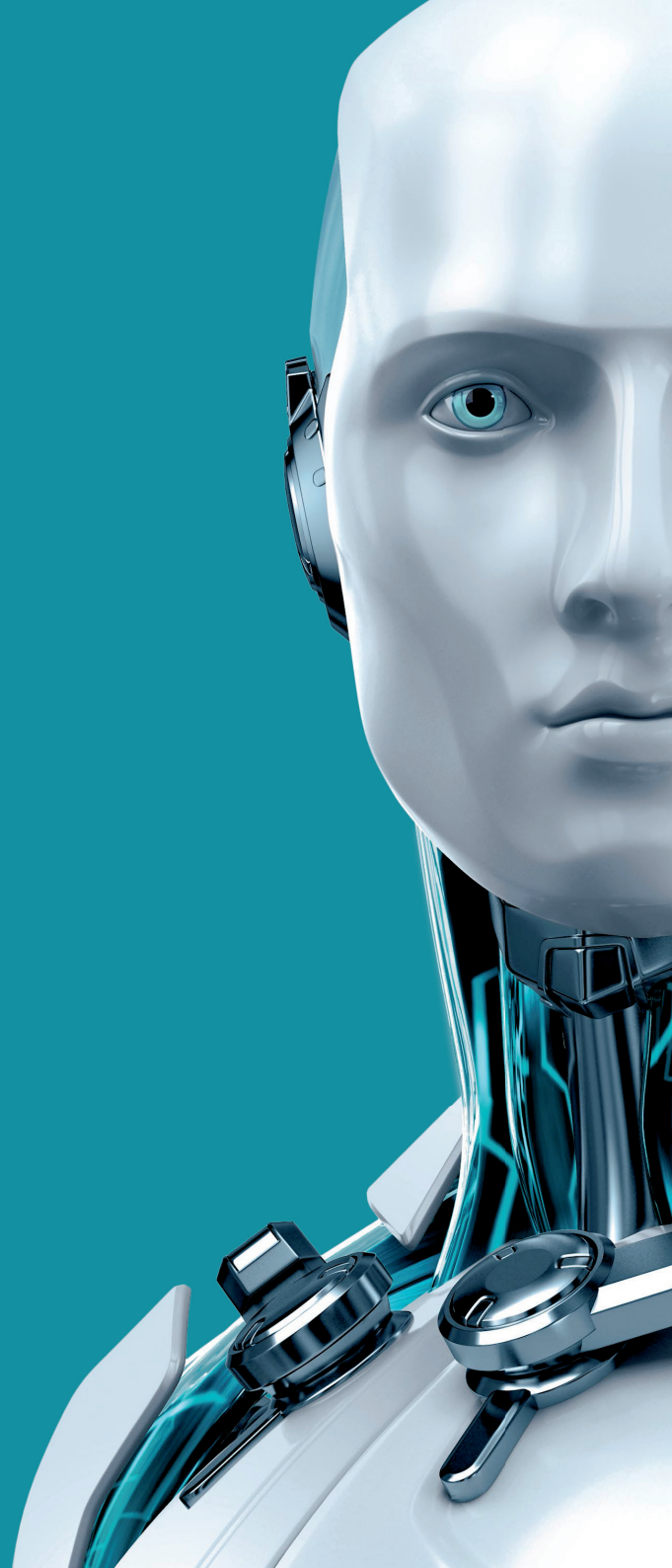
ОФИСНЫЙ КОНТРОЛЬ И DLP safetica

ESET TECHNOLOGY ALLIANCE



safetica

Safetica предлагает полноценный комплекс DLP (Data Loss Prevention), который закрывает широкий спектр угроз безопасности, связанных с человеческим фактором. Решение защищает компанию от спланированных или случайных утечек данных, злонамеренных действий инсайдеров и BYOD рисков, а также помогает повысить продуктивность работы персонала.

Философия безопасности Safetica основана на трех принципах: полнота, гибкость и удобство в использовании.

Safetica – полнофункциональное корпоративное решение, предотвращающее утечки данных. Safetica позволяет создавать отчеты о деятельности сотрудников и обеспечивает соблюдение политик безопасности компании.

Наши преимущества

Полноценное DLP решение	Охватывает все основные каналы утечек данных. Является агентным DLP с возможностями сетевого DLP решения.
Быстрое развертывание	Минимальное время развертывания среди продуктов данного класса благодаря гибкому подходу к блокировке каналов утечки данных.
Высокий уровень защиты от несанкционированного доступа	Обеспечивает постоянную защиту даже от пользователей с правами администратора.
Специальные функции защиты от утечек	Защищает данные от кражи путем несанкционированной печати, копирования в буфер обмена, виртуальной печати, преобразования фалов, архивации и шифрования.
Агностический подход	Не ограничивается отдельными протоколами или приложениями.
Четко определенные политики данных	Возможно задавать безопасные зоны – менеджеры выбирают места, откуда нельзя перемещать конфиденциальные данные, и Safetica обеспечивает их безопасность.
Точный мониторинг времени	В отчетах показано время реальной активности пользователей на посещенных веб-сайтах или в приложениях (открыть – не значит использовать).
Автоматическая оценка и оповещение	Выбирает наиболее важные зарегистрированные данные и отправляет сводный отчет назначенным получателям. Полная информация предоставляется по мере необходимости.

Как это работает

Рабочая станция – конечная точка, с которой взаимодействует пользователь. Сотрудники работают с критически важными бизнес-данными, выходят в интернет, получают и отправляют электронную почту, направляют документы на принтер, подключают съемные носители. Safetica DLP развертывает агент (**Safetica Endpoint Client**) на рабочие станции и поддерживает регулярную связь с ними через сервер (**Service Management Safetica**). Сервер создает базу данных деятельности сотрудников на рабочих станциях и распространяет политики безопасности на каждое устройство или пользователя.

Основные возможности

Полная защита от утечек данных	Охватывает все каналы утечки данных, оставаясь простым с точки зрения установки и эксплуатации решением. См. «Охват событий на конечных точках».
Производительность и тенденции	Предупреждает руководство компании о резких изменениях в работе персонала и показывает динамику производительности отдела или сотрудника за отчетный период. Эти данные указывают на возможные риски безопасности.
Отчет об активности	Раскрывает различные нарушения безопасности, проверяя все действия пользователя на предмет признаков потенциальной утечки до фактической передачи данных.
Email DLP	Предотвращает отправку конфиденциальных данных нежелательным получателям. Записывает информацию обо всех сообщениях с конфиденциальными файлами и хранит эти сведения для будущих отчетов и расследования инцидентов.
Контроль приложений	Включает выбранный пакет приложений, связанных с работой, и блокирует остальные, создавая безопасную среду. Нерабочие приложения могут быть доступны только в течение определенного периода времени.
Web-контроль	Легкое внедрение AUP (Политики приемлемого использования) с заранее выбранными категориями и фильтрацией по ключевым словам.
Контроль печати	Ограничивает данные, которые можно напечатать; устанавливает ограничения доступа к печати для отдельных пользователей и отделов.
Контроль устройств	Предотвращает подключение неавторизованных устройств на рабочем месте. Общие порты могут быть разрешены для конкретных устройств или заблокированы для всех.
Режимы информирования и тестирования	Помогает компаниям постепенно разворачивать защиту данных, тестируя все возможные конфликты ПО и непредвиденные ситуации без остановки бизнес-процессов.
Мгновенная классификация данных	Защищает новую информацию сразу после создания или получения конфиденциального файла.
Единая консоль управления	Safetica Management Console позволяет управлять безопасностью и отчетностью, объединяет все настройки по защите данных компании, отчетность и политики блокировки.
Проверка SSL/HTTPS	Контролирует безопасные соединения, включая веб-сайты с использованием протокола HTTPS, мессенджеры, приложения с защищенными соединениями и защищенную электронную почту.
Минимальная совокупная стоимость владения (TCO)	Нет необходимости покупать дополнительное оборудование и ПО. Агенты Safetica, развернутые на конечных точках, также предотвращают утечки данных в корпоративной сети.
Гибкость использования	Универсальный подход Safetica позволяет контролировать любые приложения, протоколы обмена сообщениями и электронной почты.

TECHNOLOGY ALLIANCE

ESET Technology Alliance объединяет стратегически выбранные компании, специализирующиеся на разных областях информационной безопасности, и сочетает проверенные технологии ESET с инновациями партнеров.

Охват событий на конечных точках

Отчетность и блокировка деятельности

- Все операции с файлами
- Долгосрочные тенденции, краткосрочные колебания активности
- Веб-сайты (включая трафик HTTPS) с учетом времени активности и неактивности
- Электронная почта и веб-почта
- Поиск ключевых слов (поддержка большинства машин, а также Windows Search)
- Мгновенный обмен сообщениями (независимо от приложения – все протоколы)
- Использование приложений и учет времени активности и неактивности
- Виртуальные, локальные и сетевые принтеры
- Активность экрана (интеллектуальный сбор данных)
- Отслеживание нажатия клавиш на клавиатуре

Предотвращение утечек данных

- Все жесткие диски, USB, FireWire, SD/MMC/CF карты, SCSI диски
- Передача файлов по сети (защищенная, незащищенная)
- Электронная почта (SMTP, POP, IMAP, Microsoft Outlook/ MAPI протоколы)
- SSL/HTTPS (все браузеры и приложения со стандартным управлением сертификатами)
- Копировать/Вставить, Буфер обмена, Перетягивание
- Виртуальные, локальные и сетевые принтеры
- Bluetooth, ИК/LPT/COM параллельные порты
- CD/DVD/BluRay устройства для считывания и записи данных
- Контроль доступа к файлам определенных приложений
- Создание снимка экрана

Варианты использования

Защита важной корпоративной информации	Когда безопасные зоны для конфиденциальных данных заданы, Safetica проверяет каждое взаимодействие с важными файлами. Обнаружив запрещенное действие, решение блокирует его или принимает другие выбранные меры. Действия, определенные компанией, могут включать информирование ИБ-специалиста о каждом событии, шифрование данных, а также предложения других безопасных мест для хранения. Информация на ноутбуках и флэш-накопителях защищена даже за пределами компании.
Управление съемными устройствами	Safetica позволяет управлять подключением различных устройств к компьютерам компании, перекрывая один из каналов утечек данных.
Соответствие нормативным требованиям	С клиентом **Safetica Endpoint Client**, установленным на компьютерах компании, и политикой управления, настроенной в консоли управления **Safetica Management Console**, вы можете соблюдать правила, которые регулируют движение и использование конфиденциальных данных.
Контроль производительности	Даже без использования интерфейса **Safetica Management Console** менеджеры могут получать регулярные сводные отчеты о выбранных пользователях или группах.

Архитектура

1. Осуществляется запись действий и внедрение политики через небольшое приложение агента.
2. Данные автоматически передаются из сетевых компьютеров к серверу вместе с синхронизированными данными ноутбука при подключении к сети. Настройка клиента синхронизируется в обратном порядке.
3. Все данные доступны для просмотра в приложении управления, где также могут быть изменены любые параметры.
4. Safetica поддерживает несколько ответвлений с помощью единой консоли управления.

Системные требования

Safetica Endpoint Client

- Двухъядерный процессор
- 2 Гб оперативной памяти
- 2 Гб дискового пространства
- Microsoft Windows 7 32-разрядные и 64-разрядные и более новые ОС Windows

Сервер (Service Management Safetica)

- Четырехъядерный процессор
- 4 Гб оперативной памяти
- 100 Гб дискового пространства. (база данных + резервные копии)
- Microsoft Windows Server 2008 R2 или более поздней версии

MS SQL (база данных для сервера)

- Microsoft SQL Server 2008 32-разрядные и 64-разрядные и более поздние версии (в том числе EXPRESS)

  WebSafetica доступна только в MS SQL 2012 и выше (в том числе EXPRESS)