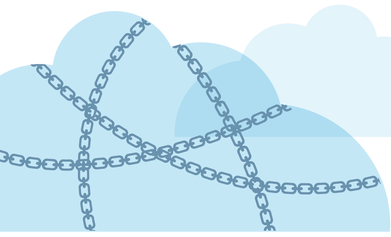
Cisco Spark

Безопасность Cisco Spark

Кто хранит ключи от ваших облачных данных?
Ваш провайдер? У него есть доступ к вашему контенту? Он дает вам контроль? Или близко не подпускает к облаку?

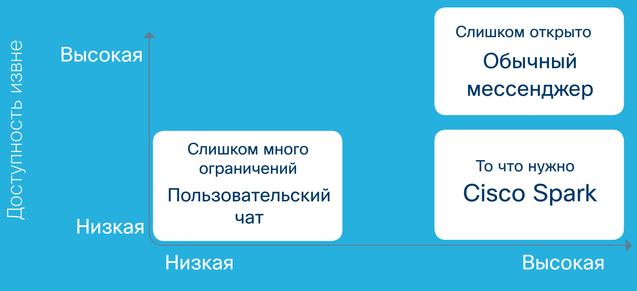
Обычные мессенджеры? Слишком открыто.
Стандартные мессенджеры могут представлять угрозу для безопасности, ведь они осуществляют прямой доступ к содержимому для выполнения своих функций: поиска сообщений, перекодирования контента или интеграции со сторонними приложениями.



Пользовательский чат? Слишком много ограничений.
Пользовательские приложения для чатов обычно заточены на обеспечение конфиденциальности. Для этого в них используется сквозное шифрование, но при этом приложения имеют ограниченную функциональность и масштабируемость.

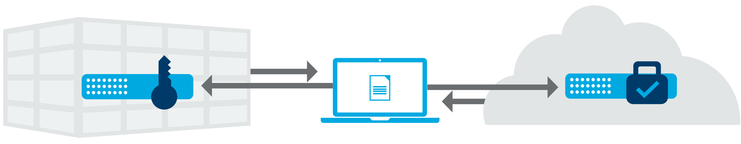
Cisco Spark? То что нужно.
Cisco Spark™ объединяет лучшее из двух подходов выше. Это облачная платформа для совместной работы со сквозным шифрованием, позволяющая ИТ-инженерам выбирать, что из контента может быть доступно Cisco и третьим сторонам.

Какой вариант подходит для вашей модели обеспечения безопасности?



Теперь ключи у вас. Сквозное шифрование и предоставление контроля заказчикам

В Cisco Spark используется открытая архитектура, обеспечивающая безопасную выдачу ключей шифрования и предлагающая вашим заказчикам эксклюзивный контроль над этими ключами для защиты конфиденциальных данных. Это означает, что контент шифруется на пользовательском клиенте и остается зашифрованным, пока не попадет к получателю. Никакие посредники не имеют доступа к ключам шифрования, если компания не предоставила им такого доступа в явном виде.



Локальный сервер ключей

Облачный сервер хранения контента

Подробнее >

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Cisco, логотип Cisco и Cisco Spark являются товарными знаками или зарегистрированными товарными знаками компании Cisco и (или) ее аффилированных компаний в США и других странах. (1606R)