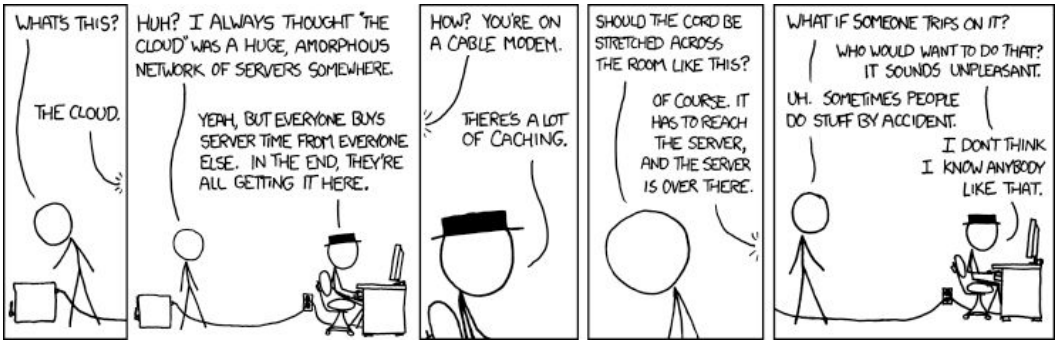
Intro to The Cloud (& Cloud Security)

Ian Flournoy, Christian Martin

What is “The Cloud”?

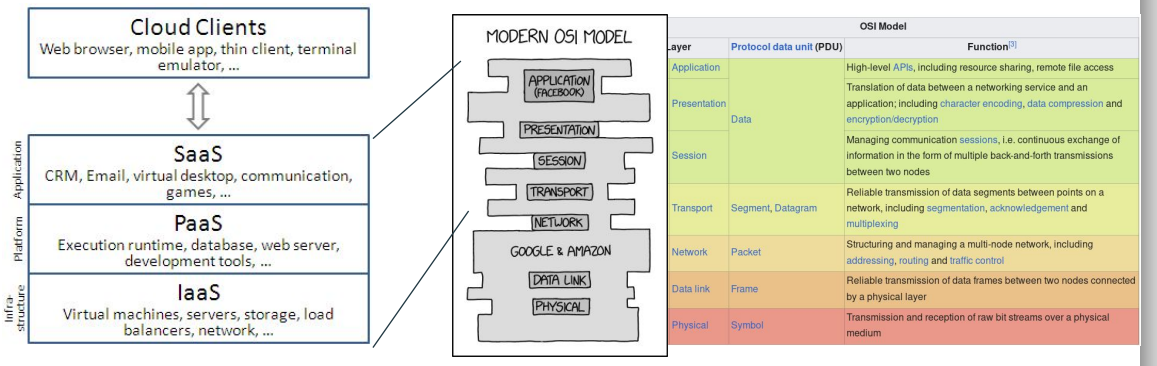


[Poll audience for their thoughts]

Seriously though, “there is no cloud, it’s just someone else’s computer” is very true, even if some opinion writers consider it a gross oversimplification. It’s true that “the cloud” is essentially where you stop caring about the specific server, but in the context of privacy & security the expression is only more true.

Images:

What makes up The Cloud? (SOA & OSI models)



OSI Model		
Layer	Protocol data unit (PDU)	Function[3]
Application	Data	High-level APIs, including resource sharing, remote file access
Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

OSI layers 4-7 are confusing in the differences between them, so we're going to shift over to SOA there.

OSI model = Open Systems Interconnection model
SOA = Service-Oriented Architecture (commonly referred to XaaS ("X as a Service"))

OSI L1: Physical

- ISPs
- Data centers
- Tenants within data centers
- Co-location providers

Security Concerns:

- Physical barriers at entrance
  - Often inc. biometric measures
- Physical access to racks

https://en.m.wikipedia.org/wiki/Data_center_security

Image:

OSI L2/L3/L4

- Firewalls
- VLANs
- Other software-defined networking (VPC)
- Load Balancing

Security Concerns:

- Blocking obvious attacks
  - DDoS
  - Scanning/sniffing
  - IDP/IPS
- Isolation of tenants

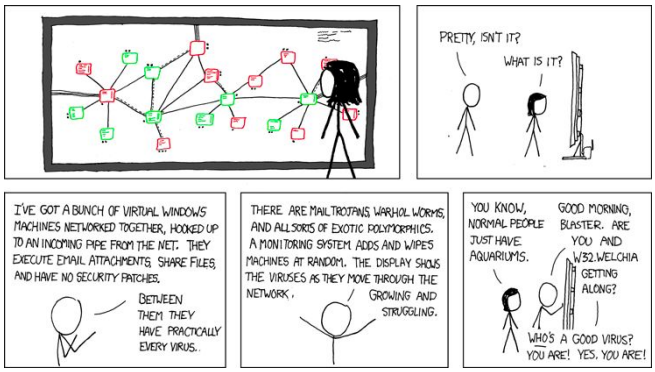


Image:
CC-BY-NC 2.5 xkcd.com

IaaS: Infrastructure as a Service

- VMs
- Raw resources (e.g. storage, network)
- Management
  - Scaling
  - Backups
  - Orchestration

Security Concerns:

- Isolation of tenants
  - Networking (see also OSI L2-L4)
  - Host execution attacks
- Host access to VM

Examples:

- AWS EC2, Google Cloud Platform, Azure, DigitalOcean, any VPS provider

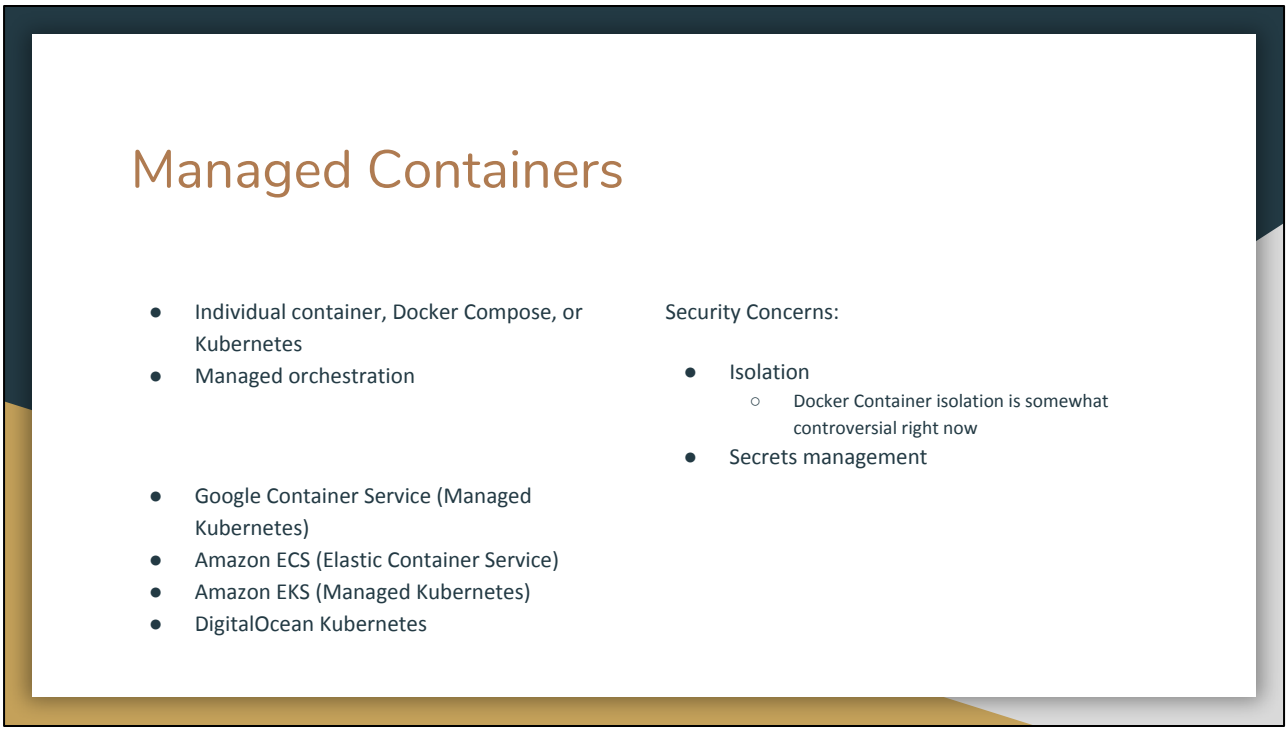
At this point, all further slides have concerns about security as you're relying on the provider to have everything secure. Main points include isolation of tenants & access to data.

Still worried about / have to manage:

- VM/OS security
- Network security
- Backups
- Scaling

Raw/expensive resources -> if access keys / credentials are leaked/stolen can lead to high cost

Image:
Fair Use (as part of a commentary/criticism); © Scott Adams Inc.



There isn't a consistent name for this yet, and it isn't XaaS/SOA, but it's worth mentioning here because it's between IaaS & PaaS and it's a growing, relevant area of The Cloud

More reading on Docker security:
https://www.oreilly.com/ideas/five-security-concerns-when-using-docker
https://opensource.com/business/14/7/docker-security-selinux (Part 1 of 2)
https://opensource.com/business/14/9/security-for-docker (Part 2 of 2)
https://www.bleepingcomputer.com/news/security/runc-vulnerability-gives-attackers-root-access-on-docker-kubernetes-hosts/

PaaS: Platform as a Service

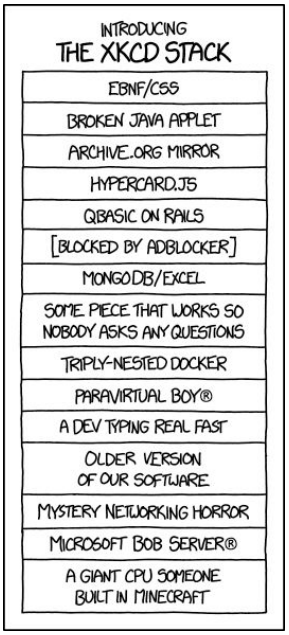
- Managed hosting
- Runtime(s) pre-configured

E.g.

- On pushing to a Git repo a container is automatically provisioned with the correct language version & connected to the internet
- Traditional shared hosting
- Heroku/Heroku-ish
- OpenShift/OKD

Security Concerns:

- Isolation



LAMP could count as one of the earliest instances of PaaS

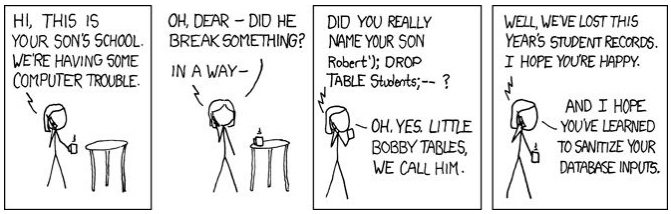
Image:

SaaS: Software as a Service

- Pre-configured instance of a piece of software
- Common examples are databases & web platforms
- Might have some runtime options
- Managed
  - Access
  - Runtime
  - Network
  - Orchestration

Security Concerns:

- Isolation
- Access
- Reliance on vendor's application security



Complete reliance on vendor for the software stack to work; user often only has control over content.

App security:

- How many password dumps have there been? Someone left a SQL instance open to the internet…
  - And MongoDB, Redis, Postgres, S3 Buckets...

Hosted DNS as an example of a classic SaaS?

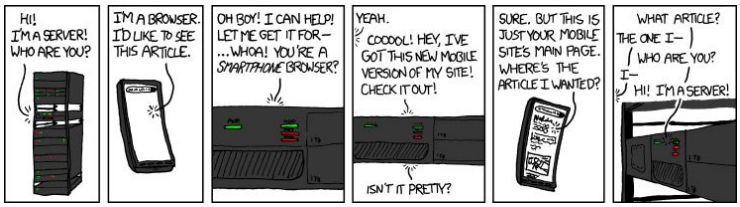
Image:

Serverless/FaaS (Function as a Service)

- Small script that gets run based on a trigger
  - Google Cloud Functions
  - Amazon Web Services - Lambda
  - Cloudflare Workers
- Managed
- Often on edge routing
  - Fastly VCL (Varnish Configuration Language)
  - PubNub Functions

Security Concerns:

- Isolation
- Reliance on vendor's application security



CloudFlare Workers: https://blog.cloudflare.com/cloud-computing-without-containers/

Image:

Questions?

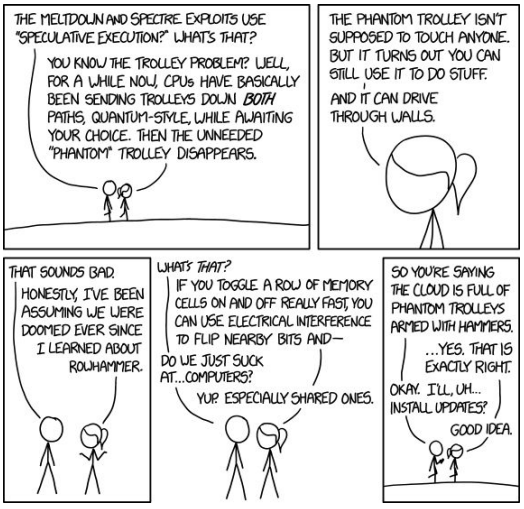


Image:
CC-BY-NC 2.5 xkcd.com
Fair use (as part of a commentary/criticism): The Simpsons