Cryptallit NSM

Защита информации на файловых серверах организации

Возможности Cryptallit NSM

Защита информации в сетевых папках на файловом сервере компании

Контроль доступа к защищаемой информации на основе группировки пользователей

Шифрование информации на файловых серверах, с применением стойких криптографических алгоритмов

Защищенное взаимодействие между рабочей станцией и файловым сервером

AAA Аутентификация и авторизация пользователей при доступе к защищаемой информации

Групповая работа пользователей с зашифрованными файлами в сетевых папках на файловом сервере

Модуль сетевой безопасности системы ***Cryptallit NSM***, реализует максимально надежный метод противодействия утечкам ценной информации при помощи стойких алгоритмов шифрования. Основным объектом защиты системы являются сетевые папки на файловом сервере компании.

Шифрует и контролирует доступ

Система обеспечивает прозрачное, для пользователей, шифрование файлов и папок на дисках файловых серверов. Для доступа к защищенной информации сотруднику необходимо пройти, только двухфакторную аутентификацию, у себя на компьютере и далее работать с информацией в защищенных сетевых папках в обычном режиме.

Создает наиболее важный рубеж защиты

При возможном взломе периметра безопасности, злоумышленник может получить доступ к файловому серверу, однако вся ценная информация в сетевых папках будет защищена шифрованием, что предотвратит ее компрометацию.

Реализует защиту от администраторов ИТ

Cryptallit NSM позволяет обеспечить надежную защиту файлов от привилегированных пользователей. Администраторы домена, серверов или рабочих станций обладают максимальными полномочиями в ИТ-инфраструктуре, однако не смогут получить доступ к информации в зашифрованных паках и файлах.

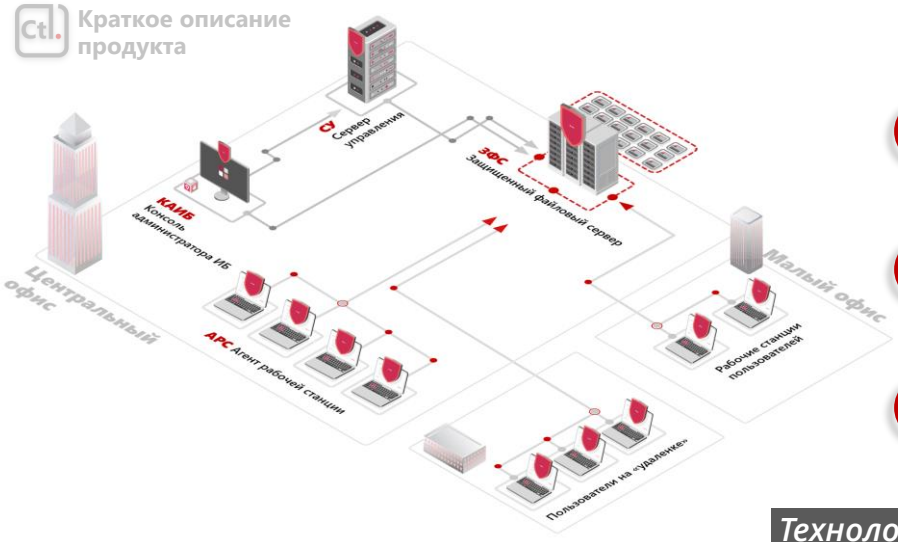
Обеспечивает безопасную работу «на удаленке»

Гибридный график работы стал нормой для современных организаций. Обработка конфиденциальной информации осуществляется в офисе, из дома и «в дороге». При этом дистанционная работа с защищенными сетевыми папкам остается безопасной, как для локальных пользователей, так и для сотрудников, работающих «на удаленке».

Обеспечивает безопасность данных в ЦОД

Размещение файлового сервера с ценной информацией во внешнем дата-центре всегда связано с повышенным риском компрометации этой информации, ведь персонал дата-центра имеет физический доступ к серверу с конфиденциальными данными. Cryptallit NSM надежно защищает информацию от возможных злонамеренных действий персонала дата-центра. Доступ и работа авторизованных сотрудников остаются на высоком уровне комфорта.

Краткое описание продукта



- ***Централизованное управление агентами на рабочих станциях***
- ***Простая интеграция с существующей инфраструктурой***
- ***Простой и быстрый ввод системы защиты в рабочую эксплуатацию***

Технологические преимущества Cryptallit NSM

Максимальная надежность механизмов защиты информации

Для защиты данных применяются наиболее стойкие отечественные или зарубежные алгоритмы шифрования, исключающие возможность успешного криптоанализа и компрометации защищаемой информации. Схема выработки и обмена ключами шифрования соответствует требованиям рекомендаций ТК.26

Высокая производительность защищенного файлового сервера

При работе пользователей с защищаемыми ресурсами все криптографические операции производятся на клиентском ПО, а файловый сервер и вовсе не содержит активных элементов системы. Вся нагрузка по шифрованию распределяется по рабочим станциями пользователей. Такая высокопроизводительная архитектура системы дает максимальную масштабируемость криптографических функций.

Возможность автономной работы пользователей с защищенными данными

При работе пользователя с защищенной сетевой папкой Cryptallit NSM кеширует файлы локально на рабочей станции в защищенном виде. При отключении пользователя от корпоративной сети сохраняется возможность безопасной работы с кэшированными данными. При повторном подключении к сети все локальные данные синхронизируются с соответствующей сетевой папкой.

https://cryptallit.ru

sales@cryptallit.ru

+7(495)215-27-23