

Совместное решение InfoWatch Traffic Monitor и Lumension Device Control для защиты конфиденциальных данных

Масштабы утечки данных из-за случайного или умышленного использования съемных носителей информации или электронных каналов передачи данных достигли критического уровня. На сегодняшний день практически каждая компания хотя бы однажды сталкивалась с ситуацией, когда важные конфиденциальные данные были утрачены. Одновременно ежегодно возрастают и затраты на устранение последствий подобных инцидентов, так в 2009 году средние расходы на устранение последствий одной утечки данных составили 6,75 млн.долл.США.

Для защиты корпоративной информации от несанкционированного распространения компании InfoWatch и Lumension предлагают совместное решение на основе продуктов [InfoWatch Traffic Monitor](#) и [Lumension Device Control](#). Совместное решение сочетает в себе преимущества отдельных продуктов и гарантирует пользователям полный контроль над оборотом конфиденциальной информации, включая централизованное управление использованием съемных носителей – наиболее типичным маршрутом утечки информации из корпоративной сети.

Совместное решение [InfoWatch](#) и [Lumension](#) осуществляет:

- Мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых или копируемых на съемные носители
- Предотвращение нарушений корпоративной политики безопасности посредством блокирования неразрешенных действий сотрудников
- Централизованное хранение данных в едином неизменяемом архиве и их категоризацию для последующего анализа и, при необходимости, сбора доказательной базы при судебном разбирательстве

Компоненты решения

Совместное решение включает в себя продукты [InfoWatch Traffic Monitor](#) и [Lumension Device Control](#), которые являются инструментами контроля выполнения требований стандартов и законодательных актов в области информационной безопасности, таких как PCI/DSS, Basel II, SOX, HIPAA (для США) и др.

InfoWatch Traffic Monitor

[InfoWatch Traffic Monitor](#) – комплексное модульное решение по защите информации от внутренних угроз, которое позволяет контролировать различные каналы передачи данных. Решение обеспечивает защиту как на уровне рабочей станции, так и на уровне шлюза, перехватывая и анализируя данные, отправленные через почтовую систему, web, системы обмена сообщениями, распечатываемую или копируемую на съемные носители.

Перехваченные данные анализируются по формальным атрибутам (время/дата отправки, отправитель/получатель, размер/тип/название файла и др.). Затем происходит извлечение и контентный анализ содержимого перехваченных данных. 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.

Вся перехваченная информация сохраняется в централизованном архиве на неограниченное время. Сохраненная информация тщательно категоризируется и может быть использована как для мониторинга текущей активности сотрудников, так и для ретроспективного анализа и сбора доказательной базы при проведении судебного расследования.

Преимущества InfoWatch Traffic Monitor

- Точная идентификация конфиденциальной информации благодаря совместному использованию нескольких технологий контентного анализа
- Надежная защита периметра корпоративной сети благодаря контролю над различными каналами передачи данных, включая копирование и печать
- Поддержка различных типов и форматов файлов
- Предустановленные правила обработки и база контентной фильтрации, чтобы позволить компаниям немедленно воспользоваться всеми возможностями решения по защите данных
- Централизованный неизменяемый архив для мониторинга текущей активности сотрудников и ретроспективного анализа
- Гибкая схема интеграции: интеграция «в разрыв», поддержка ICAP, перехват в режиме копии (SPAN, port mirroring и др.)

Lumension Device Control

Lumension Device Control обеспечивает централизованное назначение политик безопасности для съемных устройств и использования данных (например, только чтение или чтение и запись/шифрование). Используя принцип «белого списка»/«по умолчанию запретить», администратор решения может централизованно управлять устройствами и данными в корпоративной сети. Lumension Device Control позволяет компаниям использовать съемные носители информации, что повышает производительность работы, и одновременно существенно снижает риск утечки данных и его потенциальные последствия.

Основные характеристики Lumension Device Control:

- Принцип «белого списка»/«по умолчанию запретить»
- Принудительное шифрование для съемных носителей
- Фильтрация по типу файлов
- Временный/запланированный доступ
- Разрешения с учетом контекста
- Централизованное управление/роли администраторов
- Ролевой принцип распределения доступа
- Программный агент, защищенный от взлома
- Гибкая масштабируемая архитектура

Преимущества Lumension Device Control

- Защищает данные от потери или кражи
- Обеспечивает безопасное использование съемных устройств (USB-накопителей и др.), что позволяет повысить производительность и эффективность работы
- Повышает качество контроля соблюдения политики безопасности
- Позволяет осуществлять точный контроль благодаря гибкому разграничению доступа

Преимущества совместного решения

- Категоризация сохраненных данных для ретроспективного анализа и сбора доказательной базы при проведении расследования
- Точная идентификация конфиденциальных данных, покидающих корпоративную сеть, благодаря совместному использованию нескольких технологий контентного анализа
- Масштабируемость и гибкая схема интеграции для минимизации затрат на внедрение
- Инструмент контроля выполнения требований российских и международных стандартов и законодательных актов в области обеспечения информационной безопасности

Контакты: