Сервисы для безопасности облачных служб

Модели обслуживания облачных сервисов

- Сначала необходимо выбрать метод обслуживания, исходя из которого будут представлены защитные методы сервисов для безопасности облачных служб.
- Для каждого метода существует несколько сервисов защиты облачных сервисов.

Всего существует 3 метода: SaaS, PaaS и IaaS.

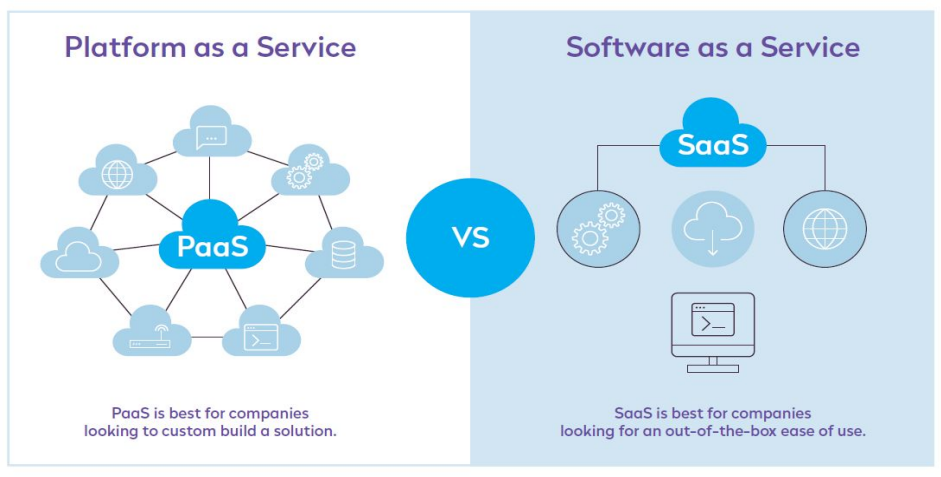
SaaS означает “программное обеспечение как сервис”, Software as Service.

PaaS означает “платформа как сервис”, Platform as Service.

IaaS означает “инфраструктура как сервис”, Infrastructure as Service.

О SaaS подробно

- В SaaS вы используете программное обеспечение, приложения и операционные системы провайдера, который полностью контролирует функционирование облачной инфраструктуры.
- По большому счету, вы управляете лишь своим аккаунтом (группой аккаунтов) с возможностью вносить незначительные изменения в некоторые настройки приложений. Примером данной услуги могут послужить YahooMail, Google Disk, Office Online и

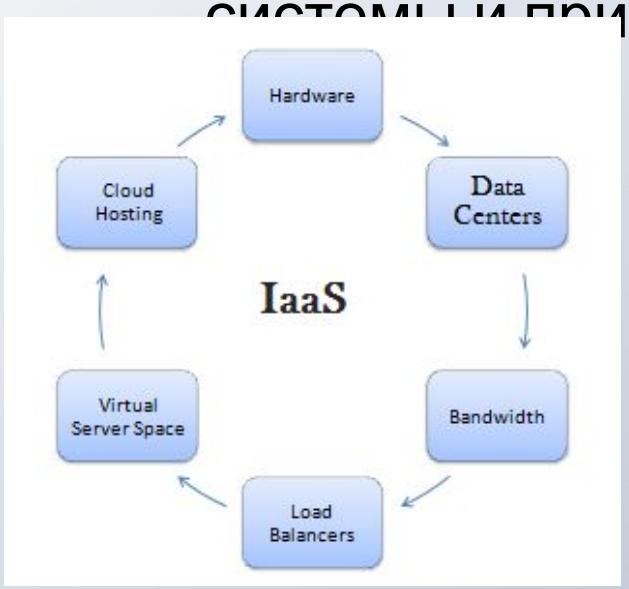


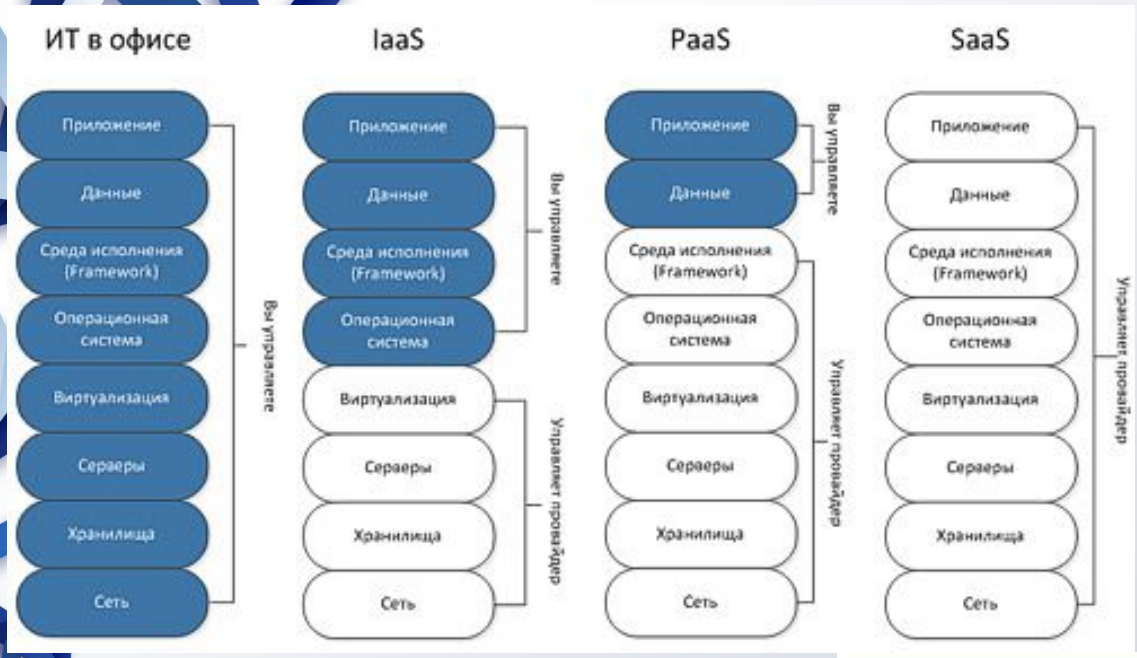
О PaaS подробно

- В PaaS вы получаете возможность установки собственного программного обеспечения и построения приложений уровня Saas.
- Тем не менее, контроль операционных систем, серверов, хранилищ данных по-прежнему остается за провайдером.
- Самым простым примером здесь может послужить хостинг, где вы устанавливаете свою CMS, модули и плагины к ней, а также получаете доступ к MySQL, PHPMyAdmin и др.

О IaaS подробно

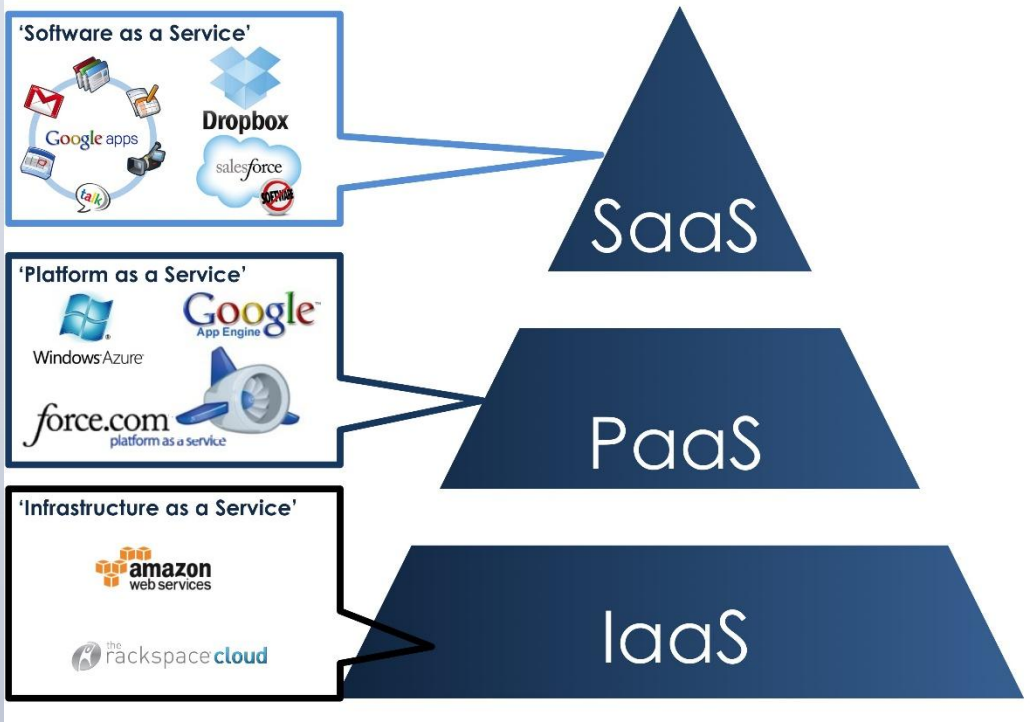
- В IaaS у вас еще больше свободы – провайдер предоставляет лишь физический фундамент вычислительных мощностей (виртуальных машин), на основе которых вы можете развернуть свою облачную инфраструктуру и реализовать собственные решения уровня PaaS и Saas, контролируя устанавливаемые операционные системы и приложения





Сравнение IaaS, PaaS и SaaS

Компании, использующие разные модели обслуживания



Требования к защите SaaS

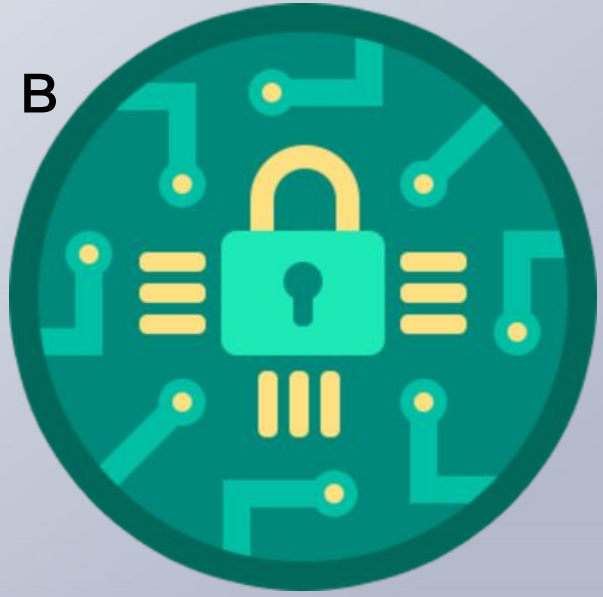
- 1. Система должна предоставлять защиту и управление доступом для функций, основанных на полномочиях.
- 2. Пользовательские данные могут размещаться в информационной среде внутри предприятия. Система должна предоставлять механизмы аутентификации пользователей с использованием данных, размещенных во внутренней информационной среде.
- 3. В силу строгих требований арендаторов к изоляции данных и исполнению нормативных требований пользовательские данные могут размещаться в выделенной базе данных, предоставляе по требованию.

Имеются три типа средств защиты

- 1. Средства, интегрируемые внутри виртуальной платформой «облака».
- 2. Наложенные средства защиты, обеспечивающие защиту облачного периметра.
  Как правило, к технологиям защиты, предполагающим интеграцию на уровне виртуальной платформы, относятся решения, позволяющие обеспечить разграничение доступа пользователей и администраторов к ресурсам «облака».
- 3. Выбор конкретных средств защиты, интегрируемых внутри «облака», зависит от особенностей виртуальной платформы и осуществляется с учетом ее специфики.
  К технологиям защиты, используемым на уровне облачного периметра, относятся межсетевое экранирование, шифрование трафика, предотвращение вторжений и пр.

Сервисы безопасности «облака»

1. Межсетевое экранирование (Firewall)
2. Предотвращение вторжений (IDS / IPS)
3. Создание защищенных каналов связи (VPN / SSL VPN)
4. Защита от атак типа «отказ в обслуживании» (DoS/DDoS)
5. Антивирусная защита
6. Антиспам-защита



Требования к защите PaaS(от Microsoft!)

- Использование централизованного репозитория удостоверений
- Преимущества использования аутентификации Azure AD вместо аутентификации SQL
- Ограничение доступа по IP-адресу
- Шифр нных

IaaS.. Как его защищать?

- Двойная аутентификация: сначала человек логинится на телефоне, через несколько секунд ему приходит на телефон сообщение с уникальным кодом доступа, который должен быть введен в панель управления сервером для получения доступа.
- Необходимо всегда поддерживать актуальную версию всех антивирусов и т. п.
- Выбирайте известного вендора IaaS, чтобы у него не [illegible] язвимостей с его стороны.