INFOWATCH®

INFOWATCH TRAFFIC MONITOR

Предотвращение утечек информации и контроль информационных потоков

InfoWatch Traffic Monitor — первая российская DLP-система, которая с помощью технологий искусственного интеллекта предотвращает утечки конфиденциальной информации, прогнозирует риски и повышает уровень автоматизации работы службы ИБ в условиях быстрых изменений.

Эпоха неопределённости: новые вызовы ИБ

С начала 2022 года в России было зафиксировано 350 млн. утёкших записей. Это более чем на 200% выше, чем за весь 2021 год. И это только те утечки, о которых стало известно. Перестройка ИТ-инфраструктуры вследствие требований импортозамещения, изменение модели угроз и кратный рост атак — такова новая реальность ИБ. Для того, чтобы сохранять стабильность и целостность данных в своей организации, службам ИБ теперь необходимо сфокусировать внимание на инструментах, автоматизирующих их работу и освобождающих время для решения стратегических задач.

Эволюция решений для защиты данных

2019	2023
Только 20–30% данных организации закрыты политиками безопасности DLP	**Защита 100% данных** с помощью технологий искусственного интеллекта
Акцент на бумажную безопасность	**Автоматизация работы ИБ** для обеспечения реальной безопасности
Мониторинг действий сотрудников на рабочем устройстве	**Прогнозирование рисков** на основе динамических моделей поведения сотрудников
Статические преднастроенные отчёты	**BI-система для динамического анализа** данных DLP и построения любых отчётов

DLP-система Traffic Monitor полностью отвечает требованиям импортозамещения. Внесена в реестр отечественного ПО, сертифицирована ФСБ, Министерством обороны, ЦБ РФ, ФСТЭК России. Поддерживает российские операционные системы РЕД ОС, Astra Linux и ALT Linux, базы данных PostgreSQL и PostgreSQL Pro, службы каталогов Samba DC, ALD Pro, FreeIPA.

DLP-система нового поколения: гибкость и готовность к быстрым изменениям

Защита 100% данных при помощи технологий искусственного интеллекта

Растущий объём данных, меняющаяся структура коммуникаций, фактическое отсутствие периметра требуют более глубокого уровня автоматизации и технологий анализа больших данных. Мы более 15 лет применяем технологии искусственного интеллекта для анализа контента. Traffic Monitor автоматизирует аудит данных, настройку политик безопасности и прогнозирование рисков — ресурсоёмких и критически важных задач ИБ.

Надёжность DLP-системы Traffic Monitor подтверждена отраслевыми наградами:

- Премия «Лучшее ИБ-решение — 2021», TAdviser
- Премия «Автоматизированное обучение новым категориям», ТБ Форум
- Премия «Инновация года — 2022», CNews

Соблюдение требований регуляторов

Приостановка деятельности организации из-за несоблюдения требований регуляторов даже на один день может грозить многомиллионными убытками. Также не стоит забывать о планируемом введении оборотных штрафов за утечки данных и невыполнение требований надзорных органов. Traffic Monitor помогает соответствовать требованиям 152-ФЗ, 395-ФЗ ст. 26, 224-ФЗ, ФСБ, ФСТЭК и другим нормативным актам.

Выявление неправомерных действий сотрудников и прогнозирование рисков

Нелояльные сотрудники — одна из главных причин утечки конфиденциальных данных. Причины бывают разные, например, экономические мотивы или идейные соображения. Мониторинг действий сотрудников помогает не только оценить эффективность их работы, но и собрать доказательную базу для расследования инцидентов.

Но новая парадигма ИБ — это профилактика нарушений на основе анализа больших данных. В этом поможет инструмент предиктивной аналитики в составе Traffic Monitor — UBA-система на основе искусственного интеллекта для прогнозирования возможных рисков. Автоматический рейтинг подозрительных сотрудников на основе динамических моделей их поведения покажет, на кого стоит обратить внимание в первую очередь.

BI-система для анализа данных

DLP-система нового поколения должна иметь гибкие и мощные средства для анализа данных. Обработка информации в режиме онлайн, выбор нужных срезов, переход к различным представлениям, сужение или расширение выборки, удобная визуализация — далеко не полный список возможностей динамического графа связей и виджетов Traffic Monitor. Построенная на «геймдев»-технологиях, система может быстро оперировать большими объёмами данных от десятков тысяч пользователей.

Автоматизация ИБ

Новые вызовы и угрозы требуют новых возможностей для защиты информации. Службы ИБ перегружены и им нужны инструменты для автоматизации их работы и сокращения времени на актуализацию политик безопасности, анализ ситуации, разбор событий и расследование инцидентов. Traffic Monitor даёт возможность актуализировать политики безопасности так часто, как это необходимо, в 3–4 раза быстрее расследовать инциденты и прогнозировать риски за счёт анализа больших данных. Автоматизация ИБ позволяет сфокусировать внимание на наиболее критичных событиях и подозрительных персонах.

Контентный анализ текстовых и графических файлов с помощью ИИ

2000 сотрудников создают примерно 2 миллиона событий DLP-системы в день. Точность детектирования позволяет избежать затрат времени специалистов службы ИБ на обработку ложноположительных срабатываний и не пропустить важные инциденты.

- **Защита текстовых документов с обучением на данных заказчика.** Автоматическое обучение на документах заказчика с помощью искусственного интеллекта. Достаточно «показать» системе набор документов одной тематики, и она автоматически обучится классифицировать похожие в ту же категорию
- **Защита изображений любого типа с помощью машинного зрения.** Анализ изображений для их классификации и поиска конфиденциального содержимого. Позволяет искать и контролировать в информационном потоке изображения любого содержания, даже если было изменено разрешение, расширение файла, присутствуют блики и т. д. Traffic Monitor «понимает», что изображено на любой картинке
- **Защита персональных и других именованных данных.** Детектирование персональных и других именованных данных (список клиентов, прайс-листы, складские остатки и т. п.) с помощью запатентованной технологии защиты данных из корпоративных БД. Для анализа 10 000 000 записей требуется менее 0,1 секунды
- **Категоризация всех документов компании.** Система регулярно сканирует файловые хранилища и рабочие станции и анализирует трафик. Найденные файлы исследуются и с помощью технологий искусственного интеллекта делятся на категории по смыслу. Специалист службы информационной безопасности видит всю информацию, понимает, где она хранится, и может быстро настроить политики безопасности

Универсальный перехватчик файлов

Возможность перехвата файлов из любого приложения. Не зависит от протокола приложения, способа шифрования и специфики передачи данных конкретным приложением.

Автоматизация настроек политик безопасности

При внедрении и последующей настройке политик безопасности нужно понимать, какая информация есть в компании и где она хранится. Автоматизированный анализ информационного поля позволяет регулярно категоризировать все документы. Для каждой такой категории при помощи технологий искусственного интеллекта создаётся лингвистическая модель, на основе которой можно настроить политику безопасности за одну минуту.

Контроль использования данных на личных устройствах сотрудников

На личных устройствах не установлен агент, а в случае использования облачных сервисов трафик циркулирует за пределами корпоративного периметра, то есть отсутствуют точки перехвата трафика. Интеграция с облачными системами позволяет контролировать, какие данные попадают на личные устройства.

Контроль копирования конфиденциальных документов в ненадлежащее хранилище внутри корпоративной инфраструктуры

Документ может быть выложен в сетевое хранилище, где будет доступен более широкому кругу сотрудников, чем предполагает его уровень конфиденциальности. Мониторинг и блокировка перемещения файлов внутри корпоративной сети предотвращают такие нарушения.

Защита данных DLP-системы

DLP-система аккумулирует огромное количество данных и сама по себе представляет хранилище информации. Ролевая модель, позволяющая гибко настроить политики доступа сотрудников отдела ИБ к той или иной информации, расширенный аудит их действий и защита от подбора пароля позволяют надёжно защитить данные, собранные DLP-системой.

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 tm.infowatch.ru
+7 495 22 900 22

Сопровождение проектных работ на всех этапах.

Техническая поддержка при пуско-наладке и эксплуатации системы.

Постоянное развитие и новые релизы каждого продукта, в среднем, 2 раза в год.

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 высокое качество и уникальность технологий, но и чувство уверенности, которое возникает от сотрудничества с InfoWatch благодаря сопровождению клиентов на всех этапах проектных работ.

/InfoWatchOut /InfoWatch

Министерство обороны Российской Федерации

Федеральная таможенная служба

Фонд социального страхования

Федеральная налоговая служба

Ростех

Газпром Внииагаз

Райффайзенбанк

Home Credit Bank

МТС Банк

СОГАЗ Страховая группа

e.on

Московский вертолетный завод им. М.Л. Миля

Сухой

ОДК

О'КЕЙ

SPSR express

STADA

НИАРМЕДИК Сеть семейных клиник

Магнит