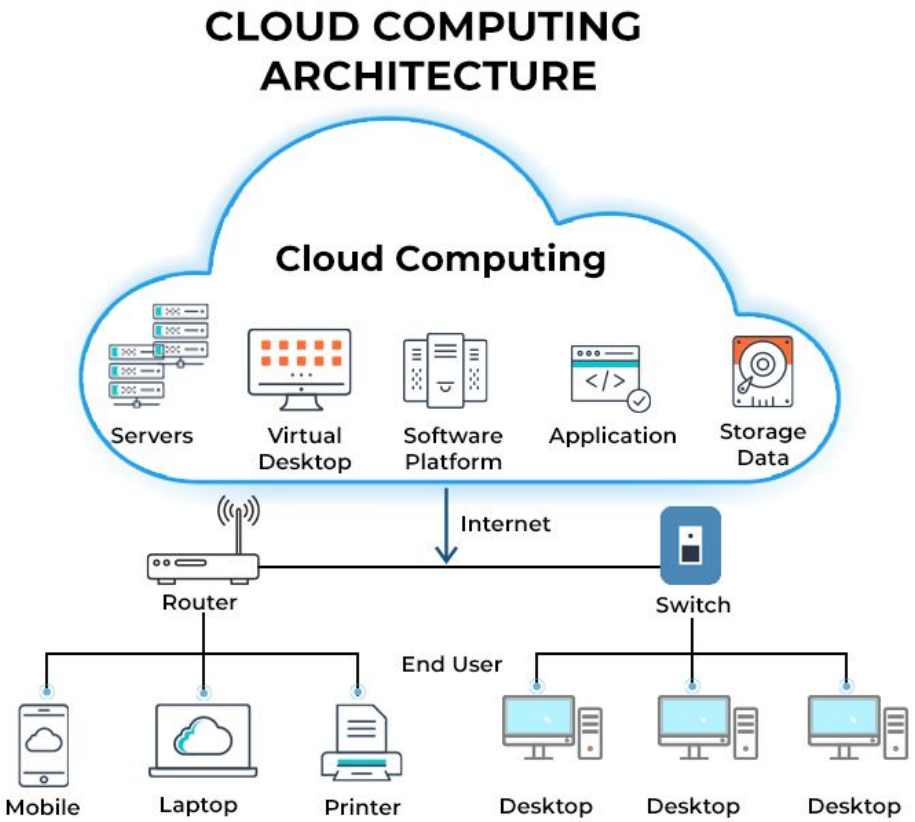
Primer to Cloud Security

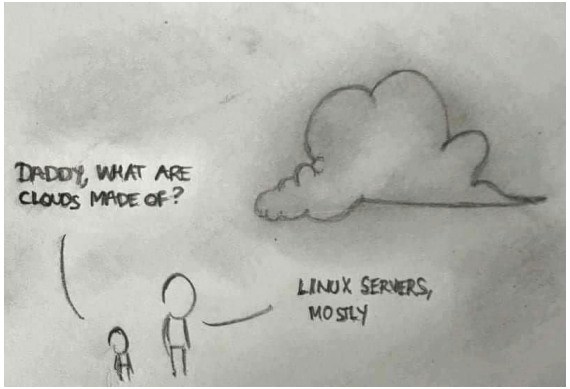
What is Cloud?

Let's get on the same page!

CLOUD @CERN

The Cosmics Leaving Outdoor Droplets (CLOUD) experiment uses a special cloud chamber to study the possible link between galactic cosmic rays and cloud formation





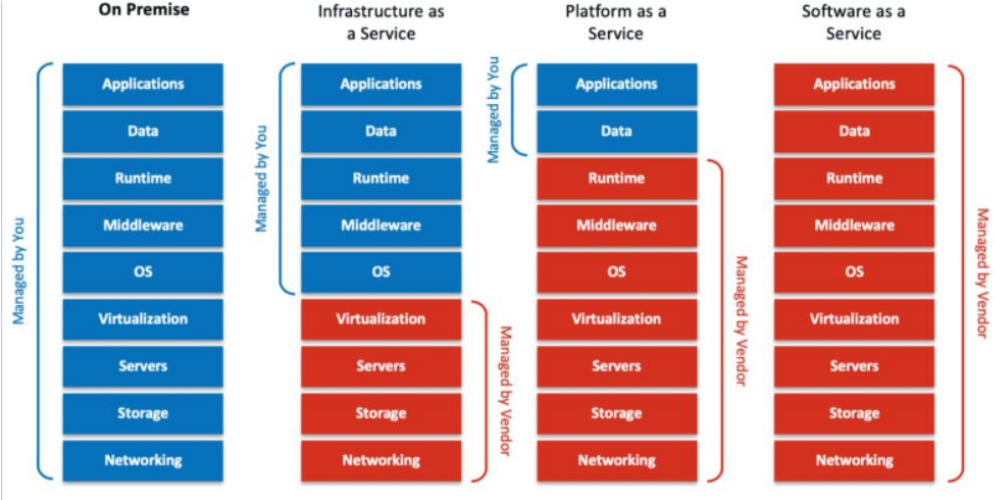
Providing computing resources (data storage, computing power) as a service

Cloud Computing Models

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)



Source

CERN's cloud is an Infrastructure-as-a-Service

A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings

Different aspects of Cloud Security

Build time

Security practices ensure that the code and container images are free of vulnerabilities before they are deployed

- Static Application Security Testing (SAST) - Analyze source code (e.g., SQL injection, buffer overflow)
- use secure images
  - check for any known CVEs
- reduce attack surface
  - minimal container images

Deploy time

involves the secure configuration and deployment of the containerized application

- configuration validation
- image scanning
- access control - roles to limit who and what can access the infrastructure

Runtime

- ensures that the application remains secure when it is live and serving users
- monitoring and logging
- secure high-value resources

Security Practices we use at CERN

- OIDC for access controls to clusters (provided as IaaS)
- Firewall - outer perimeter firewall blocks incoming access to systems on the CERN site
- Guidelines for best practices
  - Minimal base images
  - Running container with least privileges
- Vulnerability scanning for images

- Software Bill of Materials (SBOM)
- Policy controller - with default security policies
- Real time security monitoring and alerts


Thank you in German
Danke!