INFOWATCH®

INFOWATCH DEVICE CONTROL

контроль использования внешних устройств

Один из самых опасных видов утечки — кража данных с использованием внешних устройств, ведь злоумышленник может скопировать на флешку большой объём конфиденциальной информации. А остановить и изъять у него устройство можно только в организациях со строгим контрольно-пропускным режимом.

Заблокировать внешние устройства на всех компьютерах зачастую невозможно: это помешает работе сотрудников. Оптимальное решение — разрешить использование в соответствии с легитимными процессами: только доверенные устройства, только тем сотрудникам, кому это нужно по работе, и только на разрешённых ПК.

Типичные ограничения привычных решений класса Endpoint security

негибкая система разграничения доступа

нет возможности делать точечные исключения — разрешить конкретному сотруднику использовать конкретную флешку на конкретном ПК

EPS в зоне ответственности ИТ-департамента

ИБ приходится делать запросы на получение данных или на ограничение доступа сотрудникам из групп риска

нет интеграции с другими СЗИ

сложно связать события DLP-системы, мониторинга действий сотрудников и попытки использования внешних устройств

неудобное назначение правил

когда политик безопасности десятки или сотни, сложно добавить новое правило и не «поломать» то, что уже работает

Ваши преимущества с InfoWatch Device Control

Предотвращайте утечки через внешние устройства без ущерба для бизнес-процессов: правила доступа можно задавать массово, но с любой детализацией и исключениями

Быстро анализируйте, как используют внешние устройства сотрудники, задействованные в инциденте ИБ, который расследуете: события InfoWatch Device Control связаны с данными об информационных потоках, хранении и доступе к информации, о действиях сотрудников за ПК

Безопасно перепроверяйте, что новое правило не повлияет на работу тех, на кого распространяться не должно: с помощью эмуляции срабатывания политик, а не в «боевом» режиме

Оперативно назначайте новые и уточняйте приоритет ранее созданных правил: в удобном интерфейсе, где всё понятно с первого взгляда

Ваши возможности с InfoWatch Device Control

Отслеживать попытки нарушить запрет подключения внешних устройств на ПК под Windows, Astra Linux, РЕД ОС и Alt Linux

Дополнять доказательную базу по расследованиям инцидентов ИБ

Разрешить использование внешних устройств строго в рамках необходимых бизнес-процессов и запретить во всех остальных случаях

Быстро создать правило на новое внешнее устройство, сопоставив заявку на подключение и список событий

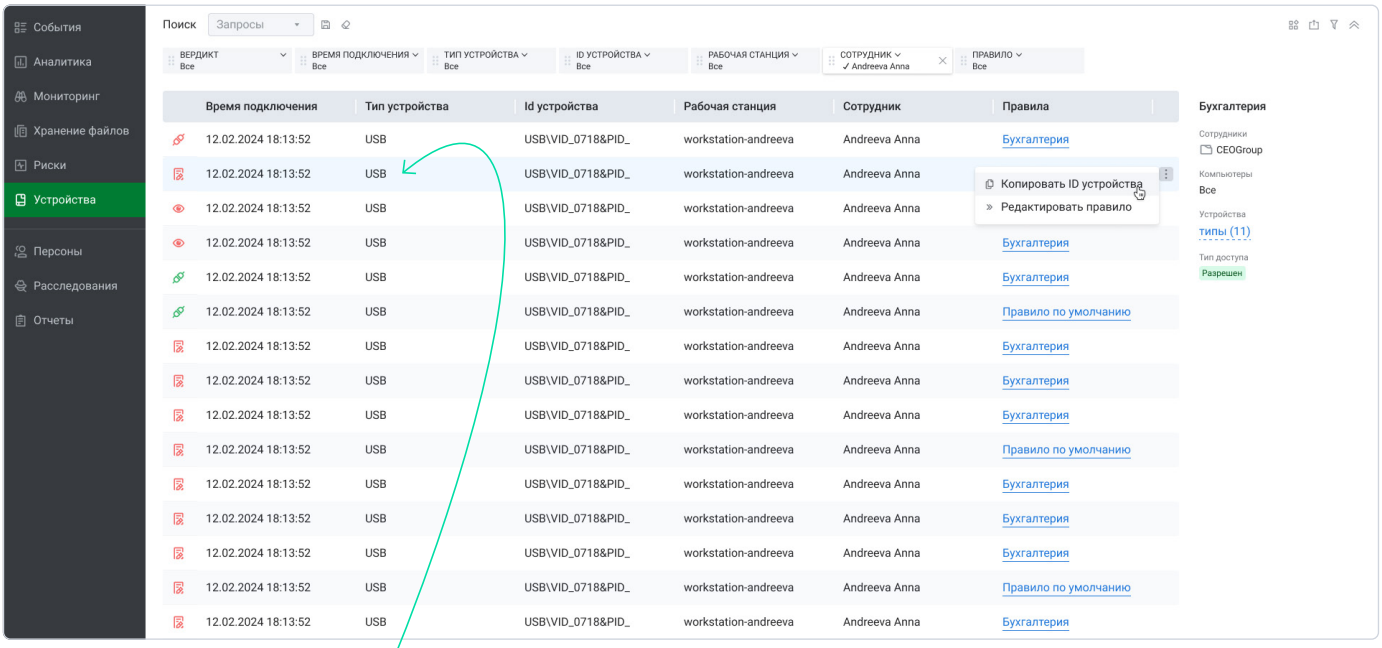
Как работает InfoWatch Device Control

Отображает кто, за каким ПК и как использовал внешние устройства

- подключение
- просмотр информации
- редактирование информации
- неудачные попытки неавторизованного подключения

Работает в едином интерфейсе продуктов InfoWatch для защиты данных — Центре расследований

Это позволяет быстро обогащать доказательную базу по инцидентам ИБ. Факты использования устройств можно сопоставить со всеми остальными действиями сотрудников за ПК, а также данными использования, хранения и получения доступа к конфиденциальной информации.



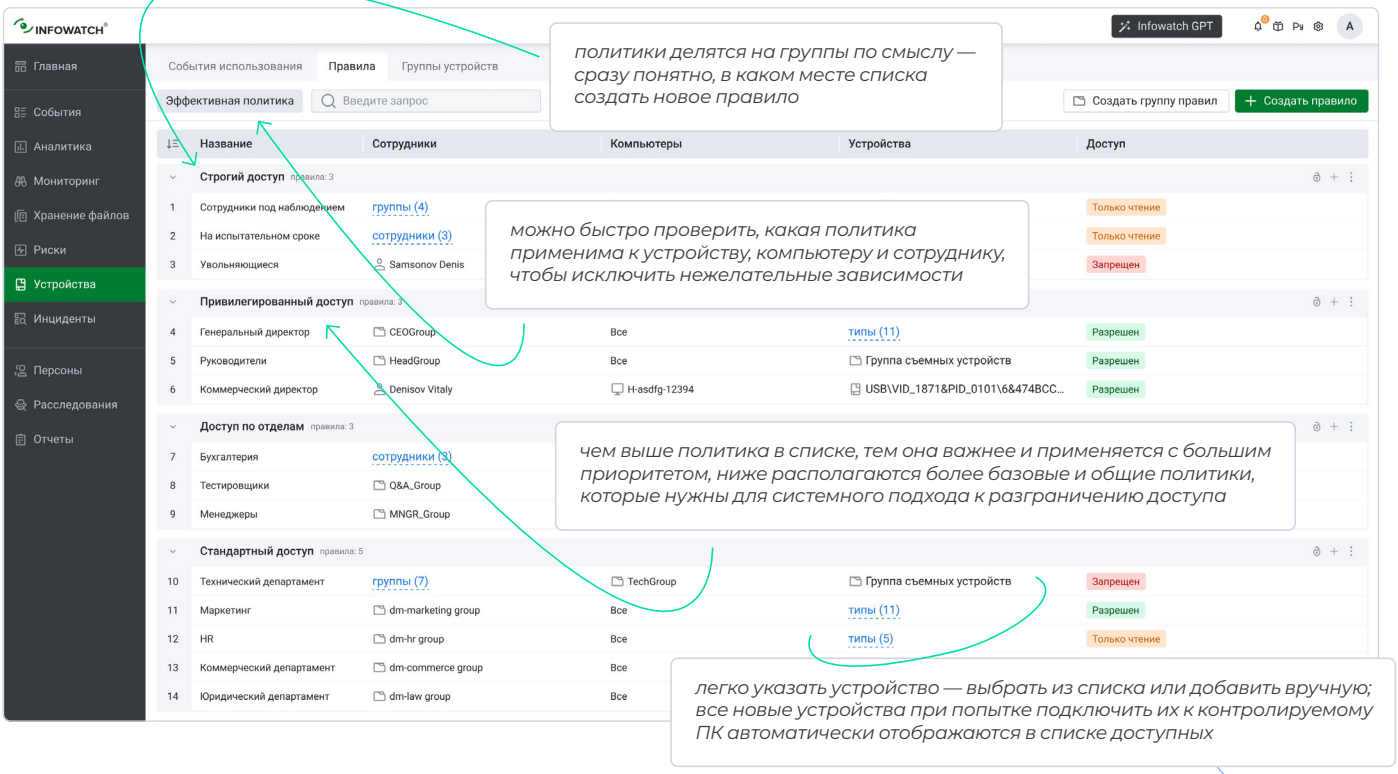
Например, специалист ИБ увидел попытку нарушить запрет подключения флешки на вкладке «Устройства». Без переключения между окнами и перестройки фильтра перешёл в раздел «Персоны» и оставил комментарий «был инцидент» в досье сотрудника. Затем в разделе «Мониторинг» на таймлайне детально посмотрел его действия до инцидента. В разделе «Хранение файлов» узнал, какую информацию сотрудник хранит на своём ПК. Сохраняя фокус на сотруднике, перешёл в «Аналитику» и на графе связей посмотрел его круг общения. Если на карте коммуникаций нашёл подозрительные события, по клику добавил их в «Расследования».

Гибкая система прав доступа обеспечивает должный баланс информационной безопасности и удобства бизнес-подразделений по использованию устройств

Специалист ИБ может выстроить систему прав по иерархии отделов или устройств, организационно-хозяйственной структуре с любыми исключениями — например, для высшего руководства.

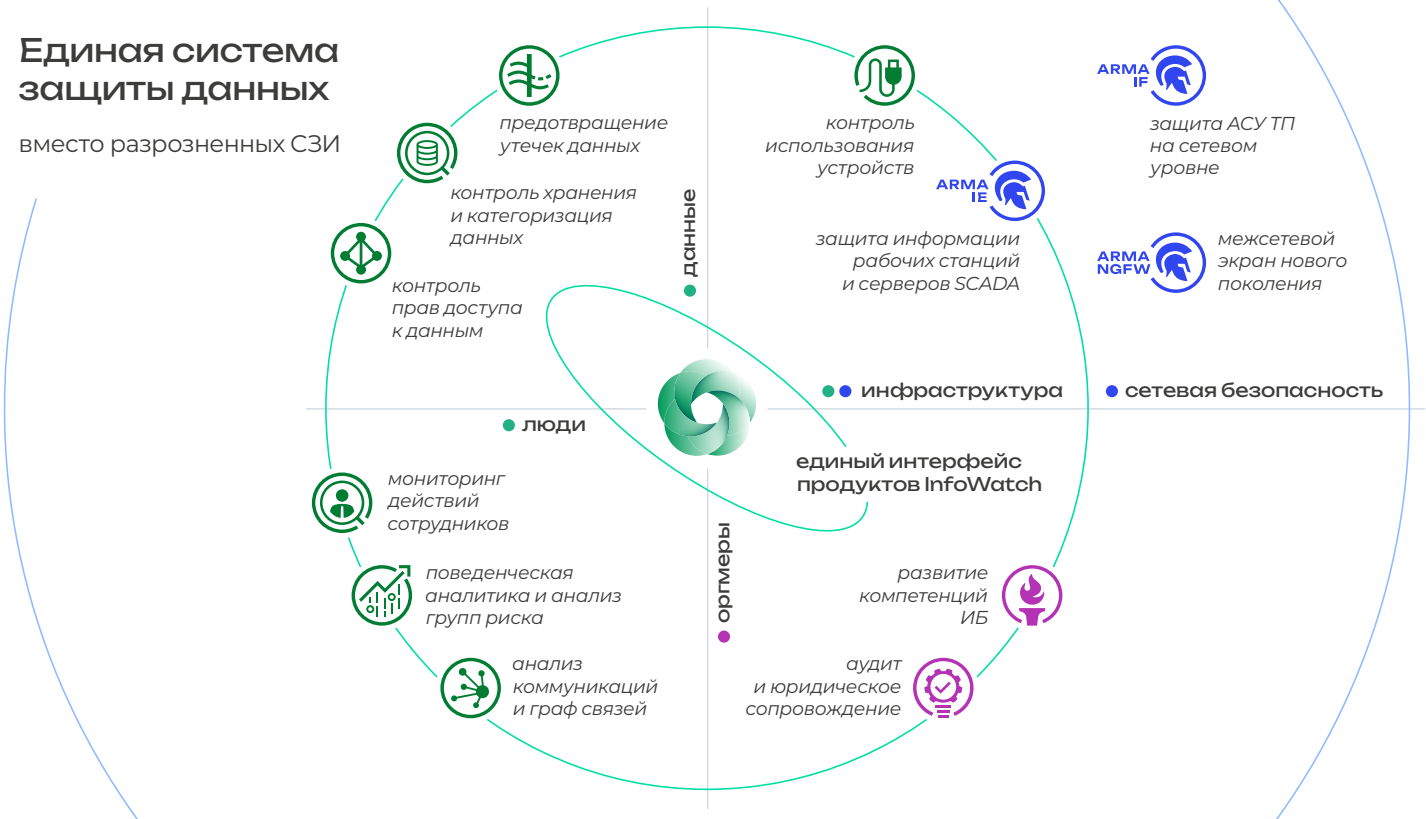
Назначайте правила

- на сотрудников и группы — например, отделы
- на конкретные ПК и группы ПК
- на типы устройств (флешки, диски, принтеры, модемы и др.), конкретные и группы
- на доступ к устройствам — разрешён, запрещён, только чтение



Единая система защиты данных

вместо разрозненных СЗИ



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
infowatch.ru

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 крупного бизнеса и государственных организаций. Лучшие инженеры, математики и лингвисты с 2003 года обеспечивают технологическое преимущество InfoWatch в области защиты от современных киберугроз информационных и кибербезопасности КИИ.

Признанный эксперт и лидер рынка DLP-систем России и СНГ, InfoWatch успешно развил свои решения в направлении всесторонней защиты данных, не ограничиваясь задачей борьбы с утечками информации. Подтверждением экспертизы и технологического преимущества InfoWatch являются более 4000 проектов для коммерческих и государственных организаций в двадцати странах мира.

Две трети из пятидесяти 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

Министерство обороны РФ
Центральное таможенное управление
Федеральная налоговая служба
Министерство энергетики РФ
Министерство сельского хозяйства РФ

мои документы
Банк России
Альфа Банк
ГАЗПРОМБАНК
СОВКОМБАНК
banki.ru
Русский Стандарт Банк
АЛЬФА СТРАХОВАНИЕ
MOEX МОСКОВСКАЯ БИРЖА
Яков и Партнёры
ВЕРТОЛЕТЫ РОССИИ
ДОМ РФ
ТРАНСНЕФТЬ
РОСНЕФТЬ
ГАЗПРОМ ДОБЫЧА
РОСАТОМ
МОСВОДОКАНАЛ
Внуково
МГТС
ТТК ТрансТелеКом
ТАСС
Mareven
CG CAPITAL GROUP
ОСТАНКИНО