Облака, гибрид и ЦОД – за и против

сентябрь 2019

системный архитектор

Сергей Юцайтис

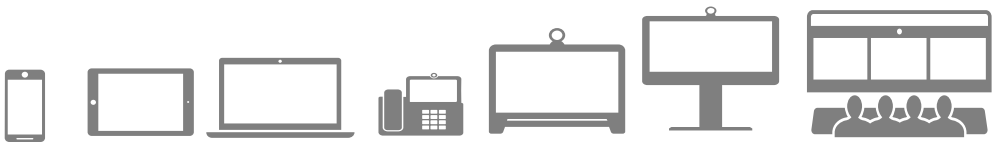
Видео+Конференция 2019

Облако / Гибрид / Датацентр – критерии сравнения

Стоимость Надежность Безопасность

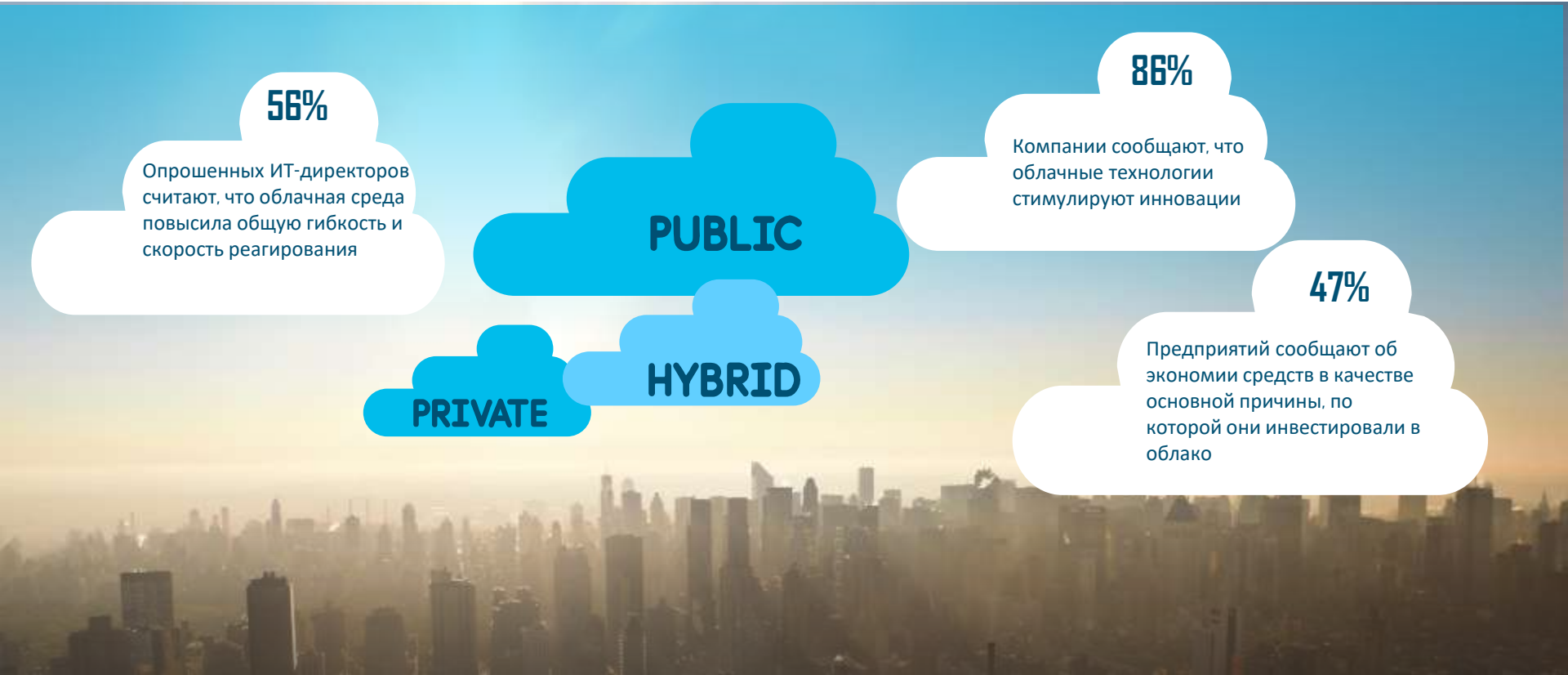
Функционал Возможность интеграции

Скорость внедрения / масштабируемость Управляемость и поддержка



Чем облака могут помочь бизнесу? Какие преимущества и недостатки разных вариантов предоставления сервисов -

Облако / Гибрид / Датацентр



Стоимость

Лицензии (on-prem)

подписка
(облако/ гибрид)

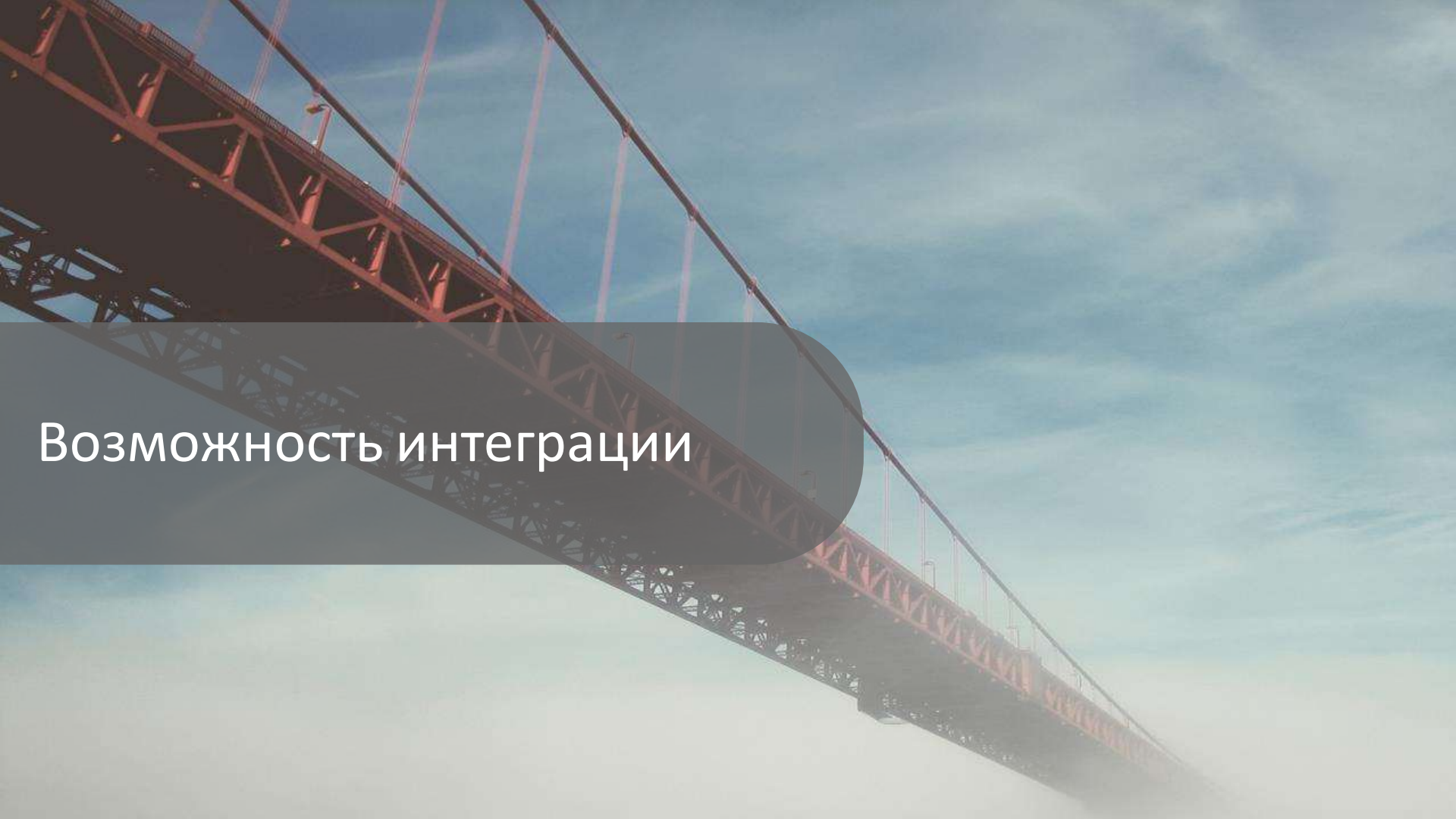
Серверное оборудование датацентра

Терминалы

Стоимость подписки / лицензий

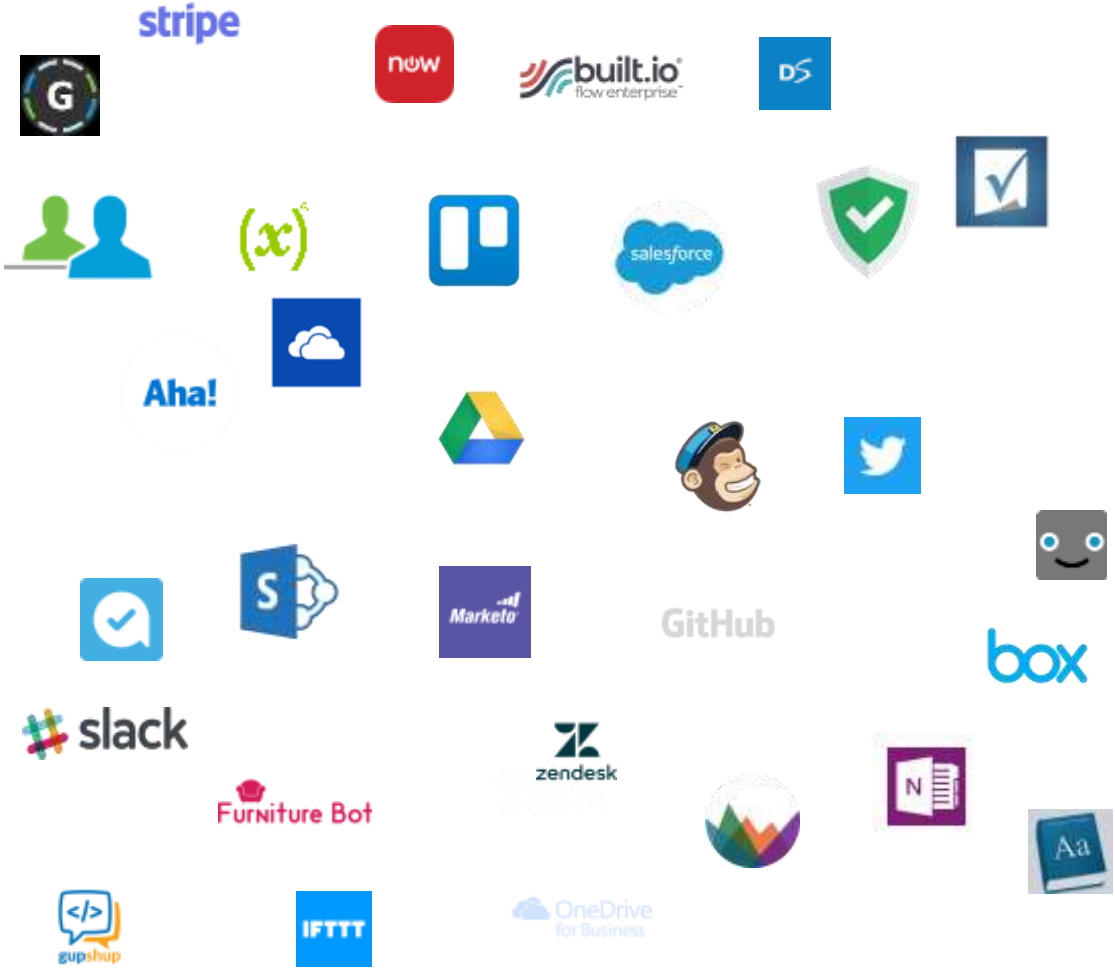
В облаке 40 конференций по 1000 участников в каждой (200 из них видеотерминалы) с записью - 16320 $ в год + 40 регистраций терминалов в облаке

40 регистраций видеотерминалов на CUCM или Expressway это уже 27300 $ + 5382 $ в год стоимость сервисного контракта


Возможность интеграции

Из наиболее популярных SaaS сервисов

34 уже интегрированы с Webex Teams



Source: BetterCloud: State-of-the-SaaS-Powered-Workplace

Webex Teams интеграция (в том числе с решениями Компаний - конкурентов)

Новое!

Предотвращение потери данных и архивирование, Теперь с решением от Palo Alto - Networks Aperture

Cisco Cloudlock

skyhigh

actiance

paloalto NETWORKS

globalRELAY

(Cisco Advanced Services предложение)

VERINT verba

netskope

bitglass

Symantec

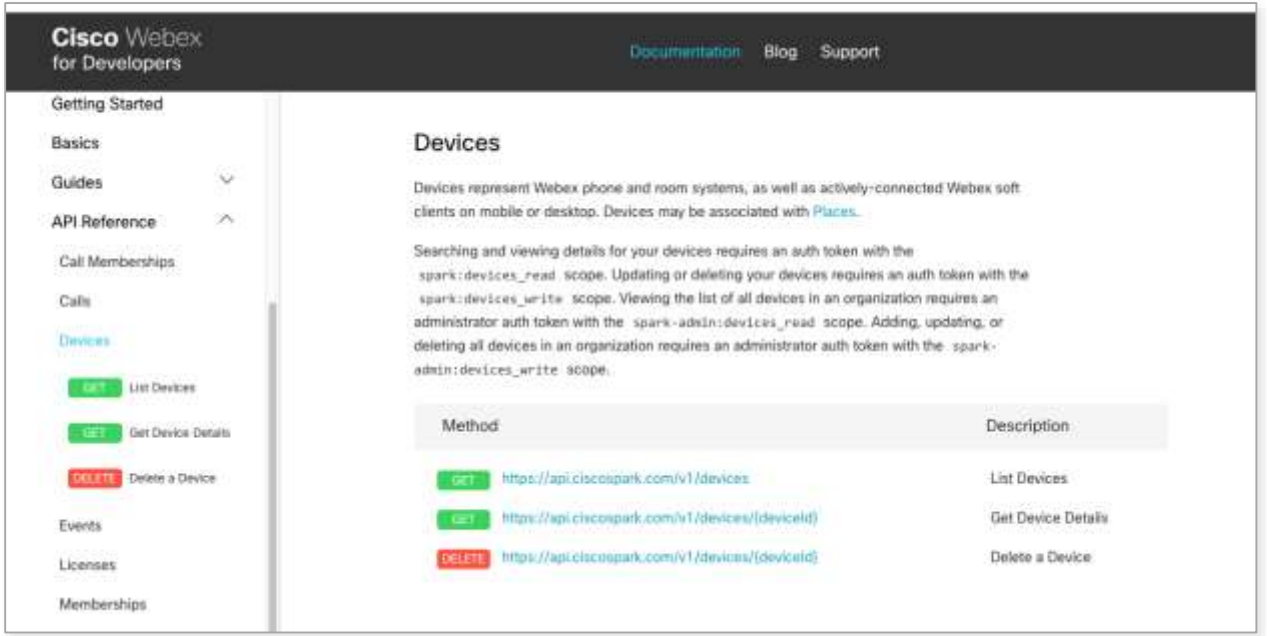
Новое

Webex для разработчиков

Управляйте любым

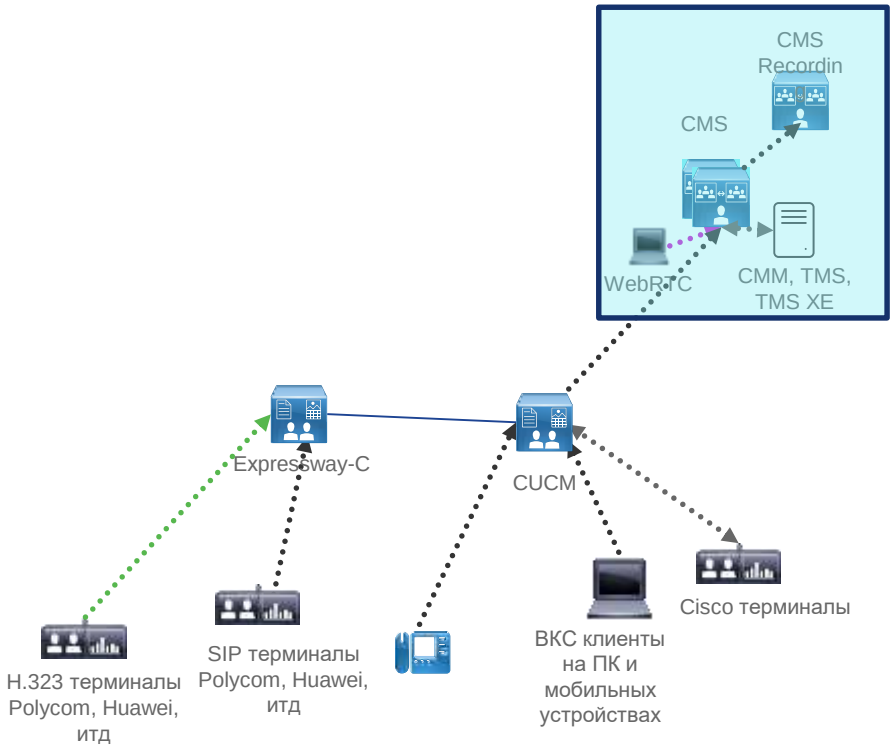
с Cisco Cloud Command API.

В дополнение – новое ПО терминалов позволяет с них HTTP POST запросы, свою очередь, реализует полноценную, RESTFUL коммуникацию, позволяющую дополнить сервисами от других производителей.

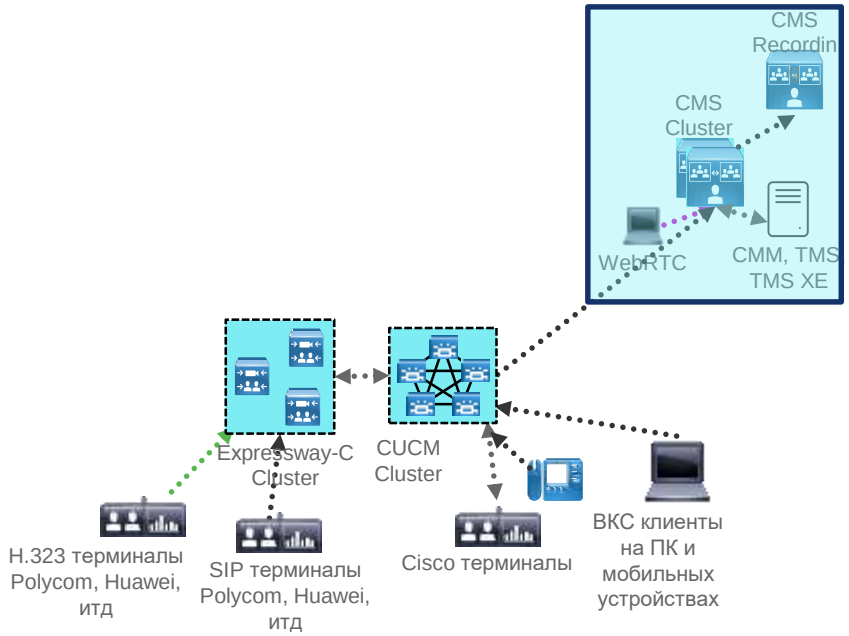



НАДЕЖНОСТЬ

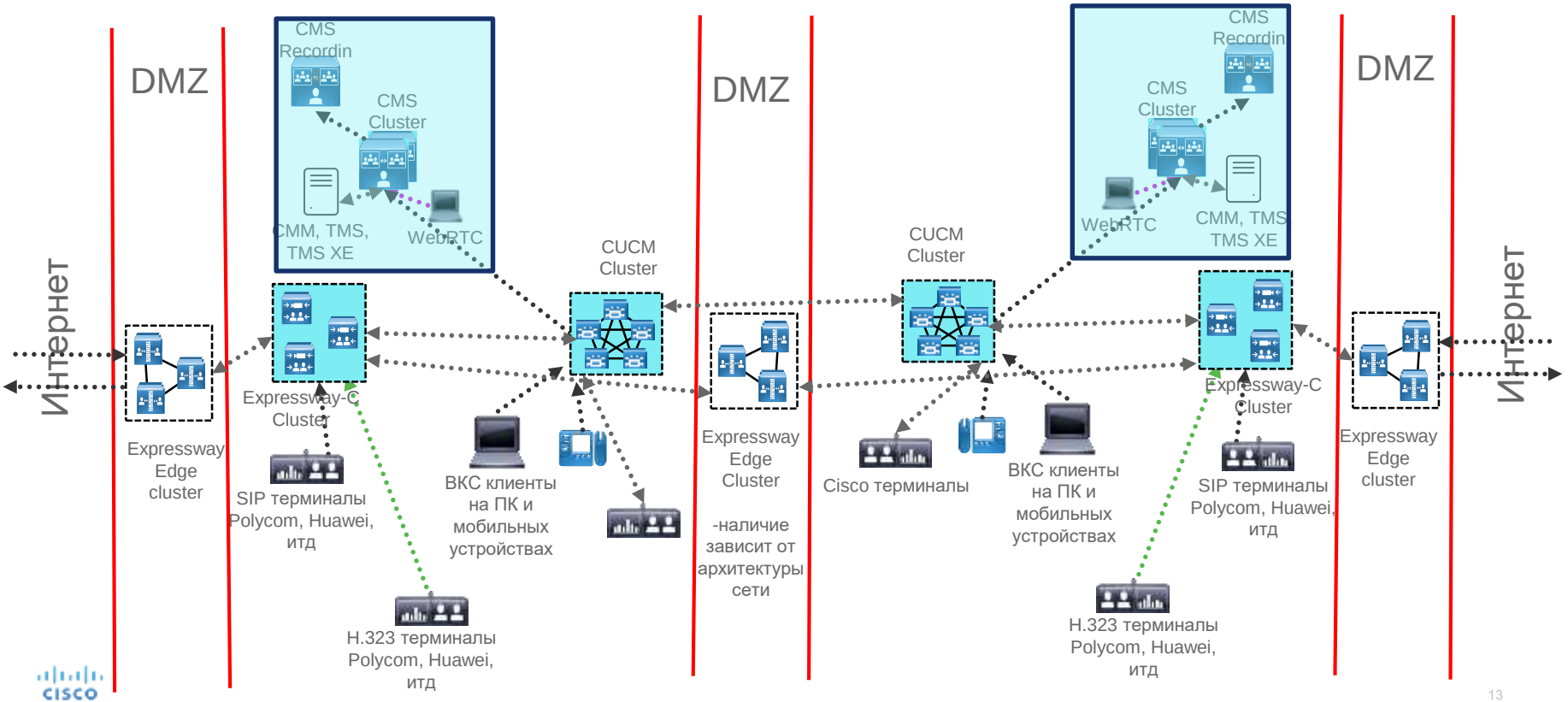
Архитектура решения для совместной работы в датацентре (показаны основные компоненты решения)



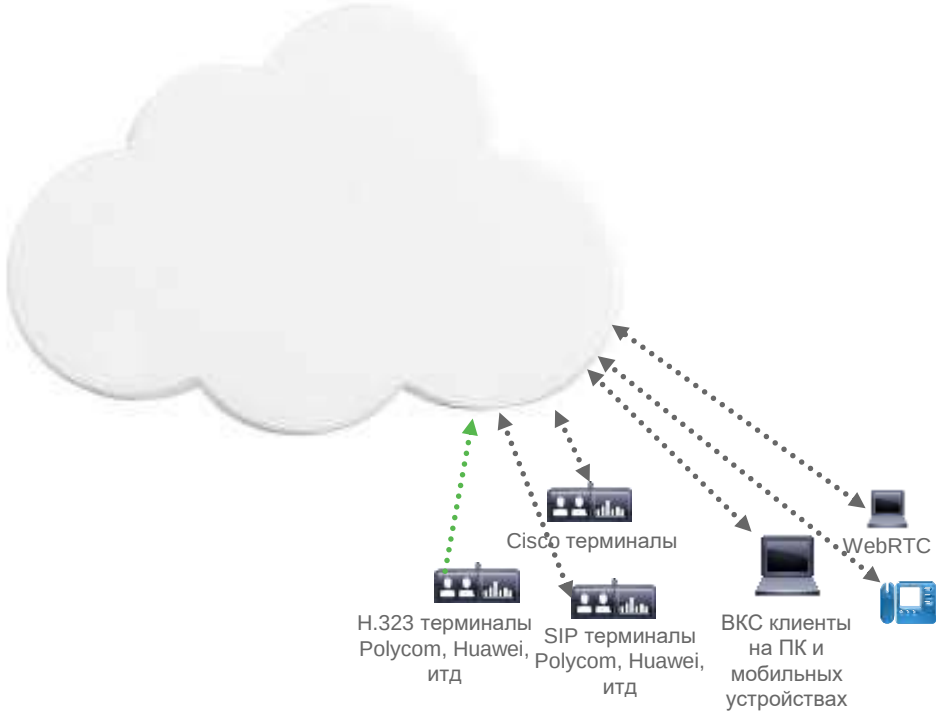
Архитектура решения для совместной работы в отказоустойчивом датацентре (показаны основные компоненты решения)



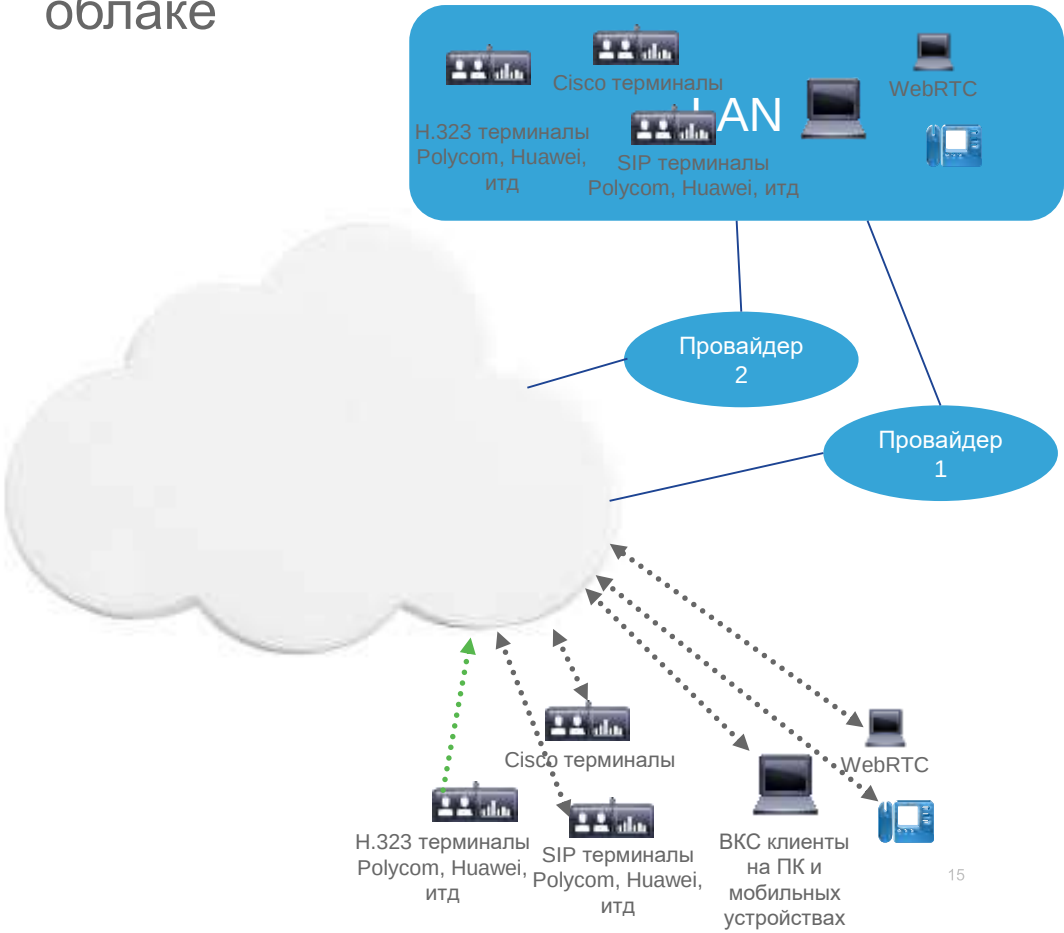
Архитектура решения для совместной работы в отказоустойчивом датацентре георасределенных предприятий (показаны основные компоненты решения)



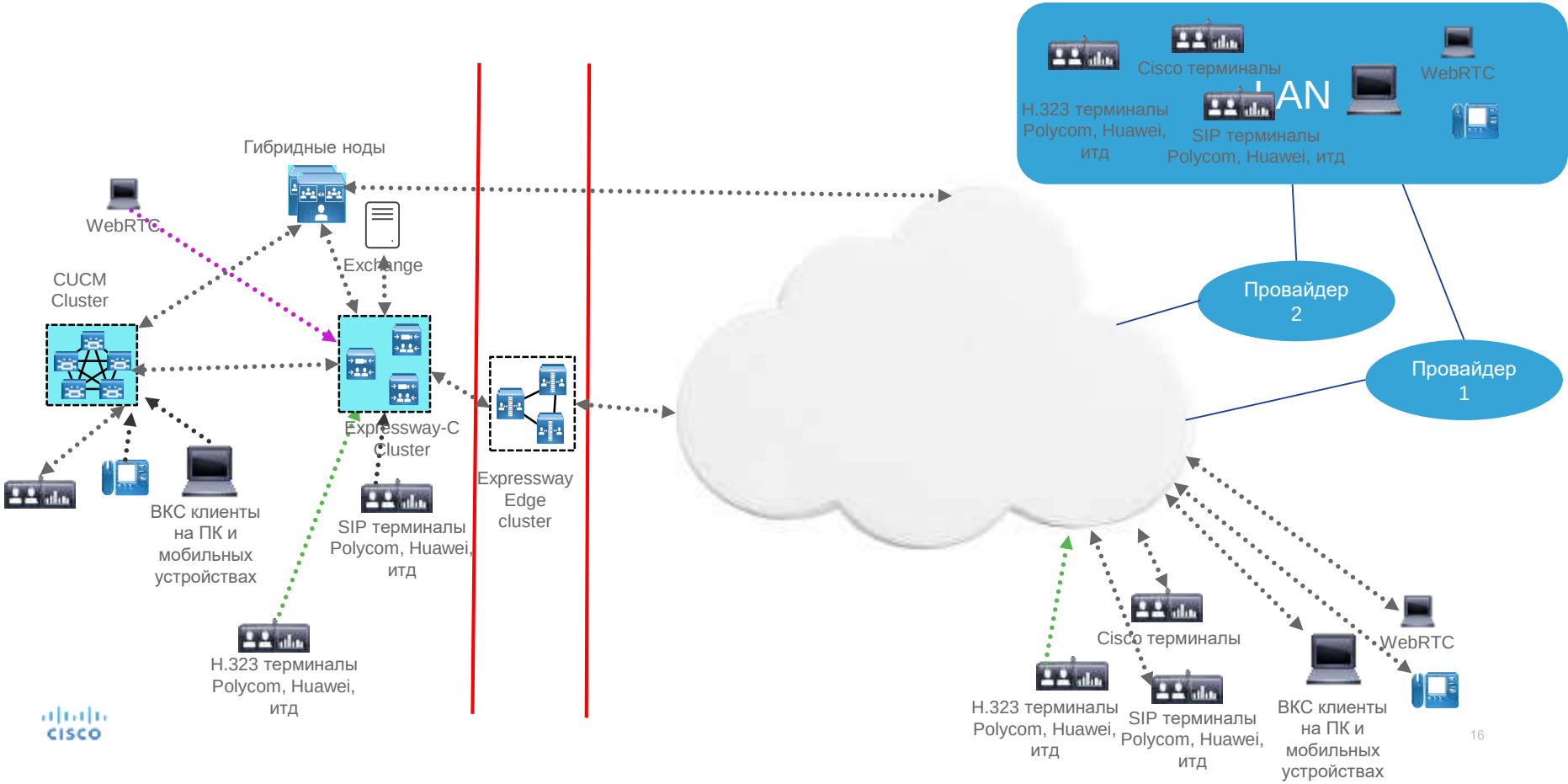
Отказоустойчивая архитектура решения для совместной работы в облаке



Отказоустойчивая архитектура решения для совместной работы в облаке



Отказоустойчивая архитектура решения для совместной работы в облаке



Cloud first,
not cloud only

И тем не менее…

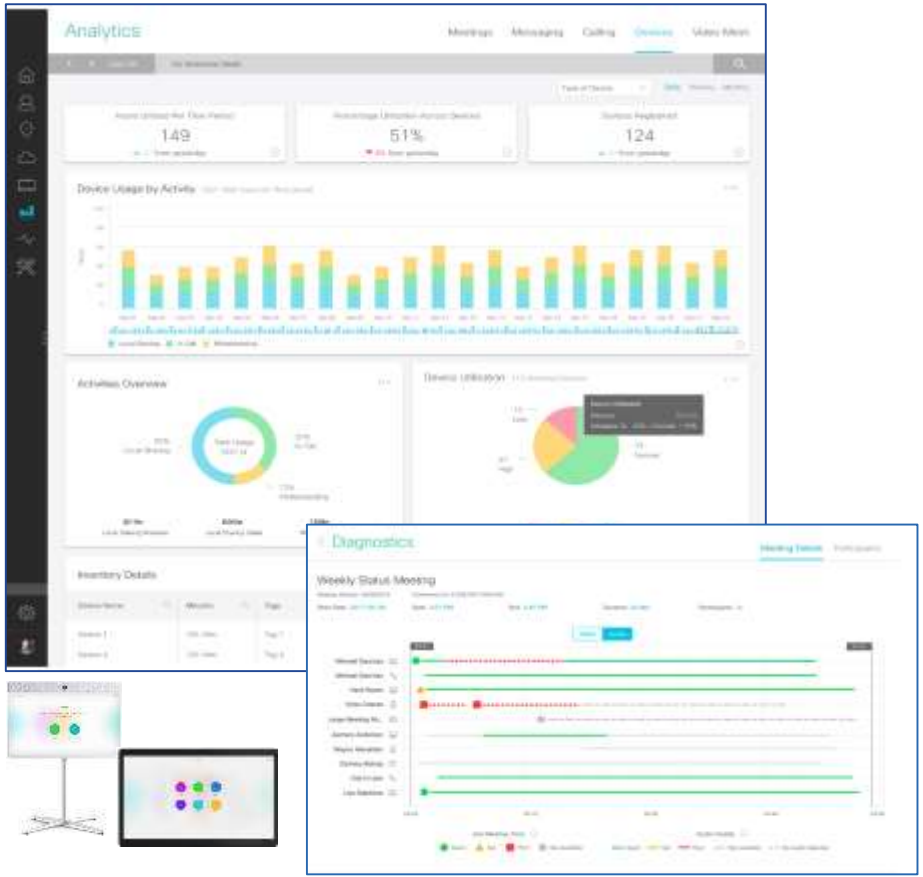
Аналитика: Лучшая видимость устройств

Новое!

Обновленная статистика по использованию устройств

- Включает информацию о проведенных встречах, контенту (в том числе локально демонстрированному) и использованию «белой доски»
- Детализация, фильтрация и интерактивный просмотр данных.
- Группировка устройств по степени использования (High, Medium и Low)

Диагностика конференций улучшена в части подключенных к облаку устройств. Диагностика теперь показывает качество подклчений с Webex Room и Webex Board&



Продвинутая диагностика

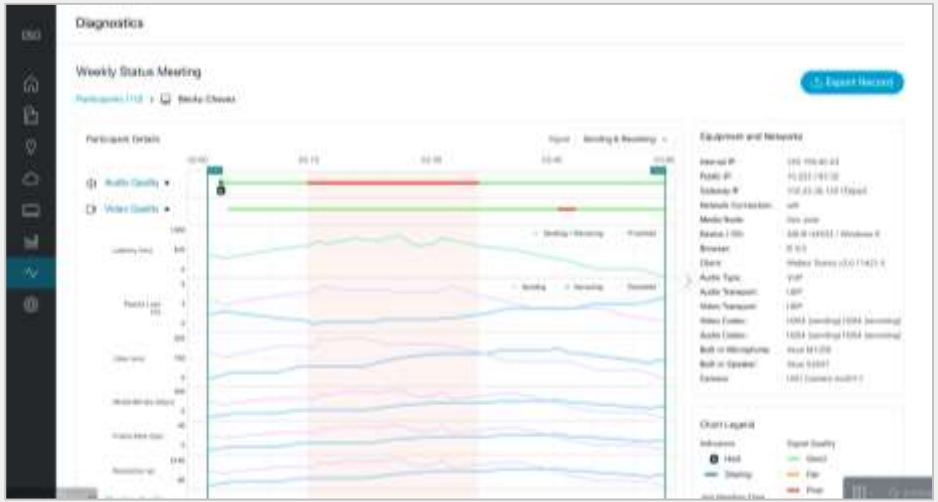
Дает полную видимость сети и устройств IT администраторам

Доступно в облаке

Позволяет IT администраторам диагностировать и исправлять проблемы с качеством видео и аудио Webex **без вмешательства Cisco TAC**

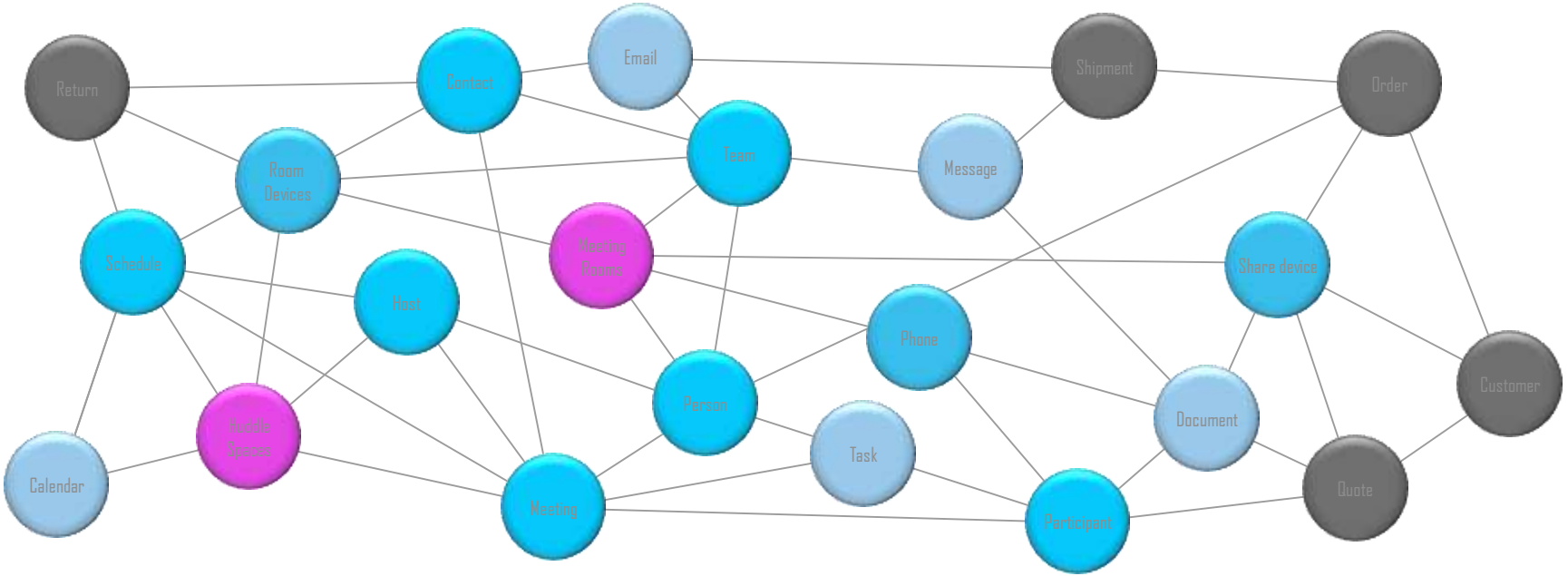
Обеспечивает видимость 20+ метрик подключений и конференций в режиме реального времени, позволяя IT администраторам быстро установить источник проблем качества:

- Оборудование и ПО пользователя (загрузка CPU)
- Информация о подключении
- Изменение метрик подключения с течением времени



Webex Graph: продвинутая аналитика

Информация становится по настоящему полезной, если доступна тогда, когда Вы в ней нуждаетесь и в том объеме, в котором нужна.



Команды + Инструменты + Пространства + Устройства + Бизнес процессы

Режим «компаньона»

Возможность подключения к любой видеосессии Webex Board в качестве источника презентации.

Доступно в облаке

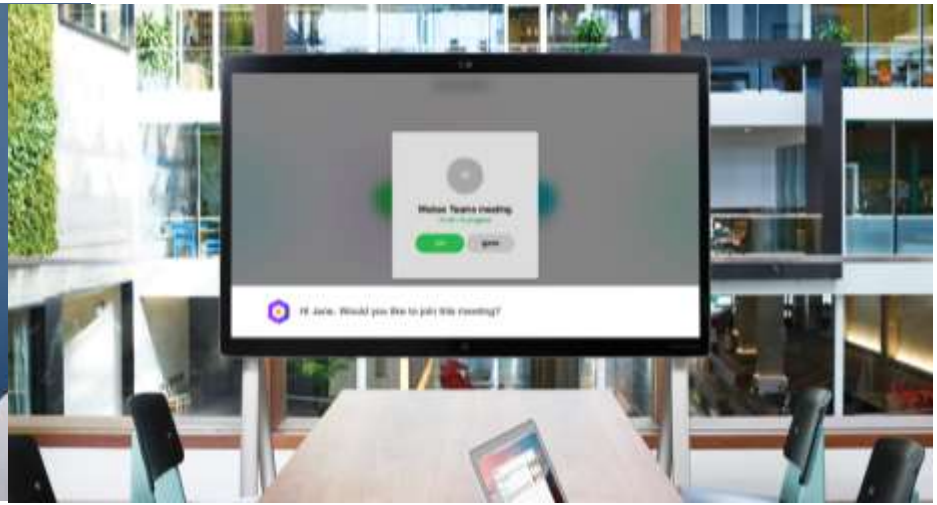
Впервые в индустрии!

Соединение Cisco Room устройств для видео с Webex Board для цифровой доски

Webex ассистент и проактивное подключение

Webex ассистент знает что Вы вошли в комнату и спросит Вас о подключении к конференции, когда она начнется.

Доступно в облаке



People Insights

Позволяет участникам встречи получать информацию о других участниках

Уже доступно в облаке

Webex конференции

Уже доступно в облаке

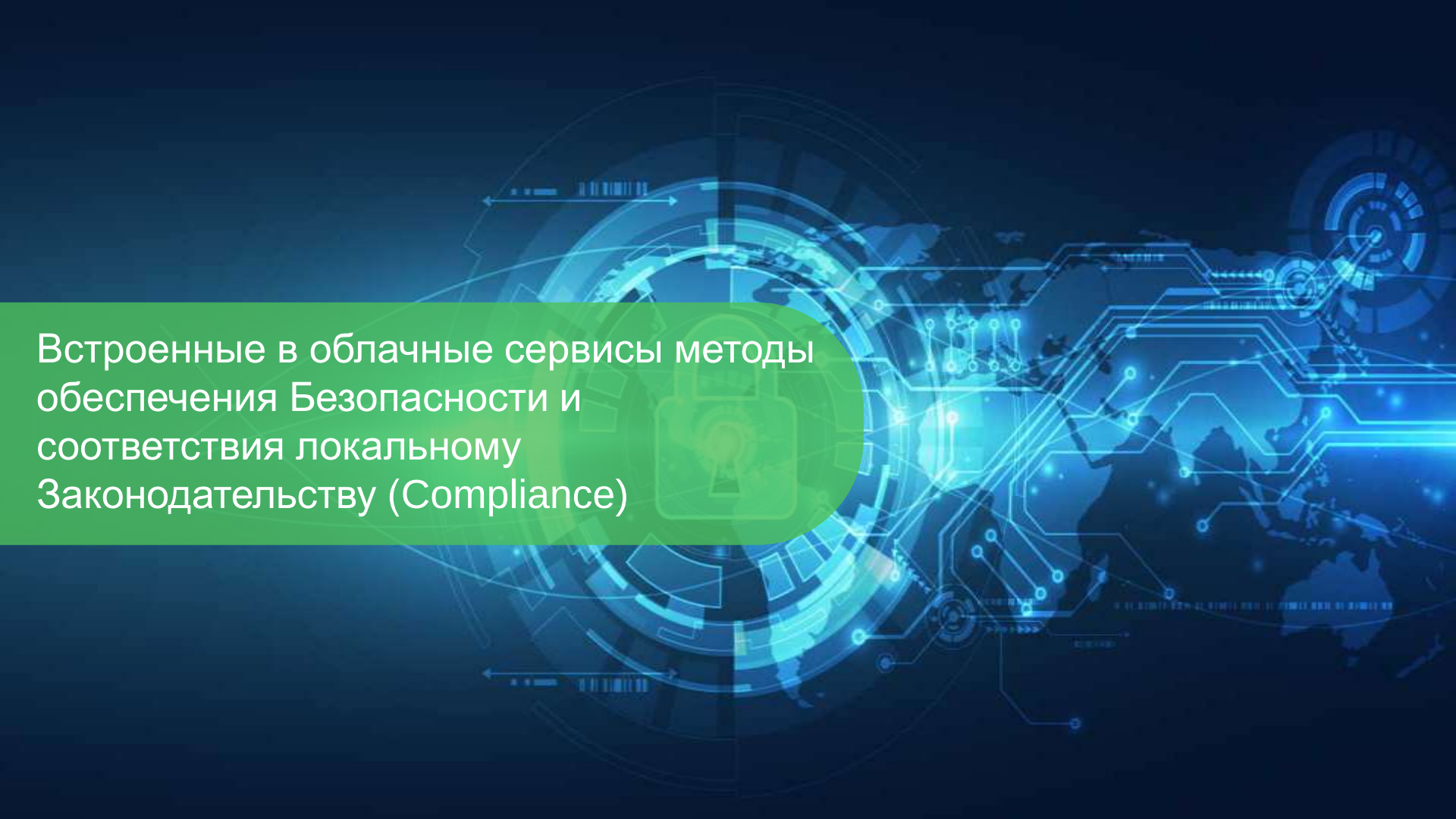
Webex Teams

people.webex.com

Скоро будет доступно в облаке:
Q4 CY 2019

Jabber

Встроенные в облачные сервисы методы обеспечения Безопасности и соответствия локальному Законодательству (Compliance)



Международная сертификация

Лучшие практики

Сертификация дата центра

- ISO 27001/ISO 27017
- ISO 9001
- SOC 2 Type 2 and SOC 3
- Cloud Computing Compliance Controls Catalog (C5)

Обеспечение приватности

- HIPAA: Data privacy and security provisions for safeguarding medical information
- GDPR: Processing by an individual, a company, or an organization of personal data relating to individuals in the E.U.

Трансграничный контроль

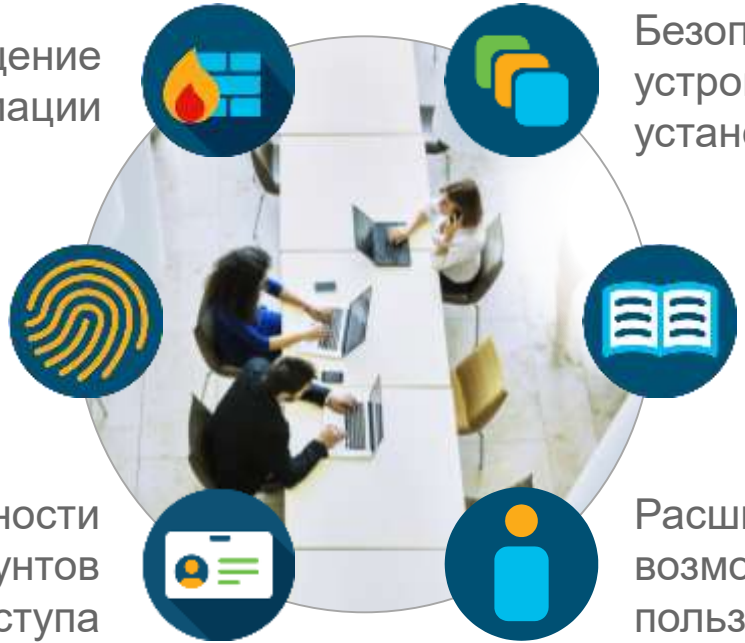
- E.U.-U.S. privacy shield
- Swiss-U.S. privacy shield
- APEC cross-border privacy rules

Комплексный (360 градусов) подход к обеспечению безопасности и комплаенса

Предотвращение потери информации

Безопасность приложений и устройств на которые они установлены

Безопасность и приватность данных



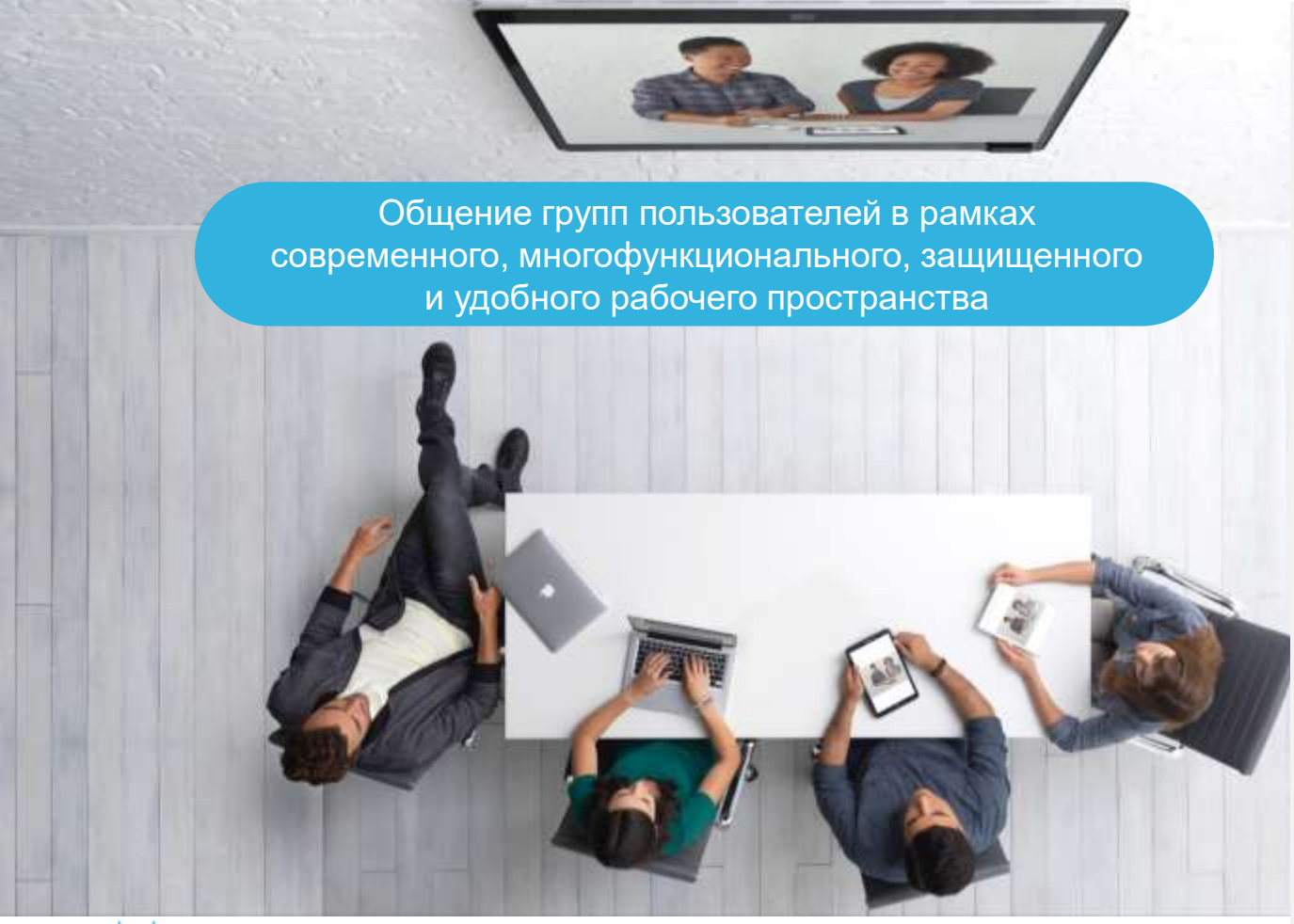
Соблюдение законодательства

Обеспечение безопасности пользовательских аккаунтов и доступа

Расширение возможностей пользователя

Расширение возможностей IT

- Определение времени хранения данных
- Обеспечение безопасности пользовательских устройств : защита PIN / управление паролем
- Удаленное управление устройствами на которых сохранен контент с возможностью стирания данных и обнулением устройства
- Уменьшение риска случайного обмена конфиденциальными файлами с помощью средств управления общего доступом к файлам и их пересылке, благодаря возможности контроля и блокирования внешних коммуникаций
- Защитите свою инфраструктуру, заблокировав доступ к не корпоративным учетным записям пользователей, пока сотрудники находятся в корпоративной сети (на компьютере и в Интернете)
- Ведите журнал активности пользователей и аудит журнал действий администраторов



Общение групп пользователей в рамках современного, многофункционального, защищенного и удобного рабочего пространства

- Поисковый сервис + e-Discovery
- Шифрование
- Аудит
- Стирание устройств
- Время хранения (Retention)
- Комплаенс
- Аналитика
- Двух факторная аутентификация
- Управление мобильными устройствами
- Архивация
- Отзыв токена доступа

“Производительность на 1-м месте”

- Не хочет встретиться с неожиданной блокировкой или ограничениями на управляемым Компанией корпоративном устройством
- Ожидает от IT соответствующей ей производительности
- Слышала о потерях информации и получению к ней не санкционированного доступа при краже или потере устройств

Проблема

- Нужна мгновенная настройка нового устройства BYOD
- Высокая безопасность при использовании
- Защитите информацию, если устройство потеряно

Решение

- Автоматический провижионинг новых устройств без привлечения Администратора
- Защита **ПИН** для всех устройств
- **Удаленное удаление контента** и отзыв токенов доступа
- Соответствующий (важный для пользователя)контент переносится в долгосрочный **архив**

“Game changer”

- Следует Корпоративной стратегии
- Отвечает за особо секретные проекты и инвестиции
- НЕ доверяет никому– ни IT, ни Cisco

Проблема

- НЕ хочет чтобы в IT могли просматривать его контент
- Только он должен управлять кто имеет доступом к материалам по каждому из проектов
- Должен соответствовать требованиям Компании в части предоставления доступа к данным

Решение

- **Настройка его собственных пространств (spaces)** для внутреннего и внешнего общения
- **On-premises управление ключами шифрования**
- Весь трафик встреч и сообщений является собственностью только его Компании
- **Весь контент сохраняется в соответствии настроенной IT политике хранения**
- Поиск по контенту и его извлечение, кроме допущенных к нему владельцем пространства может быть осуществлен только специально авторизованными Компанией лицами

“Я верю в систему”

- Работает в кредитном отделе
- Обрабатывает конфиденциальные транзакции
- Предполагается, что ее ИТ-системы защищают ее и полностью доверяет им

Проблемы

- Все политики по соответствию правилам Компании всегда должны применяться и контролироваться

Решение

- Аутентификация в облаке должна быть **разрешена только** через корпоративный SSO
- Применение политик по контролю предоставления доступа к информации, использующих системы Предотвращения Потери Данных (DLP), должно проводиться умно (smartly) и надлежащим образом

Методы обеспечения безопасности в облаке – разделение сфер

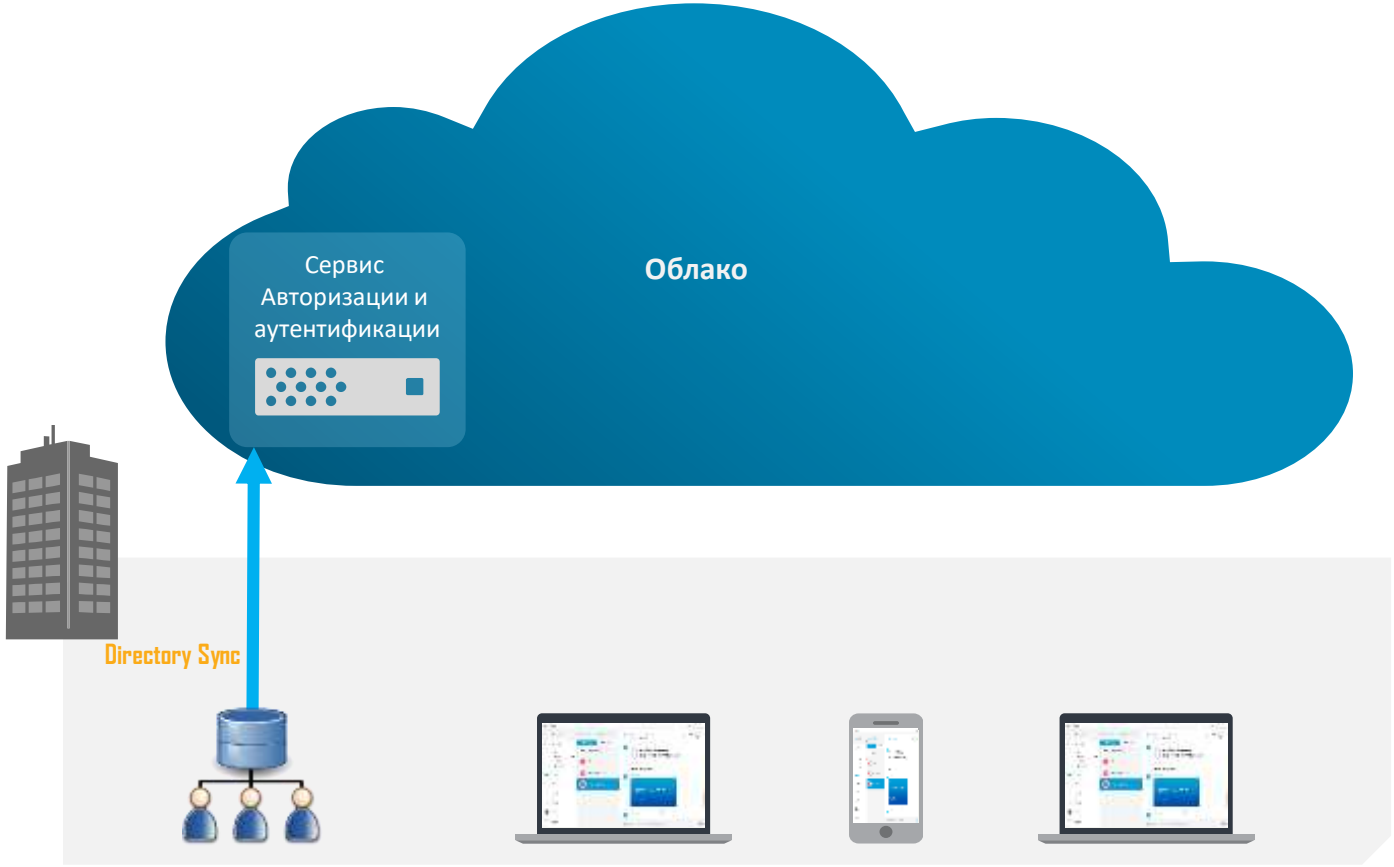
Webex логически и физически разделяет функциональные компоненты в облаке

Сервис идентификации (Identity Services), хранящие пользовательские данные (например, адреса электронной почты) отделены от:

Сервиса шифрования, индексирования и поиска, которые в свою очередь отделены от:

сервиса хранения данных

Синхронизация и загрузка данных пользователей для аутентификации



Пользователи могут быть синхронизованы с облаком Webex из AD предприятия

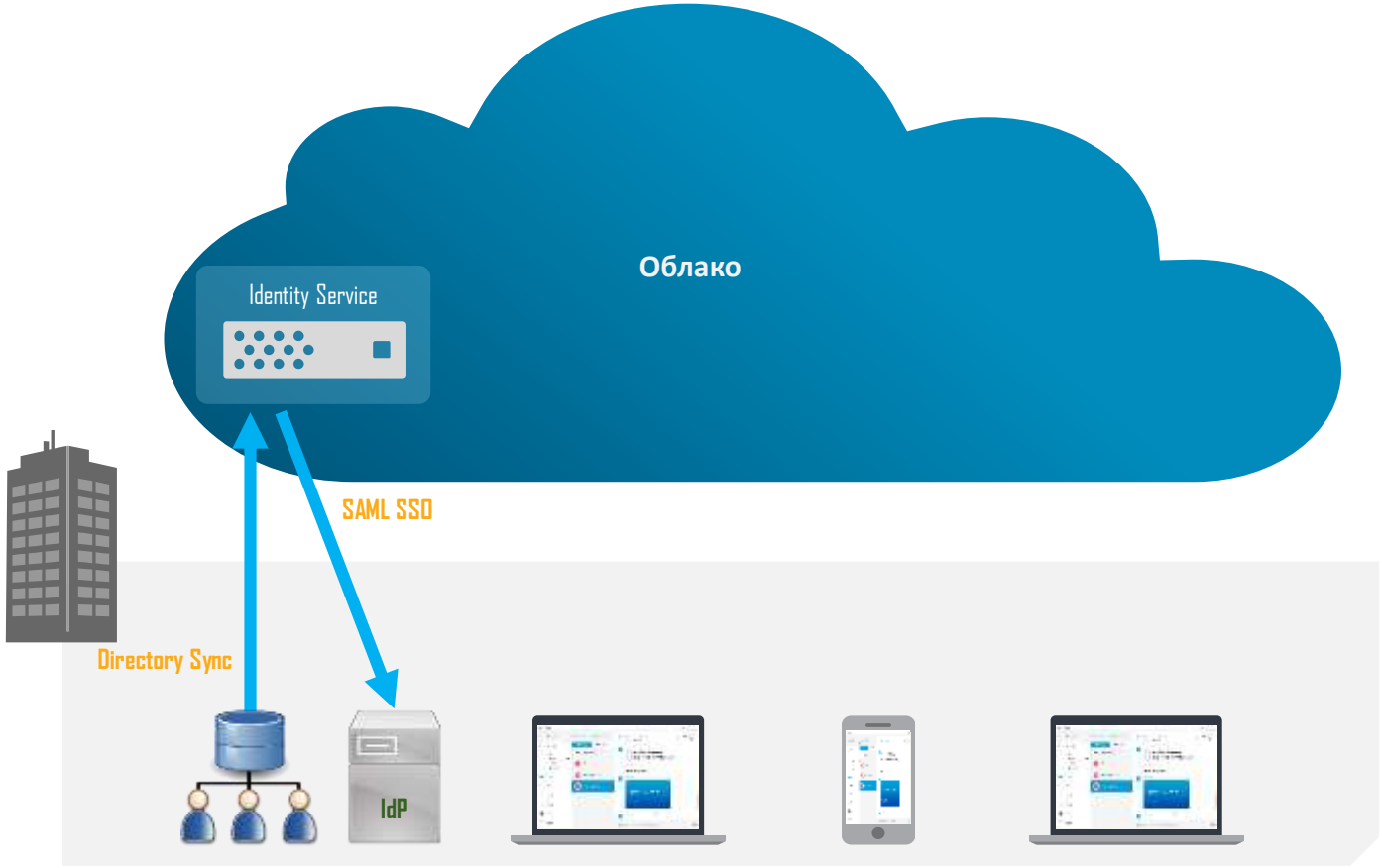
Могут быть синхронизованы различные атрибуты

Запланированные сессии синхронизации могут отслеживать изменения пользователей

Пароли не синхронизуются-
Пользователь :

1) Задает Webex Teams пароль, или
2) Использует SSO для Auth

SAML SSO аутентифткация

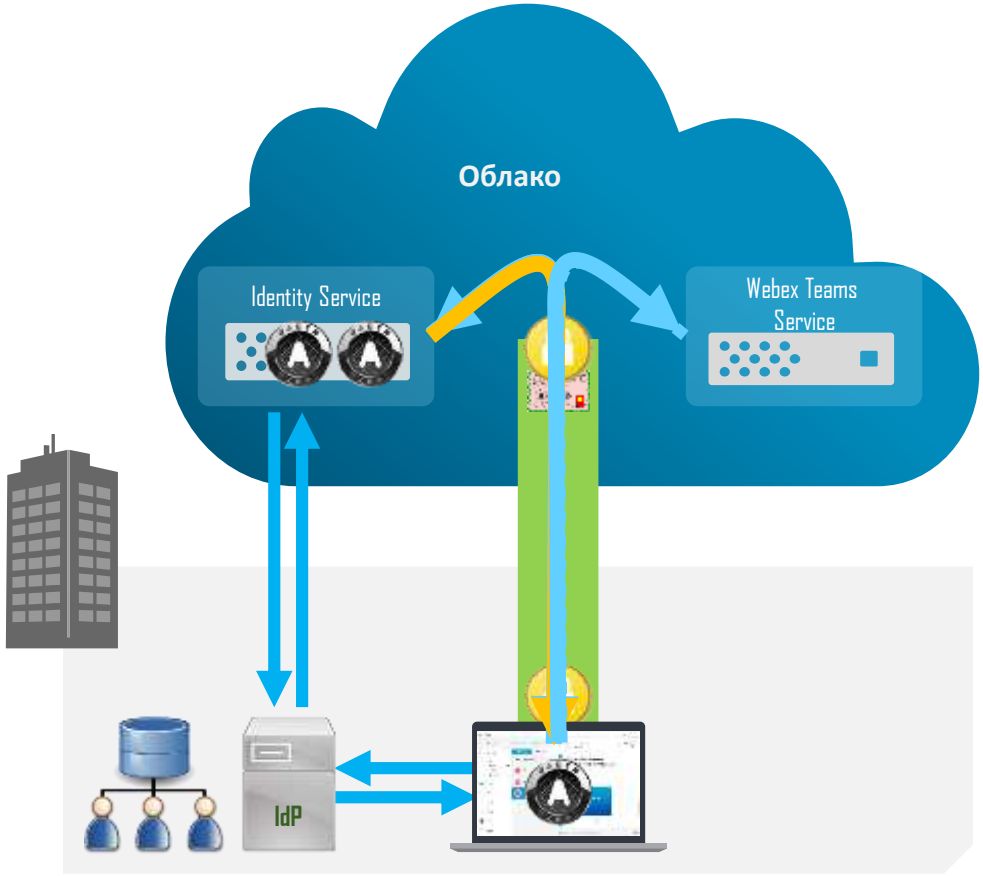


SSO для аутентификации пользователя:

Администратор может настроить Webex Teams для работы с существующим SSO решением

Webex Teams поддерживает Identity Providers использующих Security Assertion Markup Language (SAML) 2.0 & OAuth 2.0

Webex Teams Приложение – подключение к облаку



1) Пользователь скачивает и устанавливает приложение
2) Приложение устанавливает безопасное TLS соединение с облаком
3) Облачный Identity Service запрашивает у ползователя e-mail ID
4) Пользователь аутентифицируется облачным Identity Service, или IdP (SSO) предприятия
5) OAuth токены доступа (Access) и обновления доступа (Refresh) создаются и пересылаются приложению

- Токены доступа содержат детали облачных ресурсов к которым пользователю авторизован доступ
- Приложение использует полученные токены для регистрации в облачных сервисах через безопасные каналы связи.

Webex Teams Apps : Шифрование сохраненных данных

Какие данные сохраняются и шифруются:

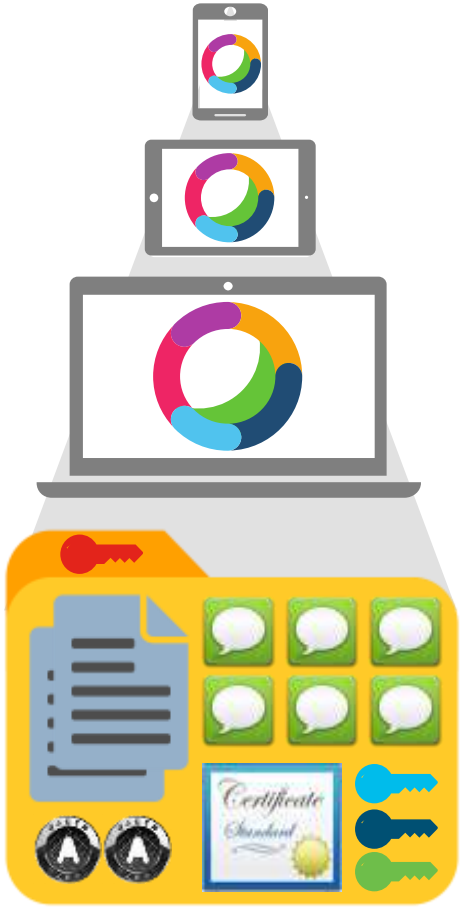
Space и их ключи шифрования
Встречи и их ключи шифрования
Белые доски (Whiteboards) и их ключи шифрования
Сообщения
Файлы
(Выбранная пользователем папка для загрузки файлов)
Токены авторизации

Загруженные данные шифруются с использованием:

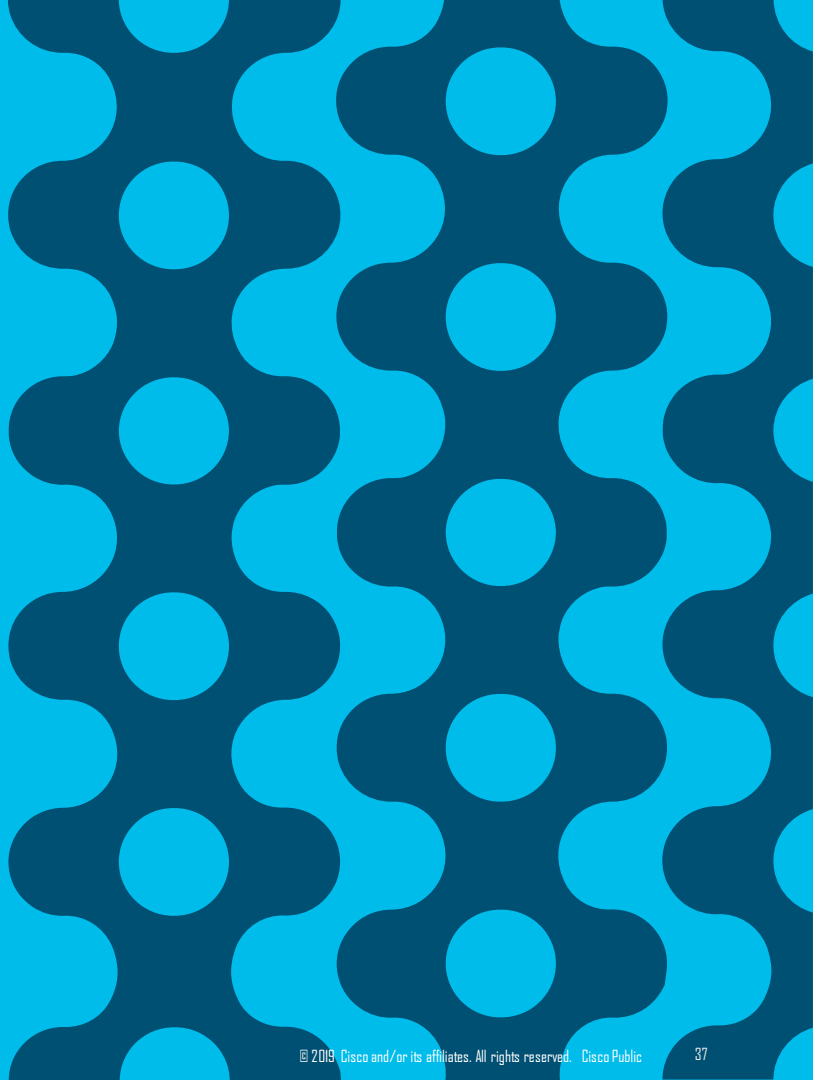
AES-256-GCM (Windows, Mac)
AES-128-GCM/CCM (iOS/Android)

Мастер ключ сохраняется в OS secure Store

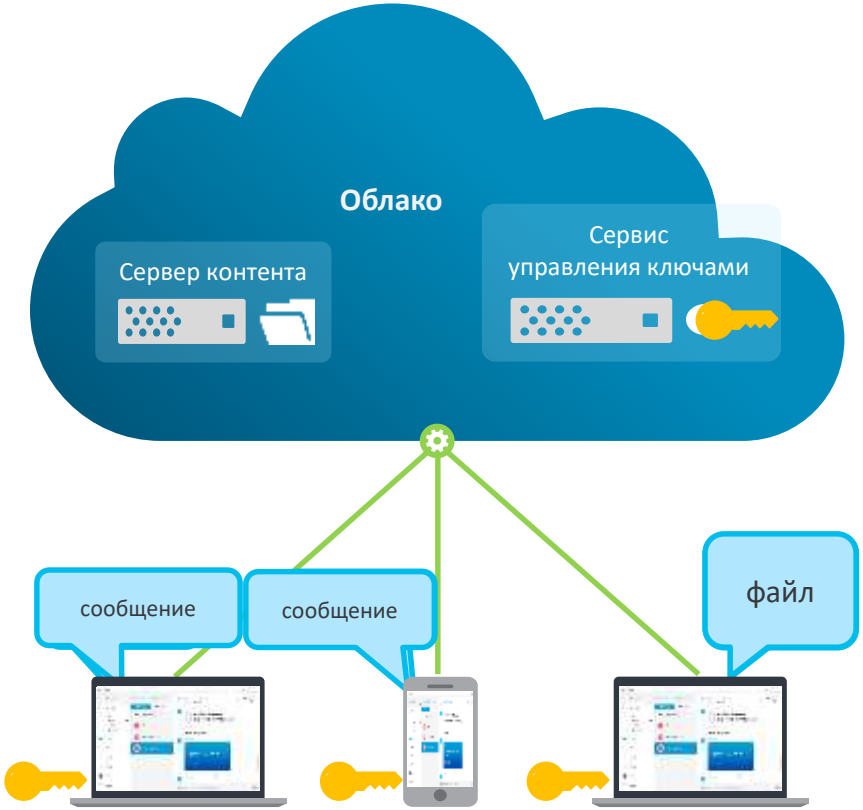
Возможность стирания данных для мобильных OS



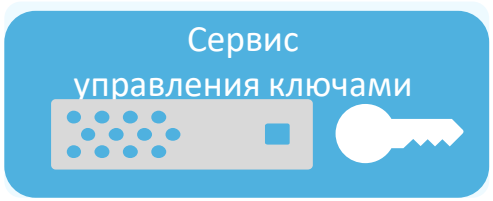
Безопасность облака: Сообщения и контент



Шифрование сообщений и контента



Для шифрования используется AES256-GCM cipher

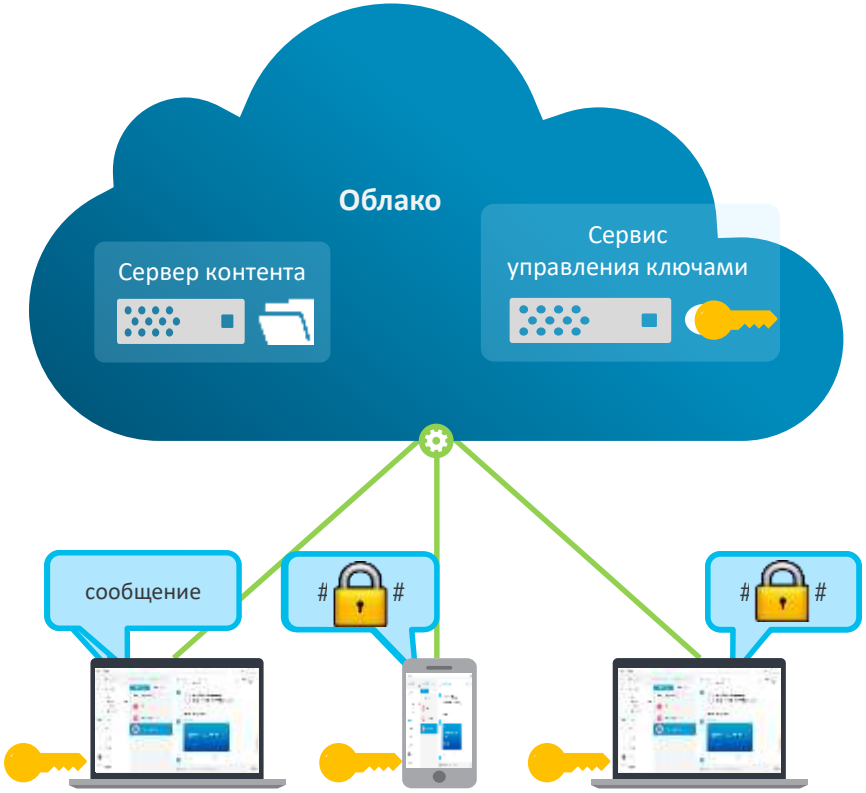


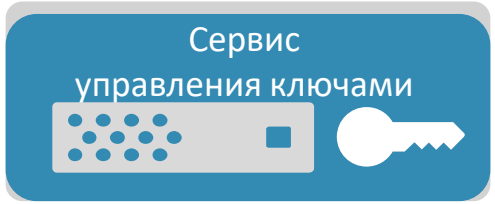
Любые сообщения или файлы, отправленные Приложением, шифруются перед отправкой в Webex Cloud.

Приложение Webex Teams запрашивает ключ шифрования сессии у службы управления ключами

Каждое пространство (Space) Webex использует свой ключ шифрования сессий.

Расшифровывание сообщений и контента





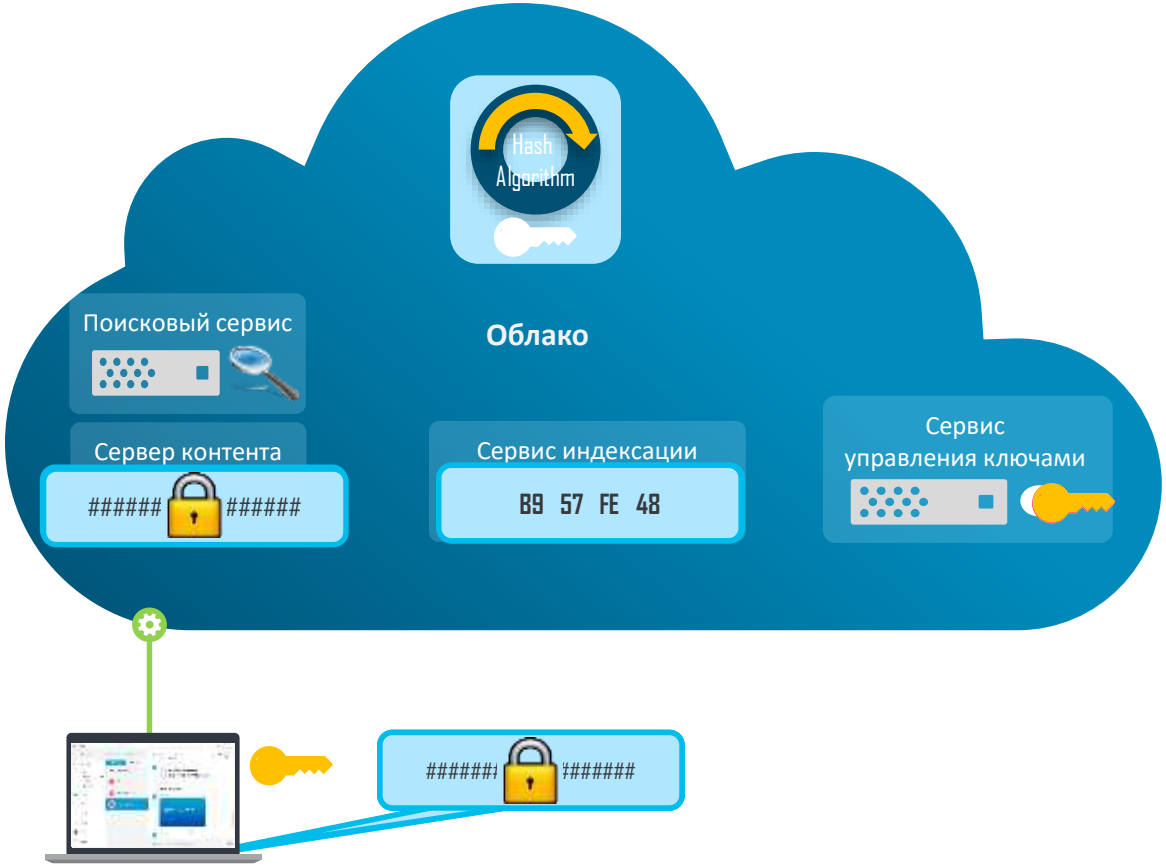
Зашифрованные сообщения, отправленные приложением, хранятся в облаке Webex, а также отправляются в каждое другое приложение в этом пространстве (Space) Webex.

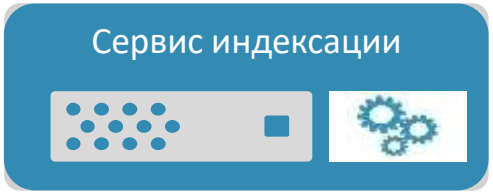
Зашифрованное сообщение также содержит ссылку на ключ шифрования сессии.

При необходимости Webex Teams приложения могут перезапросить ключи шифрования у службы управления ключами.

Безопасность облака : Поиск и индексация контента

Поиск в Webex Teams Spaces: создание поискового индекса





Служба индексирования: позволяет пользователям искать имена и слова в зашифрованных сообщениях, хранящихся на сервере контента, без расшифровки содержимого.

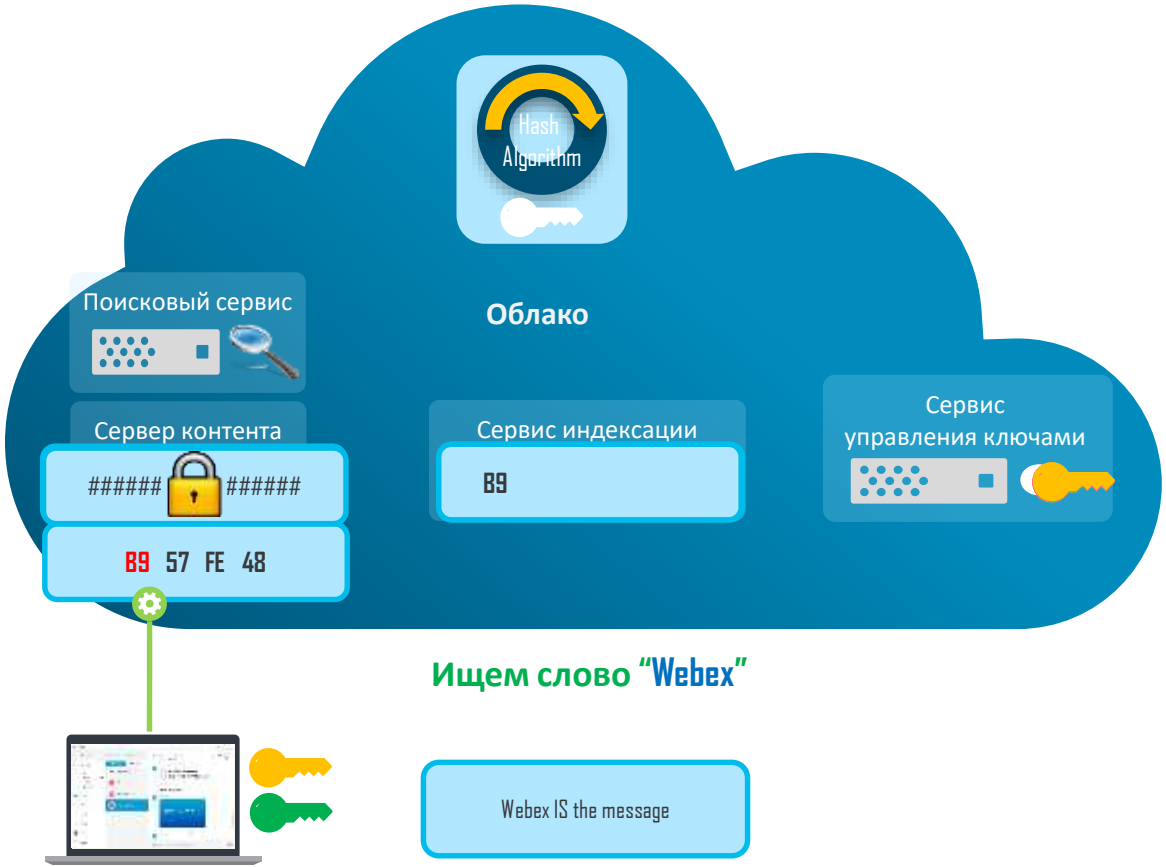
Поисковый индекс строится путем создания хеша* фиксированной длины для каждого слова в каждом сообщении внутри Space.

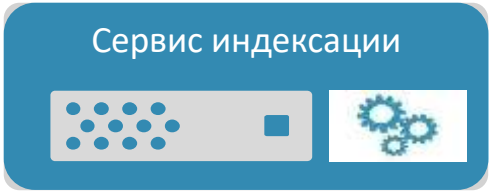
Хешированные индексы для каждого пространства (Space) хранятся контент сервисом

* Новый (SHA-256 HMAC) hashing key (поисковый ключ) используется для каждого из пространств (Spaces)

Webex Teams spaces : Запрос поискового индекса

Ищем слово "Webex"





Приложение отправляет поисковый запрос с использованием безопасного соединения в службу индексирования

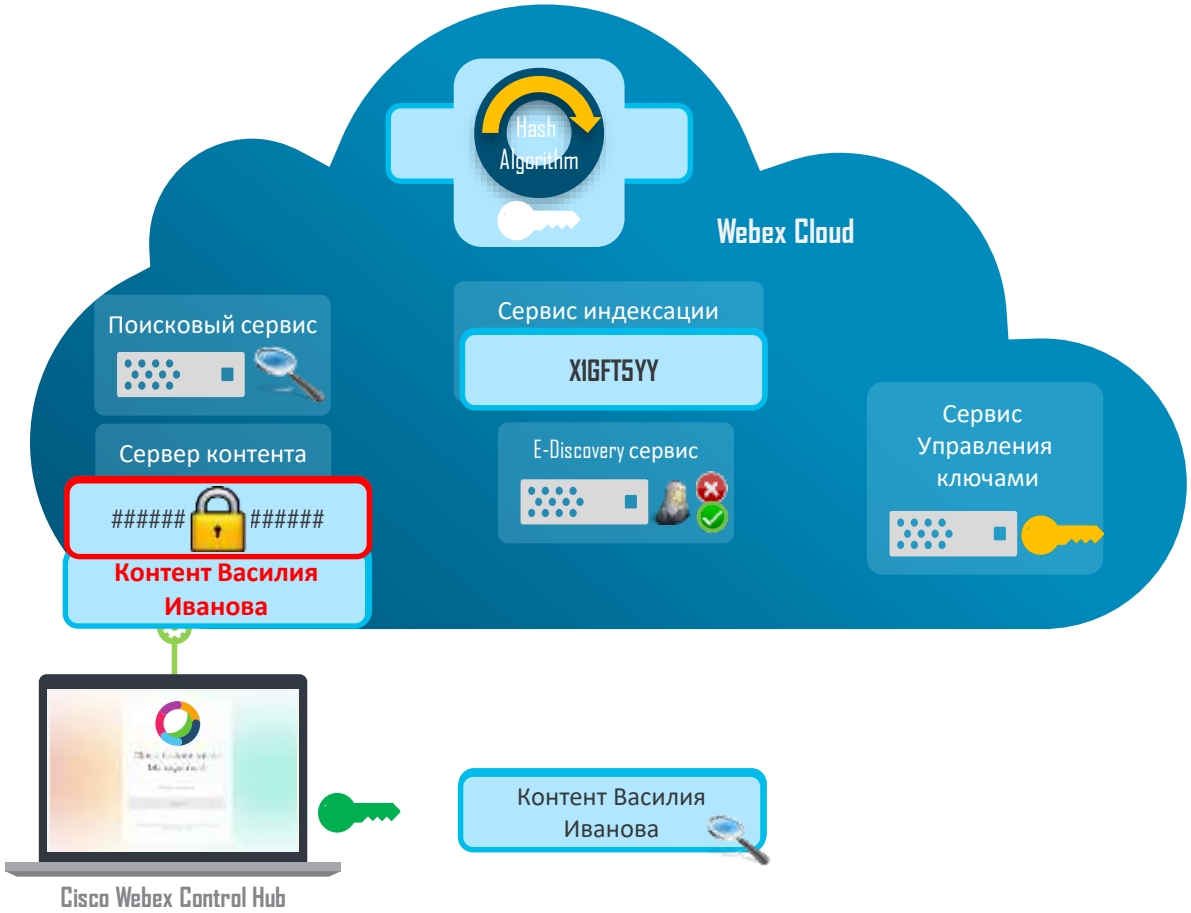
Служба индексирования использует поисковые ключи, специфичные для каждого Space, для хеширования поисковых терминов.

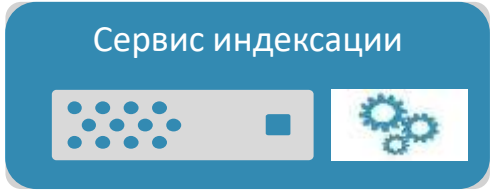
Служба поиска ищет совпадения в хеш-таблицах и возвращает соответствующий им контент приложению*

- Ссылка на ключ шифрования сессии отправляется с зашифрованным сообщением.

Безопасность облака : сервис E-Discovery

Webex Teams E-Discovery сервис : (1)



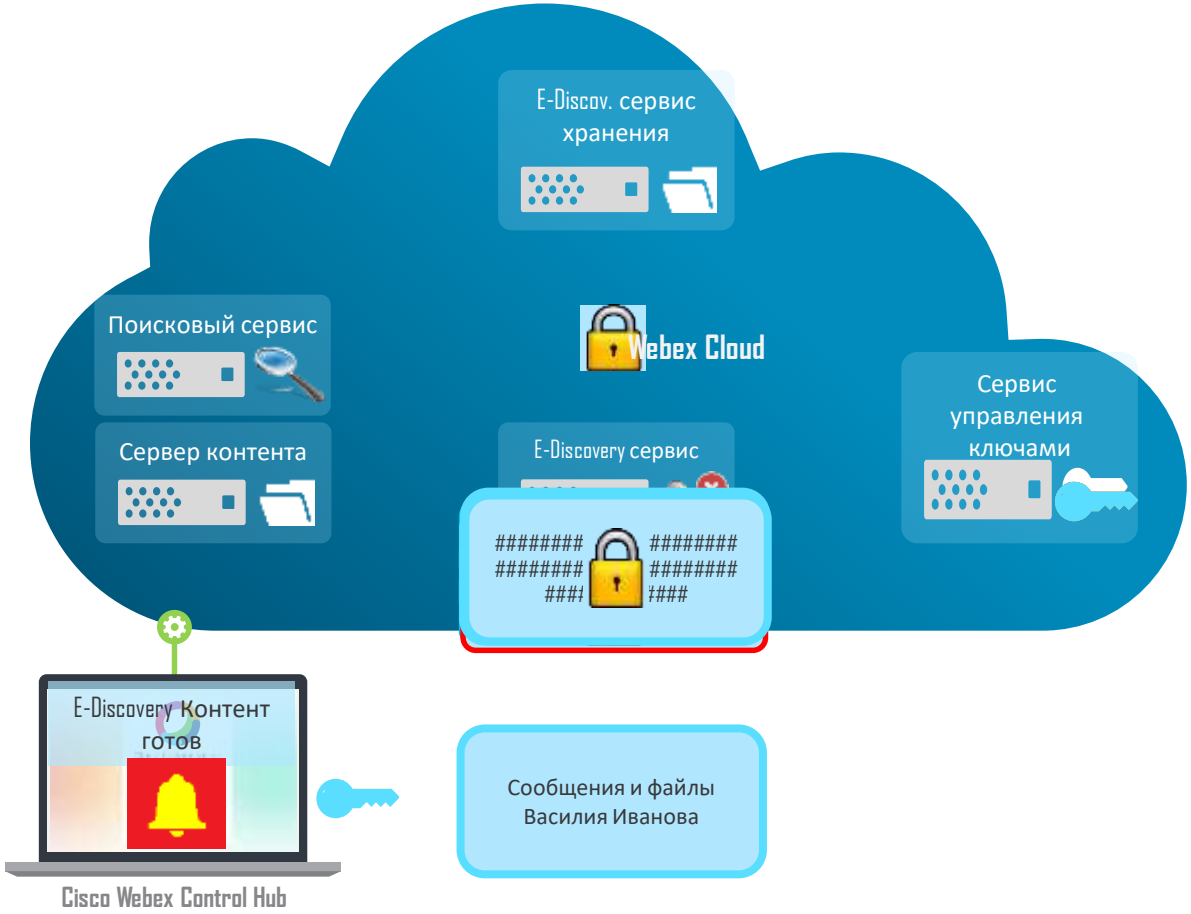


Уполномоченное лицо Компании выбирает данные запрашиваемые у E-Discovery, например: входящие в диапазон дат/ тип контента/ имя пользователя

Сервис индексации запрашивает поиск соответствующего хешированного контента

Контент сервер возвращает требуемый контент E-Discovery сервису

Webex Teams E-Discovery Service : (2)



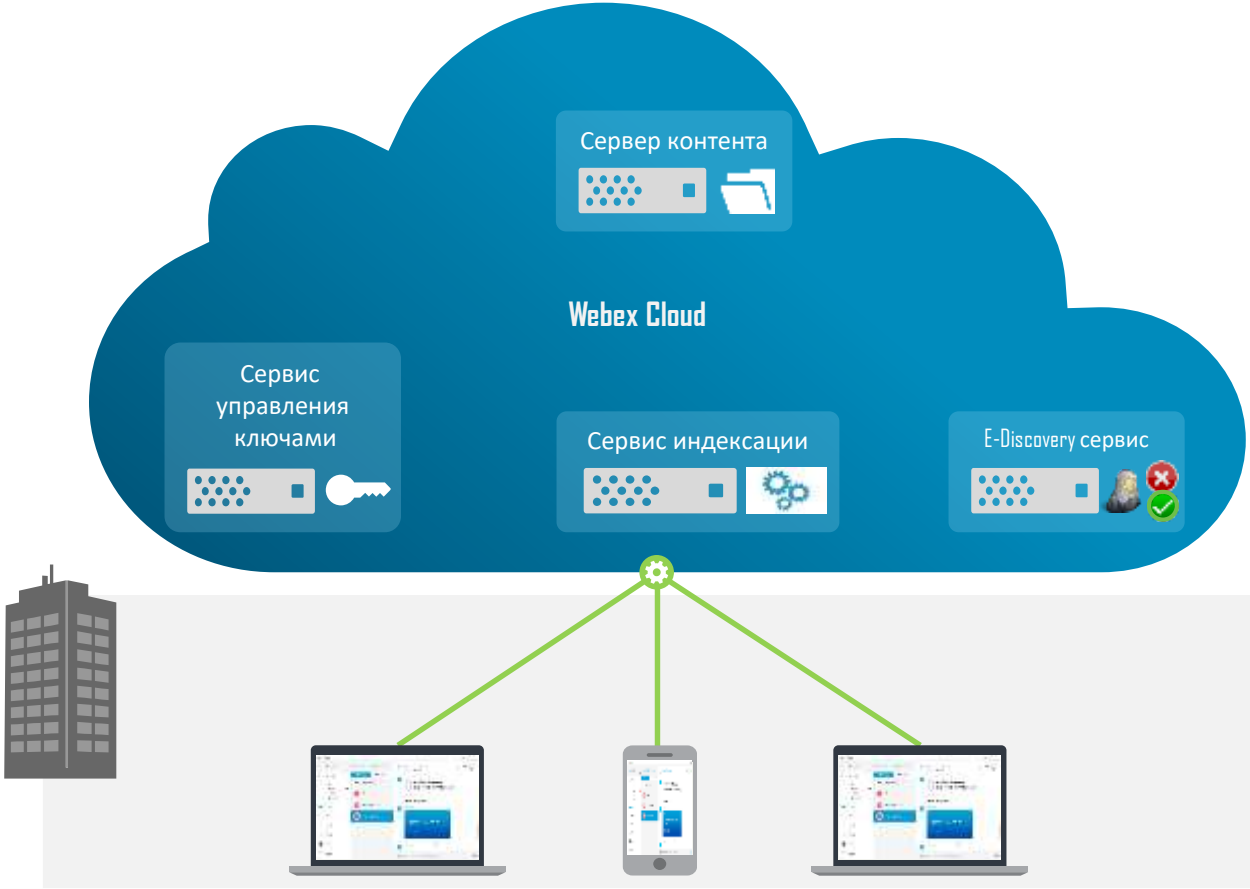
E-Discovery сервис :
Расшифровывает контент, полученный от сервера контента, затем архивирует его и кодирует для пересылки E-Discovery сервису хранения

E-Discovery сервис хранения:
Отправляет сжатый и зашифрованный контент Администратору (или уполномоченному его контролировать).

Управляемая локально безопасность: Гибридные данные

Упрощенная схема архитектуру гибридного сервиса

Гибридная нода безопасности (Hybrid Data Security - HDS)



Гибридные сервисы

=

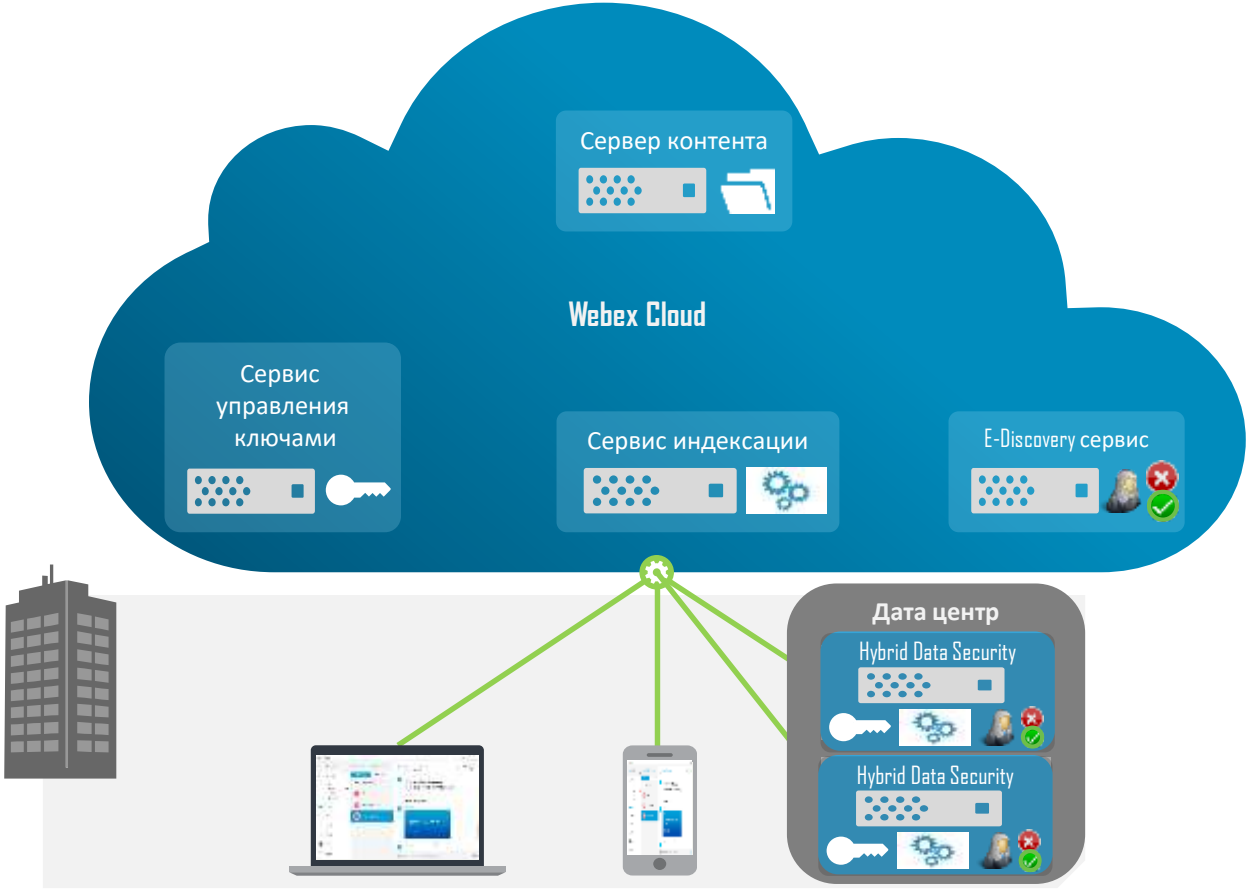
В ЦОД предприятия:

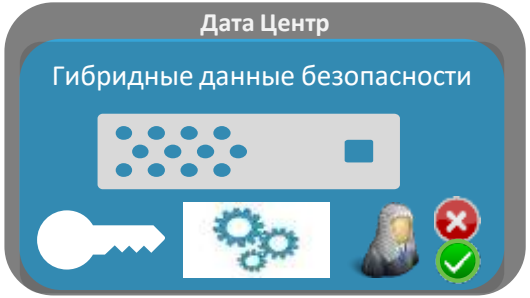
Сервис управления ключами

Сервис индексации

E-Discovery сервис

Безопасность гибридных данных- Масштабируемость



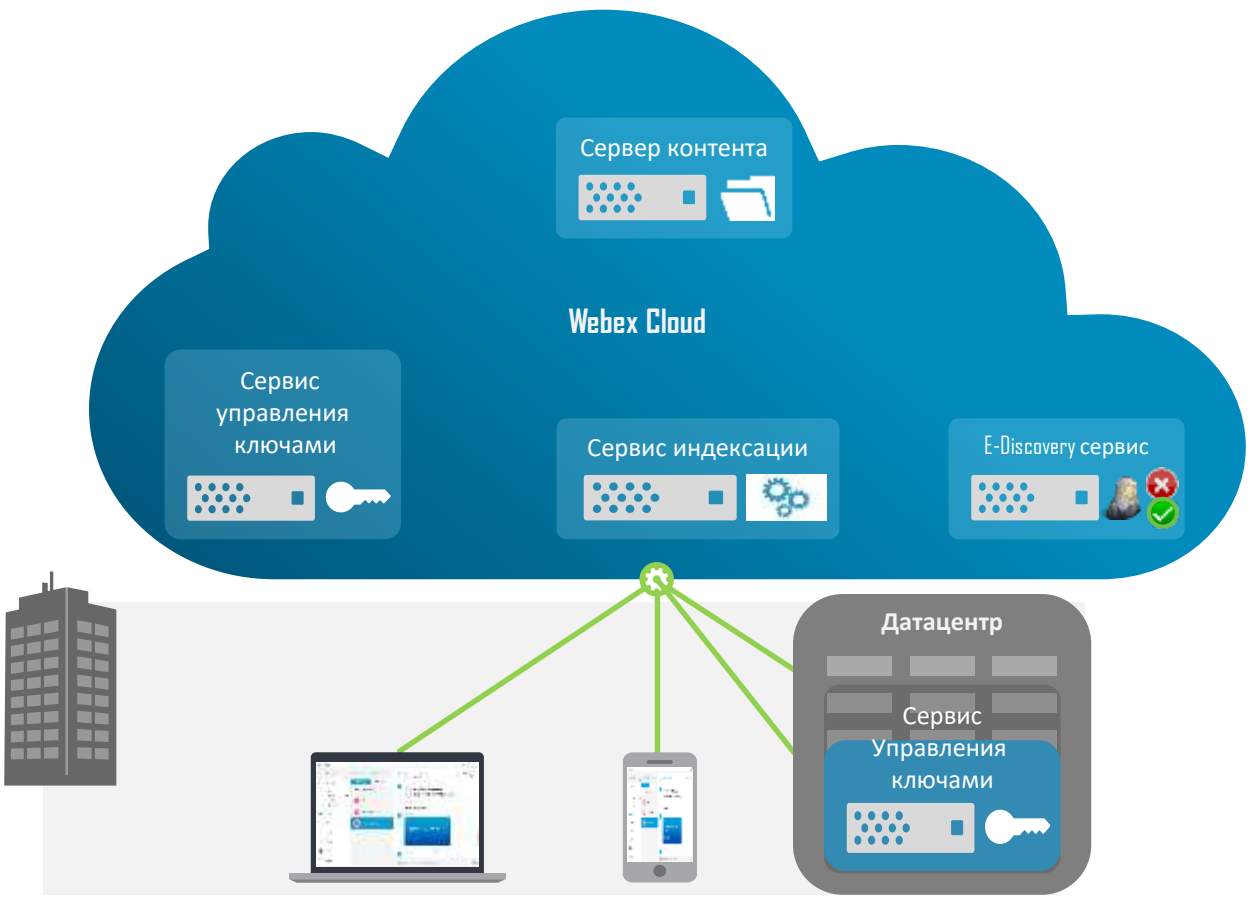


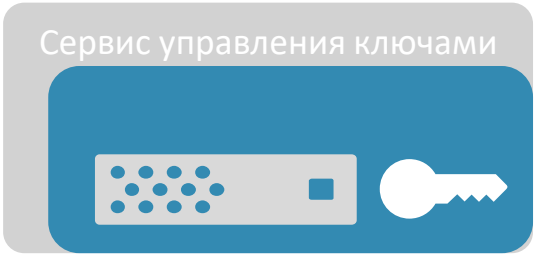
До 5 HDS может быть размещено для распределения нагрузки

Управляются из облака

Локально можно получить данные о загрузки только через syslog

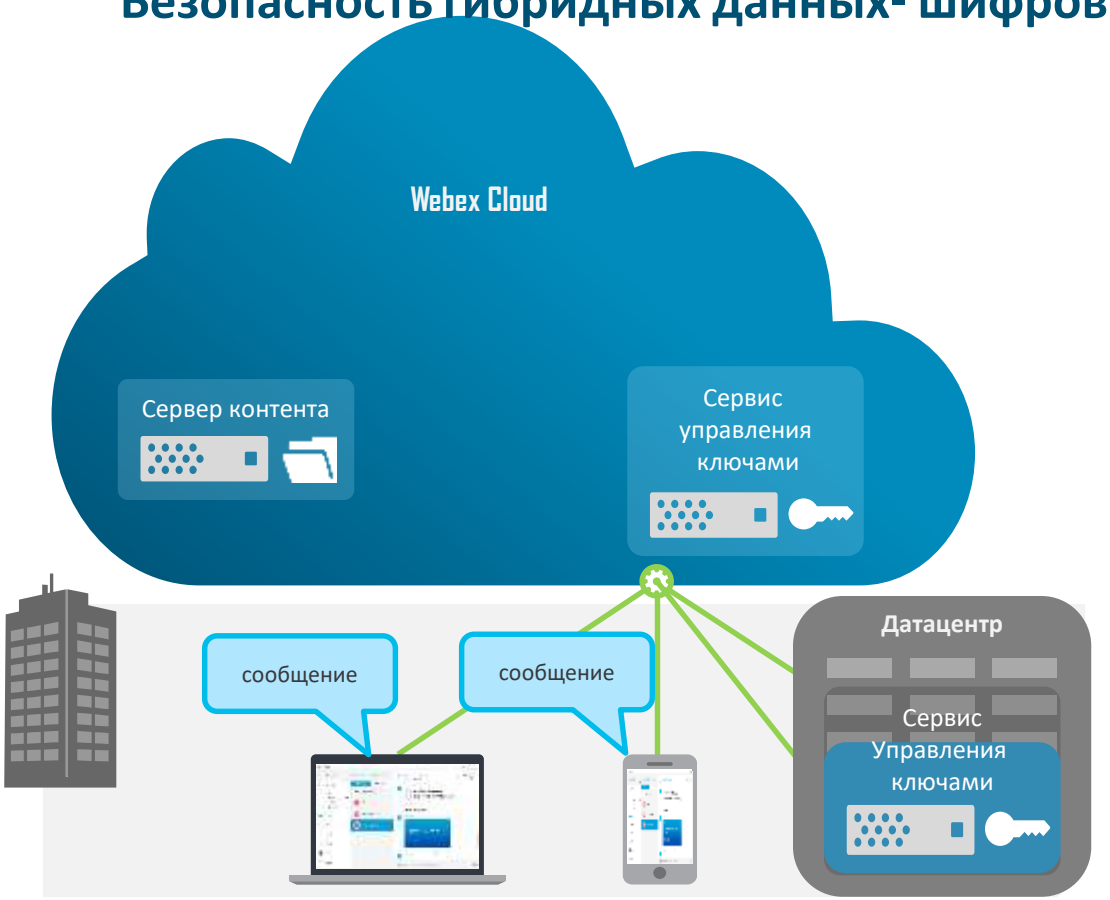
Безопасность гибридных данных- Управление ключами шифрования

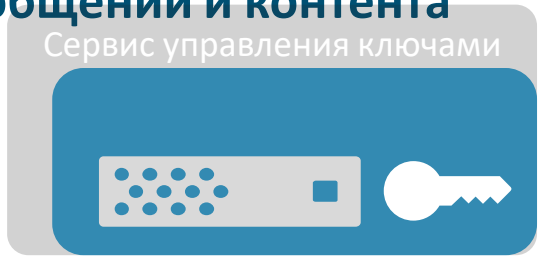




Сервис управления ключами в локальном датацентре выполняет те же функции что и в случае облака,
НО
все ключи, которыми зашифрованы сообщения и контент - хранятся и управляются локально

Безопасность гибридных данных- шифрование сообщений и контента





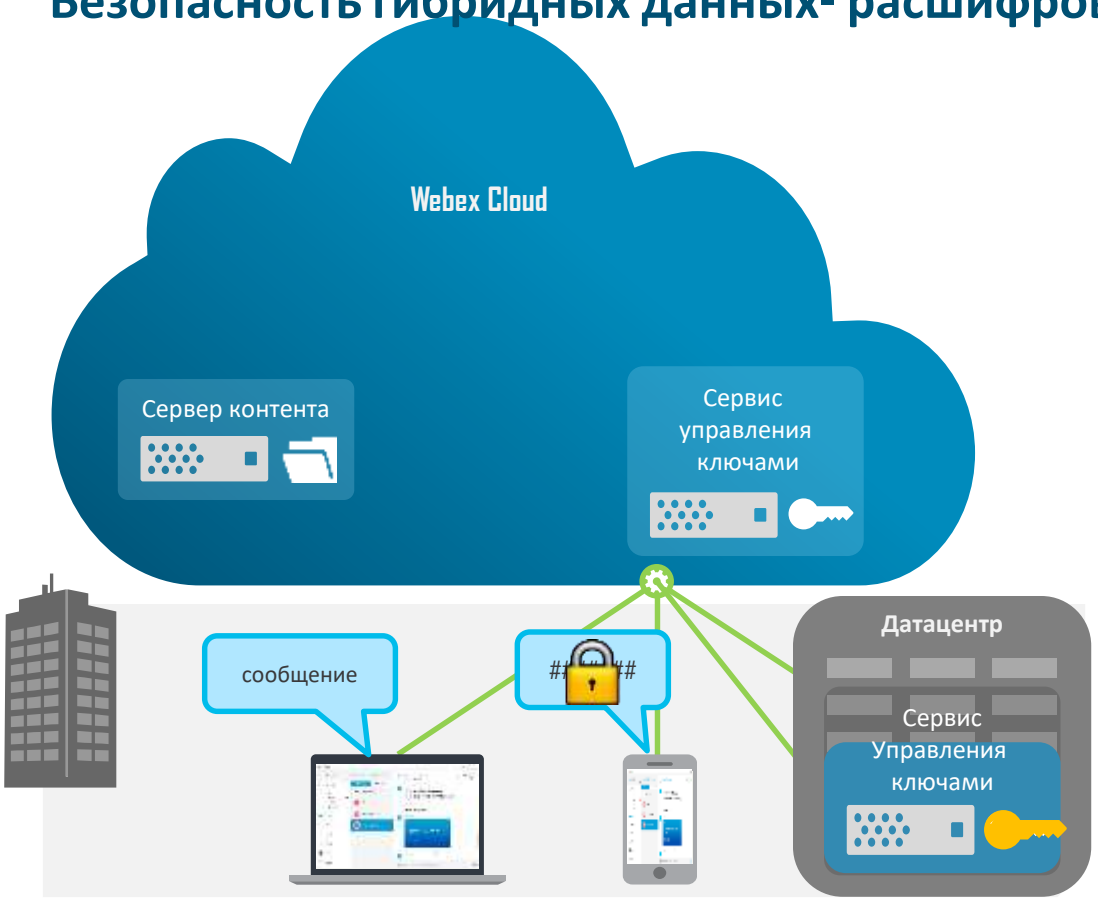
Приложение запрашивает ключ шифрования с HDS сервиса управления ключами

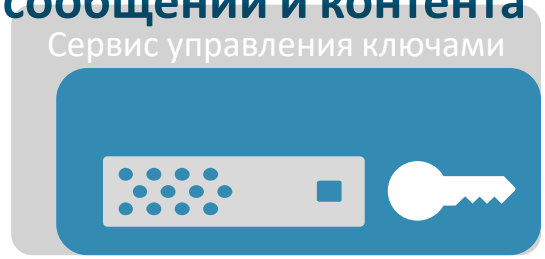
Все сообщения и файлы шифруются до передачи в облако

Зашифрованные сообщения и файлы сохраняются в облаке

Ключи шифрования хранятся локально

Безопасность гибридных данных- расшифровывание сообщений и контента





Шифрованные сообщения сохраняются в облаке

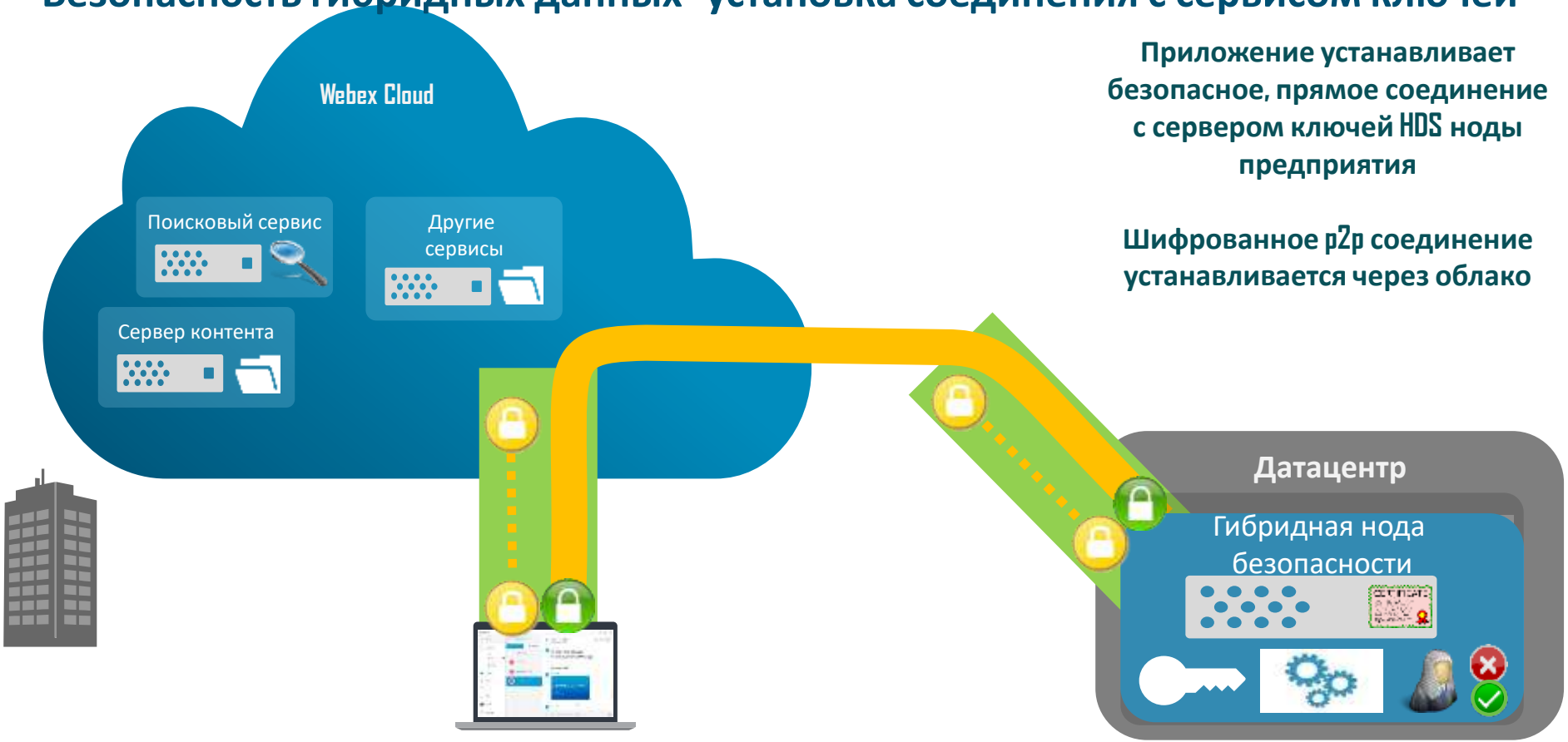
Сообщения рассылаются каждому приложению, которое является участником этого пространства (space) и содержат ссылку на их ключ шифрования на HDS сервере управления ключами

При необходимости приложение может запросить ключ у HDS сервера управления ключами

Безопасность гибридных данных- установка соединения с сервисом ключей

Приложение устанавливает безопасное, прямое соединение с сервером ключей HDS ноды предприятия

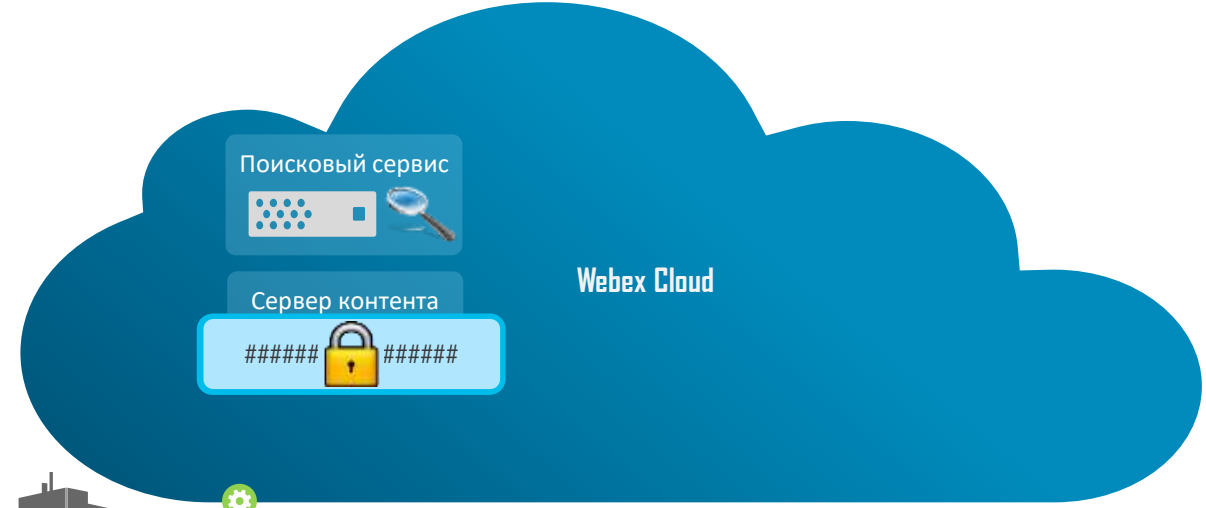
Шифрованное p2p соединение устанавливается через облако

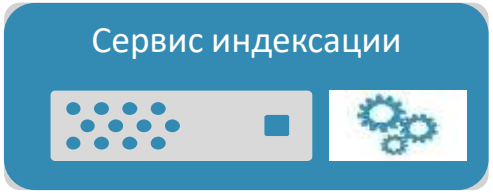


От приложения в облако – TLS

От приложения к HDS (ECDHE- AES-256-GCM)

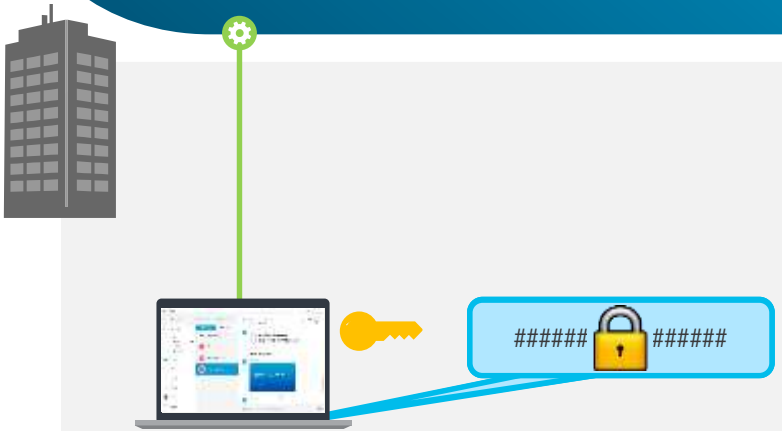
Безопасность гибридных данных- : Поиск и сервис индексации





Сервис индексирования:

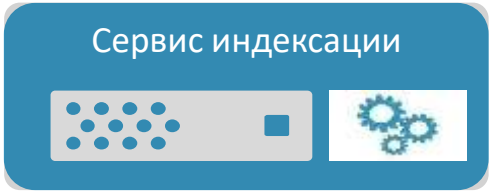
Позволяет пользователи искать с использованием слов и имен, без расшифровки контента, хранящегося на сервере контента

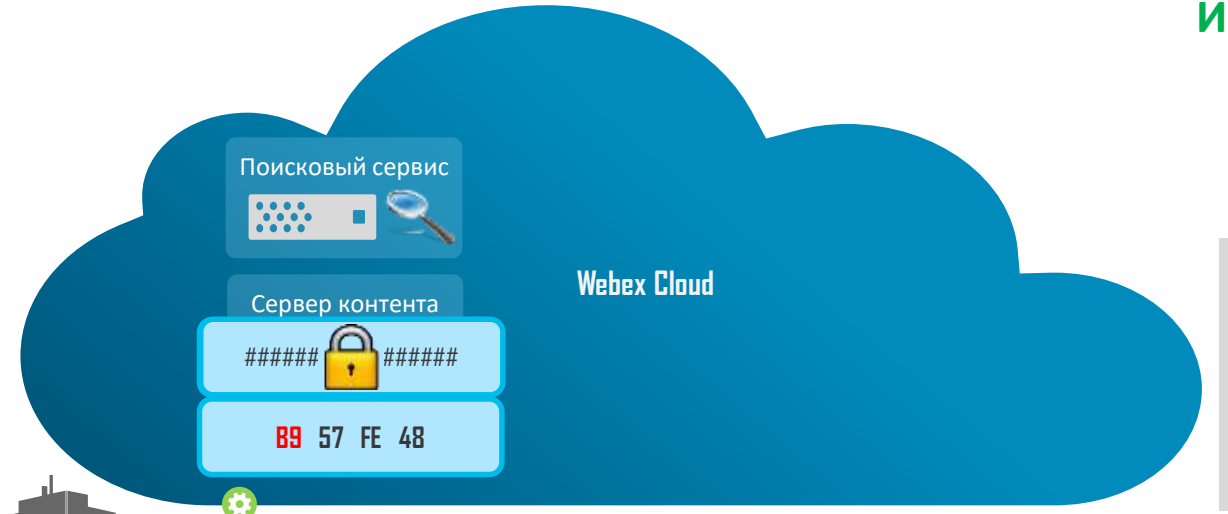


* Новый ключ хеширования (поисковый ключ) используется для каждого пространства

Безопасность гибридных данных : Запрашиваем сервис индексации

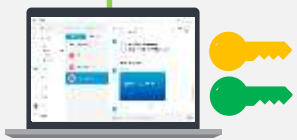
Ищем слово “Webex”





Сервис индексирования посылает хешированный индекс поискового запроса приложения поисковому сервису

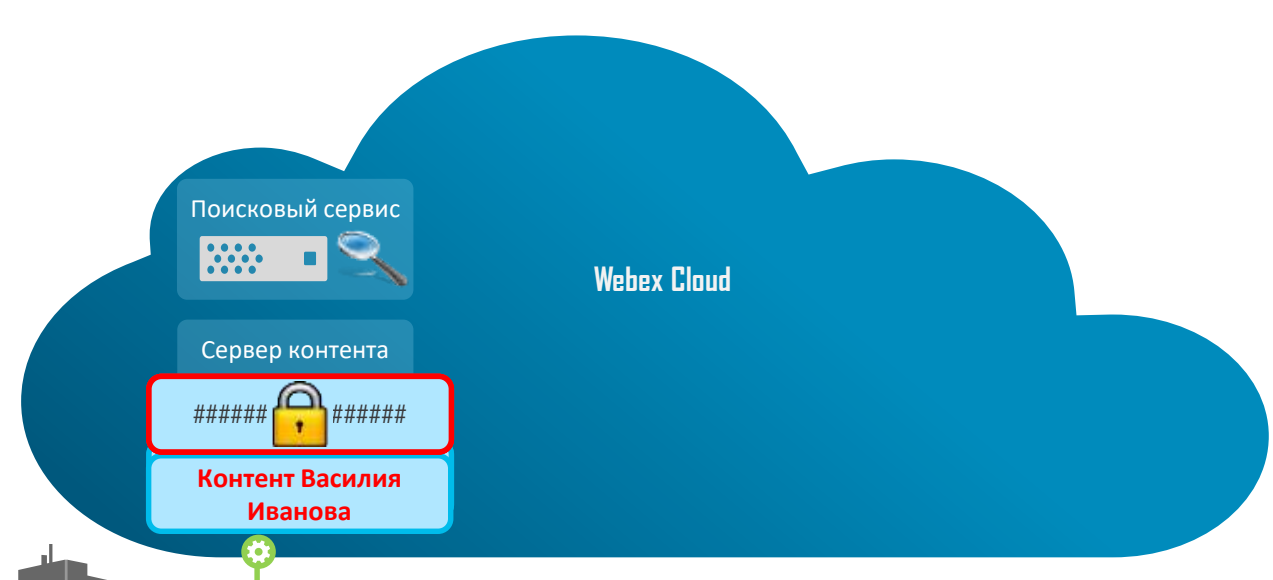
Ищем слово “Webex”

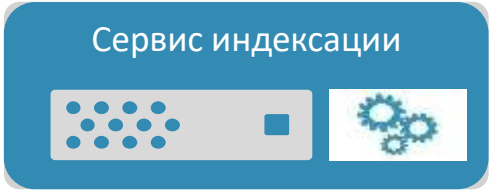


Webex содержится в сообщении

*Ссылка на ключ шифрования сессии включена в сообщение

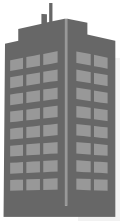
Безопасность гибридных данных : E-Discovery Service : (1)

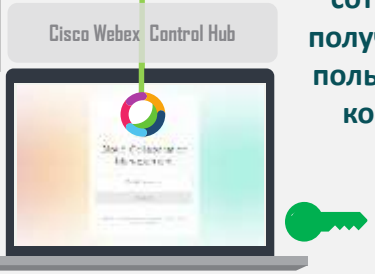




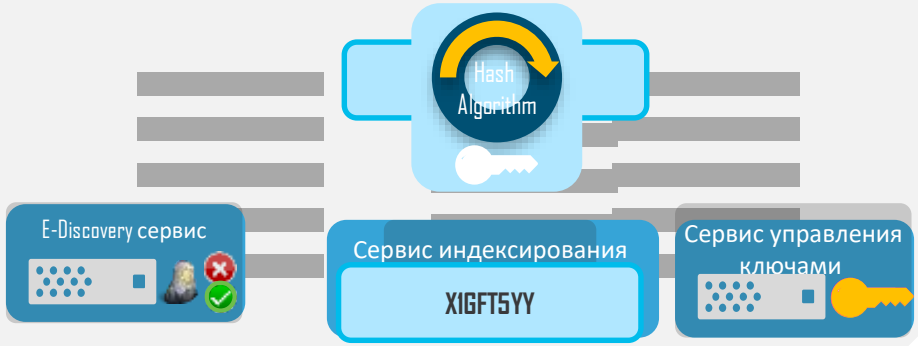
Сервис индексирования посылает хешированные критерии поискового запроса поисковому сервису

Сервер контента возвращает соответствующие им данные E-Discovery сервису

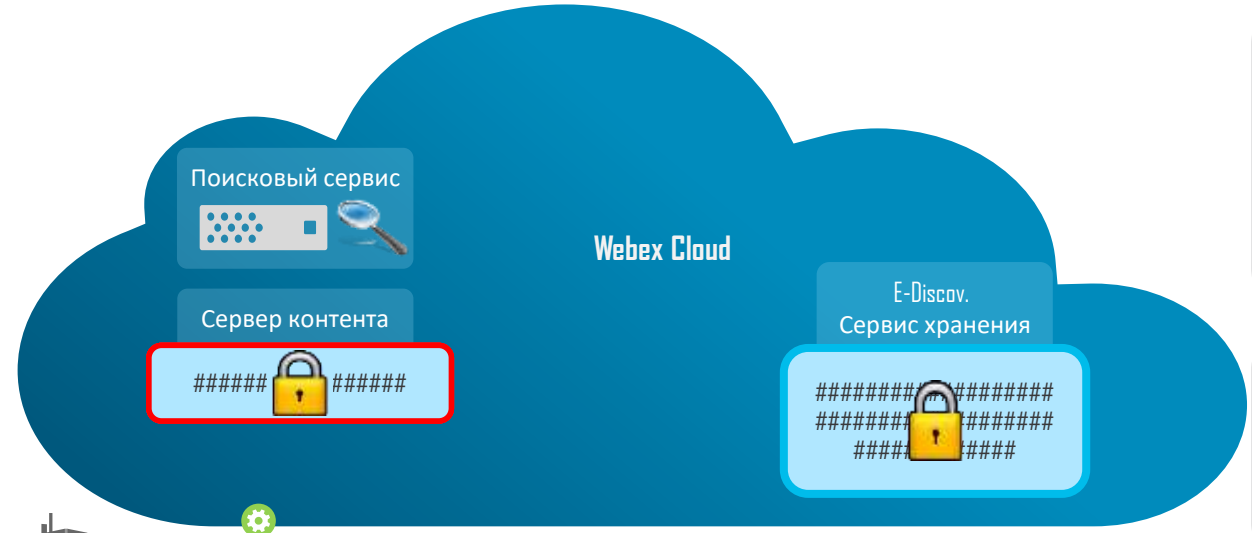




Уполномоченный Компанией сотрудник безопасности хочет получить от E-Discovery сообщения пользователя: диапазон дат/ тип контента/ имя пользователя

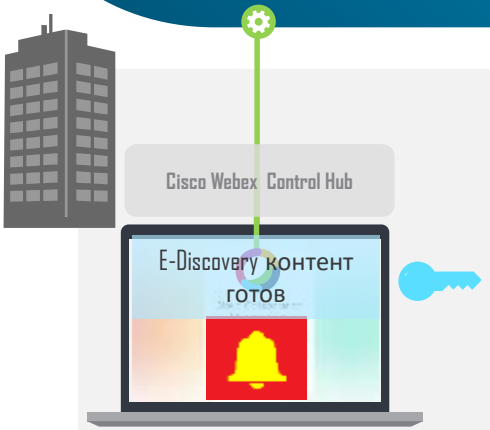


Безопасность гибридных данных : E-Discovery Service : (2)

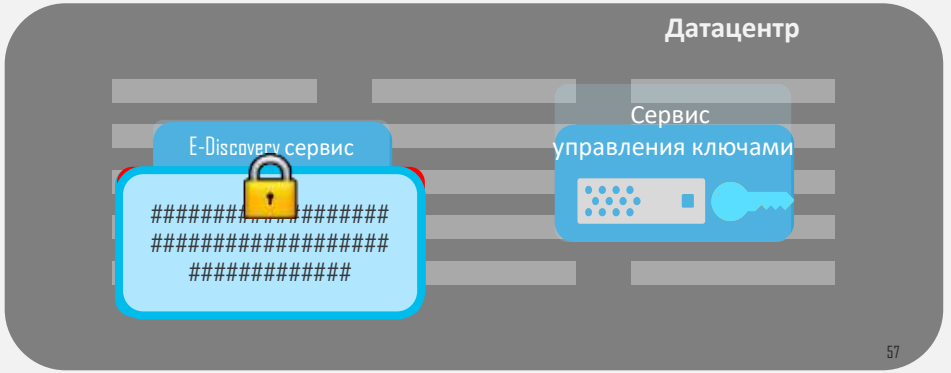


E-Discovery сервис:
Расшифровывает материалы с сервера контента, потом сжимает их и заново шифрует перед отправкой на E-Discovery сервис хранения

E-Discovery сервис хранения:
Отправляет сжатый и зашифрованный контент Администратору



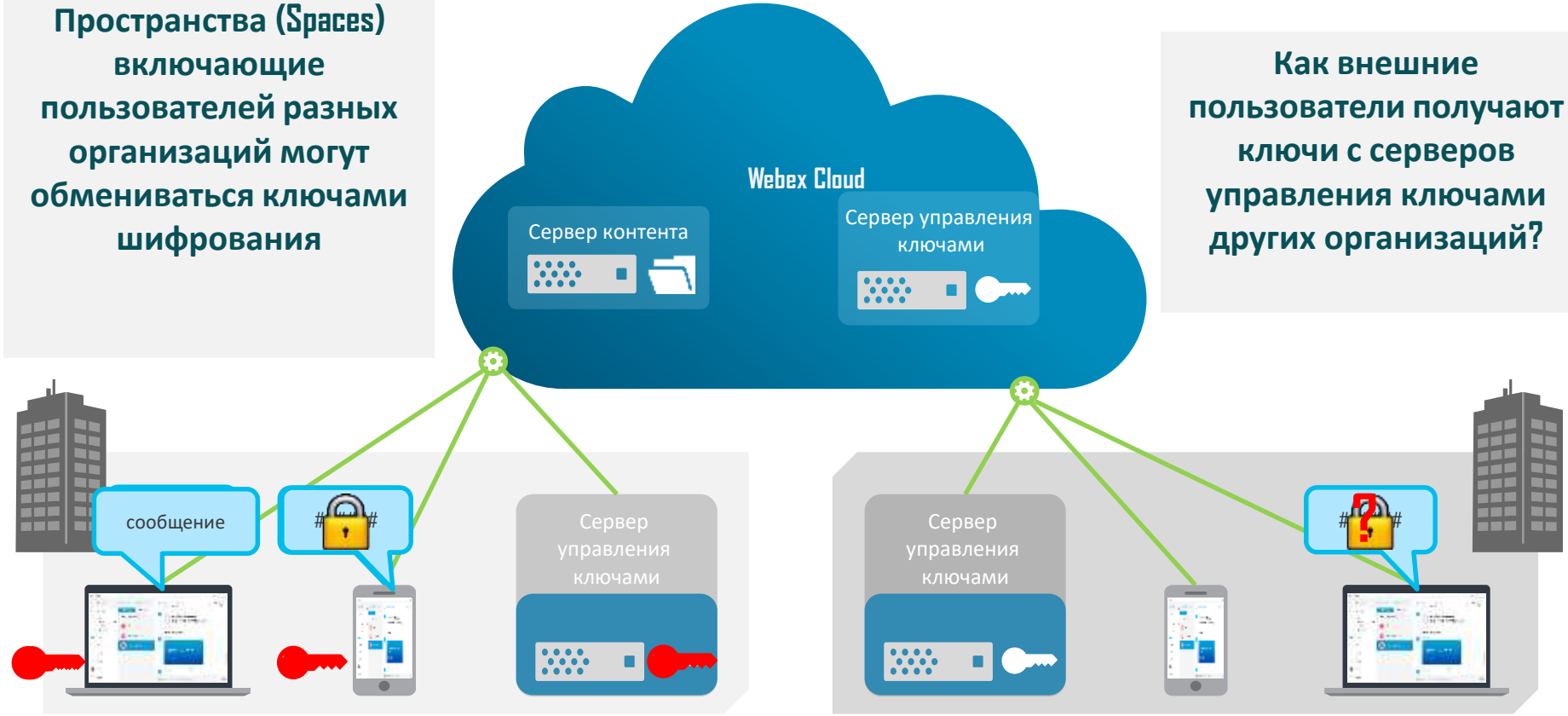
Сообщения и файлы Василия Иванова



Управляемая локально безопасность : Федерация серверов управления ключами

HDS: Ключи шифрования и пользователи из других организаций

Пространства (Spaces) включающие пользователей разных организаций могут обмениваться ключами шифрования

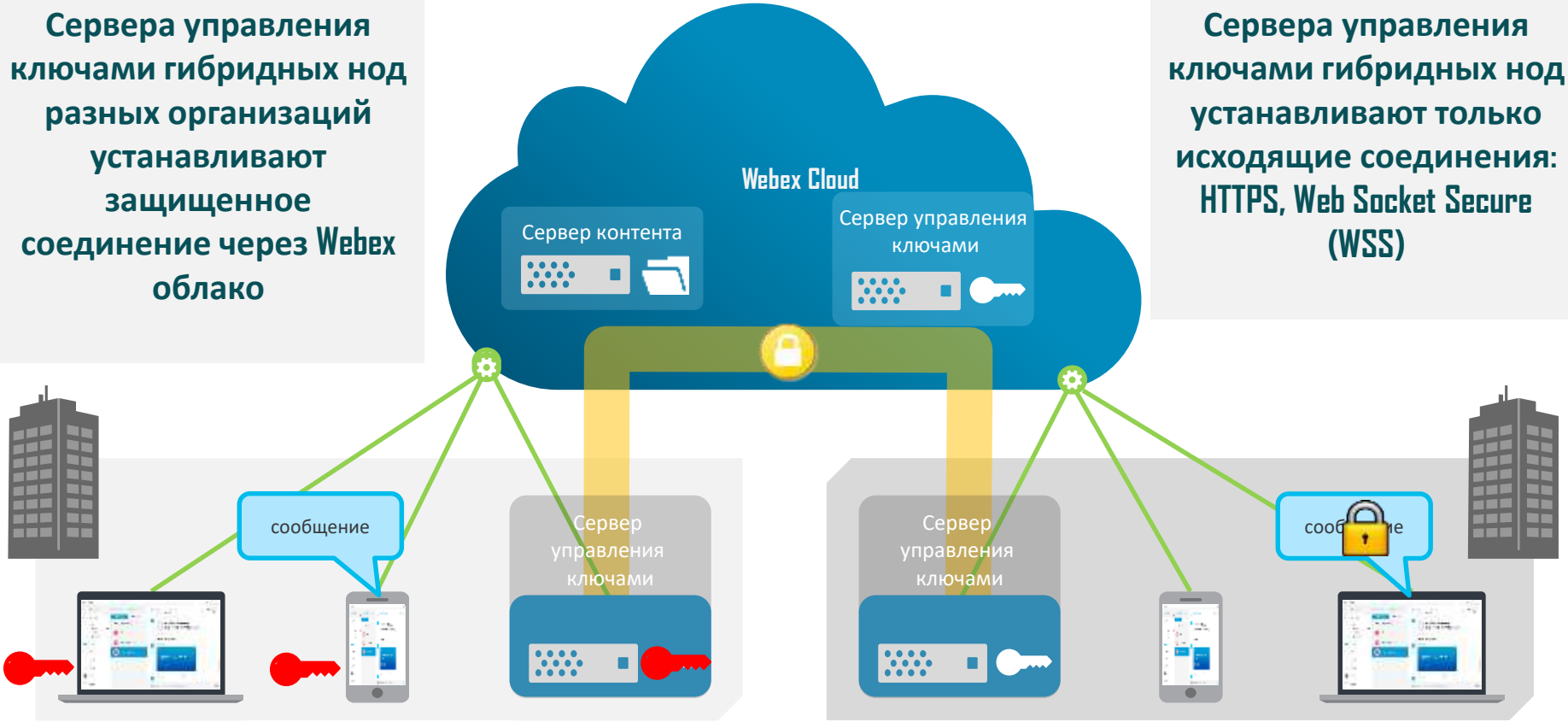


Как внешние пользователи получают ключи с серверов управления ключами других организаций?

HDS: Федерация серверов управления ключами

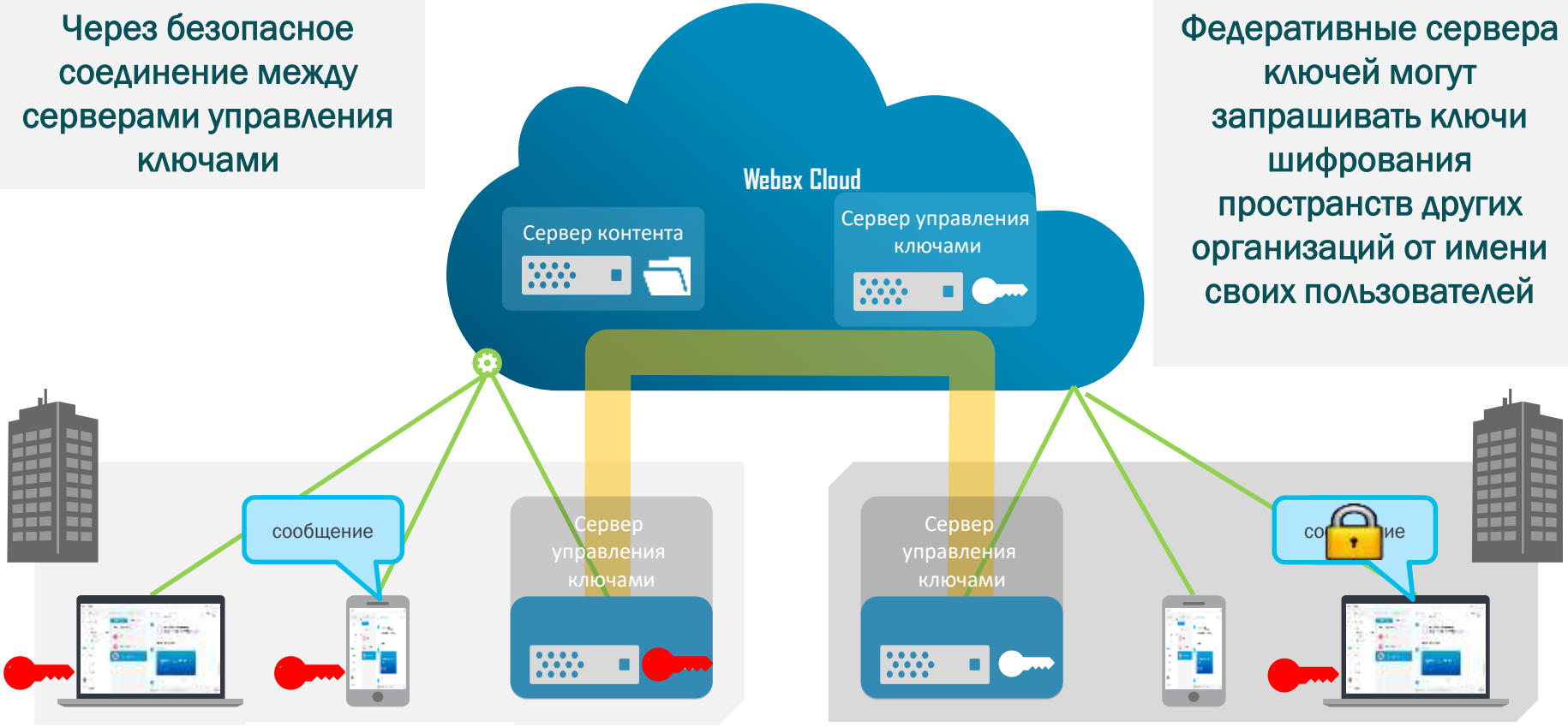
Сервера управления ключами гибридных нод разных организаций устанавливают защищенное соединение через Webex облако

Сервера управления ключами гибридных нод устанавливают только исходящие соединения: HTTPS, Web Socket Secure (WSS)



HDS: Федерация серверов управления ключами

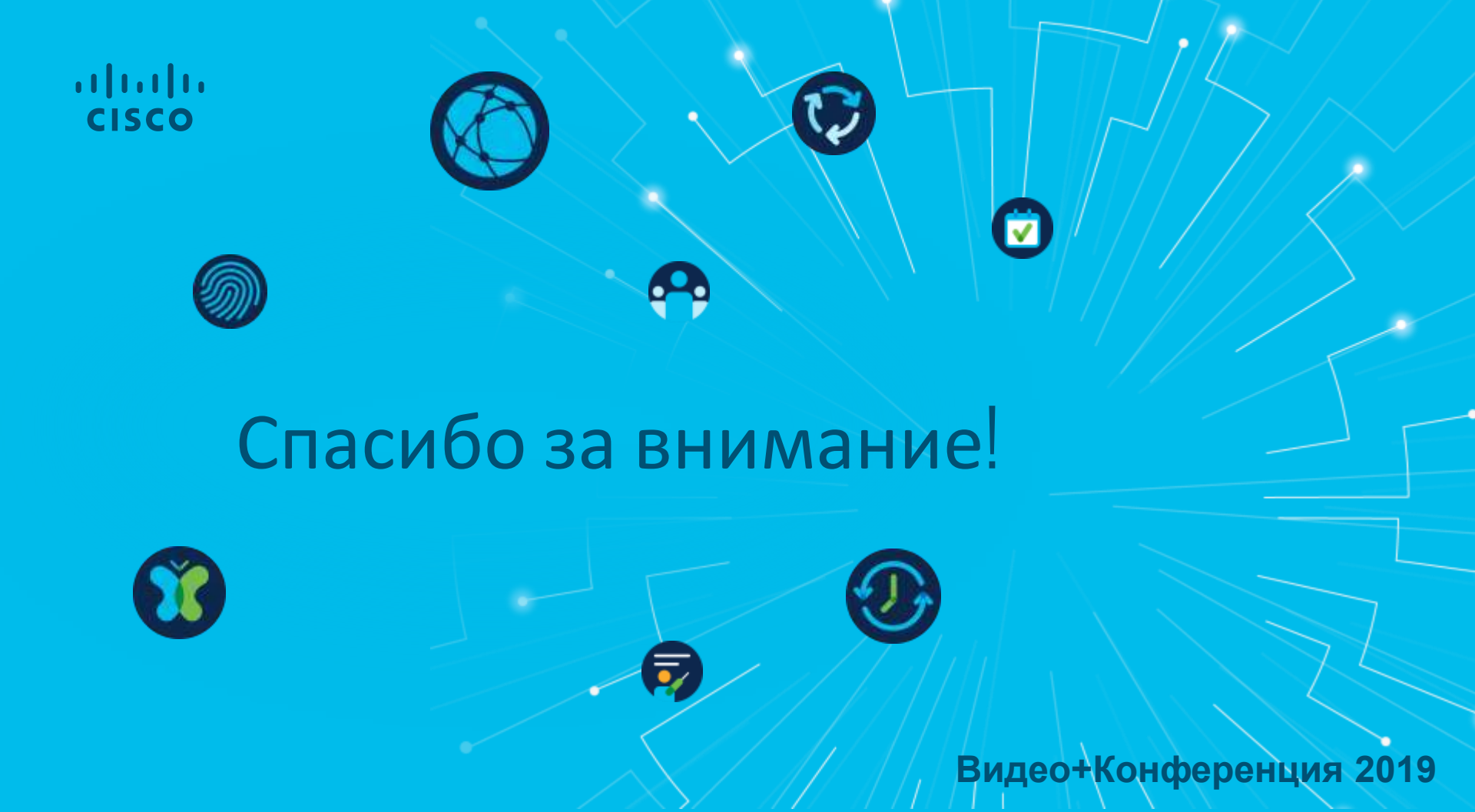
Через безопасное соединение между серверами управления ключами



Федеративные сервера ключей могут запрашивать ключи шифрования пространств других организаций от имени своих пользователей

Подведем итоги:

	Датацентр	Гибрид	Облако
Стоимость			X
Надежность	X	X	X
Безопасность		X	
Функционал		X	X
Возможность интеграции		X	
Скорость внедрения / масштабируемость			X
Управляемость и поддержка			X


cisco
Спасибо за внимание!
Видео+Конференция 2019