

safetica

SAFETICA ONE

Защита от утечек данных и внутренних угроз



safetica ONE

Защита от **утечек данных**
и **внутренних угроз**

- ✓ **Простое** в обслуживании решение с минимальными в своем классе системными требованиями
- ✓ **Надежная** защита от утечек данных и внутренних угроз информационной безопасности
- ✓ **Соответствие** нормативным требованиям и корпоративным политикам работы с данными



Safetica против человеческого фактора

Safetica закрывает все основные каналы утечки данных и защищает от широкого спектра угроз, связанных с человеческим фактором. Решение предотвращает случайные утечки, защищает от злонамеренных действий инсайдеров и рисков BYOD, а также решает проблемы эффективности труда персонала.

Любой бизнес так или иначе оперирует данными. Если конфиденциальная информация будет потеряна или украдена, пострадает репутация компании и ее прибыльность. Утечка данных может повлечь и юридическую ответственность.

Средний ущерб компании от утечки данных составляет **\$4,24 миллиона**.*

60% компаний малого бизнеса **прекращает свою деятельность в течении 6 месяцев** после серьезной утечки данных.**

* Международный опрос Global Cost of Data Breach Study, Ponemon Institute и IBM Security, 2021

** Как утечки данных влияют на малый бизнес, withlayr.com, 2017

Доступное решение для любой компании

Safetica - простое в использовании решение для защиты от внутренних угроз и предотвращения утечек, доступное компаниям любого размера.

ГЛУБОКИЙ АНАЛИЗ ПОВЕДЕНИЯ

Safetica выявляет подозрительные действия сотрудников до того, как они приведут к потере времени и средств, проводит глубокий анализ поведения и обеспечивает понимание внутренних процессов в компании.

ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ

Safetica поможет уберечь вашу компанию и ваших сотрудников от последствий возможной утечки данных и других рисков, без необходимости нанимать дополнительных специалистов по информационной безопасности.

ПРОСТОЕ ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ

Safetica разработана таким образом, чтобы заказчик мог внедрить и настроить продукт силами собственного IT-отдела. Развертывание занимает в среднем от 5 часов, первые отчеты будут готовы в течение недели.

Чем **Safetica** поможет вашему бизнесу?

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

80% компаний ежегодно сталкиваются с инцидентами информационной безопасности, включая утечки данных. Средний ущерб от утечки составляет 4,24 млн долларов, при этом до 60% малых компаний после крупного инцидента прекратит свое существование в течение полугода. Safetica защищает от утечек ваши данные, независимо от того, где они хранятся и кто их использует.

СОБЛЮДЕНИЕ НОРМАТИВОВ

Safetica помогает соблюдать законодательные требования и стандарты в области защиты данных, включая GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, CCPA.

ЗАЩИТА ОТ ИНСАЙДЕРОВ

Около трети сотрудников хотя бы раз в своей карьере вредили работодателям – копировали данные, чтобы использовать на новом месте работы (40%), удаленно подключались к корпоративным ресурсам после увольнения (7%), уничтожали документы (5%). Safetica выявляет подозрительное и потенциально опасное поведение персонала, а также колебания производительности.

ОБУЧЕНИЕ ПЕРСОНАЛА

Сотрудники, работающие с корпоративными данными, не всегда обладают знаниями о правилах безопасности. Возросли и риски в связи с переходом на удаленную работу. С помощью Safetica вы можете обучать сотрудников тому, как правильно и безопасно работать с конфиденциальными данными в офисе и за его пределами.

SAFETICA ЗАЩИЩАЕТ ОТ УТЕЧЕК:

- персональные данные
- стратегически важные документы
- базы клиентов
- платежные данные, например, реквизиты банковских карт
- интеллектуальную собственность (промышленные образцы, ноу-хау)
- контракты



Safetica
Discovery



Safetica
Protection



Safetica
Enterprise

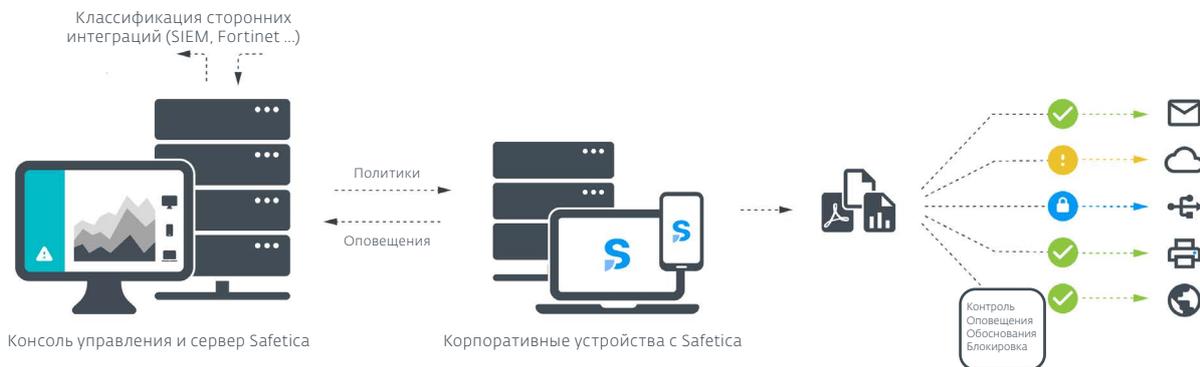
Safetica UEBA

Safetica Mobile

Продукты

Дополнительные
модули

Как работает Safetica?



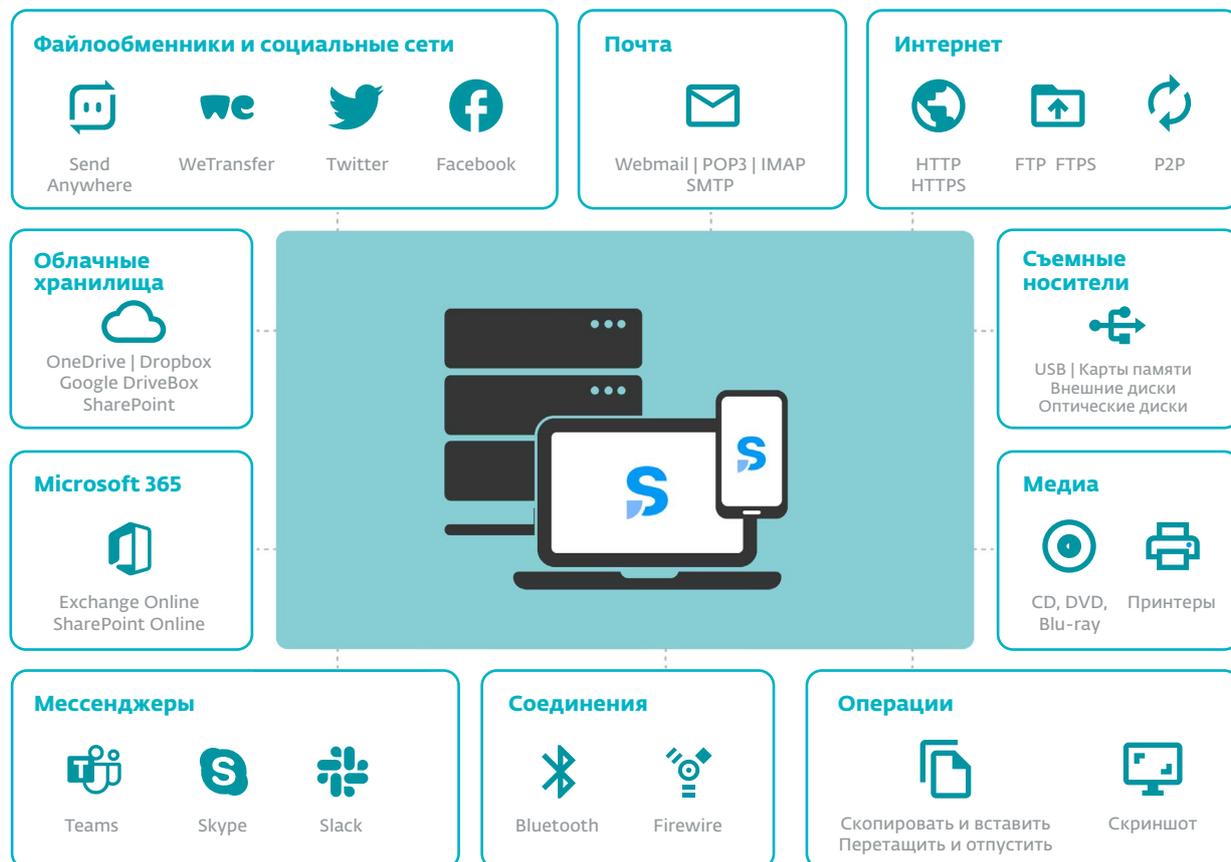
Сервер баз данных работает с журналами событий безопасности рабочих станций. Консоль Safetica Management Console позволяет пользователям управлять политиками безопасности и отображать всю собранную информацию.

Все действия записываются, и политики безопасности применяются на ПК, ноутбуках, планшетах и смартфонах с Safetica.

Конфиденциальные данные защищены по всем каналам.

Safetica закрывает все основные каналы утечки данных

Safetica закрывает от утечек все основные каналы связи и платформы, защищая данные, где бы они ни находились и куда ни передавались.



Safetica Discovery:

ключевые преимущества

Посмотрите, как используются данные компании, где они хранятся и куда пересылаются. Предотвратите умышленную утечку данных с помощью журналов аудита. Откройте для себя внутренние процессы и перестройте бизнес-среду.

Safetica Discovery позволяет быстро обнаружить скрытые риски и повысить прозрачность процессов в вашей организации.



Где, когда и каким образом **используются конфиденциальные данные** вашей компании? Safetica даст четкие ответы на эти и другие вопросы.



Safetica поможет **классифицировать конфиденциальные данные** и проверить соответствие нормативным требованиям и внутренним политикам безопасности организации.



Мгновенные уведомления и расширенные отчеты позволяют легко оценить уровень риска и получить обзор инцидента.



Функция оптического распознавания символов (OCR) **обнаружит конфиденциальные данные** в сканируемых документах PDF и файлах изображений.



Развертывание Safetica **занимает от нескольких часов**, первые отчеты вы получите уже через несколько дней.



Safetica проводит глубокий анализ поведения и обеспечивает понимание внутренних процессов в компании, в том числе за счет интеграции с **PowerBI или Tableau**.

Возможности продукта

Посмотрите, как используются данные компании, где они хранятся и куда пересылаются.

- ✓ Поддержка Windows и macOS
- ✓ Интеграция в один клик с Microsoft 365
- ✓ Проверка и классификация данных
- ✓ Простой переход на старшее решение
- ✓ Подходит как для локальных, так и для виртуальных машин



Консоль управления Safetica ONE обеспечит детальное понимание всех происходящих действий с конфиденциальными данными.

Safetica Protection: ключевые преимущества

Safetica Protection выявляет риски, обучает сотрудников, предотвращает злонамеренные действия инсайдеров и ошибки. Сочетание поведенческой аналитики, классификации данных и технологии защиты от утечек создает безопасную среду для ведения бизнеса.



Сохраняйте **контроль потоков** конфиденциальных данных и рисков безопасности с помощью поведенческого анализа и проверки контента.



Получайте **регулярные отчеты о безопасности** и уведомления об инцидентах в режиме реального времени.



Используйте **функцию зонирования**, чтобы защищать конфиденциальные данные просто и интуитивно.



Функция **теневого копирования** утекших данных позволяет создать доказательную базу для расследования инцидента.

УСТАНОВИТЕ ЧЕТКИЕ ПОЛИТИКИ ДЛЯ ВСЕХ КАНАЛОВ ДАННЫХ

Настройте политики безопасности, используя индивидуальный или групповой подход. Выберите желаемый рабочий процесс с настраиваемыми действиями, от фоновой проверки до уведомлений и блокировки.

ОБНАРУЖИВАЙТЕ ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ И АНАЛИЗИРУЙТЕ ВНУТРЕННИЕ РИСКИ

Реагируйте на потенциальные угрозы до инцидента с помощью раннего обнаружения аномального поведения сотрудников и факторов риска данных. Safetica ONE использует продвинутое контентное распознавание символов (OCR) для обнаружения конфиденциальных данных в сканируемых документах PDF и файлах изображений.

НАУЧИТЕ СОТРУДНИКОВ БЕЗОПАСНОЙ РАБОТЕ С ДАННЫМИ

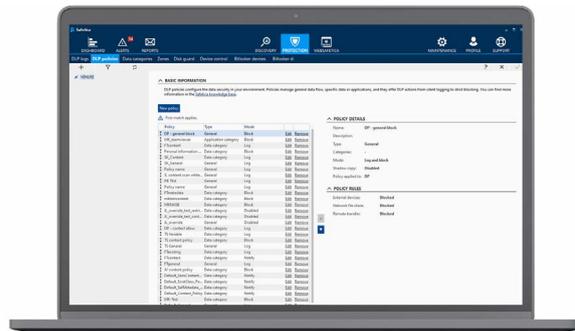
Отображение уведомлений при потенциальном нарушении пользователем политик безопасности. Постройте безопасные процессы для работы с наиболее важными данными и обучайте сотрудников.

ПОСТАВЬТЕ ВСЕ ПОДКЛЮЧЕННЫЕ УСТРОЙСТВА ПОД КОНТРОЛЬ

Ограничьте использование портативных устройств или запретите несанкционированные подключения к мультимедийным ресурсам. Управляйте корпоративными мобильными устройствами и отслеживайте данные, которые покидают облако Office 365. Safetica остается полностью активной независимо от наличия сетевого подключения. Все собранные записи синхронизируются, как только соединение будет восстановлено.

Возможности продукта

На основе контентной проверки, анализа внутренних рисков и заданных политик Safetica Protection может определить, кто и когда рискует вашей конфиденциальной информацией. В зависимости от того, в каком режиме работает Safetica, возможна блокировка рискованных действий, информирование администратора или напоминание вашим сотрудникам о правилах безопасности.



Консоль управления Safetica ONE обеспечивает детальную настройку политик безопасности, категорий данных и отчетов.

Safetica Enterprise:

ключевые преимущества

Safetica Enterprise расширяет возможности DLP и защиты от внутренних угроз за счет дополнительного контроля рабочих процессов, автоматизации и бесшовной интеграции со сторонними инструментами. Это продукт, дополняющий стек решений корпоративной ИТ-безопасности.



Автоматическая интеграция сторонних решений и функции для расширенных вариантов использования



Управление рабочими процессами на конечных точках



Поддержка Active Directory и **мультидоменных сред**



Персонализация Safetica с использованием **фирменного стиля** вашей компании

БЕСШОВНАЯ ИНТЕГРАЦИЯ

Совместимость с **Microsoft 365** и **Fortinet** обеспечивает расширенный контроль устройств, находящихся вне офиса, и создает комплексное решение безопасности конечных точек и сети.

Все инциденты могут быть автоматически отправлены в SIEM систему, например, **Splunk**, **IBM QRadar**, **LogRhythm** или **ArcSight** для дальнейшего расследования.

REST API позволяет передавать данные Safetica ONE в службы аналитики и визуализации, такие как **Power BI** или **Tableau**.

УПРАВЛЕНИЕ РАБОЧИМИ ПРОЦЕССАМИ

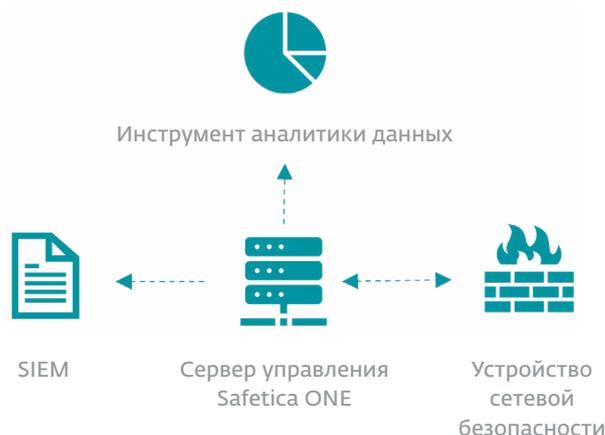
Набор функций позволяет определять и настраивать рабочие процессы сотрудников вне зависимости от используемых ими данных.

Вы можете обеспечить соблюдение определенного процесса и заблокировать другие способы выполнения действия с данными.

Управление рабочим процессом включает политики приложений и экспертные настройки политик для согласования рабочего процесса пользователя с процессами компании.

Возможности продукта

- ✓ Поддержка Windows и macOS
- ✓ Интеграция в один клик с Microsoft 365
- ✓ Интеграция сетевых устройств Fortinet
- ✓ API для передачи данных Safetica в Power BI или Tableau
- ✓ Мгновенная доставка уведомлений на почту
- ✓ Проверка контента файлов на основе предварительно заданных правил
- ✓ Контентная классификация на основе заданных подходов



UEBA: ключевые преимущества

Модуль аналитики поведения пользователей и объектов Safetica UEBA входит в состав основных продуктов и позволяет детально отслеживать действия сотрудников и выявлять потенциальные угрозы безопасности. Обеспечьте бесперебойные бизнес-процессы даже при удаленной работе.



Распознавайте нежелательные действия сотрудников

с помощью аудита активности и автоматической категоризации используемых приложений и веб-сайтов, посещаемых пользователями.



Анализируйте структуру коммуникаций

с регистрацией входящих и исходящих электронных писем и уважением к приватности сотрудника.



Отслеживайте аномалии поведения сотрудников

с помощью обзора и визуализации тенденций и изменений.



Оптимизируйте использование ресурсов компании

на основе обзоров об эксплуатации оборудования и дорогостоящих лицензий программного обеспечения.



Получайте расширенные отчеты и мгновенные уведомления

о подозрительной активности пользователей даже в режиме дистанционной работы.



Будьте в курсе поиска работы

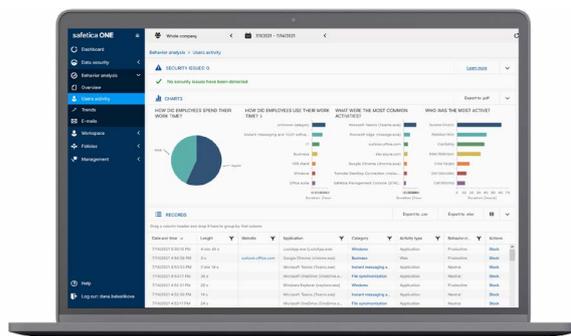
вашими сотрудниками, уход которых может представлять угрозу безопасности данных в будущем.

ИДЕНТИФИКАЦИЯ АНОМАЛИЙ

Проводите анализ деятельности отдельных сотрудников, сравнивая их действия с реальными рабочими обязанностями. Проверьте, посещает ли кто-нибудь опасные веб-сайты или использует нежелательные приложения.

ПРОЗРАЧНОСТЬ ДАЖЕ НА УДАЛЕНКЕ

Предоставляйте руководителям отчеты об их сотрудниках. Будьте в курсе происходящего, когда пользователи работают дома или в командировке. Предотвращайте риски безопасности и управляйте эффективностью, выявляя неактивных сотрудников или их подозрительные действия.



WebSafetica предлагает простой для понимания обзор всех возможных угроз в едином интерфейсе управления.

Safetica Mobile:

Ключевые преимущества

Safetica Mobile - это инструмент управления мобильными устройствами (MDM), который повышает безопасность данных на смартфонах и планшетах, делая их надежной частью вашей ИТ-среды.



Защищайте данные на мобильных устройствах

Разделяйте рабочие приложения и данные в защищенной рабочей среде, выявляйте вредоносные приложения, удаленно блокируйте потерянные или украденные устройства и удаляйте информацию в их памяти.



Следите за безопасностью и состоянием устройств

Получайте отчеты о состоянии устройств для выявления рисков, находите потерянные устройства с помощью определения местоположения.



Используйте централизованное управление

Контролируйте настройки и поведение приложений с помощью функции расширенного управления, задавайте политики безопасности для групп устройств, настраивайте их из единого центра.

БЕЗОПАСНОЕ УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Контролируйте все устройства компании и оперативно выявляйте угрозы. Используйте Android EMM и приложения iOS, чтобы создать рабочую область на устройствах для удаленной работы или личных целей.

АНТИВОР

Потеря или кража мобильных устройств компании - серьезная проблема, которая может поставить под угрозу ваши конфиденциальные данные. С помощью Safetica Mobile вы сможете найти корпоративное устройство или удалить с него все содержимое.

АУДИТ ДАННЫХ НА ANDROID

Проверяйте местонахождение корпоративных данных в пространстве мобильного устройства (доступно для Android версии 6+). Используя Safetica Mobile совместно с WebSafetica, вы будете получать информацию об инцидентах на одном экране, независимо от того, происходят ли они на телефоне, компьютере или в облаке Microsoft 365.

Возможности продукта

- ✓ MDM и безопасность: защищенная рабочая среда, политики устройства, управление приложениями с удаленной конфигурацией, статус безопасности
- ✓ Антивор: локализация, сильный пароль, удаленная блокировка и удаление данных

Обзор функций

Совместимость



Safetica
Discovery



Safetica
Protection



Safetica
Enterprise

Аудит безопасности



Аудит безопасности потока данных

Аудит безопасности потока данных по всем каналам, включая внешние устройства, веб-загрузку, электронную почту, обмен мгновенными сообщениями, печать и облачные хранилища



Аудит файлов и электронной почты Office 365

Аудит файловых операций и исходящих электронных писем в Office 365.



Аудит соответствия нормативным требованиям

Выявляйте нарушения наиболее распространенных правил, таких как PCI-DSS, GDPR или HIPAA во всех региональных вариациях.



Аудит безопасности рабочих процессов

Аудит использования корпоративных устройств, приложений, сетей и печати. Обнаруживайте неиспользуемые или неправильно используемые ресурсы для поддержания эффективности рабочего процесса и сокращения затрат.



Классификация проверки содержимого

Сканируйте конфиденциальные файлы (включая документы PDF и изображения) и электронные письма с помощью полной проверки содержимого – предопределенных шаблонов или настраиваемых правил и словарей.



Обнаружение подозрительной активности

Реагируйте быстро благодаря обнаружению подозрительной активности в режиме реального времени и моментальным оповещениям по электронной почте.



Защита облачных данных



Защита устройств с облачной синхронизацией

Защита данных, которые пересылаются по электронной почте и в мессенджерах, загружаются в интернет и на сетевые ресурсы.



Защита устройств с Office 365

Защита данных для Office 365 и SharePoint. Запретите совместное использование или загрузку данных, которые вы хотите хранить вне облака.



Защита информации в Azure

Обнаружение классификаций данных в Microsoft Azure Information Protection, даже в зашифрованном виде.



Защита Exchange Online

Унифицируйте политики электронной почты для устройств и облачных хранилищ. Управляйте и фильтруйте исходящие данные с устройства и Exchange Online.



Защита данных	✗	✓	✓
Электронная почта и защита сети Защита данных, которые пересылаются по электронной почте и в мессенджерах, загружаются в интернет и на сетевые ресурсы.	✗	✓	✓
Защита устройств и контроль печати Управляйте потоком данных на внешних устройствах и предотвращайте печать конфиденциальных документов на локальных, сетевых или виртуальных принтерах.	✗	✓	✓
Защита удаленной работы Избегайте утечек данных при подключении к удаленному рабочему столу. Поддержка широкого спектра решений для удаленного доступа.	✗	✓	✓
Расширенная классификация данных Используйте передовые технологии для обнаружения и маркировки конфиденциальных данных на основе происхождения, контекста рабочего процесса или типа файла. Воспользуйтесь преимуществом обнаружения метаданных, чтобы использовать сторонние классификации. Разрешите пользователям классифицировать файлы самостоятельно.	✗	✓	✓
Различные политики исправления Оперативно реагируйте на обнаруженные инциденты безопасности, чтобы расширить возможности и обучить своих сотрудников. Инциденты можно логировать, блокировать или допускать / блокировать с переопределением.	✗	✓	✓
Теневая копия инцидента Храните доказательства инцидентов, создавая теневые копии утечек данных. Теневые копии полностью зашифрованы и могут храниться на локальных компьютерах.	✗	✓	✓
Контроль рабочего пространства Определите защищенное рабочее пространство и уменьшите периметр с помощью приложений и управления веб-сайтом. Избегайте нежелательного поведения в компании и снижайте затраты на управление безопасностью.	✗	✓	✓
Зонирование Safetica Простое управление безопасным периметром данных с уникальными зонами Safetica, которые значительно сокращают количество политик защиты данных.	✗	✓	✓
Управление шифрованием BitLocker Централизованное управление локальными дисками и внешними устройствами с шифрованием BitLocker.	✗	✓	✓
Корпоративные функции	✗	✗	✓
Ребрендинг Ребрендинг уведомлений, например, изменение логотипа.	✗	✗	✓
Контроль рабочего процесса Политики приложений и экспертные настройки политик для согласования рабочего процесса пользователя с процессами компании.	✗	✗	✓
Поддержка нескольких доменов Поддержка нескольких доменов предприятия для Active Directory.	✗	✗	✓
Автоматизация безопасности	✗	✗	✓
SIEM-интеграция Автоматизированная отчетность об инцидентах в SIEM-решениях (Splunk, QRadar, LogRhythm, ArcSight и др.).	✗	✗	✓
Интеграция с FortiGate Автоматическая интеграция системы безопасности с сетевыми устройствами FortiGate для комплексной защиты устройств и сети.	✗	✗	✓
API API для передачи данных Safetica в службы аналитики и визуализации.	✗	✗	✓

Системные требования

SERVER

- Четырехъядерный процессор с тактовой частотой 2,4 ГГц
- 8 ГБ ОЗУ и больше
- 100 ГБ доступного дискового пространства
- Общий или выделенный сервер, поддержка виртуальных машин и облачный хостинг
- Требуется подключение к серверу с:
MS SQL 2012 и выше или Azure SQL
MS Windows Server 2012 и выше

MS SQL (БАЗА ДАННЫХ СЕРВЕРА)

- MS SQL Server 2012 и выше, или MS SQL Express 2016 и выше, или Azure SQL
- MS SQL Express является частью универсального установщика и рекомендуется для 200 защищенных устройств
- 200 ГБ доступного дискового пространства (оптимально 500 ГБ или больше, в зависимости от диапазона хранящихся данных)
- Общий или выделенный сервер, поддержка виртуальных машин и облачный хостинг. Его можно разместить вместе с сервером Safetica

WINDOWS CLIENT

- Двухъядерный процессор с тактовой частотой 2.4 ГГц
- 2 ГБ ОЗУ и больше
- 10 ГБ доступного дискового пространства
- MS Windows 7, 8.1, 10 (32-бит [x86] или 64-бит [x64])
- Пакет установки MSI
- .NET 4.5.2 и выше

MACOS CLIENT

- Четырехъядерный процессор с тактовой частотой 2,4 ГГц
- 2 ГБ ОЗУ и больше
- 10 ГБ доступного дискового пространства
- macOS 10.10 и выше. Для полного набора функций DLP рекомендуется 10.15 и выше

MOBILE CLIENT

- Android 6 и выше
- Службы Google Play
- iOS 10 и выше

ОБЛАЧНЫЕ СЕРВИСЫ

- Microsoft Azure, Microsoft 365

Технологические альянсы



Награды и достижения



DLP Market Quadrant
2019–2023, Специалист
(Specialist)



4,8 из 5,0 в рейтинге
на основе отзывов
пользователей
Gartner Peer Insights



В числе лидеров
отрасли в рейтинге
Forrester's Now Tech:
Data Loss Prevention,
Q1 2019



Infotech 2021: Data
Loss Prevention
Data Quadrant
Report, Лидер
(Leader)



АНТИВИРУСНАЯ ЗАЩИТА
БИЗНЕС-КЛАССА

