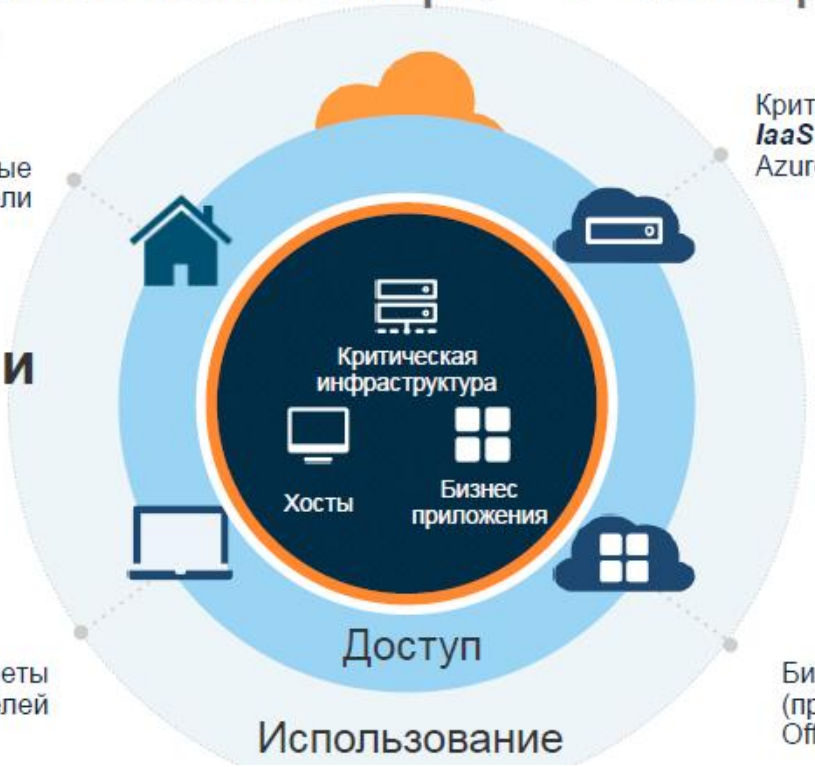
БЕЗОПАСНОСТЬ ИЗ ОБЛАКА ИЛИ ЗАЩИТА ОБЛАЧНЫХ ПРИЛОЖЕНИЙ. ДВЕ СОСТАВЛЯЮЩИЕ КОМПЛЕКСНОЙ ЗАЩИТЫ В ЭРУ ОБЛАЧНЫХ РЕШЕНИЙ

Communications
Technology
Innovations

Облачные приложения наступают

Communications Technology Innovations

Как мы работаем теперь – Расширенный периметр



Пользователи

Удаленные пользователи

Ноутбуки / Планшеты пользователей

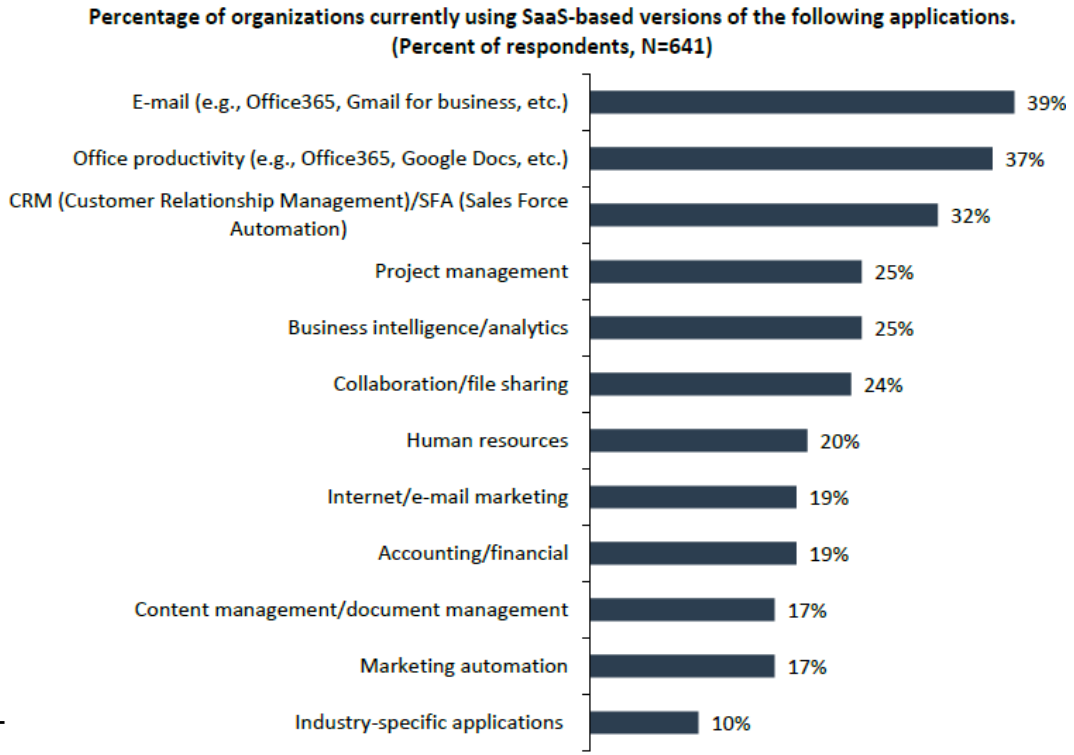
Приложения и данные

Критическая инфраструктура – ***IaaS & PaaS*** (прим:, Amazon, Azure, и др.)

Бизнес приложения - ***SaaS*** (прим:., Salesforce, Marketo, Office365, Google)

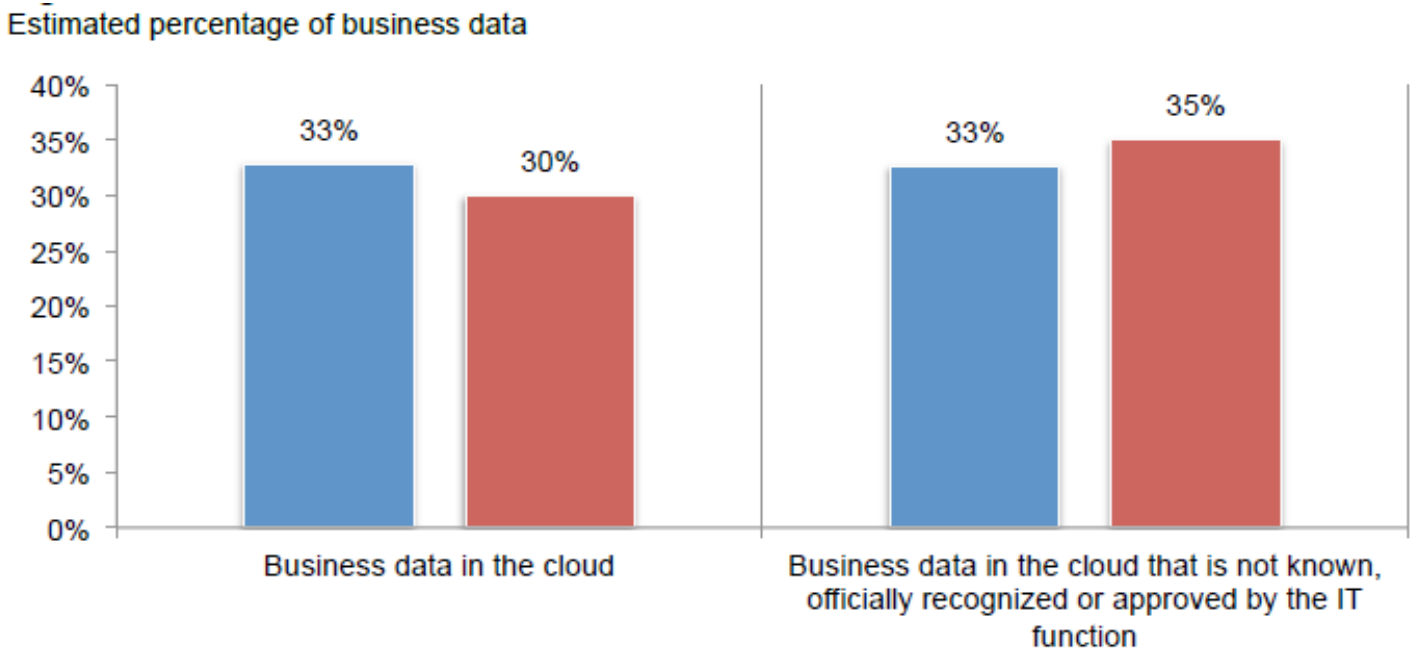
Что говорят аналитики в мире

- К 2018 году 25% корпоративного трафика будет обходить периметровые средства защиты
- К 2018 году по оценке Gartner 60% компаний, которые внедрят средства контроля и защиты облачных данных будут иметь на треть меньше инцидентов безопасности
- К 2018 году 40% внедрений Office365 будут использоваться сторонние дополнительные средства безопасности для решения задач соответствия требованиям безопасности
- К 2020 году 92 процента глобального трафика центров обработки данных будет приходиться на облачные сервисы



Проблемы теневого использования IT-сервисов

1. Пользователи используют облачные сервисы без ведома IT – ShadowIT
2. Данные бесконтрольно хранятся в облаках



Что могут дать облака с точки зрения корпоративной безопасности

CTI Communications Technology Innovations

Безопасность для облака

- Защита облачных сервисов, которые используются ИТ-службами или сотрудниками компании

Безопасность из облака

- Использование облачных средств и аналитики из облака для защиты корпоративных ресурсов (включая традиционный периметр)

Безопасность для облака - что нужно защищать?

Communications Technology Innovations

Пользователей/ Аккаунты

Кто и что делает в облачных приложениях

Скомпрометированы ли аккаунты или нет

Есть ли внутренние злоумышленники, выводящие информацию

Данные

Хранят ли пользователи запрещенную информацию в облаке

Как обнаружить нарушение политики

Как отследить утечки данных

Приложения

Как понять какие приложения используются и их риски

Есть ли сторонние приложения, которые не должны использоваться

Как отключить доступ к рискованным приложениям

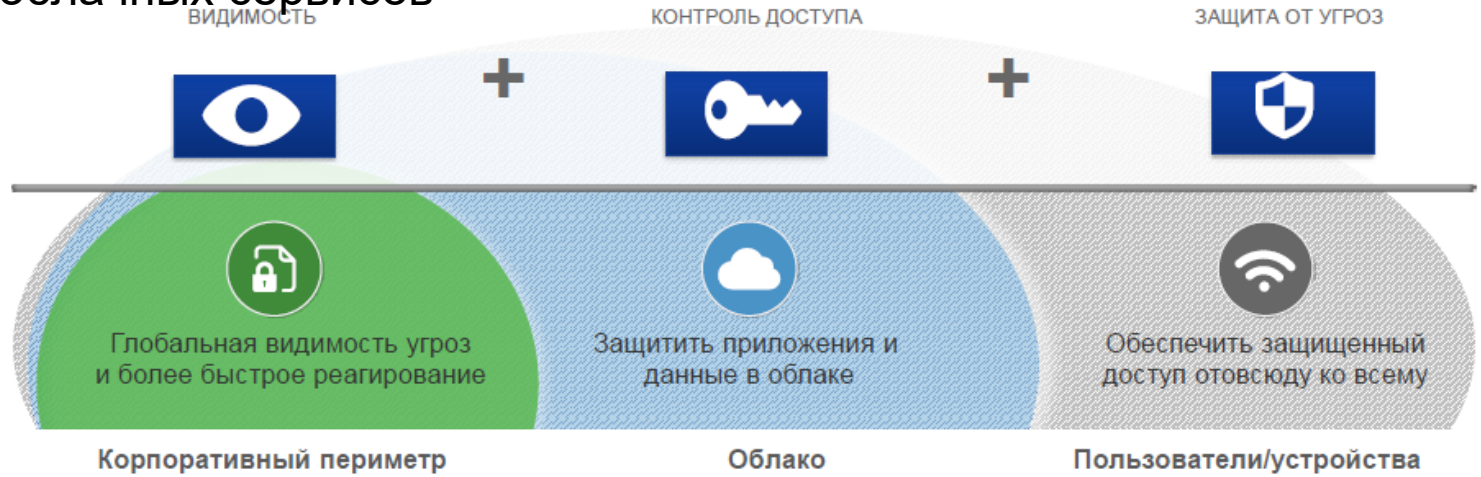
Решение CASB – защита для облачных приложений

Ключевые возможности которые предоставляют решения CASB

1. Visibility – повышение видимости и прозрачности использования облачных сервисов

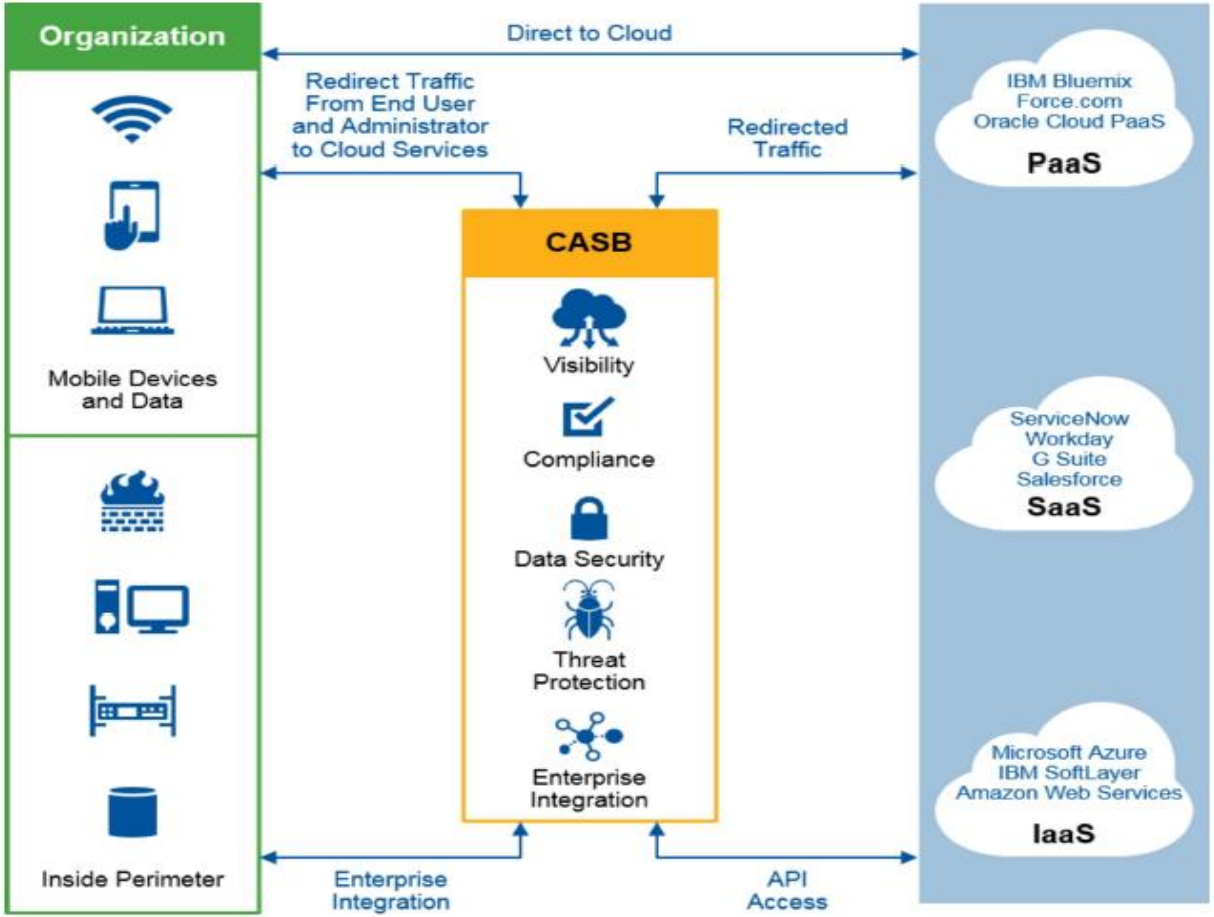
2. Защита данных в облаке при доступе к ним

3. Защита от угроз – выявление аномального поведения и идентификация ВПО посредством аналитики



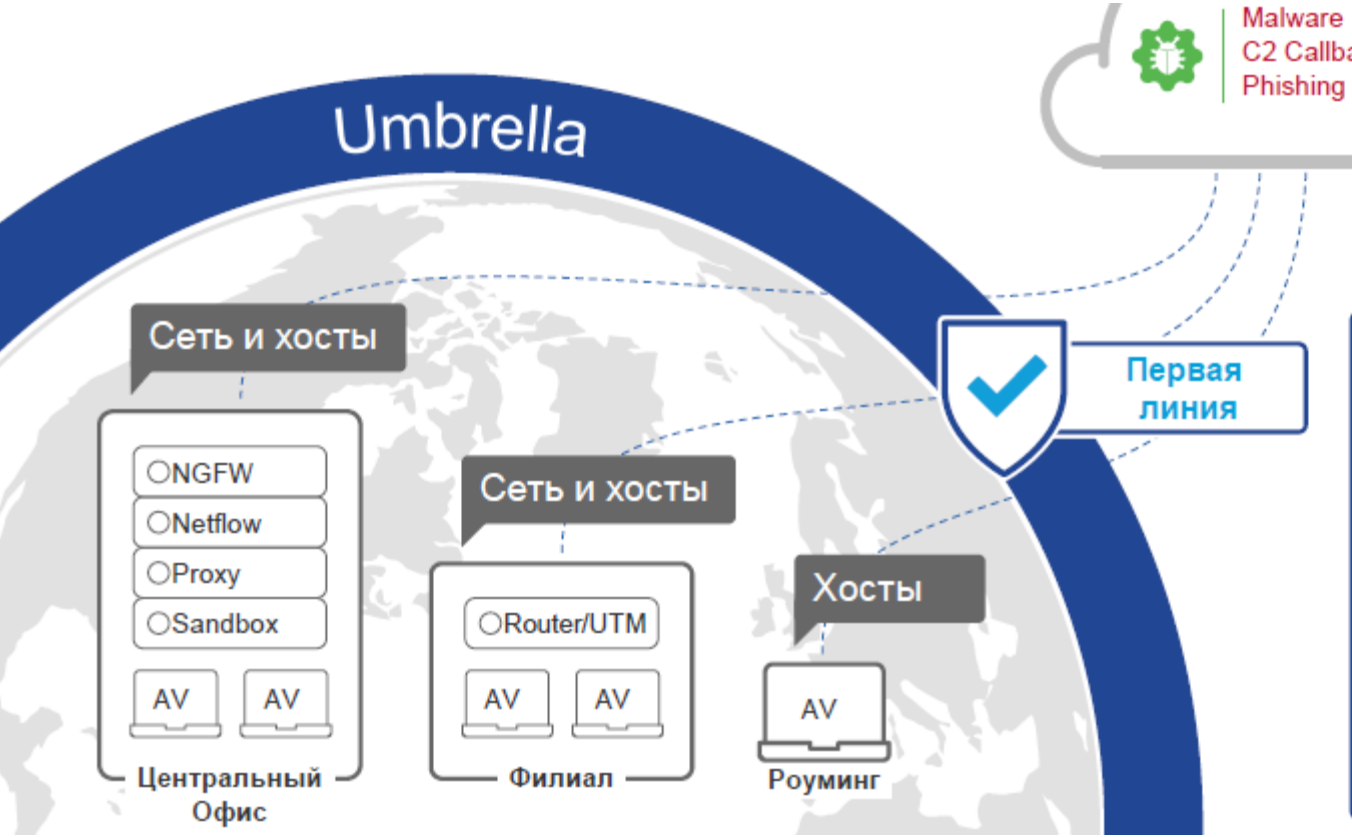
4. Аудит по доступу к облачным данным и сервисам (кто, когда, с какой целью, к каким данным, откуда имел доступ)

Архитектура развертывания CASB



Gartner Magic Quadrant for Cloud Access Security Brokers

Безопасность из облака – обеспечение защиты в любой точке



Всё начинается с DNS

Предшествует открытию файлов и установлению IP соединения

Используется всеми устройствами

Независимо от порта

Преимущества безопасности из облака

Предотвращение заражения malware
Не только обнаружение угроз

Предотвращение подключения malware к C&C
Предотвращение распространения

Защита внутри и снаружи сети
Не ограничивается устройствами отсылающими трафик на устройства защиты внутри сети

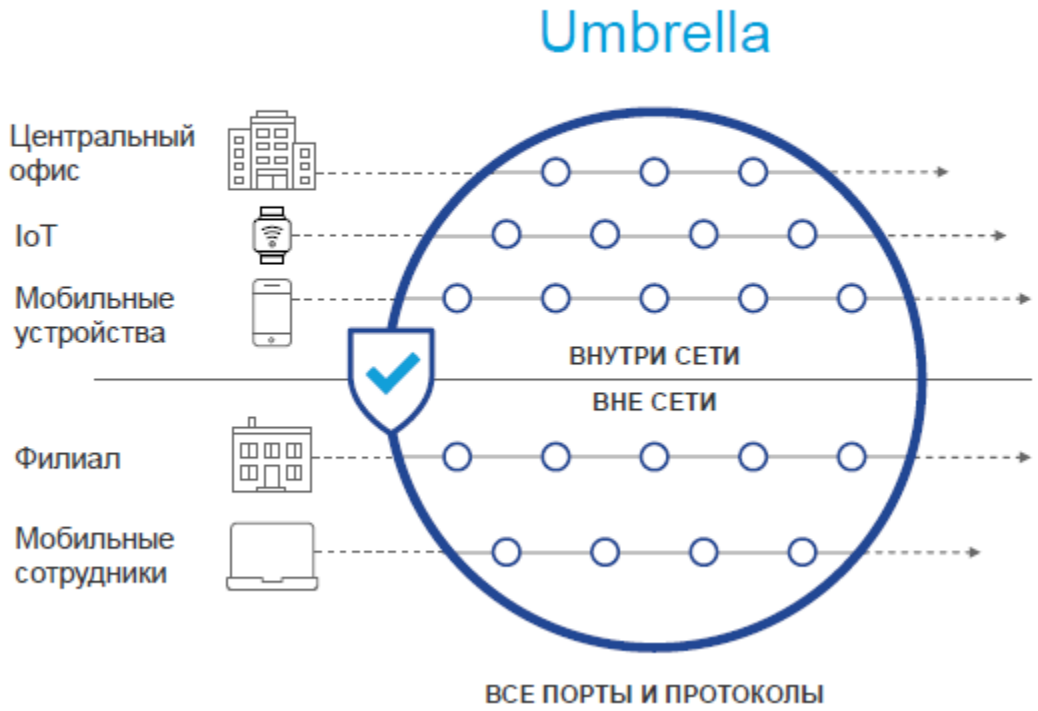
Детальный мониторинг Интернет-доступа
Для сотрудников, гостей и мобильных устройств

Встроенные и настраиваемые API интеграции
Не требует профессионального сервиса для настройки

Простота развертывания для корпоративных устройств

Communications Technology Innovations

Доступен со всех платформ и устройств



Все офисные локации

Любое устройство в сети

Мобильные хосты

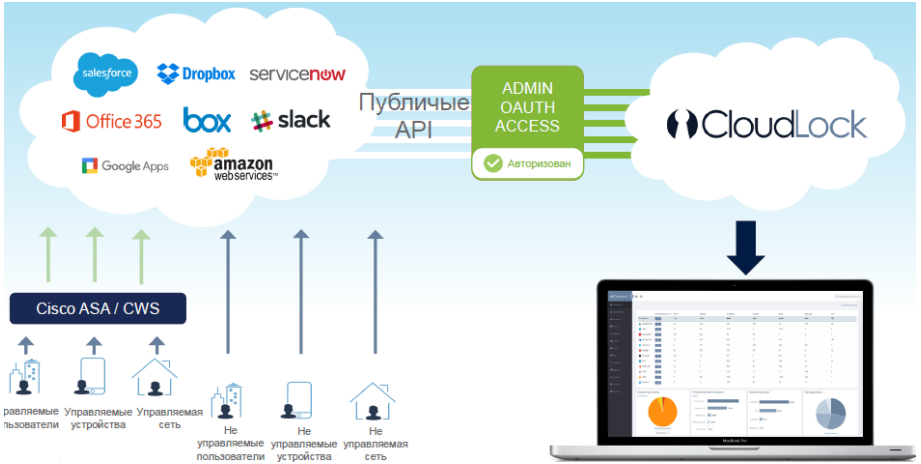
Каждый порт и протокол

Решения уже работают у наших заказчиков

- Решения CASB и облачной защиты **можно протестировать бесплатно**

- Решения **развернуты и поддерживаются в облаке Cisco Umbrella – CTI Cloud**

- Бесплатная оценка безопасности использования облачных технологий в вашей организации и оценка рисков использования облачных приложений **CTI Security Cloud Assessment**



СПАСИБО!

Communications
Technology
Innovations