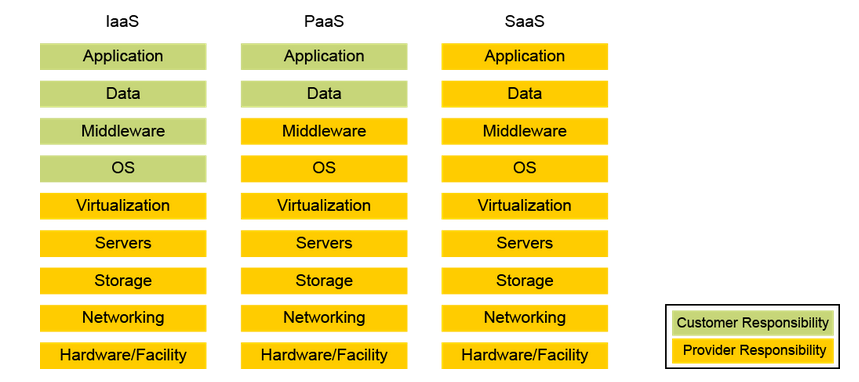
**Cloud Computing**

**Benefits**

* decreased IT staff
* lower hardware cost, and lower operating cost.
* decreased development time
* offering scalability and elasticity: as resources can be provisioned and de-provisioned rapidly, decommissioning cloud resources quickly after they are no longer needed
* better reliability and help prevent against data loss.

**Cloud Service Models**



**Cloud Deployment Models**

**Private**

* In-house managed cloud. Many companies utilize only a private cloud because of data security requirements.
* Industries such as financial, government, and healthcare have strict requirements on how data is secured, which often requires them to keep information within their firewall.
* A company has much more control and insight in a private cloud environment, however, there may not be any cost savings since they are still responsible for the IT staff, hardware, and operations.

**public cloud**

* defined as cloud services from a provider that are hosted outside of a company's walls.
* The cost of utilizing cloud services from a provider is offset by lowering the number of required IT staff and the amount of hardware that needs to be purchased and lowering the operations cost.
* large public cloud providers that offer IaaS, PaaS, Saa solutions: Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Alibaba Cloud, and Dimension Data.
* smaller companies that have public cloud offerings are: Rackspace, OpenStack, and IBM Cloud.
* Another popular public cloud offering is Apple's iCloud, which is utilized by most all iPhone and iPad users.

**Hybrid cloud**: mixture of private and public cloud services

Cloud computing attacks:

* Session hijacking: the attacker sniff traffic and intercept traffic to take over a legitimate connection to a cloud service
* DNS attack: the attacker tricks users into visiting a phishing site and giving up valid credentials
* XSS: used to steal cookies that can be exploited to gain access as an authenticated user to a cloud-based service
* SQL injection: this attack exploits vulnerable cloud-based applications that allow attackers to pass SQL commands to a database for execution
* Session riding (incompris)
* DDOS attack
* Man-in-the-middle cryptographic attack: attacker place himself in the communication path between two users.
* Side channel attack
* Authentication attack
* API attacks: APIs are configured insecurely.

There is no universal, industry-accepted framework that will provide to customers a common security audit approach for a cloud environment.

Among various documents, it is useful to identify some documents that are used as indispensable foundations:

* National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53)
* NIST Cybersecurity Framework
* ISO 27001

Securing the cloud

Cloud physical environment security

Cisco SAFE is a design methodology that prescribes proactively incorporating security into the foundational design of your network

**Reporting and Threat Visibility in Cloud**

* **Cisco Stealthwatch Cloud** is a SaaS-based solution for threat visibility into known and unknown threats and anomalous behavior in your network
* Stealthwatch cloud is deployed for two primary use cases: public cloud monitoring and private network monitoring.