



15 ЛЕТ ЗАЩИЩАЕМ
ВАШИ ДАННЫЕ

INFOWATCH ENDPOINT SECURITY

КОНТРОЛЬ ЦЕЛОСТНОСТИ ИТ-ИНФРАСТРУКТУРЫ

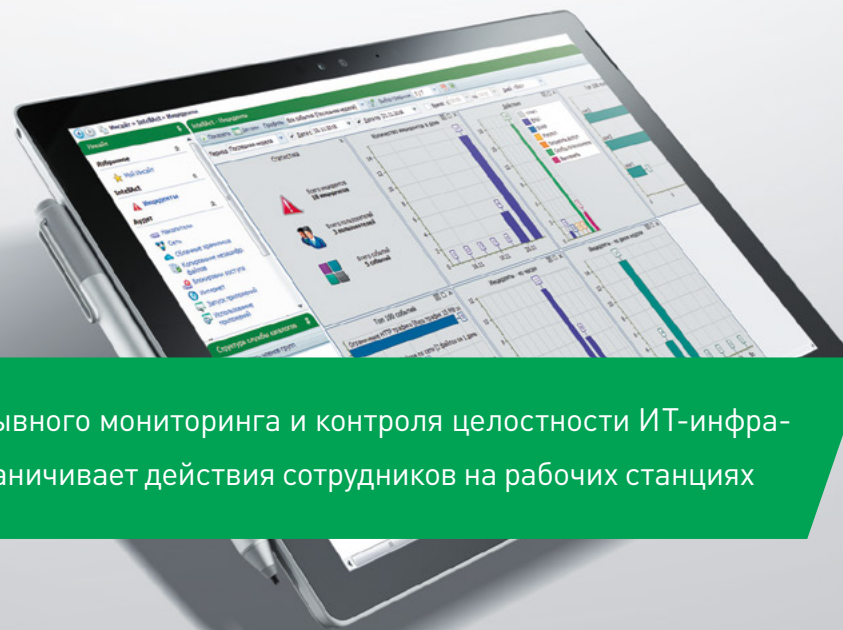


СПЕКТР ЗАДАЧ ИТ СЕГОДНЯ

Эффективное управление ИТ-инфраструктурой компании напрямую влияет на бизнес-результат. Перед ИТ-подразделениями стоит задача быстро и успешно решать проблемы пользователей, не уменьшая при этом уровень безопасности данных компании. Помимо этого, зачастую контроль ИТ-инфраструктуры тесно связан с контролем персонала, поэтому задачи службы безопасности возлагаются на плечи ИТ.

Компании нужны простые инструменты для контроля использования корпоративных систем и принятия управленческих решений. Решением этой задачи послужит инструмент, который снимет часть рутинных задач, не потеряв контроль над имеющейся ИТ-инфраструктурой.

- Комплексная защита инфраструктуры
- Прогнозирование ИТ-расходов
- Контроль действий персонала
- Автоматизация поддержки пользователей



INFOWATCH ENDPOINT SECURITY — система непрерывного мониторинга и контроля целостности ИТ-инфраструктуры, которая шифрует корпоративные данные и ограничивает действия сотрудников на рабочих станциях

КАК МОЖНО АВТОМАТИЗИРОВАТЬ КОНТРОЛЬ ИТ-АКТИВОВ



Разграничивать права доступа и возможности пользователей



Контролировать ИТ-ресурсы, рабочие станции и съемные носители



Шифровать съемные носители, локальные диски, сетевые папки и облачные хранилища

РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА

КОНТРОЛЬ ДОСТУПА

Сотрудники часто копируют корпоративную информацию на внешние носители и выносят ее за пределы компании. InfoWatch EndPoint Security позволяет управлять контролем доступа по списку разрешенных классов носителей, по авторизованным моделям устройств, по серийному номеру устройства, по списку разрешенных беспроводных сетей, а также по форматам и размерам файлов.

Помимо этого, администратор может запретить скачивание файлов через браузер, доступ к облачным файловым хранилищам (Dropbox, Microsoft OneDrive, Google Drive, Яндекс.Диск) и передачу файлов через Skype.



КОНТРОЛЬ ПРИЛОЖЕНИЙ

Обеспечивает контроль доступа сотрудников к приложениям с помощью белого и черного списков. Для оптимизации работы администратора предусмотрена возможность логического объединения приложений в пакеты программ, а также ведение белого списка приложений конкретного разработчика.

АУДИТ

В системе предусмотрена возможность ведения полного протокола действий:

- Запись действий пользователя при работе с информацией через внешние носители, сетевые папки, облачные хранилища с доступом к теневым копиям файлов из консоли управления
- Запись посещаемых веб-ресурсов и запущенных приложений с возможностью их категоризации

ФИЛЬТРАЦИЯ

Дает возможность определить форматы и типы данных, чтение и запись которых будут разрешены или запрещены сотрудникам. Содержит обширный список предустановленных форматов и позволяет добавить собственные.

INTELLACT

Позволяет администратору установить пороговые значения, с которыми система будет сравнивать показатели: копирование файлов, использование HTTP-трафика, количество дней до истечения лицензий и прочее. В случае превышения пороговых значений система считает данную активность инцидентом ИБ и может принять установленные меры.

УПРАВЛЕНИЕ ИТ-АКТИВАМИ

INSIGHT

С помощью этого модуля решение создает наглядные отчеты, которые помогут оценить и спрогнозировать использование сотрудниками ИТ-инфраструктуры компании — накопителей, сетевых и интернет-ресурсов, приложений и т. д. Insight позволяет выгрузить отчет и распечатать его, а также отправить по электронной почте сообщение о передаче данных за периметр безопасности.

ИНВЕНТАРИЗАЦИЯ

Отслеживает изменения, связанные с аппаратной частью рабочего места сотрудника (замену жестких дисков, модулей оперативной памяти, видеокарт и т. д.), и показывает объем свободного места на жестком диске.

МЕНЕДЖЕР ПАРОЛЕЙ

Централизованно хранит пароли учетных записей веб-сайтов на рабочей станции. Их можно задать вручную или сгенерировать с помощью системы.





НАДЕЖНОЕ УНИЧТОЖЕНИЕ

Функция безвозвратного удаления данных позволяет оперативно и гарантированно уничтожать данные с компьютеров сотрудников по заранее заданному расписанию или по мере необходимости.



GREEN IT

Сокращает потребление энергии, когда рабочие станции не используются. Профили Green IT позволяют отключать мониторы, переводить компьютеры в спящий режим в случае бездействия, включать и выключать компьютеры по заданному расписанию и т. д.



УПРАВЛЕНИЕ BITLOCKER

Управляет встроенным в Windows программным средством шифрования дисков.



ШИФРОВАНИЕ

ПРОЗРАЧНОЕ И НАДЕЖНОЕ ШИФРОВАНИЕ ДАННЫХ

Съемные носители, ноутбуки, облачные хранилища — наиболее уязвимые звенья корпоративной инфраструктуры. Они содержат большой объем конфиденциальной информации и слабо защищены от взломов и постороннего доступа, а также могут быть потеряны или украдены. Любая подобная ситуация может привести к репутационным и финансовым потерям.

InfoWatch EndPoint Security шифрует файлы в локальных каталогах ноутбуков и ПК, на внешних устройствах, в сетевых каталогах и в облачных хранилищах.

Шифрование данных происходит автоматически, не мешает сотрудникам и не требует дополнительных временных затрат. В зависимости от потребностей и бизнес-процессов организации в InfoWatch EndPoint Security можно использовать разнообразные типы шифрования.





Индивидуальное шифрование

Актуально для тех случаев, когда файл должен быть открыт только одним сотрудником.

Групповое шифрование

Доступ к зашифрованным файлам может быть у группы пользователей — например, у сотрудников одного отдела.

Общее шифрование

Все авторизованные сотрудники имеют доступ к чтению и записи зашифрованных файлов в любое время.

Шифрование по ГОСТ 28147-89

Доступно при установке криптопровайдера КриптоПро на сервер, компьютер офицера безопасности и рабочие станции персонала.

ПРЕИМУЩЕСТВА INFOWATCH ENDPOINT SECURITY

Масштабируемость InfoWatch EndPoint Security позволяет адаптироваться к изменениям в бизнес-процессах организации, подключая или отключая необходимые модули продукта, и обеспечивает высокий уровень доступности при увеличении нагрузок на корпоративную сеть. Архитектура InfoWatch EndPoint Security позволяет использовать его для разных сценариев в организациях любого размера.



КРУПНЫЙ БИЗНЕС

- Подходит для крупных компаний и организаций с географически распределенной филиальной структурой
- Собирает всю информацию в единой базе и управляет политиками из единого центра
- Не перегружает рабочие станции пользователей, контролируя нагрузку на сеть



МАЛЫЙ И СРЕДНИЙ БИЗНЕС

- Требуется минимальных настроек и обслуживания, быстро внедряется
- Дает представление об эффективности использования имеющихся ИТ-активов и целесообразности закупки новых
- Модульная структура: набор используемых функций определяется клиентом



- Контроль целостности ИТ-инфраструктуры
- Обеспечение замкнутости среды исполнения
- Контроль возможностей сотрудников на рабочих станциях
- Контроль нелегитимного использования ПО и ресурсов компании в личных целях
- Экономия бюджета компании на закупках ПО и железа



Бизнес-центр «Верейская плаза III»
121357, Москва, ул. Верейская, д. 29, стр. 33

+7 495 22 900 22, +7 499 37 251 74

sales@infowatch.ru

www.infowatch.ru