

Cloud Services Evaluation

CYB/340: Web And Cloud
Computing And Security

Presented by Seth Howell

8/23/2021



What Are Cloud Service Models?

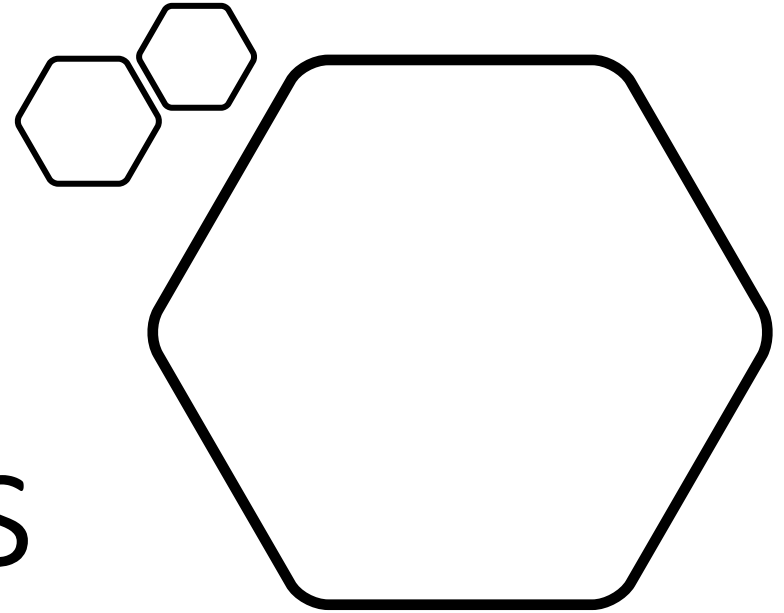


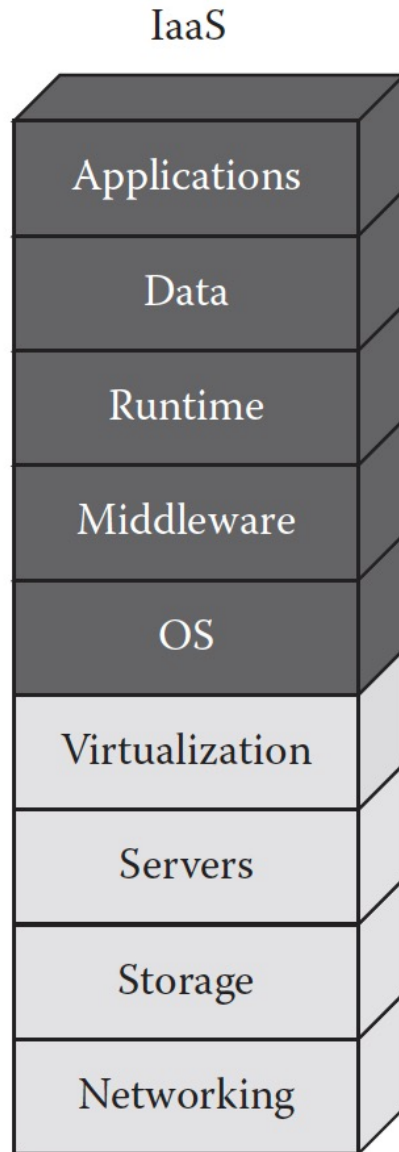
An exploration
of IaaS, PaaS,
and SaaS

The diagram features a large dark gray shape on the left containing the main title. To its right, a black hexagon contains the subtitle. Above this hexagon are two small white hexagons. A large white hexagon is positioned to the right of the black one, connected by a line that starts from the bottom of the black hexagon and curves around to the left side of the white hexagon.

For organizations who want to control
their cloud operations

Infrastructure as a Service (IaaS)





IaaS Fundamentals

IaaS providers manage the physical computer infrastructure (compute nodes, storage, network) and provide customers with virtual machines—virtual environments that can be locally installed—where the customer's IT employees can build out / install an OS and applications that utilize the CSP's physical storage. This allows customers to have maximal customizability and ownership while enjoying the five classical benefits of the cloud (on-demand self-service, broad network access, resource pooling, rapid elasticity, vertical scaling).

IaaS Benefits and Common Uses

Benefits

- All the customer's raw IT resources are covered.
- Freedom to install a chosen environment.
- Control over the environment, its security system, and its reliability.

Common Uses

- Organizations lacking a data center can use IaaS as a quick (no contract/on-demand) and scalable solution for storage.
- Development and testing (especially in AI research).
- Analytics and data.

IaaS Provider and Customer Responsibilities

CSP Responsibilities

- Managing the physical plant and securing it from physical damage/infiltration as well as securing the hardware's configuration, event data, and remote administrative access.
- Securing and managing the virtual environment (hypervisor, VM, etc.)
- Securing the network with firewalls, IDS/IPS, and other technology.
- Publishing clear governance protocol for internal management and co-management with the customers.

Customer Responsibilities

- Securing the infrastructure (especially making sure a solid OS is installed).

IaaS Security Features and Vulnerabilities

Security Features

- The hardware logs events and incidents.
- Isolation of VMs and secured baseline configurations.
- Remote administrative access.
- Firewalls, IDS/IPS, honeypots, and vulnerability assessments to secure the network.

Vulnerabilities

- Flaws in code performing migration of VMs among servers, and VM snapshot and rollback.
- Diverse data laws geographically can lead to privacy violations.
- Hardware trojans.
- DoS attacks on the network.
- Physical damage (e.g., flooding).

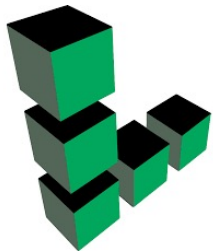
IaaS Vendors



1. **Google Compute Engine:** offers predefined and customizable VMs, preemptible machines, rightsizing recommendations, and fine-tuned resources for different workload types.



2. **Amazon EC2:** customers choose a processor, storage, networking, operating system, and purchase model. “More SAP, HPC, Machine Learning, and Windows workloads run on AWS than any other cloud.”



3. **Linode:** advertises Linux VMs, dedicated vs shared CPU, high memory, GPU, and Kubernetes.

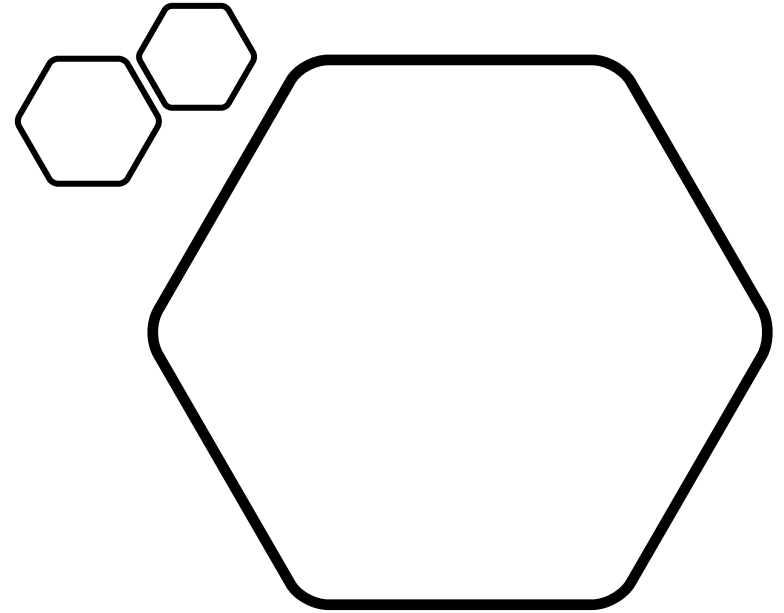
[1] <https://cloud.google.com/compute>.

[2] <https://aws.amazon.com/ec2/>.

[3] <https://www.linode.com/products/>.

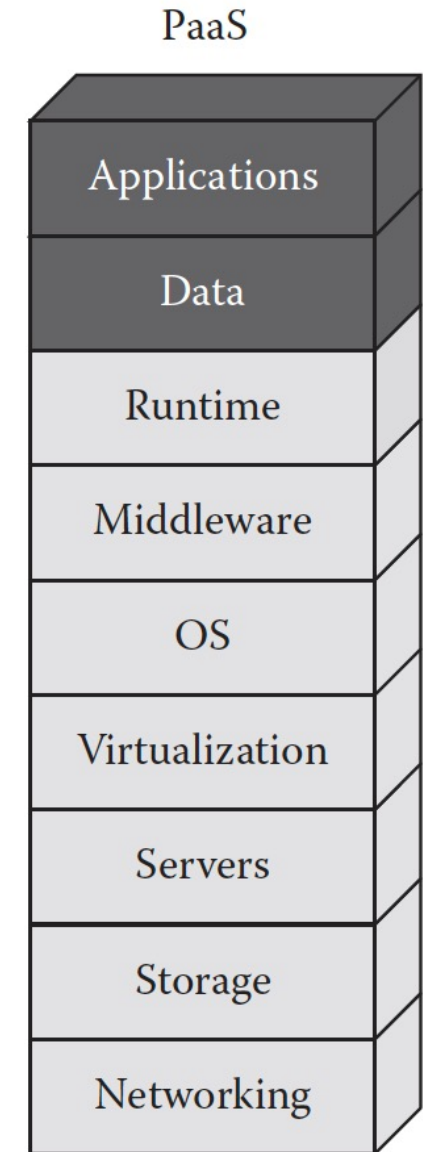
For organizations who want creative
freedom in app development

Platform as a Service (PaaS)



PaaS Fundamentals

PaaS providers manage both the infrastructure and operating system, focusing their efforts on giving customers a powerful virtual development environment to install or build applications. This often includes coding resources and documentation, web servers, and databases. Customers can subscribe to a platform that best meets their goals and then have software developers build out applications that will be virtually accessible via the CSP's OS.



PaaS Benefits and Common Uses

Benefits

- Customers will have more IT bases covered (OS, runtime, middleware) while retaining freedom and control over applications.
- Customers can build, test, deploy, update and scale applications more quickly and inexpensively they could if they had to build out and manage their own on-premises platform.
- A wide variety of resources (OS, middleware, dev tools, DBs, etc.)
- Flexibility for development teams to collaborate over the cloud.

Common Uses

- API development and management.
- Cloud migration and cloud-native development (via replatforming and refactoring).
- Agile development and DevOps.

PaaS Provider and Customer Responsibilities

CSP Responsibilities

- Managing the physical infrastructure.
- Securing the logical framework (e.g., virtual OS installation), and keeping it up to date.
- Securing communication with strong authentication, encryption, and VPNs.

Customer Responsibilities

- Secure software development, updating, and integration into the OS.

PaaS Security Features and Vulnerabilities

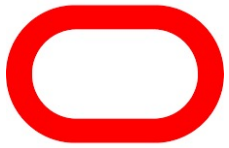
Security Features

- Encryption.
- VPNs.
- Secure and maintained OS.

Vulnerabilities

- Buffer overflows.
- TOCTTOU.
- Malicious driver or extension installations.

PaaS Vendors



1. **Oracle Cloud Infrastructure:** offers AI-empowered data analytics, app-dev with Java, and many supplementary products.



2. **Red Hat OpenShift:** a hybrid Kubernetes platform with a Linux OS and on-demand application stacks. Customer's choice of AWS, IBM, or Google Cloud as the parent infrastructure.



3. **Microsoft Azure:** offers 200+ products for software-dev, AI & ML, blockchain, app configuration, etc.

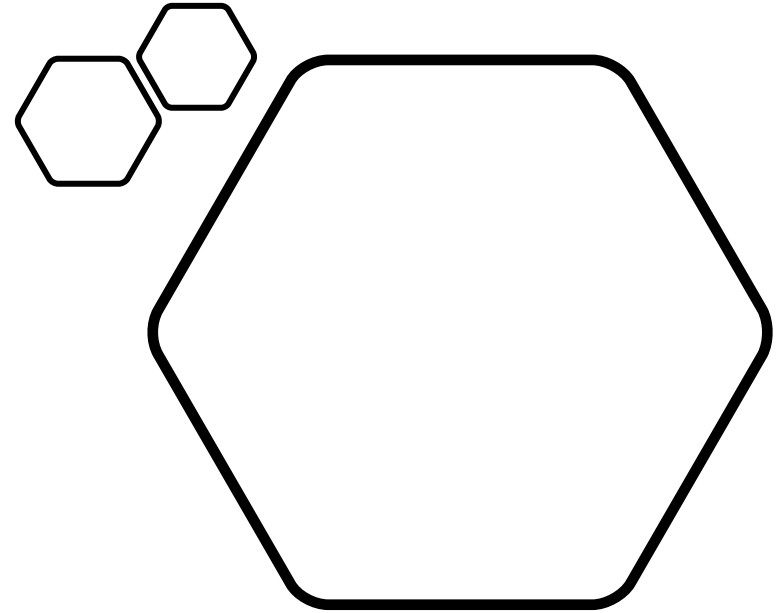
[1] <https://www.oracle.com/cloud/>.

[2] <https://www.redhat.com/en/technologies/cloud-computing/openshift>.

[3] <https://azure.microsoft.com/en-us/>.

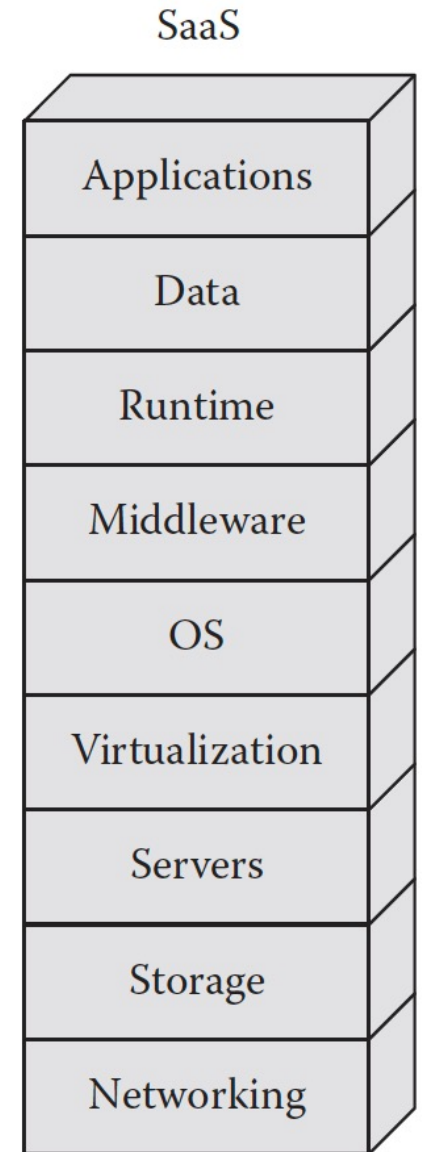
For organizations who want the full
package delivered to them

Software as a Service (SaaS)



SaaS Fundamentals

In SaaS, cloud providers seek to provide organizations with a straightforward online application toolset that will meet both general and fine-tuned customer needs. SaaS providers manage the entire hardware and software stack, leaving customers with minimal responsibilities or IT skill requirements. This makes SaaS a great resource for individuals, organizations that lack IT staff, and organizations with their own IT who only want to use SaaS for a specific use-case.



SaaS Benefits and Common Uses

Benefits

- Minimalized responsibility (e.g., no need to maintain software).
- Saved money – no need to employ an IT team.
- Customers can find software that is fine tuned to their needs.
- Protection from data loss if an employee's computer crashes.

Common Uses

- Online collaboration (e.g., google docs).
- Office productivity (e.g., the Microsoft 365 suite).
- Personal storage (e.g., files in Onedrive).

SaaS Provider and Customer Responsibilities

CSP Responsibilities

- Administrating everything (infrastructure, OS, apps, etc.), except the customer's data, and providing access to that data for customers.
- Administering, patching, and updating software.
- Securing data access via encryption, authentication, etc.

Customer Responsibilities

- Supplying and processing data within the cloud system.
- Administration of their data and managing employee access to it.
- Responsible use of SaaS-provided applications.

SaaS Security Features and Vulnerabilities

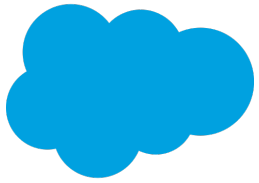
Security Features

- Symmetric and asymmetric cryptography.
- Digital signatures and SSL protocol.
- Hashing.
- Authentication.

Vulnerabilities

- SQL injections.
- Cross-site scripting.
- Cross-site request forgery.
- Buffer overflows.

SaaS Vendors



1. **Salesforce:** a huge selection of products and CRM aimed at organizations. Specifies products by industry (e.g., healthcare), and need (e.g., commerce).



2. **Google Workspace:** a public suite of email, office productivity, video communications, personal/organization storage, etc.




3. **Microsoft Office:** very similar to google workspace. The office productivity has a much more complex resource system, but less efficient live document collaboration.

[1] <https://www.salesforce.com/>.

[2] <https://workspace.google.com/>.

[3] <https://www.office.com/>.

Criteria for Evaluating Cloud Services



What things should
business leaders be on
the lookout for when they
are researching cloud
services?

The diagram features a large dark grey shape on the left containing the title. To the right, there is a cluster of three hexagons at the top left. Below them is a solid black hexagon containing a question. A line connects this solid hexagon to a larger, empty white hexagon on the right, which has a black outline.

1. Model: what service model is best for your organization?

It is vital that you have a thorough understanding of your organization's goals and assets before partnering with a CSP. Some important things to consider are:

- What level of control do you want over your data and software?
- Do you have qualified staff to build and manage within IaaS or PaaS?
- Which model will serve you best in the long-term?

If your organization simply needs a productivity/email/storage suite, or a CRM, then SaaS is a great option. However, if your organization needs a higher level of privacy and control, or is seeking to produce and test software, then IaaS or PaaS will be the better option.

2. Trust: does the CSP have a good track record?

Cloud services are proliferating as increasing numbers try to make their niche in the provider market. It's therefore vital to make sure the CSP you are looking into has successfully served organizations and can be trusted with your data. The STAR registry is a great resource to research CSP's security levels and reliability [1]. Also, if you can earn the CSP's trust, it will be useful to access their SOC 2 Type 2 audit report.

A good auxiliary question to ask is what protocols and technology the CSP is currently using to keep data secure. If the CSP has state-of-the-art encryption, a rigorous vetting system for hiring staff, and a secure infrastructure, it is likely a safe bet.

[1] <https://cloudsecurityalliance.org/star/>

3. Price: how many services do you need?

If your organization overestimates its needs, or your management lacks cloud education, then you will likely spend more than is needed and lose money by using cloud services irresponsibly. It will be useful to perform a thorough business impact analysis (BIA). This should include a recorded inventory of your organization's assets and a valuation and criticality determination of those assets. With a completed BIA and well-defined risk appetite, your management will be able to choose the best cloud subscription to host data and serve employees.

An important auxiliary is to compare competing CSPs in order to find which offers best-priced subscription model.

4. Negotiation: what relationship will your organization have with a CSP?

CSP-customer relations normally take place through contracts with SLAs. This contract will determine what responsibilities each party has, what the CSP can do with your organization's data, and what level of commitment exists. It is important to define what kind of relationship your organization wants with a CSP and to find a CSP that meets your standards or is willing to negotiate. For example, if your organization is unlikely to use a service for a long period, you should make sure the CSP you are contracting with will help transition your data to a new CSP.

Bibliography

Malisow, B. (2019). *(ISC)2® ccsp® certified cloud security professional: Official study guide* (2nd ed.). Wiley.

Vacca, J.R. (Ed.). (2016). *Cloud Computing Security: Foundations and Challenges* (1st ed.). CRC Press. <https://doi.org/10.1201/9781315372112>.

Vennam, S. (2020). *Cloud Computing*. IBM. Retrieved 25 August 2021, from <https://www.ibm.com/cloud/learn/cloud-computing>.

IBM Cloud Education. (2019). *IaaS (Infrastructure-as-a-Service)*. IBM. Retrieved 25 August 2021, from <https://www.ibm.com/cloud/learn/iaas>.

IBM Cloud Education. (2021). *PaaS (Platform-as-a-Service)*. IBM. Retrieved 25 August 2021, from <https://www.ibm.com/cloud/learn/paas>.

IBM Cloud Education. (2018). *IaaS vs. PaaS vs. SaaS*. IBM. Retrieved 25 August 2021, from <https://www.ibm.com/cloud/learn/iaas-paas-saas>.