ENDPOINT PROTECTOR | by CoSoSys

ИНФОРМАЦИОННЫЙ ЛИСТ 4.4.0.9

Предотвращение утечки данных и управление мобильными устройствами

для любой отрасли и любого масштаба бизнеса

DLP для Windows, Mac and Linux

Защита для всей сети

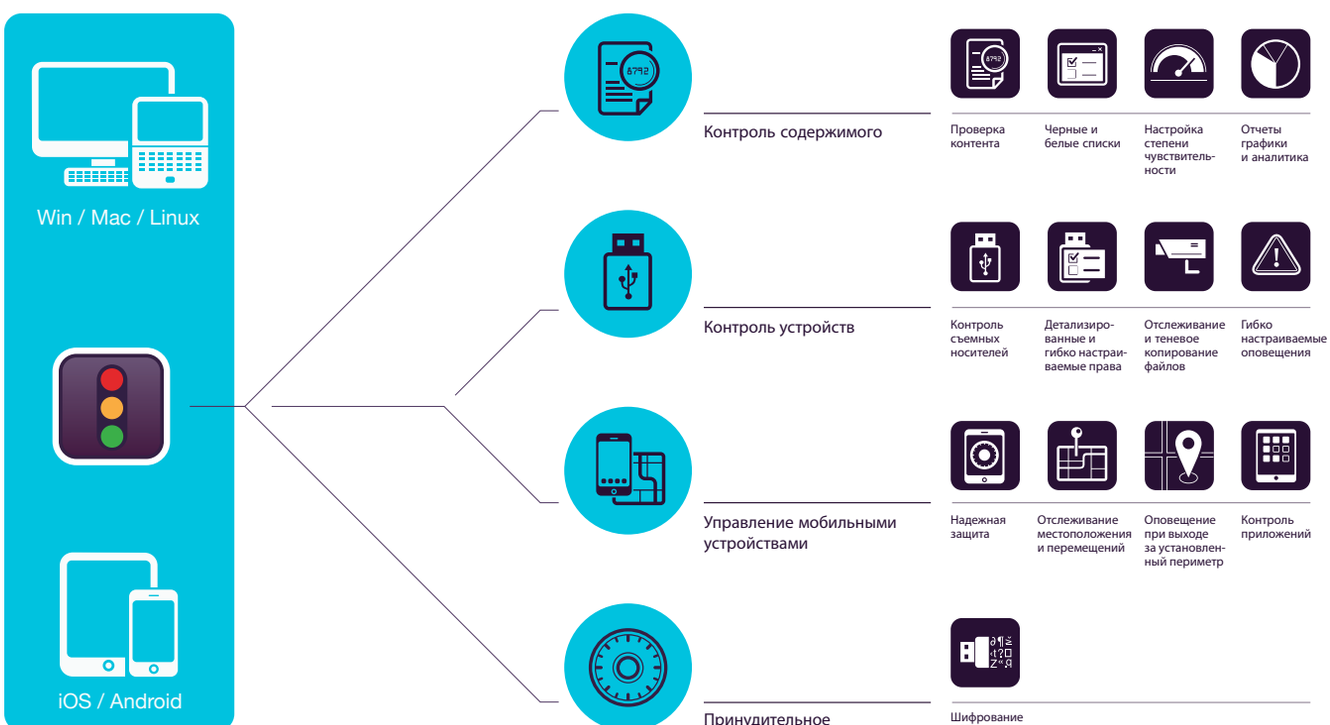
ENDPOINT PROTECTOR

by CoSoSys

Решение, которое работает "из коробки" и защищает конфиденциальные данные от угроз, связанных с использованием съемных носителей, облачных сервисов и мобильных устройств.

Мобильные устройства стремительно меняют наш подход к работе и жизни в современном мире. Endpoint Protector 4 создан, чтобы в этих условиях сохранить продуктивность и сделать работу более удобной и безопасной. Мы применяем метод "черных списков", с помощью которых можно запретить использование определенных устройств, интернет-адресов и доменных имен для конкретных компьютеров, пользователей или их групп. Это позволяет увеличить роизводительность труда, сохраняя контроль устройств и данных. Endpoint Protector 4 поставляется в виде виртуального или аппаратного устройства и может быть развернут в сети за считанные минуты. Наше решение позволяет существенно снизить риск утечки, кражи, повреждения и других способов недобросовестного использования ваших данных. Кроме того, система позволяет выполнять различные законные требования, касающиеся информационной безопасности.

Как это работает



Устройства под защитой

Контроль содержимого
для Windows, Mac OS X и Linux

Управляйте и контролируйте потоки конфиденциальной информации, которые должны (или, наоборот, не должны) покидать пределы вашей сети через различные устройства. Вы можете отфильтровывать информацию по таким параметрам, как тип файла, используемое приложение, готовые или настраиваемые стоп-листы, регулярные выражения и не только.

Контроль устройств
для Windows, Mac OS X и Linux

Отслеживайте и контролируйте использование портов для периферийного оборудования, включая USB. Устанавливайте правила доступа к ним для конкретных устройств, пользователей, групп, или для всех без исключения.

Управление мобильными устройствами
для Android, iOS и OS X

Управляйте мобильными устройствами (такими, как смартфоны и планшеты) и устанавливайте для них необходимый уровень безопасности.
Вы сможете удаленно контролировать настройки безопасности и сетевых подключений, а также используемые приложения.

Принудительное шифрование
для Windows и Mac OS X

Обеспечьте автоматическую защиту информации, которая копируется на USB-носители. 256-битное шифрование по алгоритму AES работает на различных платформах, просто в использовании и очень эффективно.

Контроль содержимого

для Windows, Mac OS X и Linux

Контролирует клиенты электронной почты: Outlook, Thunderbird, Lotus Notes. Браузеры: Internet Explorer, Firefox, Chrome, Safari. Клиенты мгновенных сообщений: Skype, Microsoft Communicator, Yahoo Messenger. Облачные сервисы и файлообменники: Dropbox, iCloud, SkyDrive, BitTorrent, Kazaa. Другие приложения: iTunes, Samsung Kies, Windows DVD Maker, Total Commander, Team Viewer. И многое другое.

Готовые фильтры содержимого

Можно создавать фильтры из готовых шаблонов, например, таких, как "номера кредитных карт" или "номера социального страхования" и многих других.

Настраиваемые фильтры содержимого

Вы можете настраивать собственные фильтры, основанные на ключевых словах и выражениях. А также создавать различные "черные списки" слов.

Фильтры на основе"регулярных выражений"

Шаблоны из регулярных выражений позволяют фильтровать контент на основе гибко настраиваемых закономерностей в тексте.

Фильтрация по типу файла

Блокируйте передачу отдельных типов файлов по расширению, даже если оно было изменено пользователем вручную.

Белые списки файлов

Если вы настроите сплошное блокирование передачи любых файлов, белые списки помогут избежать лишних срабатываний защиты.

Белые списки доменов и веб-адресов

Устанавливайте ограничения без ущерба для работы! Вы можете создавать "белые списки" и вносить туда нужные сотрудникам сайты и адреса электронной почты.

Запрещайте делать снимки экрана

Вы можете отключить возможность делать снимки экрана (скриншоты). Это значительно повысит защищенность от утечек.

Мониторинг буфера обмена

Предотвращайте утечки конфиденциальных данных путем копирования/вырезания и вставки.

Отчеты и аналитика

Отслеживайте действия пользователей, связанные с передачей файлов, с помощью мощного инструмента построения отчетов и анализа. Лог-файлы и отчеты могут также выгружаться во внешние SIEM-системы.

Панель управления и наглядные графики

Для быстрого обзора состояния системы и событий предусмотрена удобная страница с текущей статистикой и оповещениями.

Active Directory

Воспользуйтесь возможностями AD и подобных инструментов, чтобы облегчить развертывание Endpoint Protector в больших сетях. Импортируйте и синхронизируйте группы и объекты.

Устанавливайте чувствительность фильтров

Определяйте, какое количество срабатываний фильтра в документе должно приводить к запрету его передачи.

Отслеживание файлов

Записывайте все перемещения файлов, включая попытки передачи через онлайн-приложения и облачные сервисы. Полная картина действий пользователя!

Теневое копирование файлов

Сохраняйте копии файлов, переданных на разрешенные носители, а также по электронной почте, через облачные сервисы и другие приложения.

Временный пароль для работы оффлайн

Позволяет совершать копирование и перемещение файлов, когда компьютер не имеет связи с сервером Endpoint Protector. Это обеспечивает безопасность и продуктивность, даже если пользователь вне сети.

Оповещения по электронной почте

Готовые и настраиваемые оповещения по электронной почте вовремя проинформируют Вас о копировании или перемещении важных файлов.

Претовращение утечек через принтеры

Запрещайте печать конфиденциальных документов на локальных и сетевых принтерах - это еще один возможный канал утечки данных.

Соответствует правилам HIPAA

Позволяет сканировать документы на соответствие правилам обмена медицинской информацией в соответствии с актом HIPAA и другими нормативными актами.

Защита от утечек для "тонких клиентов"

Защищайте данные на терминальных серверах, с которыми пользователи работают через "тонкие клиенты"

Дополнительные возможности

Продукт содержит еще много полезных опций
info@endpointprotector.com

Контроль устройств
для Windows, Mac OS X и Linux

Контролирует USB-носители, принтеры, устройства Bluetooth, плееры MP3, внешние жесткие диски, программируемые микроконтроллеры Teensy, цифровые камеры, веб-камеры, порты Thunderbolt, планшетные компьютеры, общие сетевые ресурсы, устройства FireWire, iPhone, iPad, iPod, ZIP-диски, последовательные порты, модули PC Card (PCMCIA), биометрические устройства и многое другое.

Устанавливайте глобальные права
По умолчанию, права устройств устанавливаются для всех. Однако вы можете задавать более детальные права для отдельных устройств, пользователей и групп.

Устанавливайте права для групп
Права устройств могут настраиваться отдельно для каждой группы, что позволяет давать индивидуальные права каждому отделу компании.

Специальные разрешения для отдельных ПК
Вы можете задавать специфические права для отдельных компьютеров. Это пригодится, если компьютер выполняет какую-то особую функцию.

Особые права для отдельных пользователей
Задавайте индивидуальные права на работу с устройствами отдельным пользователям, в зависимости от их обязанностей.

Устанавливайте права для устройств
Вы можете устанавливать права даже для работы с отдельными устройствами, идентифицируя их по Vendor ID, Product ID или серийному номеру.

Дополнительные классы устройств
Права на использование могут задаваться в зависимости от типа устройств. Это облегчает управление устройствами одного производителя, но разного типа.

Доверенные устройства
Можно настраивать разные права доступа к зашифрованным устройствам, в зависимости от уровня шифрования (программный, аппаратный и т.д.)

Отслеживание файлов
Записывайте все перемещения файлов, включая попытки передачи через онлайн-приложения и облачные сервисы. Полная картина действий пользователя!

Теневое копирование файлов
Сохраняйте копии файлов, которые перемещаются на контролируемые устройства, в целях отслеживания действий пользователей.

Временный пароль для работы оффлайн
Давайте временное разрешение на подключение устройств к компьютеру, даже если он отключен от интернета или локальной сети.

Оповещения по электронной почте
Готовые и настраиваемые оповещения по электронной почте вовремя проинформируют Вас о событиях, связанных с использованием устройств.

Панель управления и наглядные графики
Для быстрого обзора состояния системы и событий предусмотрены наглядные графики.

Отчеты и аналитика
Отслеживайте действия пользователей, связанные с использованием устройств, с помощью мощного инструмента построения отчетов и анализа. Лог-файлы и отчеты можно экспортировать.

Дополнительные возможности
Продукт содержит еще много полезных опций
info@endpointprotector.com

Принудительное шифрование
для Windows и Mac OS X

Принудительное шифрование USB-устройств
Разрешите использование только зашифрованных USB-носителей - и будьте уверены в том, что вся информация, скопированная на съемные носители, будет автоматически защищена.

Надёжные механизмы защиты
Одобренное государственными организациями 256-битное шифрование по алгоритму AES, защита паролем, защита от подделки информации.

Мастер-пароль
Можно создать один главный пароль, который позволит администратору совершать любые нужные действия по управлению клиентской частью EPP.

Дополнительные функции
Шифрование также доступно для облачных хранилищ, локальных папок, CD и DVD
info@endpointprotector.com

Управление мобильными устройствами

для Android, iOS и Mac OS X

Беспроводная установка на iOS и Android

Беспроводная установка на устройства. Просто отправьте на целевое устройство SMS, сообщение электронной почты, ссылку или QR-код.

Массовая установка

Массовая установка может охватывать до 500 планшетов и смартфонов за один раз, что позволяет экономить время.

Удалённая блокировка

Блокируйте мобильное устройство удалённо, если оно было утеряно или попало в руки злоумышленников.

Отслеживание перемещений устройства

Просматривайте местоположение и историю перемещений мобильных устройств, чтобы точно знать, где находятся конфиденциальные данные

Отключайте потенциально опасные функции

Отключайте встроенные функции мобильных устройств - например, использование фотокамеры, для предотвращения утечек данных.

Звуковой сигнал для поиска устройства

Находите потерянные мобильные устройства, удаленно включая на них громкий звуковой сигнал (только для Android).

Управление мобильными приложениями

Управляйте мобильными приложениями в соответствии с политикой безопасности компании. Удаленно устанавливайте приложения на устройства сотрудников.

Управляйте сетевыми настройками

Отправляйте на мобильные устройства сетвые настройки, включая настройки электронной почты, Wi-Fi, VPN, Bluetooth, меняйте режим звонка смартфонов.

Системные оповещения

Готовые и настраиваемые системные оповещения.

Панель управления и наглядные графики

Для быстрого обзора состояния системы и событий предусмотрены наглядные графики.

Работа в режиме киоска Samsung KNOX

Блокируйте и ограничивайте использование отдельных приложений. Удаленно управляйте полтиками безопасности.

Управление устройствами на Mac OS X

На компьютеры MAC тоже можно устанавливать модуль управления мобильными устройствами, что расширяет возможности по защите данных.

Обязательное использование пароля

Обязательное использование сложных паролей позволит защитить конфиденциальные данные компании на мобильных устройствах.

Удалённое стирание

В некоторых ситуациях предотвратить утечку важных данных можно, только полностью стерев память устройства. MDM модуль позволяет легко сделать это удалённо.

Виртуальные границы для устройств

Задавайте виртуальные периметры на карте, при пересечении которых на мобильных устройствах будут применяться нужные Вам правила.

Ограничивайте функции iOS

Ограничьте возможность запуска приложений, не относящихся к работе. Например, можно отключить

Отправляйте контакты на Android

Ограничьте возможность запуска приложений, не относящихся к работе. Например, можно отключить iCloud, Safari, App Store и так далее.

Мониторинг приложений

Будьте в курсе приложений, которые ваши сотрудники устанавливают на свои устройства, чтобы четко разграничить работу и отдых.

Инвентаризация

Просматривайте информацию о парке ваших мобильных устройств - названия, типы, модели, аппаратные характеристики, версии ОС, номера IMEI, MAC-адреса и т.д.

Оповещения по электронной почте

Вы можете настроить оповещения по электронной почте о наиболее важных событиях на мобильных устройствах.

Отчеты и аналитика

Отслеживайте действия пользователей, связанные с использованием устройств, с помощью мощного инструмента построения отчетов и анализа. Лог-файлы и отчетыможно экспортировать.

Дополнительные возможности

Продукт содержит еще много полезных опций
info@endpointprotector.com

100% гибкость при установке

Наши продукты подходят для любых типов сетей - корпоративных клиентов, малого, среднего бизнеса, и даже для домашних компьютеров. Клиент-серверная архитектура Endpoint Protector позволяет легко устанавливать наше программное обеспечение в сети и управлять безопасностью данных через веб-интерфейс.
Вы можете выбрать наиболее удобный способ установки Endpoint Protector - в аппаратном или виртуальном исполнении, на базе Amazon Web Services или в "облачной" версии, и даже в виде отдельного приложения на клиентском устройстве, если нужны только базовые функции по защите конфиденциальных данных.

Endpoint Protector

Контроль содержимого, контроль устройств и шифрование доступны для компьютеров, работающих на различных версиях Windows, Mac и Linux. Управление мобильными устройствами мобильными приложениями также доступны для iOS и Android.

My Endpoint Protector

Контроль содержимого, контроль устройств и шифрование доступны для компьютеров, работающих на Windows и Mac. Управление мобильными устройствами и мобильными приложениями также доступны для iOS и Android.

Аппаратное устройство

Виртуальное устройство

Виртуальная машина

Облачный хостинг

Modules

	Защищаемые устройства					
Windows	Windows XP / Windows Vista	(32/64 bit)	●	●	●	
	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	
	Windows Server 2000 - 2016	(32/64 bit)	●	●	●	
Mac OS X	Mac OS X 10.6	Snow Leopard	●	●	●	
	Mac OS X 10.7	Lion	●	●	●	
	Mac OS X 10.8	Mountain Lion	●	●	●	
	Mac OS X 10.9	Mavericks	●	●	●	
	Mac OS X 10.10	Yosemite	●	●	●	
	Mac OS X 10.11	El Capitan	●	●	●	
Linux	Ubuntu		●	●	n/a	
	OpenSUSE		●	●	n/a	
	CentOS / RedHat		●	●	n/a	
	*Пожалуйста, проверяйте информацию о поддерживаемых версиях Linux на endpointprotector.com/linux					
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9					●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+)					●

COSOSYS

Главный офис (Румыния)

E-mail sales@cososys.com
Sales +40 264 593 110 / ext. 103
Support +40 264 593 113 / ext. 202

Германия

vertrieb@endpointprotector.de
+49 7541 978 26730
+49 7541 978 26733

Корея

E-mail contact@cososys.co.kr
Sales +82 70 4633 0353
Support +82 20 4633 0354

США

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

Official Partner

www.endpointprotector.com