SECRET DISK ДЛЯ LINUX

Защита информации от несанкционированного доступа в ОС Linux

Перевод рабочих станций сотрудников на отечественные ОС сопряжен с большим количеством вызовов. Один из них — это вопрос обеспечения безопасности информации.

Универсальный способ защитить чувствительные к утечке данные — организовать для пользователя безопасное рабочее пространство, где он может создавать, хранить и редактировать свои файлы. Необходимо, чтобы доступ к этому пространству был недоступен как для злоумышленников, так и для условно доверенных лиц, например, других пользователей или системного администратора.

Также важно оперативно внедрить средство защиты внутри Linux-сегмента и иметь возможность управлять им централизованно, независимо от степени зрелости ИТ-инфраструктуры.

Выбор инструмента для обеспечения безопасности исходит из нескольких критериев:

Простота внедрения
создание независимого Linux-сегмента важно осуществить безболезненно для действующей ИТ-инфраструктуры и в реалистичные сроки

Универсальность применения
средство защиты должно поддерживать популярные ОС семейства Linux, разрабатывающиеся российскими вендорами и распространенные в действующих ИТ-инфраструктурах

Надежность метода защиты
средство должно соответствовать как требованиям регулирующих органов, так и вызовам, стоящим перед бизнесом. Например, обеспечивать безопасность данных на ноутбуках сотрудников, которые часто отсутствуют в офисе в связи с командировками или гибридным рабочим графиком.

Угрозы безопасности данных для Linux

Отсутствие в Linux специализированных инструментов шифрования данных

Утечки конфиденциальной информации в командировках и на "удалёнке"

Дефицит совместимых средств защиты для ОС Windows и Linux

Логистические трудности бюджетирования и закупок СЗИ под Linux

Решение

Избежать компрометации чувствительных к утечке конфиденциальных данных поможет шифрование информации на рабочих компьютерах.

Злоумышленник не сможет воспользоваться данными, хранящимися в зашифрованном виде, даже если получит доступ к файлам.

Secret Disk для Linux – это система защиты информации на рабочих станциях и серверах для ОС семейства Linux. Secret Disk для Linux позволяет создать безопасное рабочее пространство на корпоративном компьютере и предотвращает утечки конфиденциальной информации.

SECRET DISK ДЛЯ LINUX

Защита информации от несанкционированного доступа в ОС Linux

Назначение Secret Disk для Linux

- Защита чувствительной к утечке конфиденциальной информации
- Разграничение прав доступа между администраторами ИТ и ИБ
- Контроль доступа пользователей к зашифрованной информации
- Двухфакторная аутентификация с помощью ключевого контейнера пользователя

Преимущества Secret Disk для Linux

- Безопасное рабочее пространство для работы пользователя
- Прозрачное для пользователей шифрование информации
- Отсутствие жесткой привязки к PKI, УЦ и службе каталогов
- Централизованное управление агентами на рабочих станциях
- Быстрый ввод в эксплуатацию на большом количестве АРМ
- Совместимость с российскими операционными системами

Функциональные возможности

- Шифрование виртуальных дисков
- Автоматическая регистрация пользователей в консоли управления администратора
- Динамическая группировка пользователей для применения политик шифрования
- Возможность массового зашифрования виртуальных дисков пользователей
- Мониторинг процесса зашифрования ресурсов на консоли управления системой
- Аутентификация с помощью ключевого контейнера пользователя
- Разграничение ролей на администратора и пользователя
- Монопольный доступ пользователя к своим защищенным ресурсам
- Управление с помощью графического интерфейса или командной строки
- Совместимость с ОС Astra Linux, РЕД ОС, АЛЬТ СП
- Поддержка ГОСТ 34.10-2018, 34.11-2018, 34.12-2018 и 34.13-2018,
- Поддержка файловых систем EXT4, FAT32
- Установка пакетов как из публичных, так и из локальных репозиториев

Аладдин

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин — ведущий российский вендор-разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры