ENDPOINT PROTECTOR | by CoSoSys

Информационный лист 5.2.0.0

Предотвращение утечки данных и управление мобильными устройствами

Для сети любого масштаба и любой отрасли

Защита данных для Windows, Mac и Linux

Защита всей сети

ENDPOINT PROTECTOR

by CoSoSys

Готовое решение для защиты конфиденциальных данных, связанных с использованием съемных носителей, облачных сервисов и мобильных устройств.

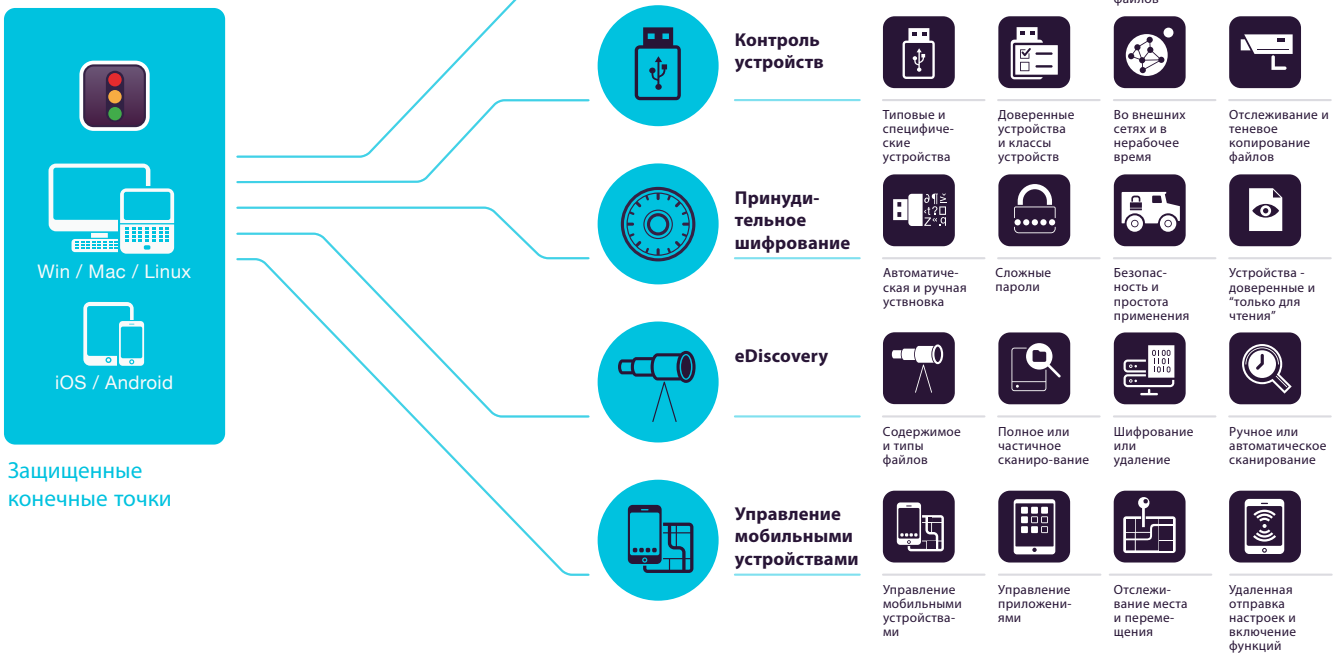
В современном мире мобильные устройства и облачные технологии широко используются как в быту, так и в работе. В этих условиях Endpoint Protector призван защитить конфиденциальные данные от утечки или кражи, при этом не создавая лишних препятствий и делая работу удобнее и безопаснее.

Подход, основанный на черных и белых списках, делает настройку политик максимально гибкой. Компания может запретить использование определенных съемных носителей или отправку информации через облачные сервисы, сканировать устройства пользователей на наличие персональных данных, при этом разрешая определенным пользователям, компьютерам или группам отправку данных на заданные адреса.

Endpoint Protector можно ввести в эксплуатацию за несколько минут. Вы можете установить его в виде программно-аппаратного комплекса или виртуального приложения. Адаптивный веб-интерфейс приложения позволяет управлять политиками и просматривать отчеты с мобильного устройства, ПК или планшета.

Endpoint Protector значительно снижает риск, связанный с внутренними угрозами, которые могут привести к утечке или краже данных. Кроме того, наше решение позволяет компании выполнять различные отраслевые требования к информационной безопасности.

Как это работает



Content Aware Protection
защита содержимого для Windows, macOS и Linux

Отслеживайте и контролируйте перемещение данных. Решайте, какие данные и по каким каналам могут покидать пределы вашей сети. Данные можно фильтровать по типу файла, приложению, готовым и собственным шаблонам содержимого, регулярным выражениям и т.д.

Device Control
контроль устройств для Windows, macOS и Linux

Отслеживайте и контролируйте использование USB и периферийных портов. Назначайте права устройствам, пользователям, компьютерам, группам, а также глобальные права.

Enforced Encryption
шифрование для Windows и macOS

Обеспечивайте автоматическую защиту данных, копируемых на USB-носители, 256-битным алгоритмом AES. Это эффективная и простая в использовании кроссплатформенная технология.

eDiscovery
поиск конфиденциальной информации на носителях для Windows, macOS и Linux

Сканируйте данные, сохраненные на пользовательских устройствах, и применяйте к ним в случае необходимости меры защиты, такие, как удаление или шифрование - если конфиденциальные данные обнаружены на неавторизованных компьютерах.

Mobile Device Management
управление мобильными устройствами

Управляйте, контролируйте и настраивайте уровень безопасности на смартфонах и планшетах. Отправляйте на них настройки безопасности, сетевые настройки, приложения и т.д.

Защита содержимого

для Windows, macOS и Linux

Почта: Outlook / Thunderbird / Lotus Notes • Браузеры: Internet Explorer / Firefox / Chrome / Safari • Клиенты мгновенных сообщений: Skype / Microsoft Communicator / Yahoo Messenger • Облачные хранилища: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Другие приложения: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • и многое другое.

Черные списки каналов утечки

Фильтрация контента, отправляемого через приложения, USB-устройства, сетевые папки и другие средства передачи данных.

Черные списки типов файлов

Блокируйте определенные типы файлов, даже если пользователь изменил их расширение.

Шаблоны контента, запрещенного для передачи

Готовые шаблоны конфиденциальных данных, такие, как номера кредитных карт,СНИЛС и другие.

Собственные черные списки контента

Создавайте свои фильтры, основанные на ключевых словах и выражениях. Создавайте словари для фильтрации контента.

Черные списки имен файлов

Черные списки могут учитывать имя, расширение файлов или и то, и другое.

Черные и белые списки расположений

Фильтры, основанные на расположении файлов на жестком диске, с возможностью включать или исключать подпапки.

Черные списки на основе регулярных выражений

Дополнительные фильтры, позволяющие находить определенные последовательности символов в передаваемых данных.

Белые списки файлов

Блокируя все прочие попытки передачи файлов, можно задать списки разрешенных файлов, необходимых для работы.

Белые списки доменов и URL

Усиливая безопасность, обеспечивайте при этом доступ к необходимым ресурсам.
Добавляйте в белый список порталы и адреса электронной почты компании.

Мониторинг скриншотов и буфера обмена

Блокируйте снятие скриншотов, а также утечку данных через функцию копирования/вставки.

Распознавание графических образов

Исследуйте содержимое изображений, чтобы отследить конфиденциальную информацию в отсканированных документах и других подобных типах файлов.

Отслеживание и теневое копирование файлов

Отслеживайте перемещение файлов по различным каналам. Получайте копии перемещаемых файлов.

Пороги срабатывания фильтров

Определяйте, какое количество срабатывания фильтра заблокирует передачу файла.

Лимит передачи данных

Устанавливайте лимит передачи данных в течение определенного периода. Лимит устанавливается на количество или размер файлов. Можно настраивать оповещения по электронной почте при достижении лимита.

Контекстное сканирование содержимого

Настраивайте дополнительный механизм сканирования конфиденциальной информации, такой, как персональные данные.

Временный оффлайн-пароль

ыдавайте временное разрешение на передачу данных на компьютерах, отключенных от сети, чтобы не мешать работе и при этом обеспечить безопасность.

Панели, отчеты и аналитика

Мониторинг перемещений файлов с помощью мощного инструмента отчетности и аналитики. Экспорт результатов в SIEM-системы.

Соответствие стандартам

Использование данного модуля позволяет обеспечить соответствие отраслевым стандартам защиты данных, таким, как PCI DSS, GDPR, HIPAA и т.д.

Защита от утечки данных через принтеры

Политики защиты от печати конфиденциальных данных на локальных и сетевых принтерах.

Защита для “тонких клиентов”

Защищайте данные на терминальных серверах при работе через тонкие клиенты.

Дополнительные функции / Доступно также множество дополнительных функций. / info@endpointprotector.com

Контроль устройств

для Windows, macOS и Linux

USB-носители / принтеры / Bluetooth / MP3 плееры / Внешние жесткие диски / Камеры / Вебкамеры / Thunderbolt / планшеты / сетевые хранилища / FireWire / iPhone / iPad / iPod ZIP-диски / последовательные порты / PCMCIA-хранилища / биометрические устройства

Детализированое назначение прав
Права устройств можно назначить глобально, для группы, пользователя или конкретного устройства.

Отслеживание файлов
Фиксируйте все перемещения или попытки копирования файлов на USB-носители.

Типы устройств и конкретные устройства
Устанавливайте права (запрет, разрешение, тголько чтение и т.д.) - для определенных типов устройств или конкретных устройств (по идентификатору вендора или серийному номеру).

Теневое копирование файлов
Сохраняйте копию файлов, перемещаемых на контролируемые устройства.

Дополнительные классы
Можно назначать права для устройств, группируя их в определяемые вами классы.

Временный оффлайн-пароль
Временно разрешайте использование устройств на компьютерах, отключенных от сети.

Политики для нерабочего времени
Применяйте политики контроля устройств в нерабочее время. Можно настроить интервал рабочего времени, а также рабочие и нерабочие дни.

Оповещения по электронной почте
Стандартные и пользовательские оповещения о наиболее критичных событиях, связанных с применением устройств.

Политики для устройств за пределами сети
Вы можете настроить политики работы с устройствами, когда компьютер находится за пределами сети. Применение основано на DNS и IP-адресах.

Панели и графики
Важнейшие события и статистика отображаются в графическом представлении.

Импорт и синхронизация с Active Directory
Интеграция с AD упрощает развертывание в крупных сетях. Синхронизируйте группы, компьютеры и пользователей со службой каталогов.

Отчеты и аналитика
Отслеживайте использование устройств с помощью мощного инструмента отчетов и аналитики. Логи и отчеты можно экспортировать.

Информация о компьютерах и пользователях
Получите больше информации об объектах сети - ID сотрудников, командах, местоположении, точных контактных данных, IP, MAC-адресах и т.д.

Дополнительные функции
Доступно также множество дополнительных функций.
info@endpointprotector.com

Принудительное шифрование

для Windows и macOS

256-битное шифрование AES / защита от фальсификации / целостность приложения / отправка сообщений пользователям / сброс к заводским настройкам / политики паролей

Принудительное шифрование USB
Разрешайте использование только зашифрованных устройств. Обеспечивайте автоматическое шифрование данных, копируемых на носители.

Сложные пароли для пользователя и администратора
Уровень сложности пароля можно устанавливать в зависимости от необходимости. Мастер-пароль позволяет производить сброс пароля пользователя.

Автоматическая установка и режим только для чтения
Установка может производиться автоматически и вручную. Можно разрешить использование устройства только для чтения в случаях, когда шифрование не нужно.

Дополнительные функции
Шифрование можно также применять к облачным хранилищам, локальным папкам, CD и DVD
info@endpointprotector.com

eDiscovery - сканирование сохраненных данных

для Windows, macOS и Linux

Типы файлов: графические / офисные / архивы / исходные коды программ / медиафайлы / и т.д. • Шаблоны содержимого: кредитные карты, персональные данные, паспорта, номера телефонов / ИНН / СНИЛА / и т.д. • Пользовательские шаблоны / имена файлов / регулярные выражения / HIPAA / и т.д.

Шифрование и дешифровка данных
Хранящиеся на устройствах конфиденциальные данные можно шифровать, чтобы предотвращать несанкционированный доступ. Предусмотрена также возможность дешифрования.

Удаление данных
Если обнаружено нарушение политики в отношении данных, они могут быть автоматически удалены.

Черные списки расположений
Фильтры, основанные на определенных расположениях файлов и папок.

Автоматическое сканирование
Помимо сканирования “с чистого листа” и инкрементного сканирования, можно назначать регулярное сканирование по расписанию – однократное, еженедельное или ежемесячное.

Отслеживание файлов
Отслеживайте перемещение файлов по различным каналам, чтобы получить ясную картинку действий пользователей.

Отчеты и аналитика
Мониторинг хранящихся у пользователей данных позволяет принимать меры для защиты информации. Логи и отчеты можно передавать в SIEM-системы.

Пороги срабатывания фильтров
Определяйте, какое количество срабатывания фильтра заблокирует передачу файла.

Соответствие стандартам (GDPR, HIPAA, и т.д.)
Использование данного модуля позволяет обеспечить соответствие отраслевым стандартам защиты данных, таким, как PCI DSS, GDPR, HIPAA и т.д.

Интеграция с SIEM-системами
Передавайте важную информацию о безопасности во внешние системы управления инцидентами.

Черные списки типов файлов
Фильтры могут находить файлы определенных типов, даже если пользователь изменил расширение вручную.

Готовые черные списки содержимого
Можно создавать черные списки на основе готовых шаблонов, таких, как номера кредитных карт или номера страхования.

Пользовательские черные списки содержимого
Фильтры можно созавать на основе слов и выражений. Также можно создавать словари для фильрации контента.

Черные списки имен файлов
Можно создавать черные списки имен файлов, задавая их имя, расширения, или и то, и другое.

Черные и белые списки расположений
Фильтры, основанные на расположении файлов на жестком диске, с возможностью включать или исключать подпапки.

Черные списки на основе регулярных выражений
Дополнительные фильтры, позволяющие находить определенные последовательности символов в передаваемых данных.

Белые списки файлов
Блокируя все прочие попытки передачи файлов, можно задать списки разрешенных файлов, необходимых для работы.

Белые списки доменов и URL
Усиливая безопасность, обеспечивайте при этом доступ к необходимым ресурсам.
Добавляйте в белый список порталы и адреса электронной почты компании.

Белые списки MIME-типов
Предотвращайте избыточное сканирование, указывая MIME-типы, которые нужно исключить из проверки.

Дополнительные функции / Доступно также множество дополнительных функций. / info@endpointprotector.com

Управление мобильными устройствами

для Android, iOS и macOS

Беспроводная установка для iOS и Android
Удаленная установка через SMS, электронную почту, ссылку или QR-код.

Массовая установка
Одновременно можно производить установку на 500 смартфонов и планшетов.

Удаленная блокировка
Блокируйте устройство удаленно в случае инцидентов, касающихся безопасности. Предотвращайте утечку данных через потернные или оставленные в ненадлежащем месте устройства.

Определение местоположения и отслеживание перемещений
Мониторинг местонахождения корпоративных мобильных устройств.

Отключение встроенных функций
Можно отключать определенные функции устройств, которые могут привести к утечке данных, например - функцию цифровой камеры.

Включение сигнала для нахождения утерянного устройства
Определяйте местонахождение утерянного устройства, удаленно включая проигрывание громкого рингтона (только для Abdroid).

Управление мобильными приложениями
Управляйте приложениями в соответствии с политикой компании. Отправляйте бесплатные и платные приложения на устройства пользователей.

Отправляйте сетевые настройки
Отправляйте на устройства сетевые настройки, такие, как настройки WiFi, VPN, Bluetooth и т.д.

Оповещения
Доступны стандартные и настраиваемые системные оповещения.

Отчеты и аналитика
Отслеживайте использование устройств с помощью мощных инструментов отчетности и аналитики. Логи событий можно экспортировать.

Режим киоска для Samsung Knox
Ограничивайте использование устройства, разрешая запускать на нем только определенное приложение.

Управление MacOS
Устройства на MacOS можно подключать также через модуль управления мобильными устройствами, что дает ряд дополнительных возможностей.

Принудительная защита паролем
Применение этой политики заставляет пользователей применять на своих устройствах надежные пароли.

Удаленное стирание информации
В случае необходимости можно послать на устройство команду на удаление всех данных.

Установка геозон
Устанавливайте виртуальные периметры, в границах которых будут действовать назначенные политики безопасности.

Ограничения для iOS
Обеспечивайте использование устройств только в рабочих целях, отключив iCloud, Safari, App Store, и т.д.

Отправляйте контакты vCard на Android
Отправляйте сотрудникам контактные данные в формате vCard прямо на устройства (только для Android).

Мониторинг приложений
Отслеживайте приложения, которые пользователи устанавливают на свои устройства.

Инвентаризация устройств
Получайте подробную информацию о типах устройств, их именах, моделях, мощности, версиях ОС, операторах связи и т.д.

Создавайте оповещения по почте
Можно настроить оповещения о наиболее критичных событиях, связанных с использование мобильных устройств.

Панель обзора и графики
Для быстрого и наглядного ознакомления с наиболее важными событиями и статистикой предусмотрены графики и таблицы.

Дополнительные функции
Доступно также множество дополнительных функций.
info@endpointprotector.com

100% гибкость установки

Наши продукты подходят для любых типов сетей. Их могут использовать крупные, средние, малые предприятия и даже частные пользователи. Благодаря клиент-серверной архитектуре их легко устанавливать, а также централизованно управлять системой через веб-интерфейс. Среди вариантов установки - аппаратное и виртуальное приложение, AWS и облачная версия, и даже самостоятельное приложение - для тех, кому достаточно базовых функций.

Endpoint Protector

Модули Content Aware Protection, eDiscovery, Device Control, и Encryption доступны для компьютеров, работающих под управлением Windows, macOS и Linux . Модули Mobile Device Management и Mobile Application Management доступны также для iOS и Android.

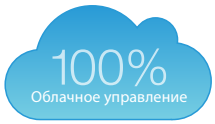
My Endpoint Protector

Модули Content Aware Protection, Device Control и Encryption работают на компьютерах под управлением Windows и Mac. Mobile Device Management и Mobile Application Management работают на iOS и Android.

Аппаратное приложение

Виртуальное приложение

Amazon



Облачное решение

Modules

	Защищаемые устройства					
Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS	macOS 10.13	High Sierra	●	●	●	●
	macOS 10.12	Sierra	●	●	●	●
	macOS 10.11	El Capitan	●	●	●	●
	macOS 10.10	Yosemite	●	●	●	●
	macOS 10.9	Mavericks	●	●	●	●
	macOS 10.8	Mountain Lion	●	●	●	●
	macOS 10.7	Lion	●	●	●	●
Linux	Ubuntu		●	●	●	недоступно
	OpenSUSE / SUSE		●	●	●	недоступно
	CentOS / RedHat		●	●	●	недоступно
	Fedora		●	●	●	недоступно
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11					●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+)					●

*Пожалуйста, уточняйте поддерживаемые версии ОС на endpointprotector.com/linux

Информационный лист 5.2.0.0

www.**endpointprotector**.com

COSOSYS

Official Partner

Главный офис (Румыния)

E-mail sales@cososys.com
Продажи +40 264 593 110 / ext. 103
Поддержка +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
Продажи +82 70 4633 0353
Поддержка +82 20 4633 0354

Северная америка

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