INFOWATCH®

INFOWATCH TRAFFIC MONITOR

Стратегия 90% компаний на 2022

Информация — критический ресурс. Аналитика — важнейшая компетенция.

Gartner

От безопасности корпоративных данных — к прогнозированию рисков и росту эффективности бизнес-процессов

Данные, обеспечивающие функционирование процессов — одна из главных ценностей организации в цифровую эпоху. Безопасность данных — критическое требование бизнеса и регулятора.

Данные циркулируют внутри и вокруг организации. Они содержат сигналы не только о нарушениях политик безопасности, но и о показателях эффективности бизнес-процессов, потенциальных рисках и новых возможностях.

DLP-система InfoWatch НАДЁЖНО ЗАЩИЩАЕТ конфиденциальные данные

Выявляет и блокирует нарушения в работе с информацией ограниченного доступа — документы, изображения, чертежи, персональные данные, базы данных, отсканированные и заполненные бланки и многое другое

Помогает соответствовать требованиям 152-ФЗ, GDPR, 395-ФЗ ст. 26, 224-ФЗ, требованиям МО, ФСБ, ФСТЭК и отраслевым стандартам

Визуализирует данные с помощью графа связей на 50 тысяч узлов, анализ 100+ млн событий в секунду в корпоративных сетях размером до 100 000 узлов. Это сокращает время на генерацию и проверку гипотез в 3–4 раза, показывает маршруты перемещения информации даже на личные адреса и USB-накопители, помогает работать с данными в организациях с распределённой структурой

Осуществляет мониторинг действий сотрудников для раннего выявления рисков и угроз ИБ, проведения внутренних расследований и сбора доказательной базы

...И АНАЛИЗИРУЕТ информационные потоки для идентификации рисков и поддержки управленческих решений

- Детектирует сомнительное или аномальное поведение сотрудников организации
- Выявляет факты распространения клеветнической, порочащей компанию и её руководство информации, в том числе в социальных сетях
- Позволяет выявить признаки корпоративного мошенничества, конфликта интересов, сговора, саботажа, сокрытия или искажения информации
- Помогает в подготовке и контроле исполнения управленческих решений
- Отслеживает маршруты распространения документов внутри компании
- Даёт инструмент поиска неэффективного взаимодействия и узких мест в коммуникациях, выявления лидеров мнений, отношения к изменениям и т. д.

Экспертная защита благодаря технологическим преимуществам InfoWatch Traffic Monitor

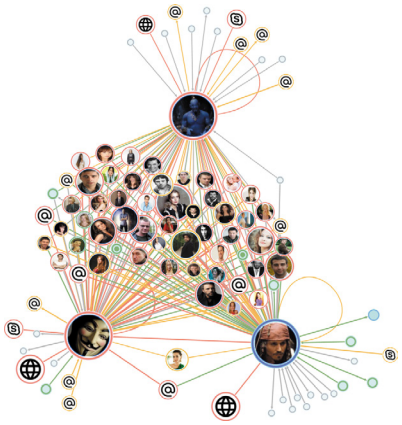
- **Контролирует все способы передачи данных:** от корпоративной почты до мессенджеров, облачных хранилищ, сетевых папок, FTP, локальных и сетевых принтеров, съёмных носителей, терминальных соединений, веб-почты и соцсетей
- **Может устанавливаться в разрыв.** Это позволяет без прерывания бизнес-процессов заблокировать и предотвратить утечку конфиденциальных данных как за периметр организации, так и за пределы внутреннего контура
- **Надёжно работает под большими нагрузками,** что доказано проектами на сотни тысяч рабочих мест, в которых система обрабатывает миллионы событий в сутки
- **Оснащён уникальными технологиями контентного анализа:**
  - — Лингвистический анализ текста на 42-х языках, на 20 языках — с поддержкой морфологии
  - — 200 отраслевых баз контентной фильтрации минимизируют количество ложных срабатываний уже на старте проекта
  - — Автоматическая актуализация отпечатков баз данных, баз цифровых отпечатков и цифровых отпечатков фотографий позволяет поддерживать политики безопасности в актуальном состоянии и защищать данные из бизнес-систем (ERP, CRM, СЭД и других)
  - — Анализатор векторной графики идентифицирует присутствие любого фрагмента конфиденциального чертежа в составе другого чертежа, даже если он был модифицирован
  - — Технологии машинного обучения — автоматическое категорирование конфиденциальных изображений без привлечения внешних исполнителей
  - — Защита сложных объектов, документов с несколькими признаками, например, детектирование сканов заполненных договоров с печатью, отсканированных и заполненных от руки анкет и форм
  - — Идентификация выгрузок баз данных — защита наборов конкретных именованных сущностей, например: ФИО, ИНН, номера паспорта, а также номенклатурных позиций или позиций прайс-листа. Интеграция через открытый API с бизнес-системами (ERP, СЭД)
  - — Защита персональных данных, номеров платёжных карт, паспортных данных, ИНН и др.
- **Интеграция с SAP, Office 365, Exchange Online** для контроля трафика в условиях удалённой работы. API для интеграции с другими внешними системами для получения статуса по инциденту и параметров события специфичного формата
- **Защита данных DLP-системы.** Расширенный аудит действий сотрудников ИБ — Политик, Запросов, Событий, Объектов защиты, Элементов настройки технологий и Периметров. Разграничение прав доступа специалистов ИБ для разделения полномочий. Защита от подбора пароля согласно рекомендациям ФСТЭК

Дополнительные инструменты расширяют функционал DLP-системы для предотвращения инцидентов информационной, кадровой и экономической безопасности.

Инструмент для контроля за действиями пользователей

- Сбор данных о действиях сотрудников для анализа рабочей активности, выявления нарушений трудовой дисциплины, нецелевого использования ресурсов компании и неправомерных действий сотрудников.
- Мониторинг всех используемых приложений, посещаемых веб-сайтов, вводимого текста, поисковых запросов на веб-ресурсах
- Получение снимков экрана
- Отслеживание всех посещаемых веб-сайтов, в том числе сайтов с агрессивной и экстремистской направленностью
- Классификация активности сотрудника с возможностью кастомизации правил с учётом специфики бизнес-процессов компании

Инструмент для визуальной аналитики данных

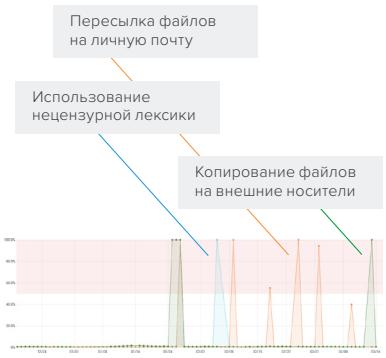


Увидеть суть. Быстрее

Визуальное представление данных DLP-системы убирает шум, подсвечивает полезную информацию и позволяет увидеть историю, скрытую за сухими фактами:

- Построить **карту коммуникаций** компании, подразделений или персон
- Отследить **маршруты перемещения** конкретных файлов или выбранных типов конфиденциальной информации
- Быстро перейти **от сводной статистики** по всей компании **к деталям** отдельных событий
- Провести расследование на основании **неполных данных**
- Выявить **медленные утечки** через USB-накопители и «теневое IT»
- Взять под контроль **личные адреса** сотрудников в условиях удалённой работы
- Разграничить **доступ к данным** для разных сотрудников ИБ
- Получить необходимую информацию для **оптимизации политик DLP**
- Подготовить **наглядный отчёт** для руководства

Инструмент для предиктивной аналитики данных



Увидеть то, что скрыто

Инструмент для предиктивной аналитики данных DLP-системы позволяет выявлять рискованные паттерны поведения сотрудников и эффективно работать с группами риска. Помогает перейти от констатации факта утечки и устранения последствий к прогнозированию и предотвращению инцидентов.

- **Автоматически выявляет отклонения** от привычного поведения и относит сотрудника к группе риска
- **Подсвечивает аномалии,** цепочки связанных событий и превышения заданных порогов
- **Уведомляет специалиста ИБ** о надвигающемся или скрыто реализующемся инциденте
- **Позволяет быстро перейти к исходным событиям** для выяснения всех обстоятельств инцидента и занесения результатов в досье сотрудника

Единое решение — совместимые инструменты

Что случилось?

Дескриптивная аналитика

InfoWatch Traffic Monitor

DLP (Data Loss Prevention) — защита данных от утечек

InfoWatch Activity Monitor

Мониторинг действий пользователей

Почему это случилось?

Диагностическая аналитика

InfoWatch Vision

Визуальная аналитика данных DLP-системы

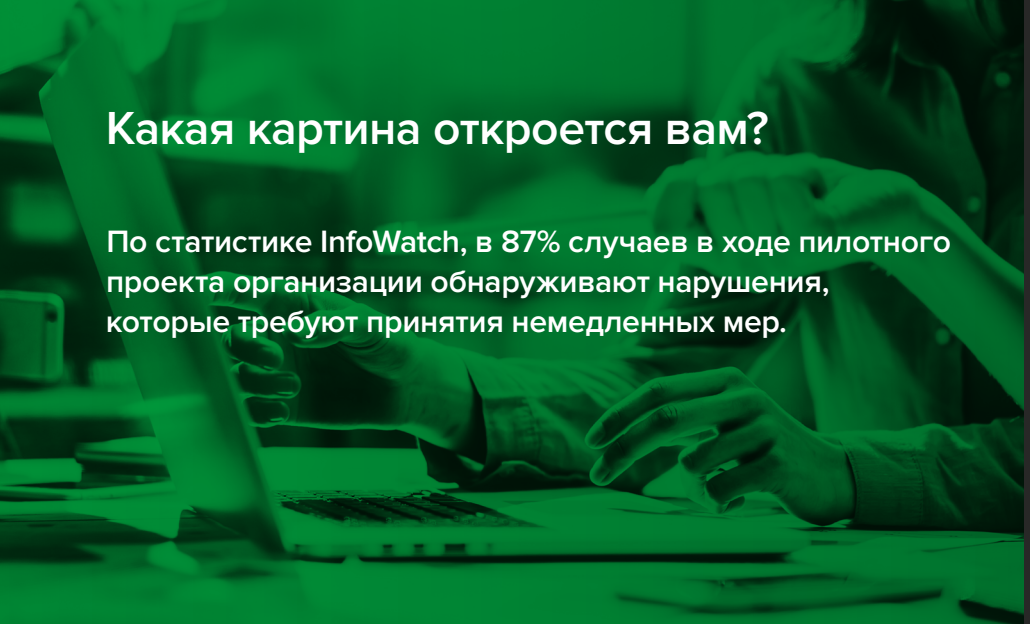
Что может произойти?

Предиктивная аналитика

InfoWatch Prediction

Предиктивная аналитика данных DLP-системы

Зрелость процессов и продвинутость инструментов



Какая картина откроется вам?

По статистике InfoWatch, в 87% случаев в ходе пилотного проекта организации обнаруживают нарушения, которые требуют принятия немедленных мер.

Свяжитесь с экспертами InfoWatch для запуска пилотного проекта в вашей организации:

sales@infowatch.ru
+7 495 22 900 22

tm.infowatch.ru

INFOWATCH®

InfoWatch — ведущий российский разработчик решений для обеспечения информационной безопасности организаций. Мощная академическая база, лучшие инженеры, математики и лингвисты с 2003 года обеспечивают технологическое преимущество InfoWatch в области защиты предприятий от современных киберугроз, информационных и инсайдерских атак.

Признанный эксперт и лидер рынка России и СНГ в области защиты корпоративных данных InfoWatch успешно выполнил более 3000 проектов для коммерческих и государственных организаций в 20-ти странах мира.

Две трети из 50-ти крупнейших компаний России (в соответствии с рейтингом «Эксперта») доверили InfoWatch выполнение масштабных и, зачастую, нестандартных проектов, связанных с информационной безопасностью. Причина такого доверия не только в качестве и уникальности технологий, но и в чувстве уверенности, которое даёт InfoWatch, когда сопровождает своих клиентов на всех этапах проектных работ.

/InfoWatchOut /InfoWatch /infowatchnews

Министерство обороны Российской Федерации

Федеральная таможенная служба

Фонд социального страхования

Федеральная налоговая служба

СБЕР БАНК · HOME CREDIT BANK · Райффайзен БАНК · МТС БАНК · СОГАЗ СТРАХОВАЯ ГРУППА

ИНФОРМ Ростех · ТРАНСНЕФТЬ · МОСКОВСКИЙ ВЕРТОЛЕТНЫЙ ЗАВОД ИМ. М.Л. МИЛЯ · СУХОЙ · ОДК

О'КЕЙ · SPSR express · МАГНИТ · KUPIVIP.RU · НИАРМЕДИК Сеть семейных клиник