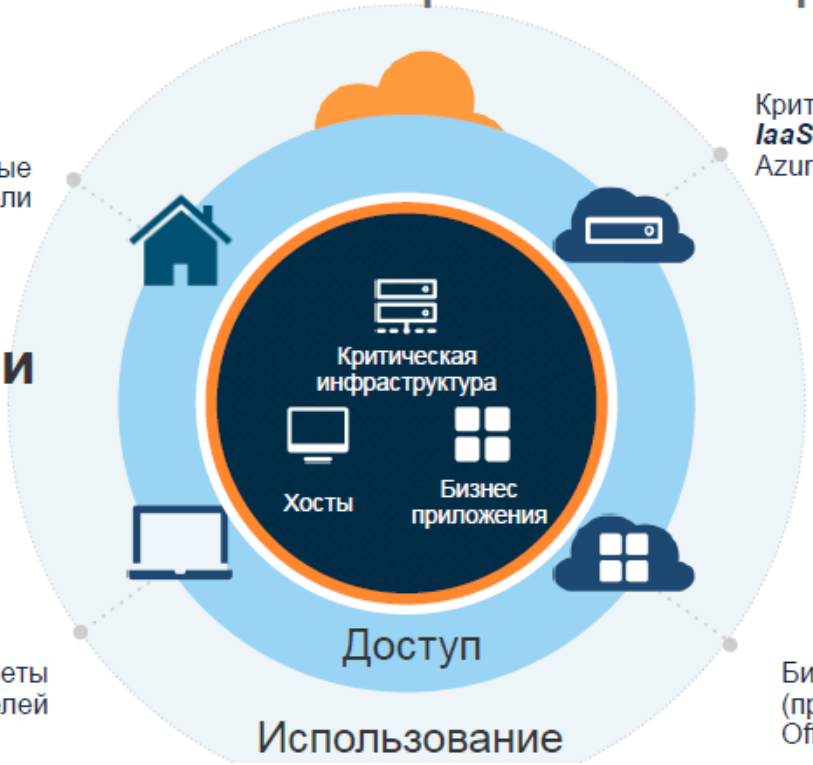
РЕШЕНИЯ ДЛЯ БЕЗОПАСНОСТИ ДАННЫХ И ЗАЩИТЫ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

Communications
Technology
Innovations

Облачные приложения наступают

Communications Technology Innovations

Как мы работаем теперь – Расширенный периметр



Пользователи

Удаленные пользователи

Ноутбуки / Планшеты пользователей

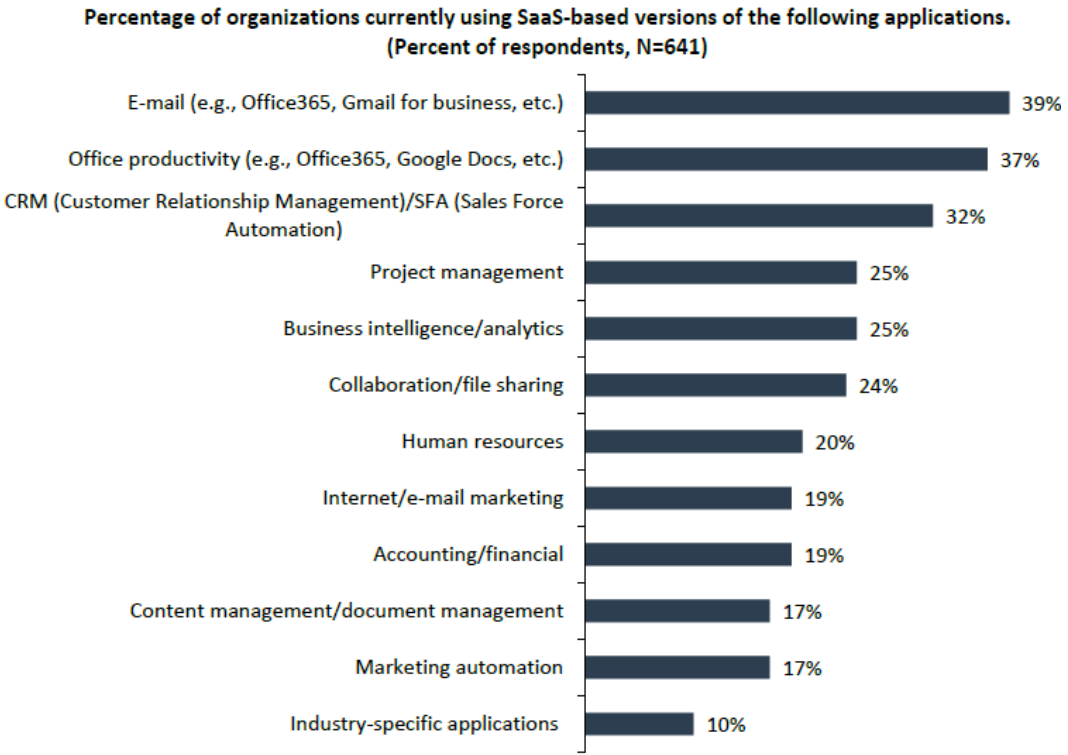
Приложения и данные

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

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

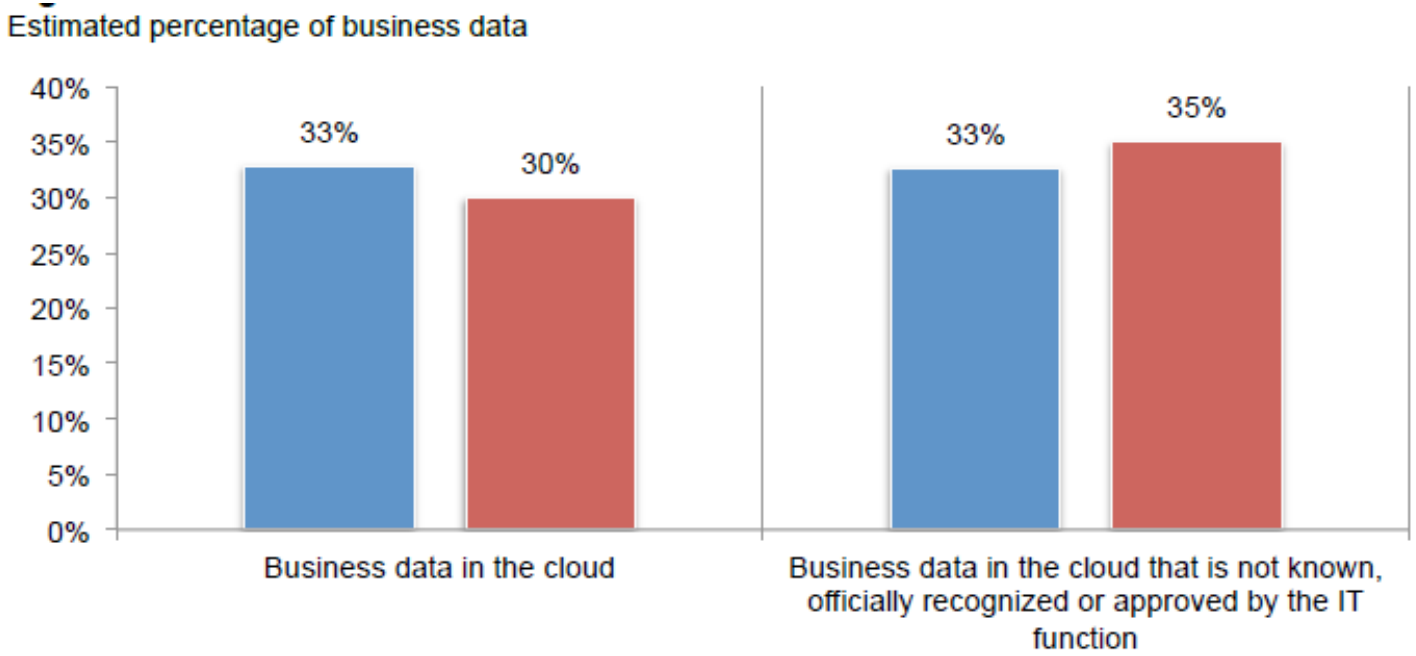
Что говорят аналитики в мире

- 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 нужно защищать в облаке?

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

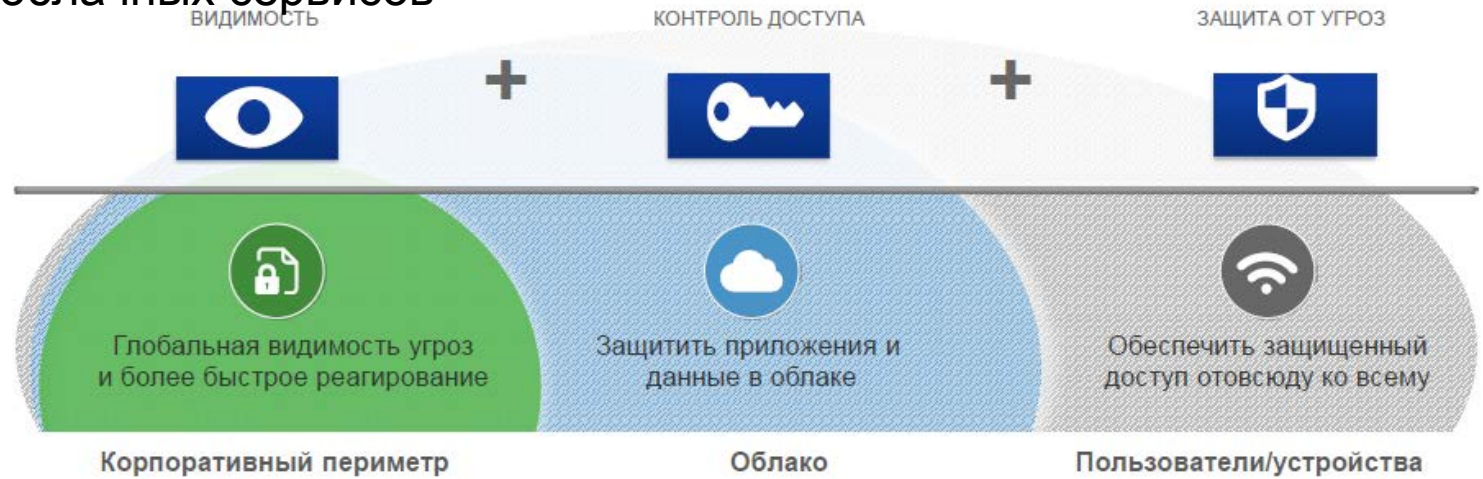
Cloud Access Security Broker - CASB

Ключевые возможности которые предоставляют решения CASB

1. Visibility – повышение видимости и прозрачности использования облачных сервисов

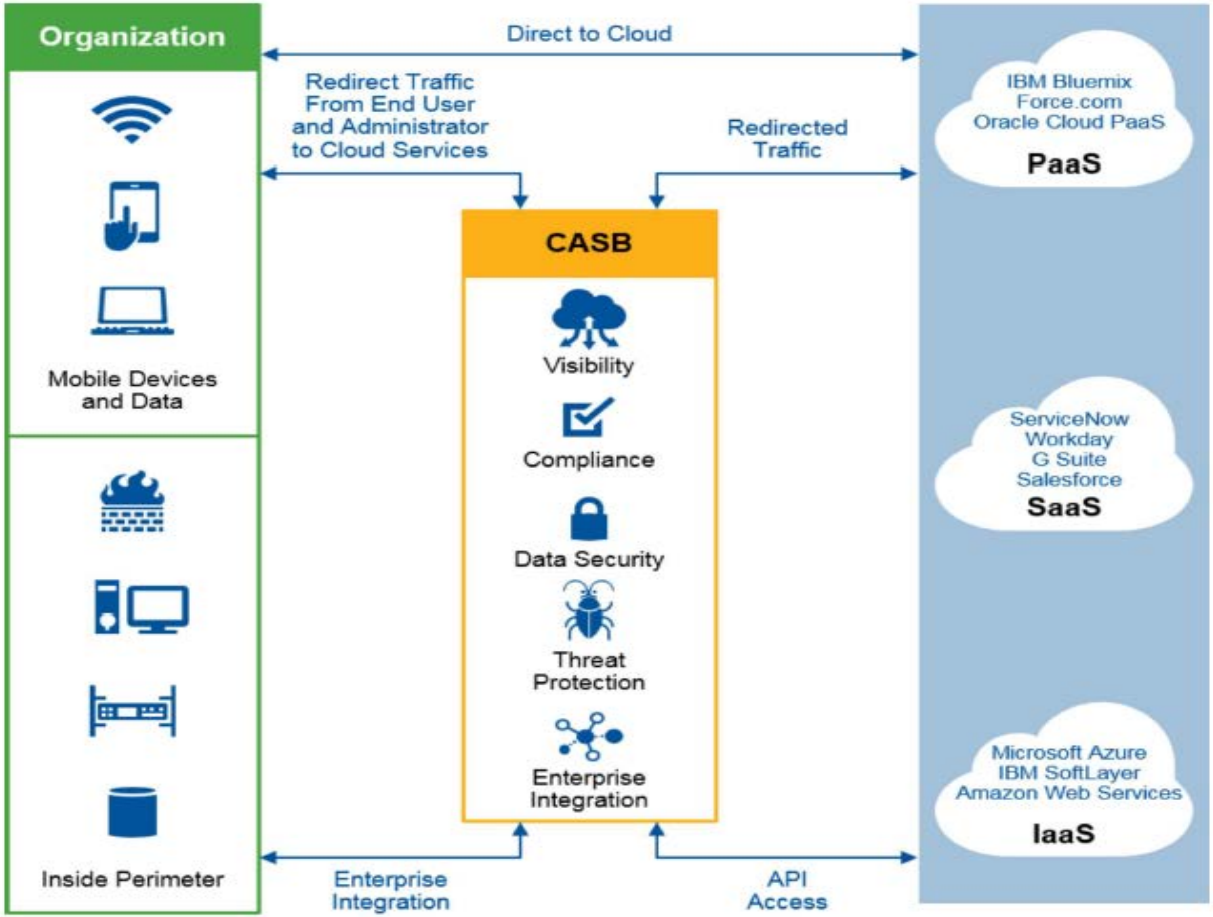
2. Защита данных в облаке при доступе к ним

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



Модели внедрения решений CASB

Communications Technology Innovations

	API	Forward Proxy	Reverse Proxy
Users			
Employees	●	●	●
Third parties (customers, partners)	●		●
Network types			
On network	●	●	●
Off network	●	●	●
Application experiences			
Web application	●	●	●
Native application	●	●	
Device types			
Managed	●	●	●
Unmanaged	●		●

Основные поставщики решений CASB

Gartner Magic Quadrant for Cloud Access Security Brokers

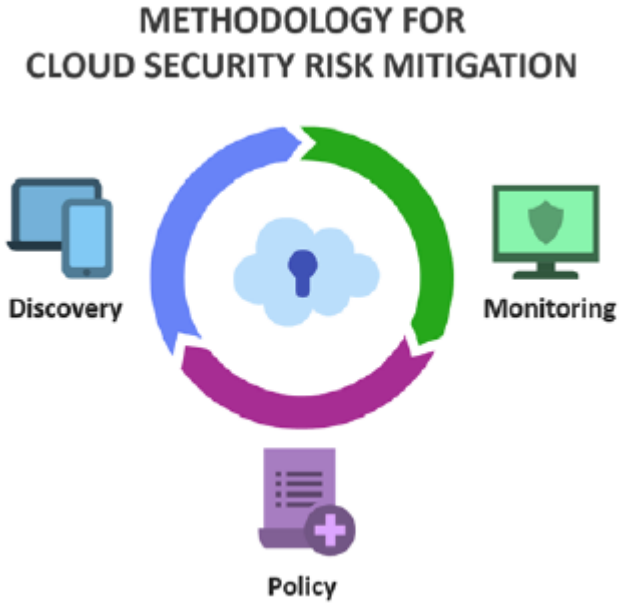
Ноябрь, 2017

Шаги оценки применимости CASB

1. Оценить предоставляет ли текущий провайдер облачных услуг соответствующие и достаточные механизмы контроля доступа и защиты приложений в облаке (могут быть достаточны для ограниченного набора облачных приложений)

2. Провести аудит текущих (Shadow IT) и планируемых к использованию облачных сервисов и требования безопасности к их использованию

3. Проработать сценарии применения и использования для конкретных облачных сервисов и приложений и определить способ реализации и интеграции технического решения CASB

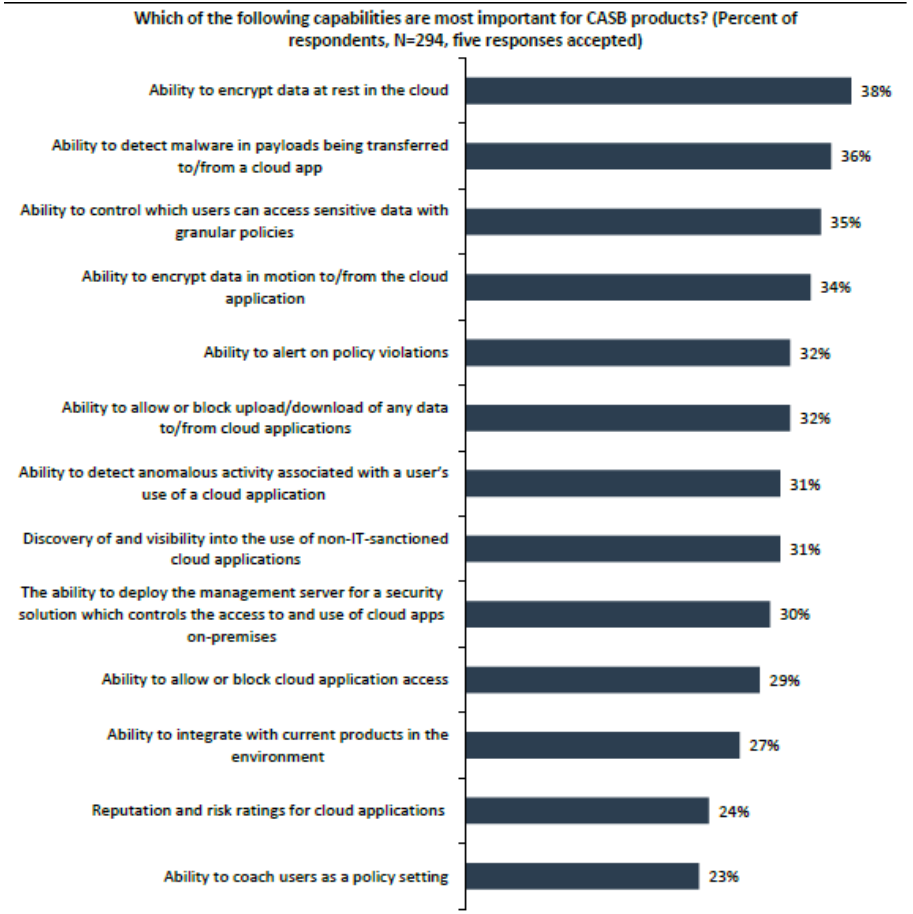


Сценарии применения для организаций финансового сектора

Communications Technology Innovations

Три основных сценария:

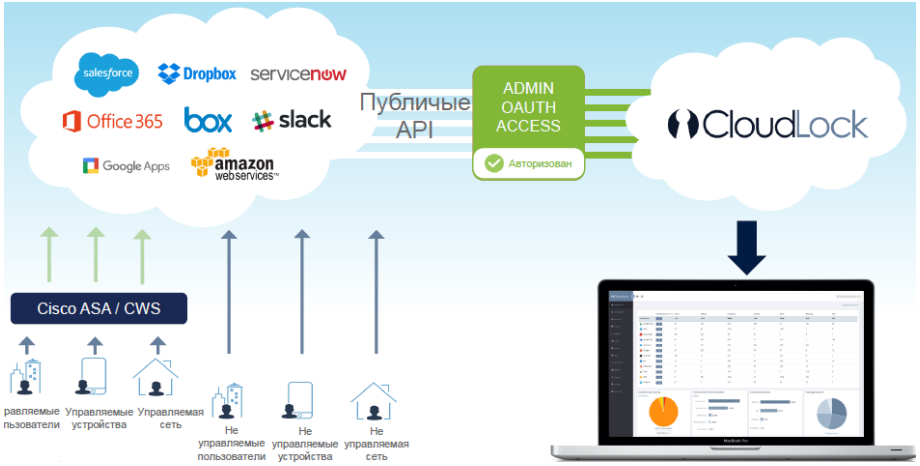
1. Аудит использования облачных сервисов и контроль за Shadow IT за периметром сети финансовой организации (ноутбуки, мобильные устройства, пользователи)
2. Планирование рисков перед переходом в облако для типовых back-end приложений (офисные приложения, обмен файлами, средства совместной работы и др.)
3. Реализация политики безопасности для защиты данных хранящихся в облаке, как для SaaS так и IaaS



Что мы предлагаем

Оценить риски использования облачных приложений уже сейчас:

CTI Security Cloud Assessment



Учитывает все аспекты безопасности при использовании облаков:

- Архитектура защиты сети и Shadow IT
- Используемые облачные приложения
- Риски использования облачных приложений и данных
- Наиболее эффективные сценарии применения CASB для организации и получаемые результаты от внедрения

В качестве выводов

1. Организации, использующие облачные сервисы **разделяют ответственность за обеспечение безопасности с провайдерами облачных услуг,** которые также могут предоставлять элементы CASB

2. Безопасность один из основных барьеров перехода на облачные сервисы
- Изменение принципа безопасности – данные принадлежат компании, но хранятся в системах, которые ей не принадлежат

3. Пути повышения доверия для финансовых организаций:
- Встраивание API для автоматизации задач взаимодействия с облаком (например, перенос или миграция данных)
- Сертификация облачного решения по требованиям безопасности
- Добавлению дополнительных механизмов безопасности CASB