

КЛАССИЧЕСКИЕ ВОЗМОЖНОСТИ INFOWATCH ENDPOINT SECURITY ВЫРАЖАЮТСЯ ПРОСТОЙ ФОРМУЛОЙ – **C.A.F.E.**, КОТОРАЯ ОТРАЖАЕТ ФИЛОСОФИЮ ПРОДУКТА КАК ПРОСТОГО И НАДЕЖНОГО ПОМОЩНИКА ДЛЯ ЗАЩИТЫ РАСТУЩЕГО БИЗНЕСА

## InfoWatch EndPoint Security:

- идеален для малого и среднего бизнеса
- подходит для компаний любой сферы деятельности и отрасли
- внимателен к бизнес-процессам компании
- доступен даже при небольших бюджетах
- простой в освоении
- легкий в установке и настройке
- не создает нагрузку на сеть
- незаметный для рядовых сотрудников
- совместим с любым ПО, в том числе антивирусным
- единая консоль управления

**C.**

## CONTROL

Контроль подключения внешних устройств

**A.**

## AUDIT

Аудит действий сотрудников

**F.**

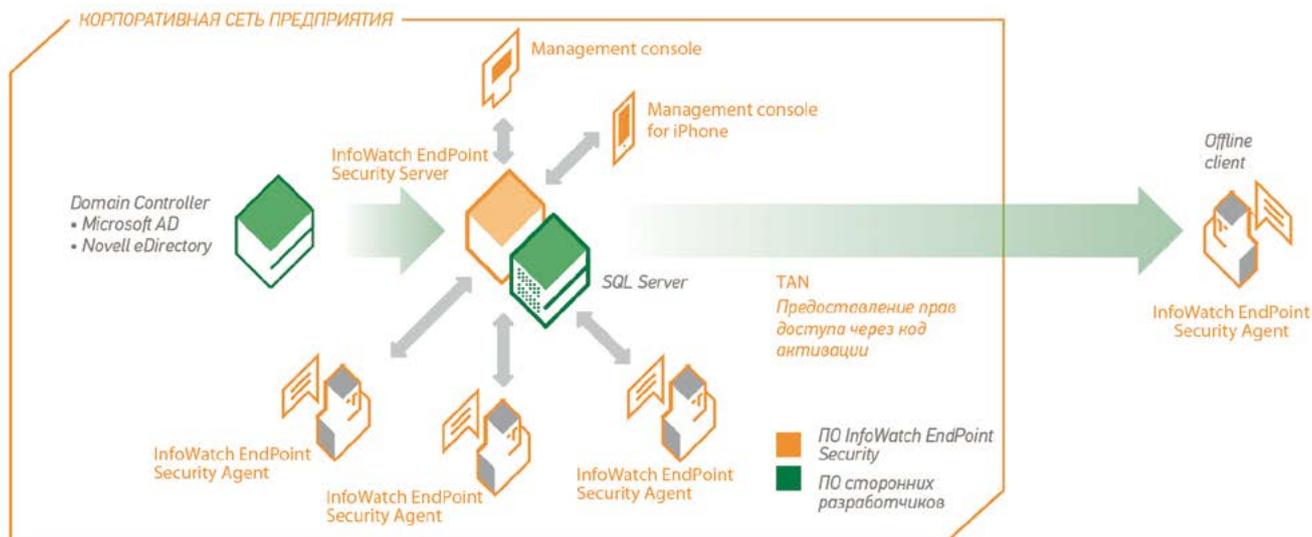
## FILTER

Фильтрация по типу данных

**E.**

## ENCRYPTION

Шифрование данных при записи на мобильные носители, ноутбуки и облачные хранилища



## ПРЕИМУЩЕСТВА ДЛЯ БИЗНЕСА



### Экономит затраты компании и снижает уровень финансовых потерь

- InfoWatch EndPoint Security **сокращает риски, связанные с утечкой информации**, в несколько раз: клиентские базы, скопированные на флешку и переданные конкурентам, могут стоить компании целого бизнеса. Продукт сводит к нулю риски потери или кражи важной информации благодаря возможности ее шифрования на любых съемных носителях, ноутбуках и при перемещении в облачные хранилища;
- **экономит трафик**: продукт работает быстро и незаметно для сотрудников, предотвращая действия и операции, которые не имеют отношения к работе;
- **экономит ресурсы персонала**: продукт настолько прост в установке, настройке и управлении, что не потребует найма квалифицированного администратора или сотрудника по информационной безопасности;
- **экономит электроэнергию**: благодаря наличию в продукте функции управления энергопитанием, можно по настроенному расписанию включать и выключать компьютеры, если сотрудники по какой-то причине этого не делают;
- **экономит на закупках дополнительного оборудования, сервисов и приложений**: продукт не требует дозакупки какого-либо оборудования или ПО, а благодаря функции шифрования многие бизнес-функции, например, документооборот, могут осуществляться через облачные хранилища, что обеспечивает экономию затрат.



### Весь необходимый функционал в одном продукте

InfoWatch EndPoint Security не содержит лишнего, ненужного функционала. Весь функционал по защите информации интегрируется в единый простой интерфейс, покрывая только по-настоящему важные области информационной безопасности.



### Внимателен к бизнес-процессам компании

InfoWatch EndPoint Security легко подстраивается под особенности рабочих процессов компании благодаря своей модульной, многокомпонентной структуре: выбирая слабые места в бизнес-процессе, вы защищаете только их, не закрывая доступ к тем ресурсам и активам, которые нужны для полноценной работы компании.



### Качественный и надежный продукт

Из 1000 компаний, установивших InfoWatch EndPoint Security, только 1% обращается в службу технической поддержки. Продукт работает безотказно, не вызывая «головной боли» ни у системных администраторов, ни у руководства и пользователей.



### Абсолютная простота и эргономичность

InfoWatch EndPoint Security устанавливается и настраивается за 20 минут сотрудником без какой-либо специальной квалификации или обучения, а управление продуктом осуществляется в пару кликов. В этом помогает интуитивно понятный интерфейс и бизнес-логика продукта.



### Доступная цена даже для небольших бюджетов

Приобретение InfoWatch EndPoint Security вписывается в операционный бюджет любой компании.



### Совместимость и производительность

InfoWatch EndPoint Security не конфликтует с корпоративными устройствами, системами и приложениями.





## ОТЛИЧНЫЙ ИНСТРУМЕНТ ДЛЯ ОПТИМИЗАЦИИ РАБОЧИХ ПРОЦЕССОВ, УВЕЛИЧЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ СОТРУДНИКОВ, СОКРАЩЕНИЯ ФИНАНСОВЫХ И РЕПУТАЦИОННЫХ ПОТЕРЬ, ЗАТРАТ НА ИТ И ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ.

Для решения специфических задач малого и среднего бизнеса InfoWatch EndPoint Security:

- находит резервы для повышения продуктивности бизнеса;
- берет на себя функции по контролю над производительностью сотрудников;
- учит сотрудников грамотно обращаться с информацией, которая имеет большое значение для эффективной работы бизнеса, а также с оборудованием компании, снижая затраты на электроэнергию и использование ресурсов компании в личных целях;
- помогает экономить на найме и обучении персонала, а также закупках дополнительного оборудования;
- позволяет соответствовать требованиям законодательства по обеспечению безопасности информации и защите устройств, на которых она хранится.

### Основные причины низкой эффективности бизнеса

«Бардак», отсутствие порядка в рабочих процессах



Сотрудники часто отвлекаются на социальные сети, развлекательные сайты



Частые проверки, высокие штрафы



Уход сотрудников с клиентской базой, переманивание клиентов



Если информация на ноутбуке была зашифрована, то потеря будет равна стоимости ноутбука, а если нет – потери могут составить сотни тысяч рублей.

С InfoWatch EndPoint Security можно минимизировать потери, защитив ценную информацию.

**4 из 5**

компаний не могут защититься от опасных программ, которые приносят с собой на флешках и других носителях сотрудники офиса.

InfoWatch EndPoint Security помогает взять под контроль все устройства и принести их под полный контроль, и, как следствие, предотвратить заражение компьютеров организации.

**70%**

сотрудников хранят на личных флешках важную конфиденциальную информацию компании (финансовые документы, базу клиентов, поставщиков, персональные данные) – для встреч, командировок, конференций, «чтобы поработать из дома» и т.д. В **60%** случаев эти флешки теряются или забываются. А клиентские базы попадают к конкурентам, нанося непоправимый вред бизнесу.

InfoWatch EndPoint Security поможет предотвратить такие последствия.

### «Безделье»

сотрудников обходится небольшим и средним компаниям в среднем 10% от месячного дохода.

InfoWatch EndPoint Security значительно сокращает расходы, вызванные разгильдяйством персонала.

**96%**

небольших и средних компаний ежегодно сталкиваются с потерей баз данных клиентов.

С InfoWatch EndPoint Security вы забудете об этой проблеме.



Включенные в нерабочее время компьютеры – довольно распространенная практика во многих офисах. В 1/3 случаев к таким компьютерам получают доступ сторонние лица, которые копируют и уносят с собой хранимую на ПК информацию.

InfoWatch EndPoint Security защищает от таких инцидентов, выключая компьютеры после окончания рабочего дня по заданному расписанию, что также способствует экономии затрат на электроэнергию.

**68%**

компаний со штатом до 200 человек становятся жертвами атак, направленных на получение доступа к файлам, хранящимся в «облаках».

InfoWatch EndPoint Security обеспечивает безопасное удаленное хранение, шифрование и контроль доступа к данным, размещенным в облачных хранилищах.

**40%**

рабочего времени сотрудники используют в личных целях – социальные сети, просмотр видеофильмов, компьютерные игры и т.д.

InfoWatch EndPoint Security сокращает эту цифру в несколько раз.

## ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

### Разграничение доступа сотрудников к важной информации



В процессе работы сотрудники активно пользуются съемными носителями, флешками, планшетами, смартфонами и другими коммуникационными устройствами – всё это несет серьезный риск того, что сотрудники скопируют и используют в личных целях важную для компании информацию. Это может нанести непоправимый вред бизнесу и репутации организации. А распространенный вирус с флешки сотрудника может поставить под угрозу всю ИТ-инфраструктуру компании, заблокировав работу основных подразделений на несколько часов или дней.

InfoWatch EndPoint Security помогает эффективно управлять рабочими процессами и грамотно разграничивать права доступа сотрудников к внешним устройствам.

InfoWatch EndPoint Security контролирует более 24 типов устройств и внешних носителей!

InfoWatch EndPoint Security обеспечивает контроль доступа к устройствам, портам, сетевым интерфейсам, сетевым каталогам и облачным хранилищам.

Продукт предлагает множество возможностей для управления правами доступа:

- по списку разрешенных классов носителей;
- по разрешенным моделям устройств (в таком случае разрешается доступ лишь к тем моделям устройств, которые находятся в разрешенном списке, доступ к остальным запрещен);
- по серийному номеру устройства (в таком случае разрешается доступ к устройствам с определенным серийным номером независимо от прав пользователя);
- по списку разрешенных беспроводных сетей (можно запретить доступ к Wi-Fi сетям, не входящим в список разрешенных).

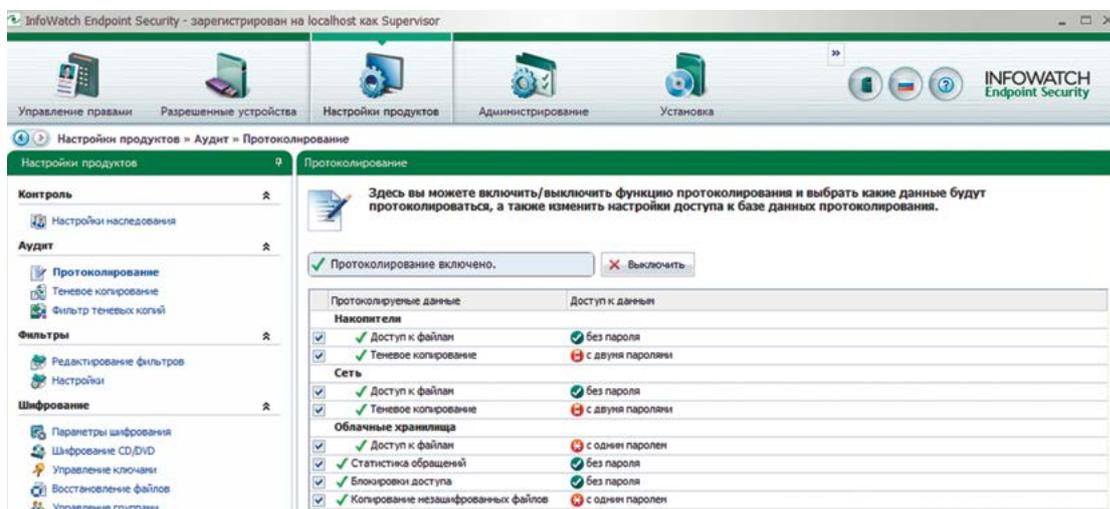
### Автоматический мониторинг нежелательных действий сотрудников

Картина рабочего времени сотрудников может быть весьма разнообразной: социальные сети, развлекательные сайты, компьютерные игры, просмотр фильмов, печать документов в личных целях. 70% всех компаний не отслеживают, чем занимаются сотрудники в рабочее время, какие файлы и данные они приносят или уносят с собой. Это нигде и никак не фиксируется.

InfoWatch EndPoint Security позволяет вести журнал событий и выявлять нецелевые действия сотрудников в отношении с важной информацией. Благодаря отчетам, которые формируются автоматически, можно выявлять «узкие» места в работе офисных сотрудников и находить резервы для повышения их производительности.

В журнале событий InfoWatch EndPoint Security отображаются действия каждого сотрудника: кто и когда выполнял те или иные операции, используя съемные устройства, телефоны, Wi-Fi сети, сетевые папки, облачные хранилища (чтение, копирование, создание или удаление).

Функция теневого копирования позволяет получить доступ к журналируемым файлам прямо из консоли продукта.



## Контроль информации во время ее копирования, хранения и использования в облачных хранилищах

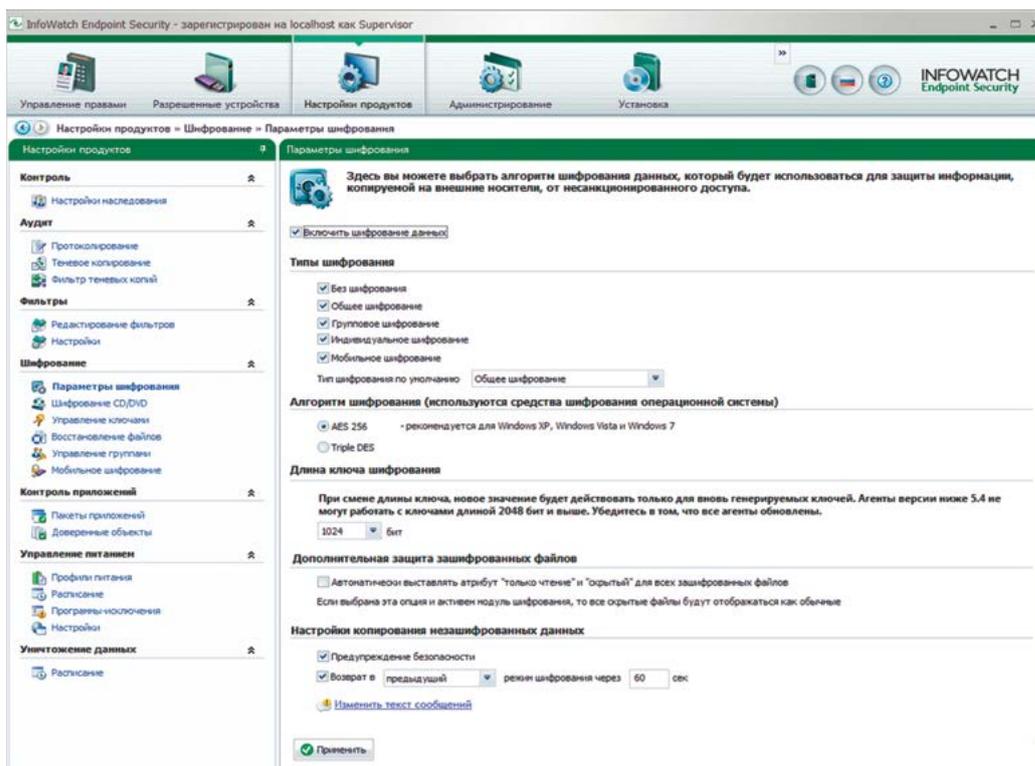
Небольшие компании активно пользуются «облаками» для обмена и хранения данных, однако лишь малая доля таких компаний задумывается о защите информации, отправляемой в «облако». Более 80% сотрудников ИТ-служб даже не осведомлены о том, сколько корпоративной информации хранится в «облаке», не говоря уже о том, что это за данные, и какую ценность для бизнеса они представляют.

InfoWatch EndPoint Security отслеживает все файлы, отправляемые сотрудниками в Dropbox, OneDrive, GoogleDrive, ЯндексДиск, VoxSync, а также регулирует эти процессы, запрещая или разрешая перемещение документов по определенному типу и формату данных.

Возможности InfoWatch EndPoint Security позволяют обмениваться файлами через облачные хранилища и не беспокоиться о безопасности информации.



Для каждого конкретного облачного провайдера, с которым сотрудничает компания, может быть выбран способ шифрования информации. При этом ключи шифрования остаются у клиента и не хранятся в «облаке», что полностью исключает возможность их попадания в чужие руки. Шифрование осуществляется на уровне файлов в прозрачном режиме, незаметном для сотрудников компании, что сводит на нет вероятность игнорирования или обхода системы, а также распространения вонне конфиденциальных документов в незащищенном виде.



### Шифрование с InfoWatch EndPoint Security – это:

#### Удобно:



Шифрование данных происходит незаметно для сотрудников, не нарушая производственный процесс

#### Прозрачно:



Данные автоматически записываются на носитель только в зашифрованном виде и расшифровываются при копировании на жесткий диск

#### Надежно:



Потеря или кража носителя не приведет к тому, что данные попадут к тем, кому они не предназначены

#### Гибко:



Шифрование для решения различных бизнес-задач: можно настроить доступ к зашифрованным файлам всем сотрудникам компании, группе пользователей (например, сотрудникам отдела) или только одному сотруднику

## Защита информации от кражи при потере ноутбуков и флешек

Съемные носители и ноутбуки – наиболее уязвимое звено в корпоративной инфраструктуре компании, поскольку сотрудники их часто теряют или «забывают».

InfoWatch EndPoint Security предлагает простой и удобный способ защитить информацию, зашифровав данные. Включив функцию шифрования в InfoWatch EndPoint Security, можно значительно повысить безопасность хранимой информации:

- никто из посторонних людей не сможет прочитать данные;
- потеря или кража устройства не повлечет за собой утечку информации;
- все данные автоматически шифруются сразу при их создании, не мешая сотрудникам и не требуя дополнительных временных затрат (прозрачное шифрование).

Продукт может шифровать информацию на ноутбуках, ПК, внешних устройствах, сетевых дисках, каталогах облачных хранилищ.

Шифрование данных происходит в фоновом режиме и абсолютно прозрачно незаметно для сотрудников. Применяется встроенный в операционную систему алгоритм шифрования AES256 с длиной ключа от 1024 до 4096 бит.

Шифрование в InfoWatch EndPoint Security может осуществляться как по инициативе сотрудника, так и в принудительном порядке системным администратором. С помощью функции мобильного шифрования InfoWatch EndPoint Security обеспечивает безопасную работу с данными, когда сотрудники находятся вне офиса.

## Управление запуском приложений

Игры, фильмы, музыка и другой развлекательный контент... Вы уверены, что сотрудники компании не смотрят сейчас новый фильм на рабочем месте? Не играют в игры? Как это отслеживается в вашей компании?

Неконтролируемое использование сотрудниками различных приложений снижает производительность труда, выполнение многих задач запаздывает, и, в конце концов, страдает весь бизнес, он становится неэффективным.

InfoWatch EndPoint Security позволяет управлять запуском приложений и контролировать доступ к ним сотрудников с помощью разрешенного (белого) или запрещенного (черного) списков. Это гарантирует, что никакая запрещенная программа или файл не будут установлены или запущены в рабочее время на компьютере предприятия.

В продукте предусмотрен режим обучения, который автоматически собирает информацию о запускаемых приложениях с компьютеров сотрудников и помогает сформировать список доверенных приложений - по разработчику ПО, расширению, сигнатуре файлов, а также настроить политики запуска приложений по сотрудникам, рабочим компьютерам и т.д.

