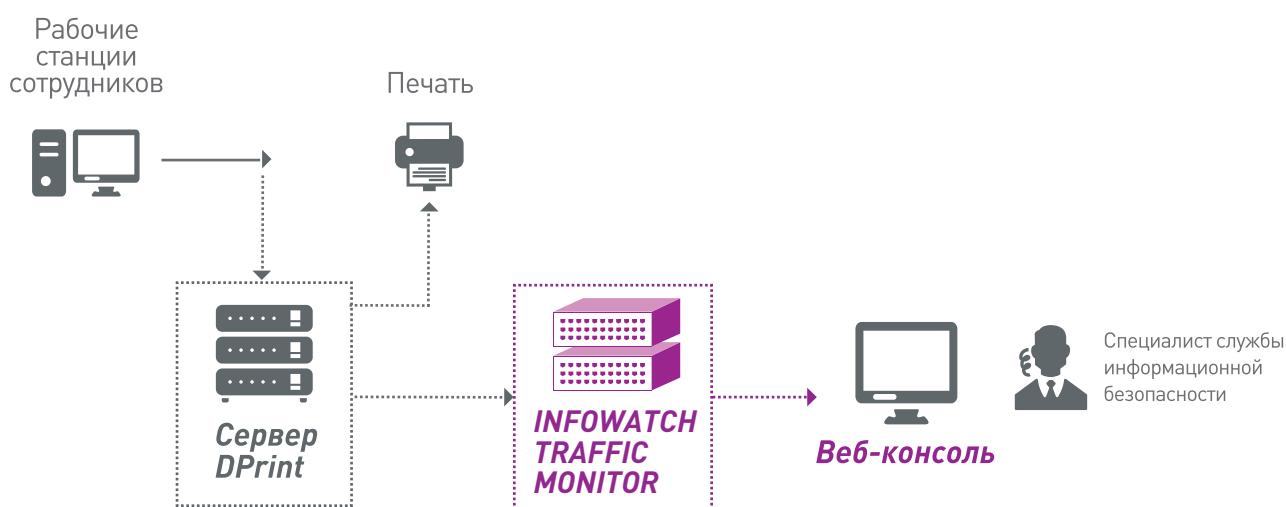
Компания InfoWatch – лидер в сфере защиты корпоративных данных на рынке России и СНГ, и компания АРТИ, специализирующаяся на автоматизированных системах контроля и мониторинга печати, разработали совместное интеграционное решение на основе двух продуктов: InfoWatch Traffic Monitor и АРТИ DPrint.



СОВМЕСТНОЕ РЕШЕНИЕ INFOWATCH TRAFFIC MONITOR И АРТИ DPRINTER



Совместное решение позволило объединить функциональные возможности двух систем. При перехвате задания на печать, DPrint передает модулю InfoWatch Traffic Monitor всю необходимую для анализа информацию, включая сам документ. InfoWatch Traffic Monitor, в свою очередь, проводит детальный анализ документа, классифицирует его, применяет политику безопасности, настроенную для печатаемых документов. Более того, параллельно с этим процессом InfoWatch Traffic Monitor работает в штатном режиме и помогает компании контролировать остальные возможные каналы утечек информации и внутренних угроз, такие как: внешние носители, электронная почта, интернет и другие.



Применяя интеграционное решение на базе АРТИ DPrint и InfoWatch Traffic Monitor Enterprise, у офицера безопасности появится возможность наблюдать все инциденты с двух систем в единой консоли. Служба информационной безопасности сможет наиболее эффективно проводить расследования инцидентов, опираясь на централизованный архив всех действий пользователей, выявляя взаимосвязи между событиями, просматривая все связанные с делом письма и документы. Комплексное решение позволит точно и однозначно определить злонамеренных сотрудников, а также выявить круг причастных лиц.

ПРЕИМУЩЕСТВА СОВМЕСТНОГО РЕШЕНИЯ INFOWATCH И АРТИ

Предотвращение возможных внутренних угроз

- Авторизация пользователей на печатающих устройствах для предотвращения «выноса» чужого документа
- Контентный анализ печатаемых документов
- Блокировка печати конфиденциальных документов
- Фильтрация и корреляция всех событий из других систем для ускорения процесса расследования инцидентов

Применение всех возможностей аналитического аппарата InfoWatch Traffic Monitor

- Контроль всех каналов передачи данных
- Создание политик безопасности специально для документов, отправленных на печать
- Классификация всех инцидентов в соответствии с политиками
- Полный и централизованный архив всех событий, позволяющий проводить расследование и анализ инцидентов ИБ

