SEAS-8414

Analytical Tools for Cyber Analytics

Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Dr. M

Welcome to SEAS Online at George Washington University

SEAS-8414 class will begin shortly

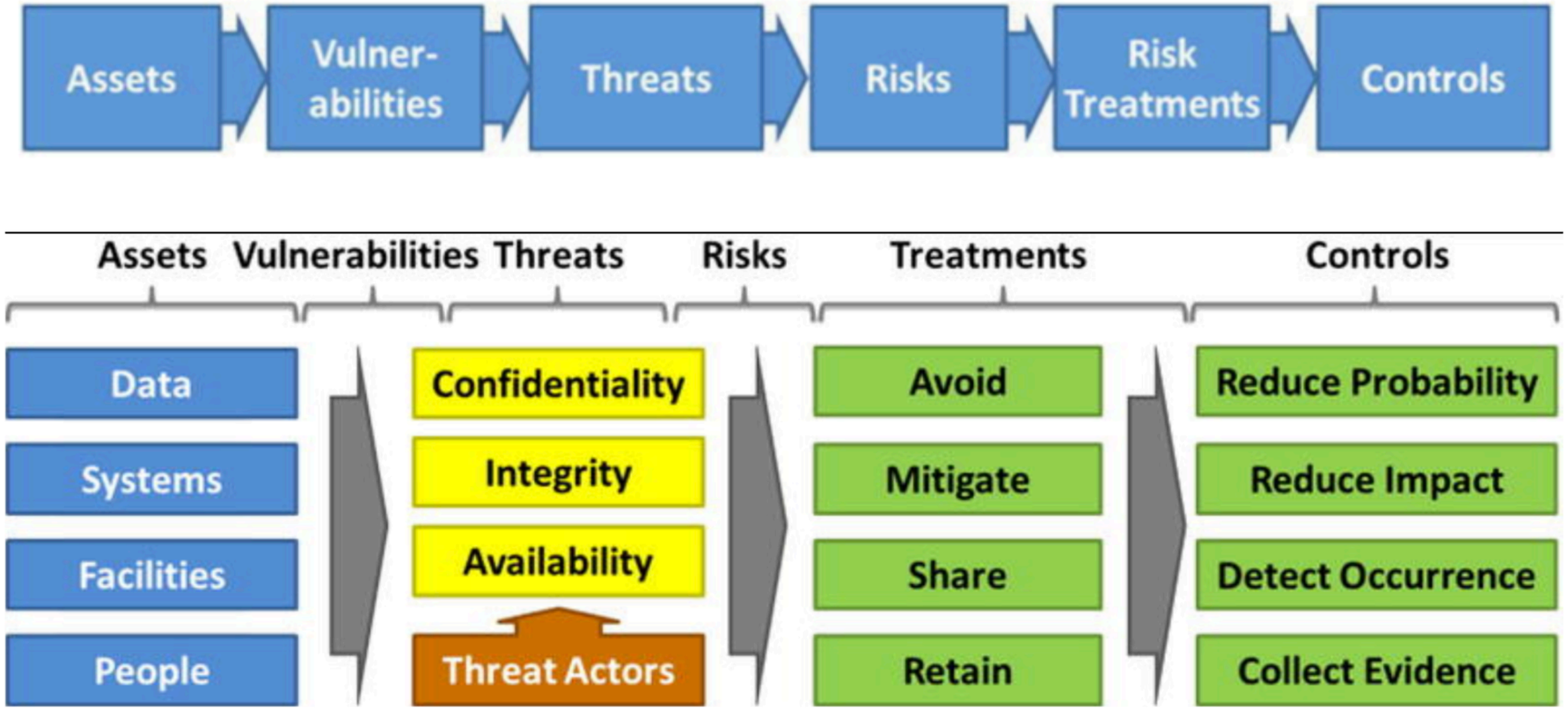
- **Audio:** To eliminate background noise, please be sure your audio is muted. To speak, please click the hand icon at the bottom of your screen (**Raise Hand**). When instructor calls on you, click microphone icon to unmute. When you've finished speaking, ***be sure to mute yourself again***.
- **Chat:** Please type your questions in Chat.
- **Recordings:** As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. Releasing these recordings is strictly prohibited.

Agenda

Week-1: Introduction to enterprise cybersecurity framework

In the first class, we will start an Internet company called GWU Secure Crypto Currency Services (gwuscc.com), which makes cryptocurrency recommendations based on personal and financial information. We will build and deploy the infrastructure in AWS Cloud (all the students are required to register for a free AWS account). We will work on identifying distinct types of cyber- attacks, attackers, and stages of attack relevant to gwuscc.com. We will explore frameworks such as MITRE ATT&CK and secure architectures such as Zero Trust to protect our start-up.

How to secure business assets?



Class-1

Structure

1. Rules of engagement
2. Idea to Application
3. Application to Infrastructure
4. Infrastucture to Security

Requirements

Working knowledge of:

- Git
- Python
- Docker
- Bash

Rules of Engagement

University Guidelines

Logistics

Course Schedule & Dates

- **Class hours**: Saturday, 9 am – 12 pm (Eastern)
- **Office hours**: Every Friday 6-9 PM ET
- **Start-End date**: October 22, 29; November 5, 12, 19; December 3, 10, 17; January 7, 14
- **Synchronous**: Attendance is mandatory, exceptions require approval.

Logistics

Textbook & Online Access

- **Textbook**: None
- **E-Textbook:** None
- **What is included in the exams?** Everything that we talk during the lectures.

Exams

Dates

- **Midterm:** from Saturday, Nov. 19, 8 pm ET, through Monday, Nov. 21, 8 pm ET.
- **Finals:** Saturday, Jan. 14, 8 pm ET, through Monday, Jan. 16, 8 pm ET.

Exam Policy Violations

See syllabus for the complete list

- **Minor**
  - Radio/TV in the background
  - Someone enters the room
  - Sitting on a couch
  - Out of camera view briefly (less than 5 minutes in total)
  - Second monitor (turned off) on the desk
  - Improper lighting
  - Incomplete room scan
  - Using headphones
  - Wearing hats, sunglasses, etc.
- **Major**
  - Browsing the web
  - Using the phone or other devices
  - Second screens
  - Out of camera view more than 5 min
  - Communicating with another individual by any means

Exam Policy Violations

Sanctions for Exam Policy Violations

- Minor
  - **1st offense**: The student will receive a warning.
  - **2nd offense**: 10% will be deducted from the exam score.
  - **Subsequent offenses**: The student could be referred to the Office of Academic Integrity.

- Major
  - **20%** will be deducted from the exam score, and the student may be referred to the Office of Academic Integrity.

Prerequisites

Cloud Accounts & Programming Language

- A free account with AWS is mandatory for both homework. You can optionally get Azure and GCP free accounts to try different CSPs.
- You can get hands-on experience with tools taught during the lecture with a laptop with permission to install (cloud orchestration) software.
- Basic Python, YAML, JSON, and Bash skills will help you practice hands-on during the lecture.

Expectations

What to and what not to

- **What to expect?**
  - You will gain the skills required to research and leverage security analytics tools.
  - You will get exposure to various security tools architecture.
- **What not to expect?**
  - This course is not a training program on any particular security tool or cloud.
  - We will not be troubleshooting problems during the class (use office hours).

Idea to Application

Introduction

The story of gwuscc.com

We want to build a financial start-up that yields 12% annually with 20% risk to capital. We leverage ML optimized trading algorithms in lucatrive financial markets such as cryptocurrencies.

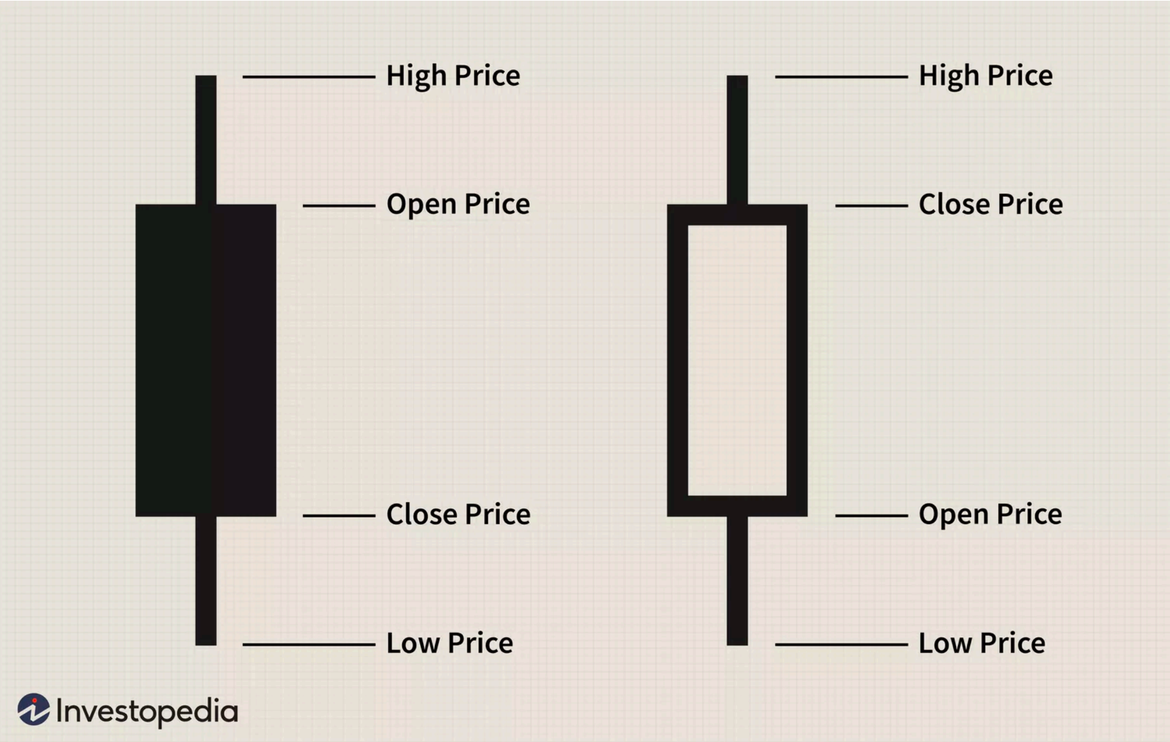
How to generate 12% returns?

- Large bank FDs are no more than 4%
- Mutual funds assure 7% returns with undefined risks.
- How can a start-up claim 12% returns with 20% risks?

Terminology

- **Symbol**: a string representing a financial assets such as stock or crypto.
- **Timeseries**: a sequence of data measured over a period of time.
- **Tick data**: a stock or cypto price data in timeseries format.

Candle Stick



Source: https://www.investopedia.com/trading/candlestick-charting-what-is-it/

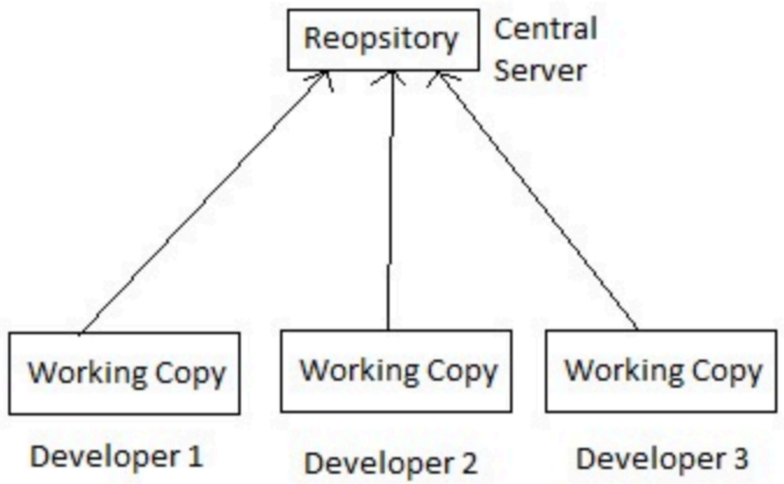
Quick Demo

I will walk you through a demo of a financial strategy using TradingView.

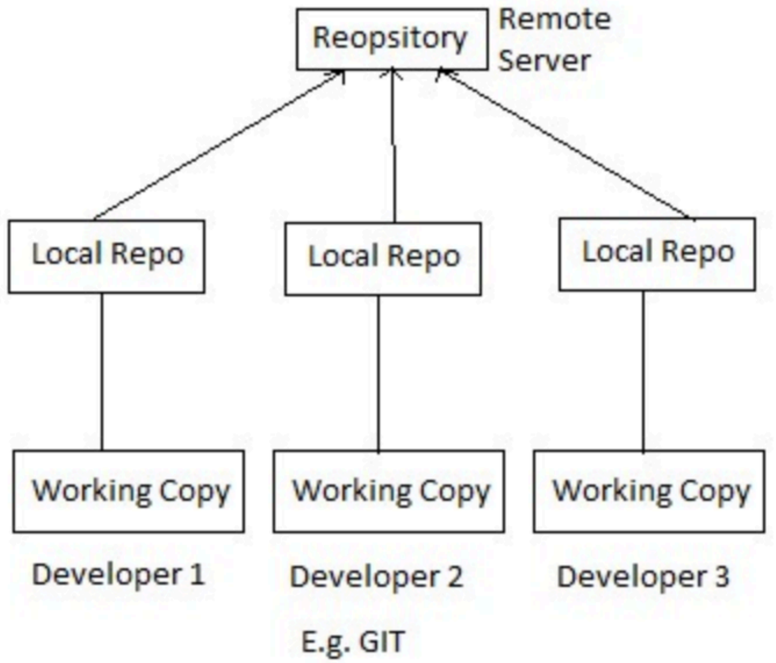
How to generate 12% returns?

- Strategy-1 (code: Elmo): RSI Short Only
  - 18% upside - 1% downside
- Strategy-2 (code: Teddy): RSI Short Only + Bollinger Bands
  - 22% upside - 1% downside
- Strategy-3 (code: Bert): Super Trend
  - 45% upside - 28% downside

Quick Intro: What is Git?



Centralized Version Control System



Distributed Version Control System

Let’s get real

1. Install Git - https://git-scm.com/book/en/v2/Getting-Started-Installing-Git

2. Install Docker - https://docs.docker.com/get-docker/

3. Get a copy of repository - https://github.com/gwuml/seas-8414.git

Download data

1. git clone https://github.com/gwuml/seas-8414.git

2. cd seas-8414

3. source .setup

4. download-history.sh

Backtest Performance

1. cat tools/strategy.env

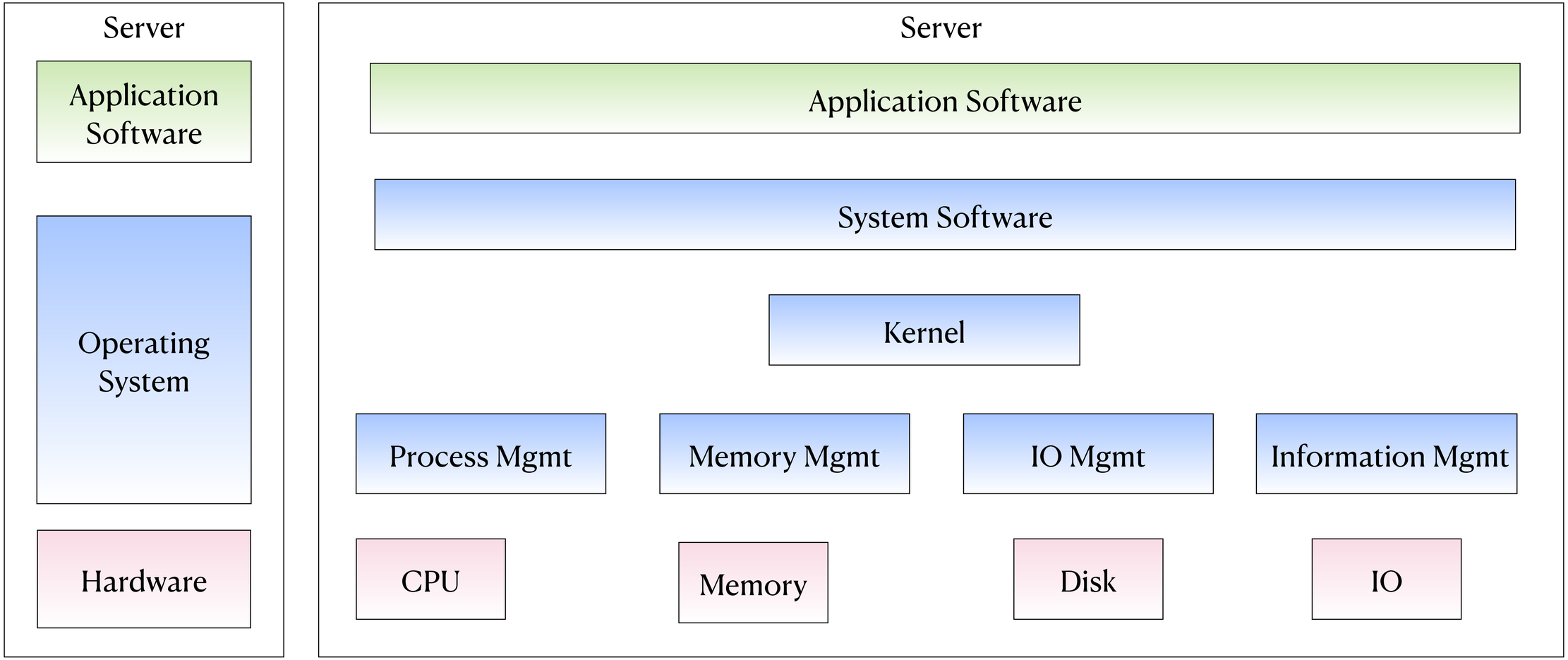
2. backtest-strategy.sh Elmo

3. backtest-strategy.sh Teddy

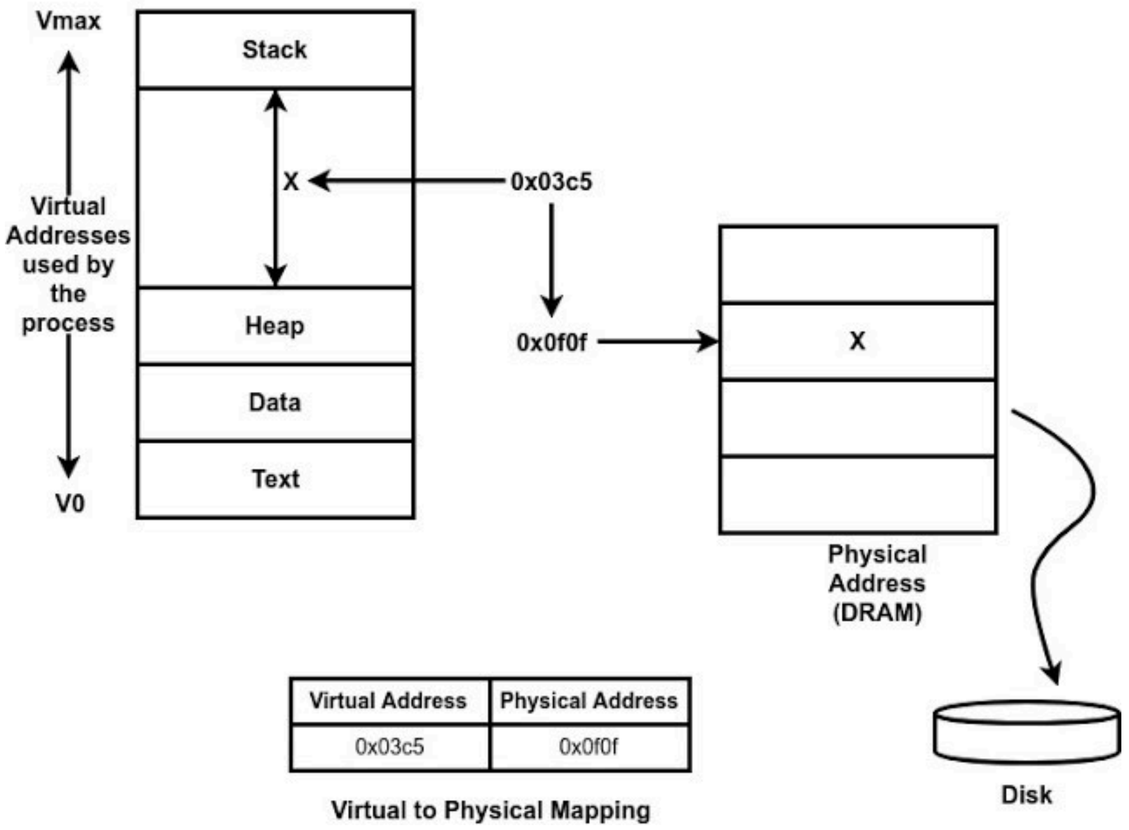
4. backtest-strategy.sh Bert

Application to Infrastructure

Anatomy of a Server

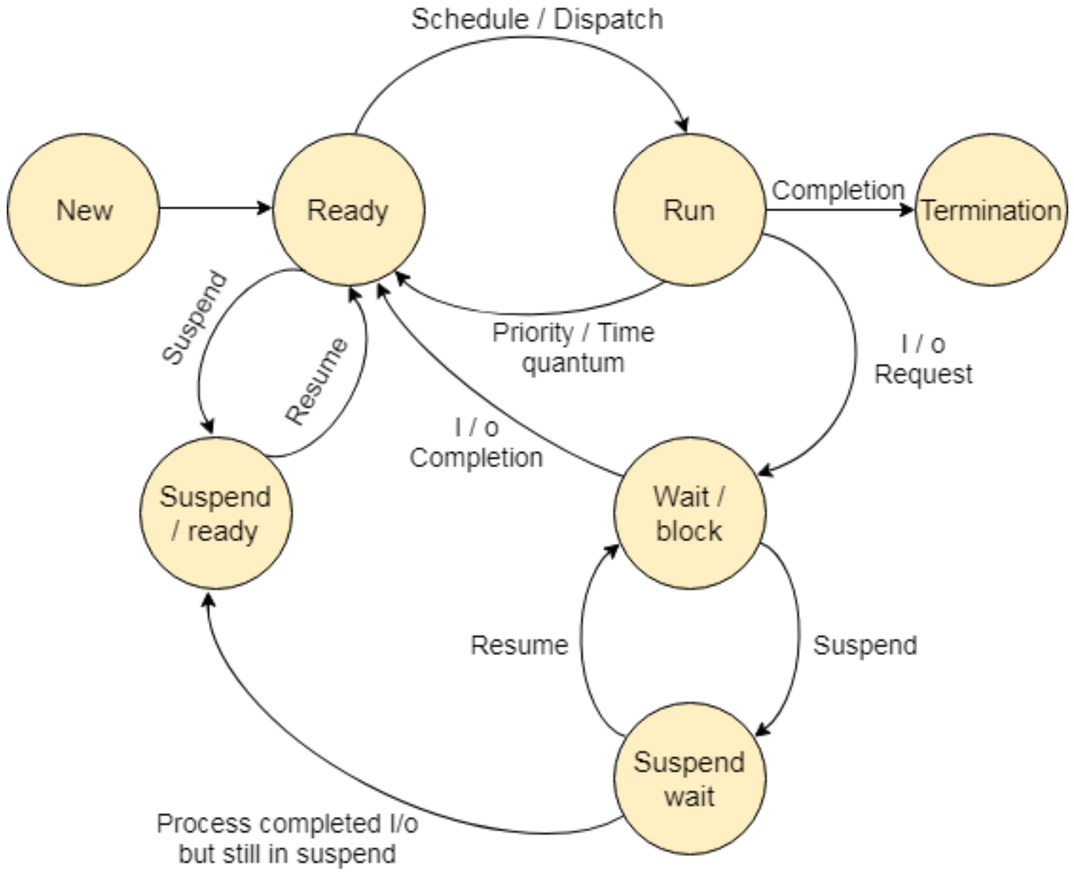


Process Management



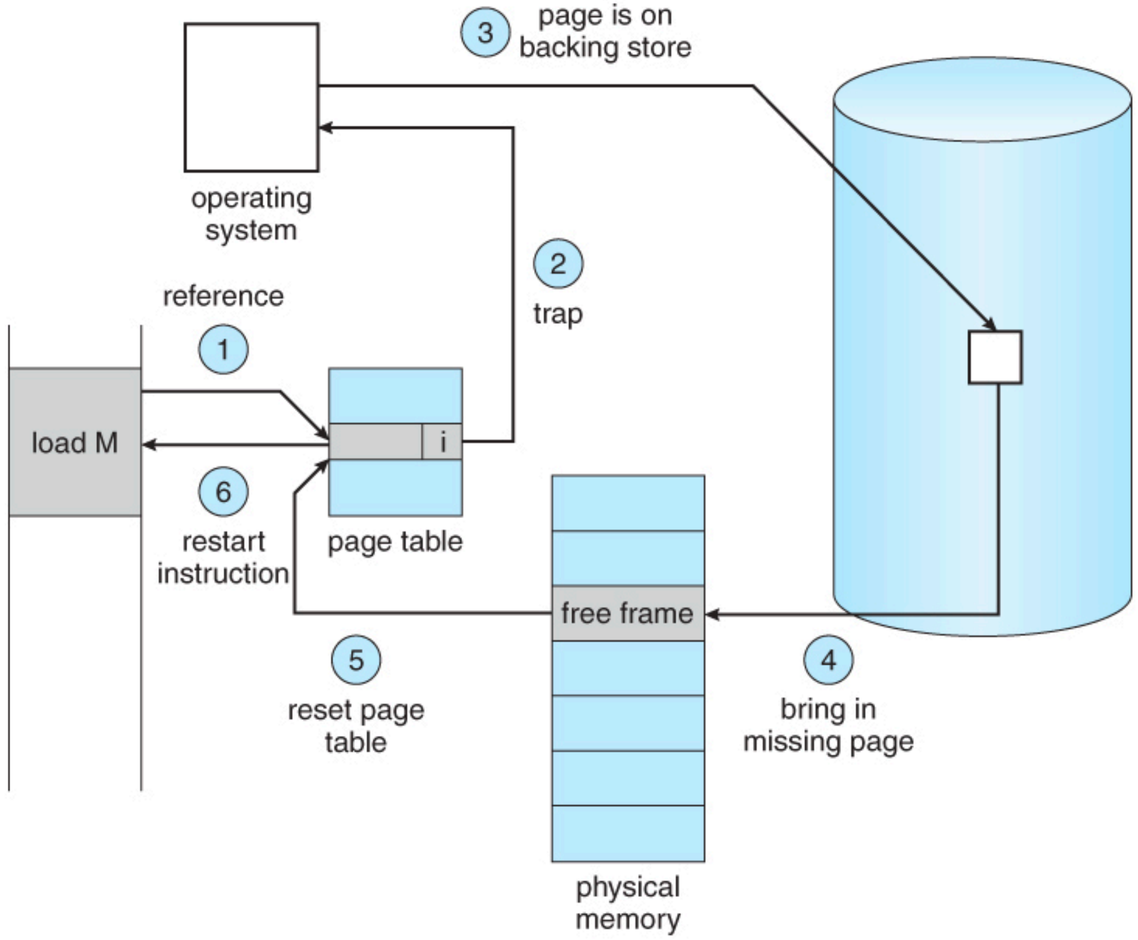
Virtual Address	Physical Address
0x03c5	0x0f0f

Virtual to Physical Mapping



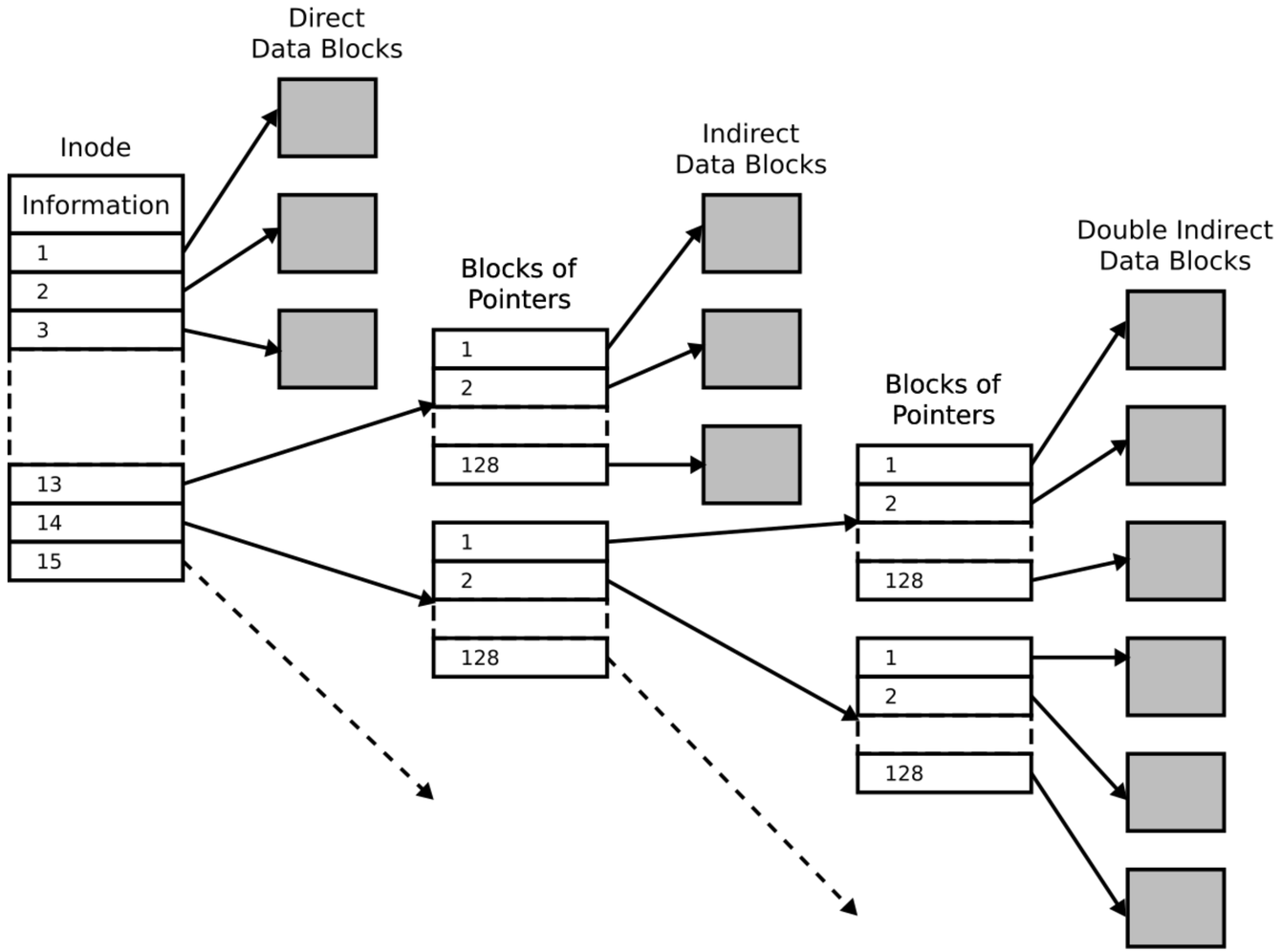
Source: Dias, Siddharth & Naik, Sidharth & Kotaguddam, Sreepraneeth & Raman, Sumedha & M., Namratha. (2017). A Machine Learning Approach for Improving Process Scheduling: A Survey. International Journal of Computer Trends and Technology. 43. 1-4. 10.14445/22312803/IJCTT-V43P101.

Memory Management



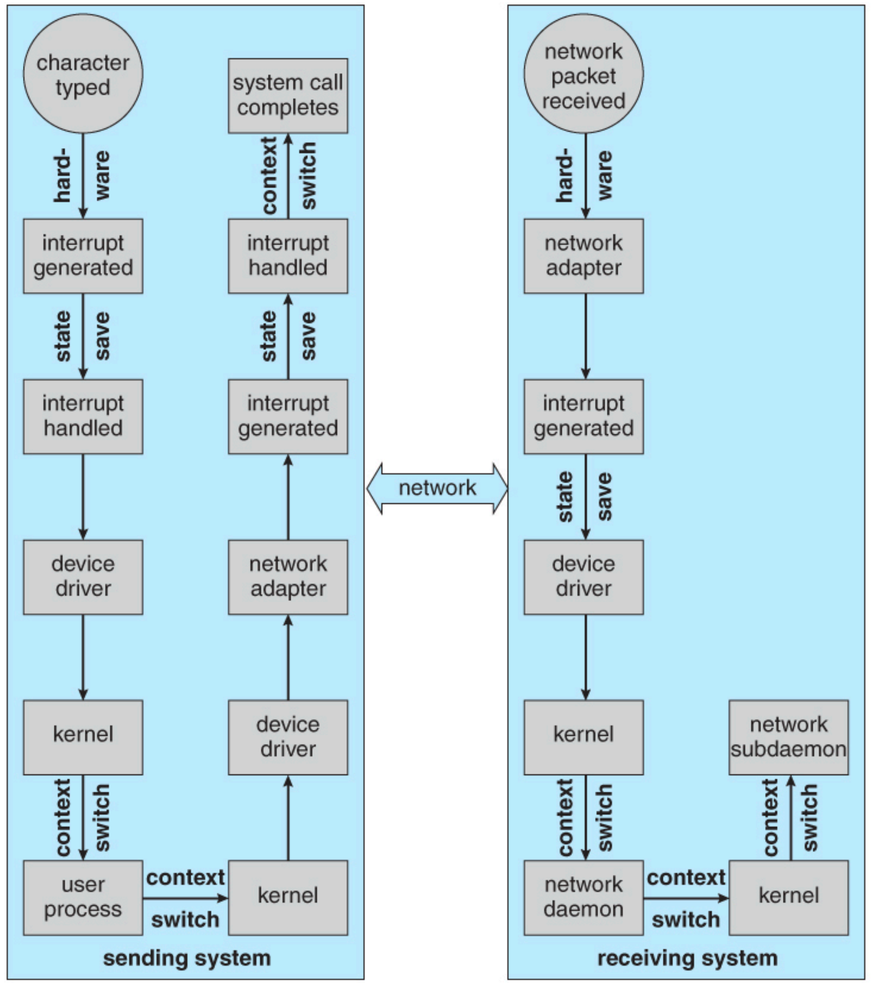
Source: https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/9_VirtualMemory.html

Information Management



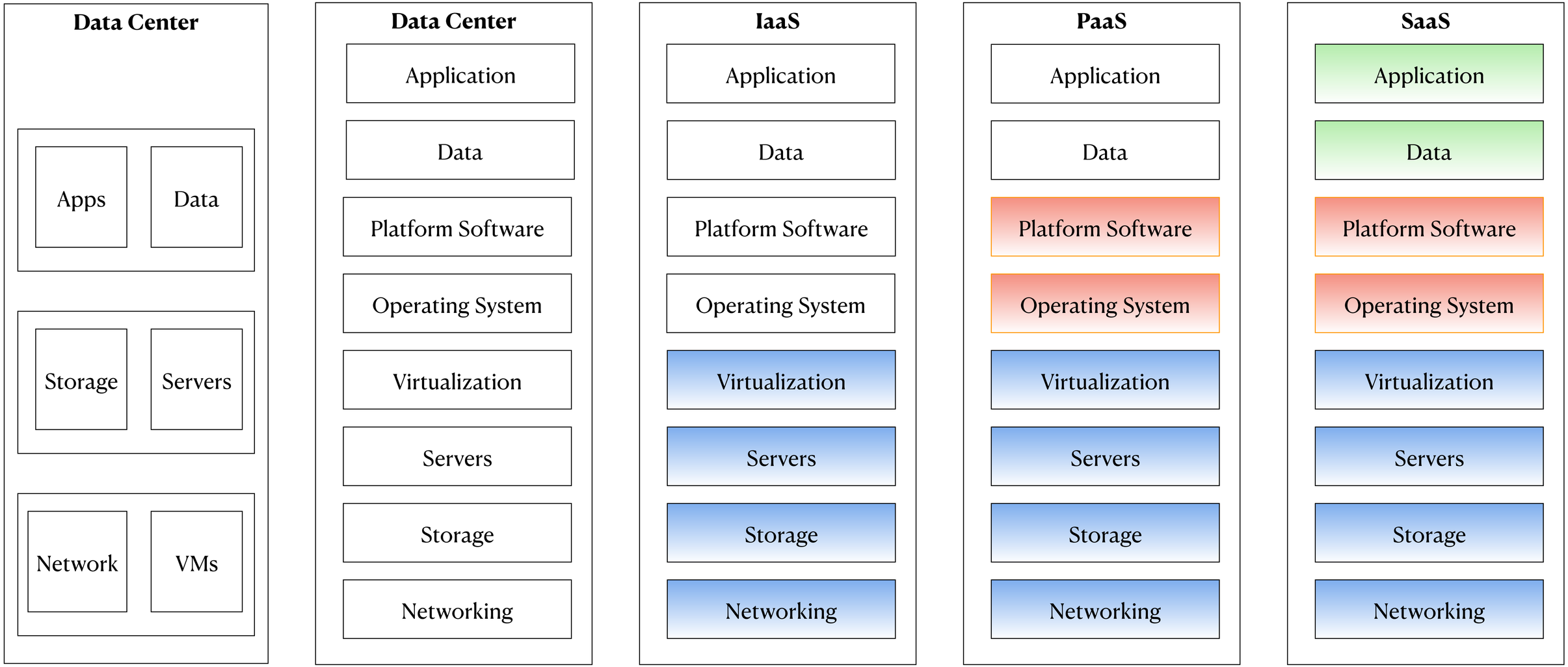
Source: https://commons.wikimedia.org/wiki/File:Ext2-inode.svg

IO Management



Source: https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/13_IOSystems.html

Data Center & Cloud Computing



Cloud Computing

NIST SP 800-145 Definition

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Practical Definition

Cloud Service has 5 Characteristics

1. On-demand self service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

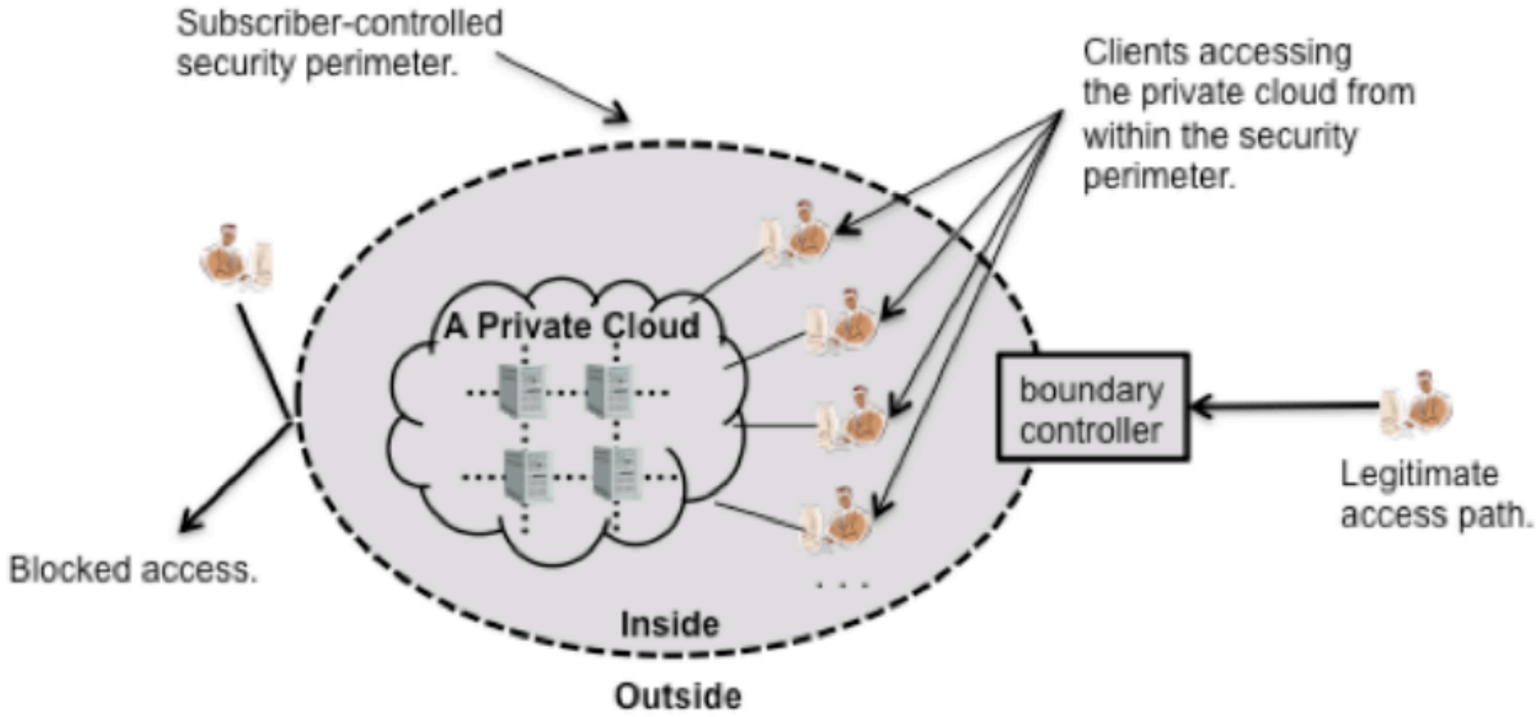
Practical Definition

Cloud Service has 4 deployment models

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

Private Cloud

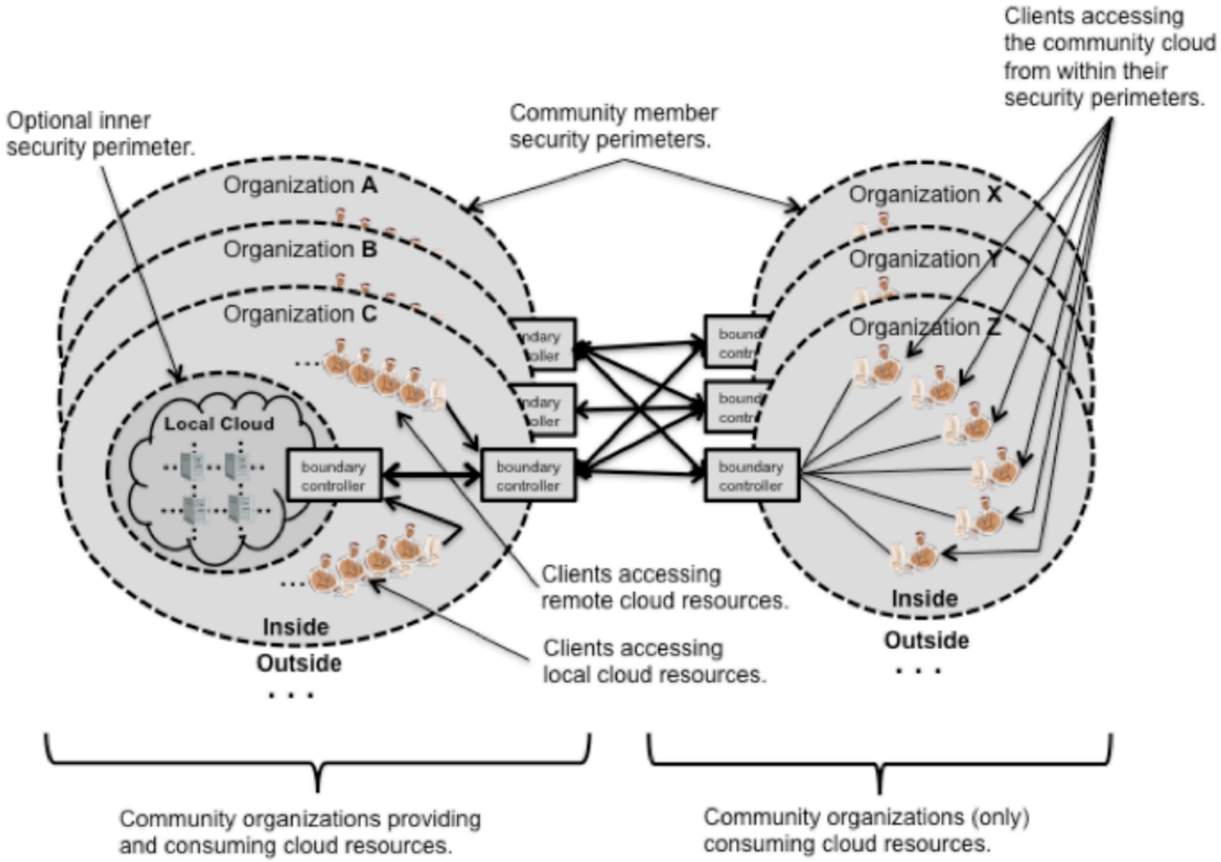
Security Posture in a Data Center



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Community Cloud

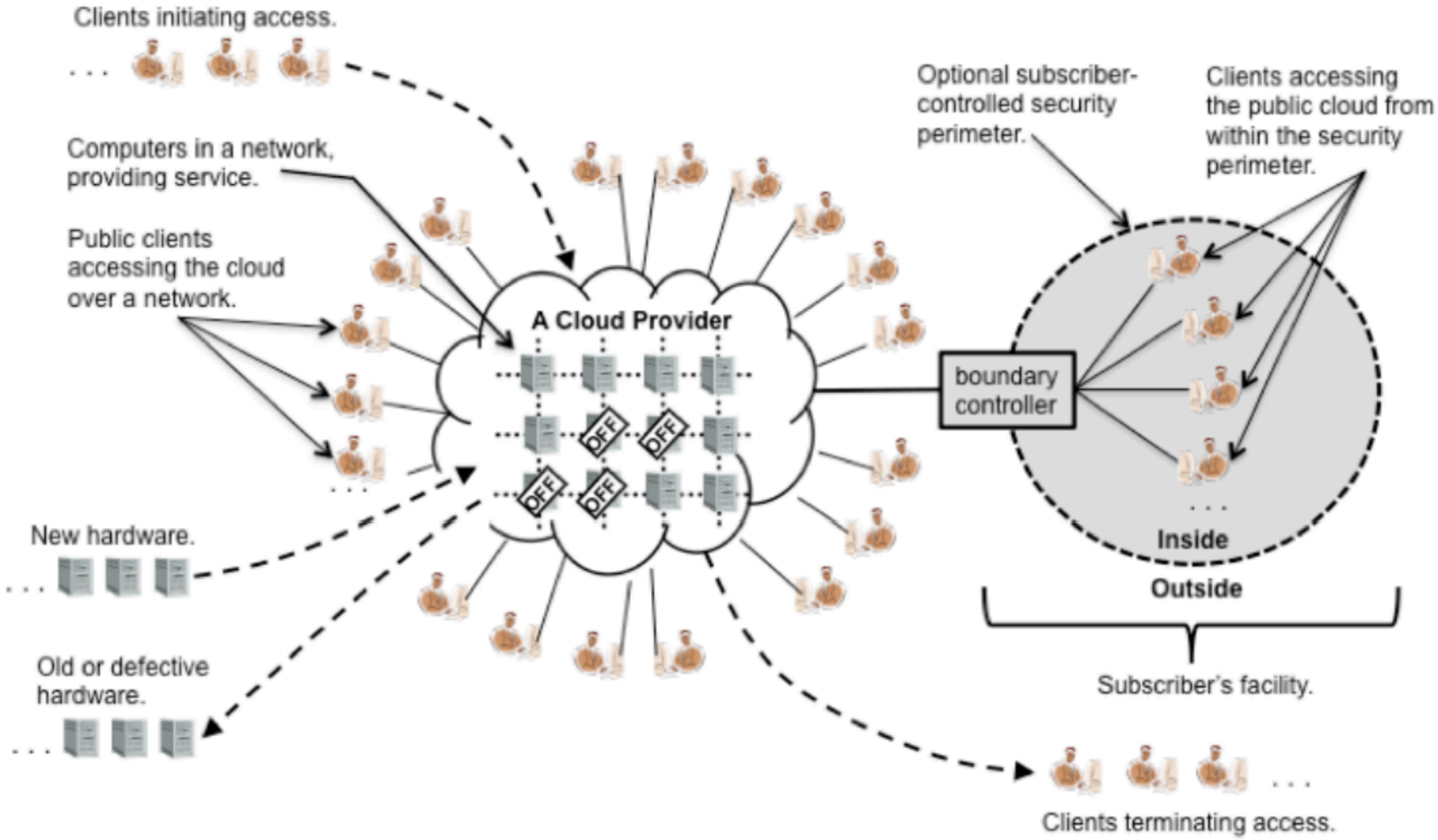
Security Posture



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Public Cloud

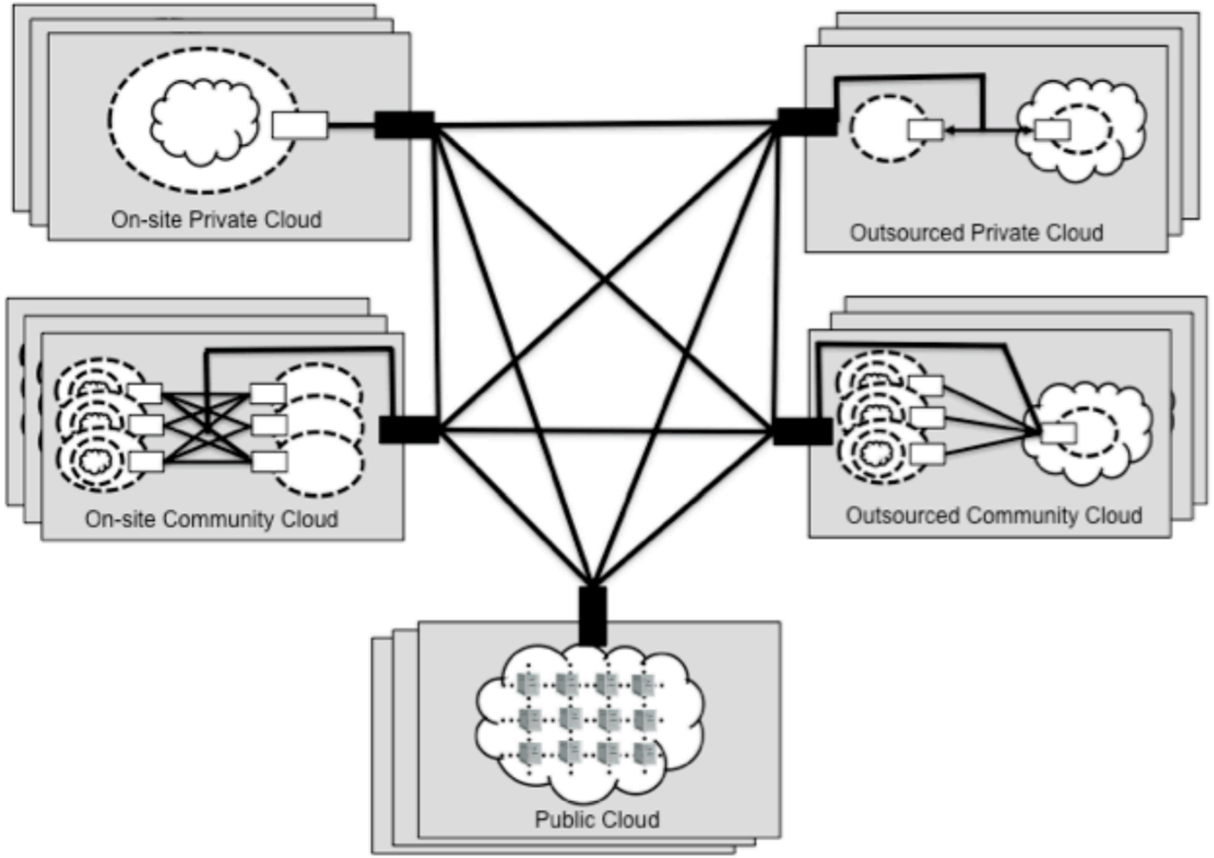
Security Posture



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Hybrid Cloud

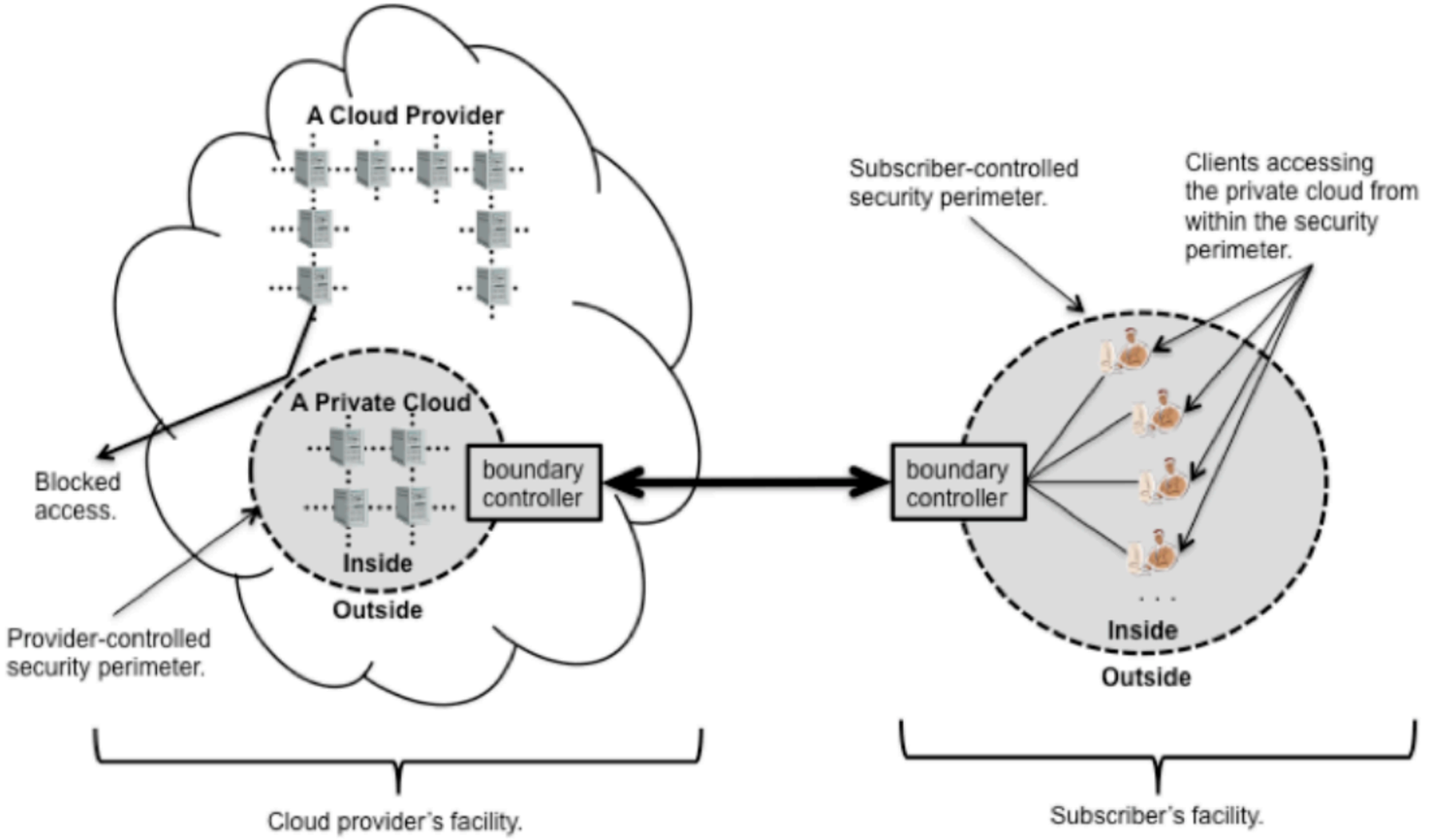
Security Posture



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Hermetically Sealed Cloud

Practical Implementation - Private Cloud Security in a Public Cloud



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

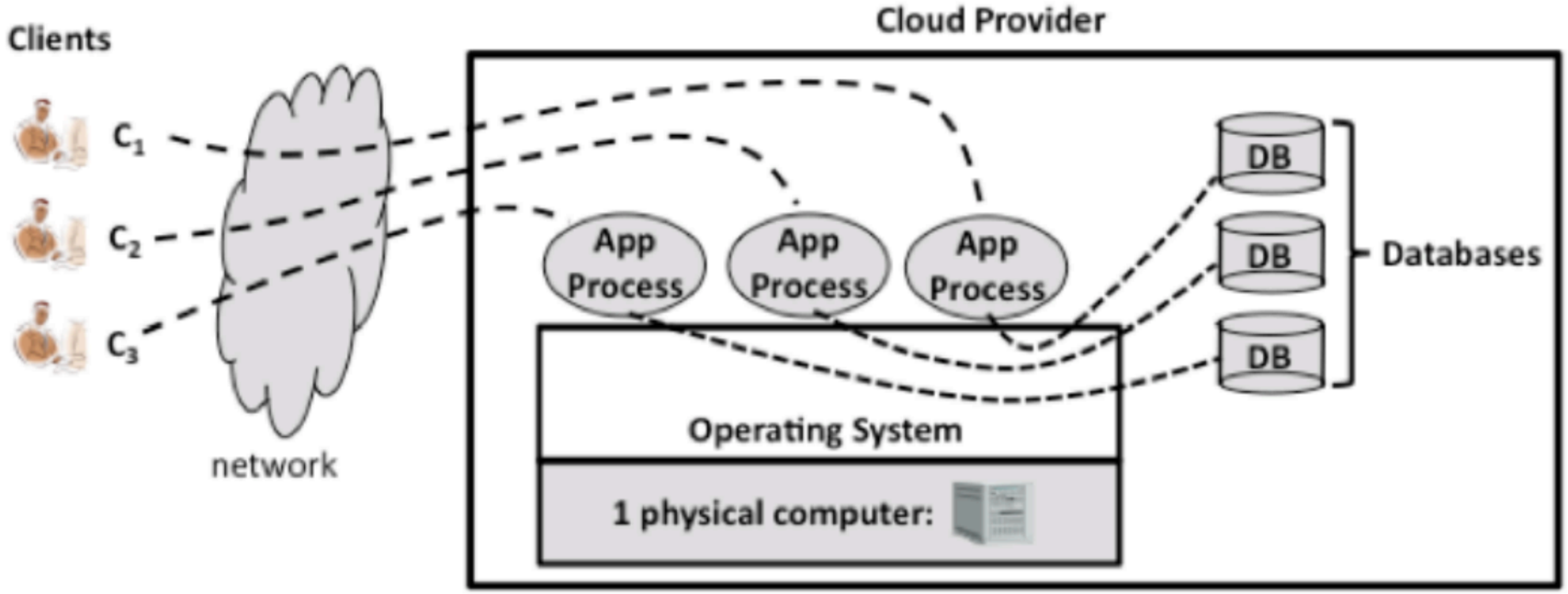
Practical Definition

Cloud Service has 3 service models

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service(IaaS)

Software as a Service

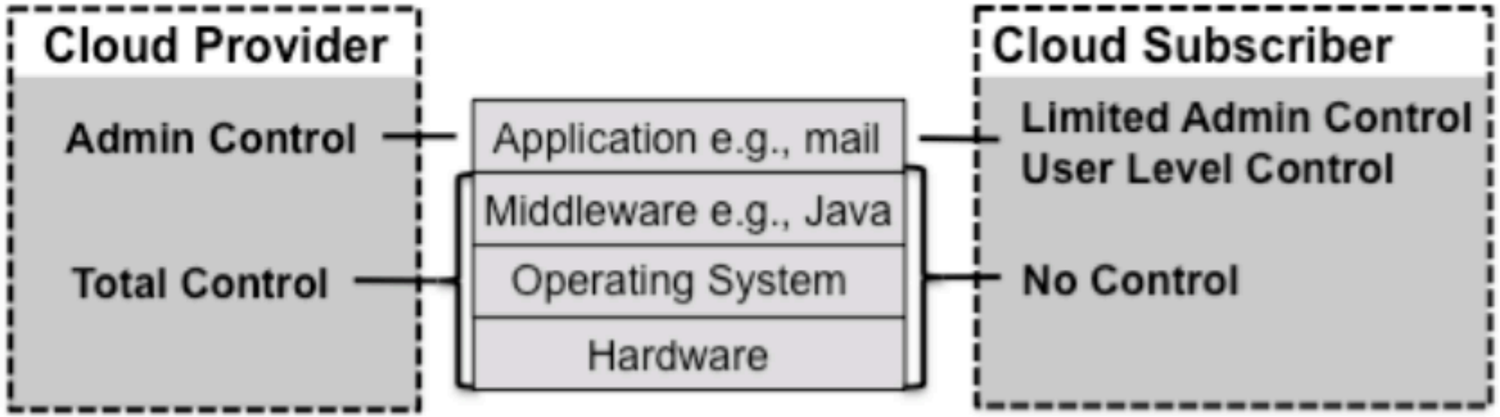
Access Pattern



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Software as a Service

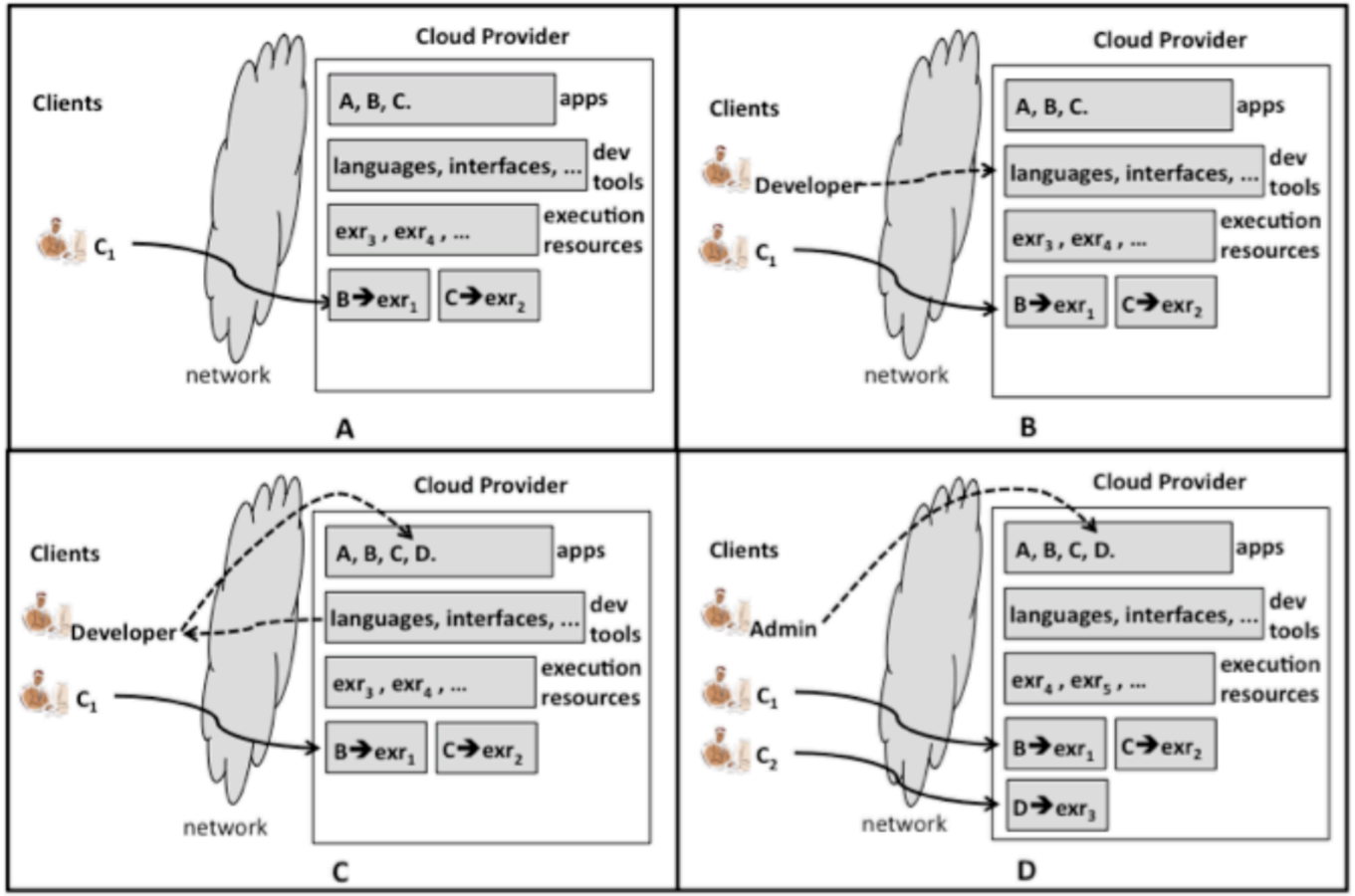
Controls Scope



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Platform as a Service

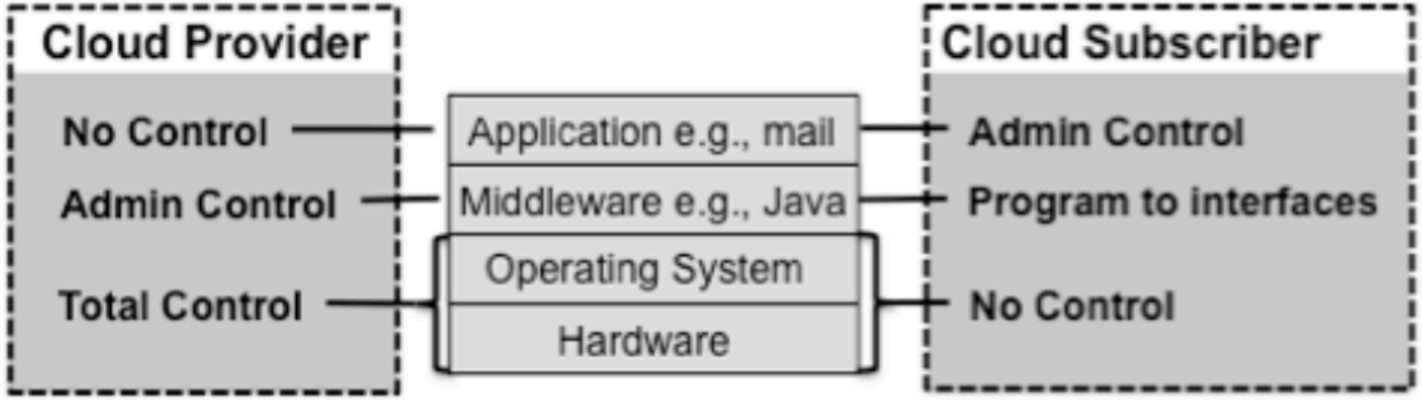
Access Pattern



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Platform as a Service

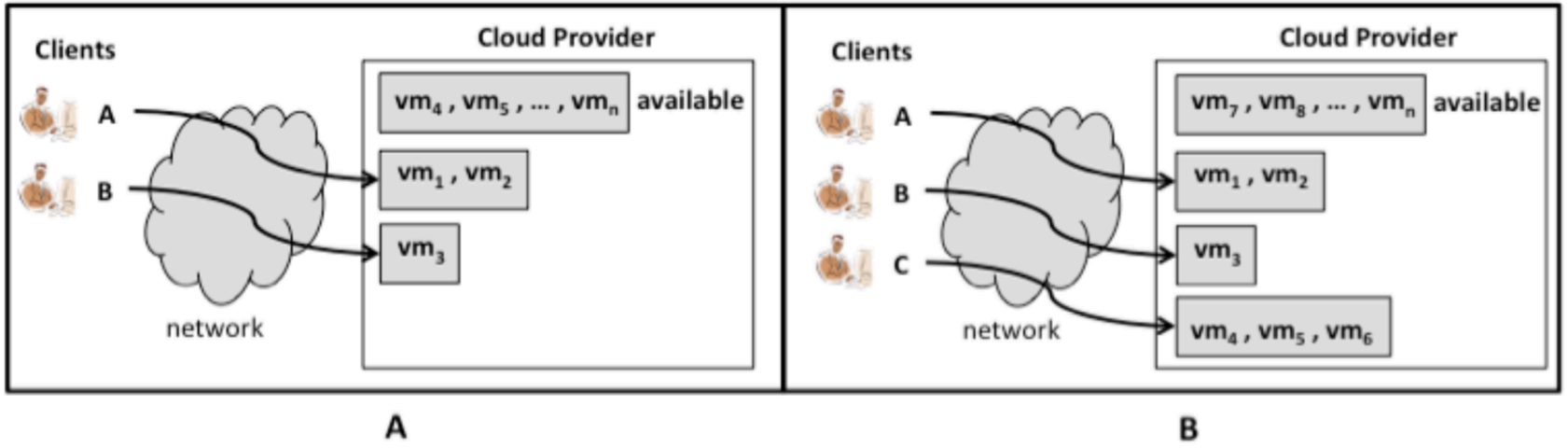
Controls Scope



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Infrastructure as a Service

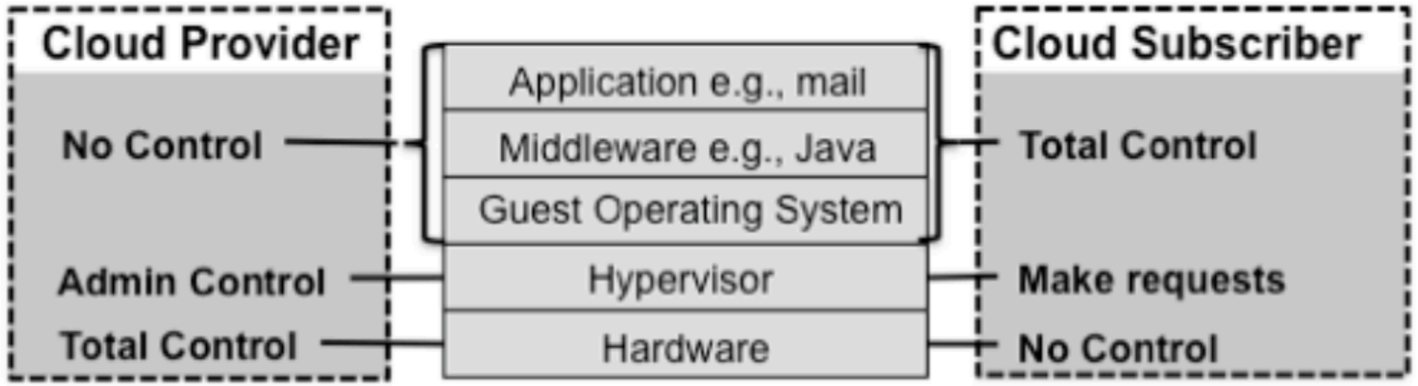
Access Pattern



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Infrastructure as a Service

Controls Scope

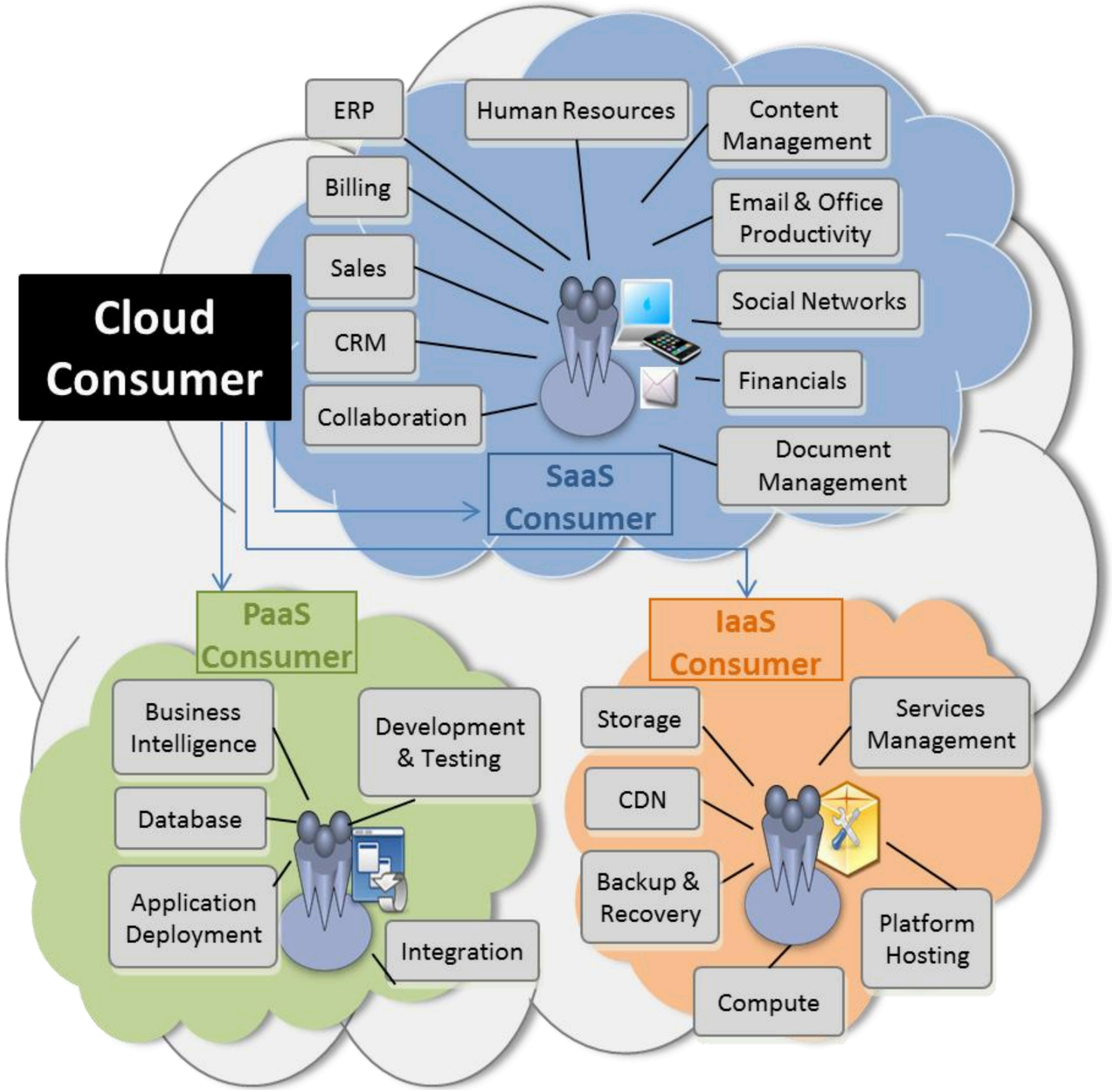


Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

SaaS vs. PaaS vs. IaaS

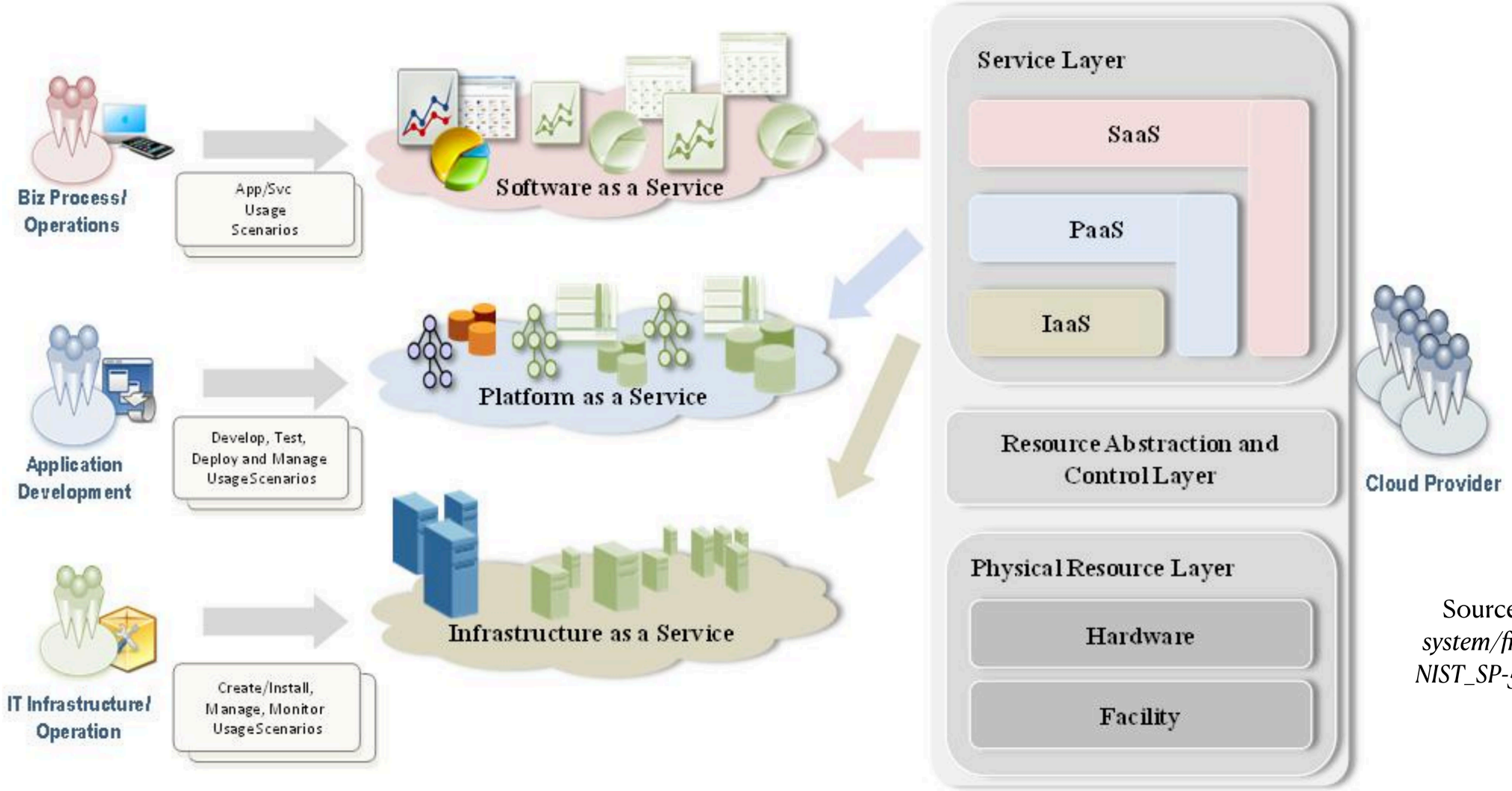
Service Models	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud system.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

SaaS vs. PaaS vs. IaaS



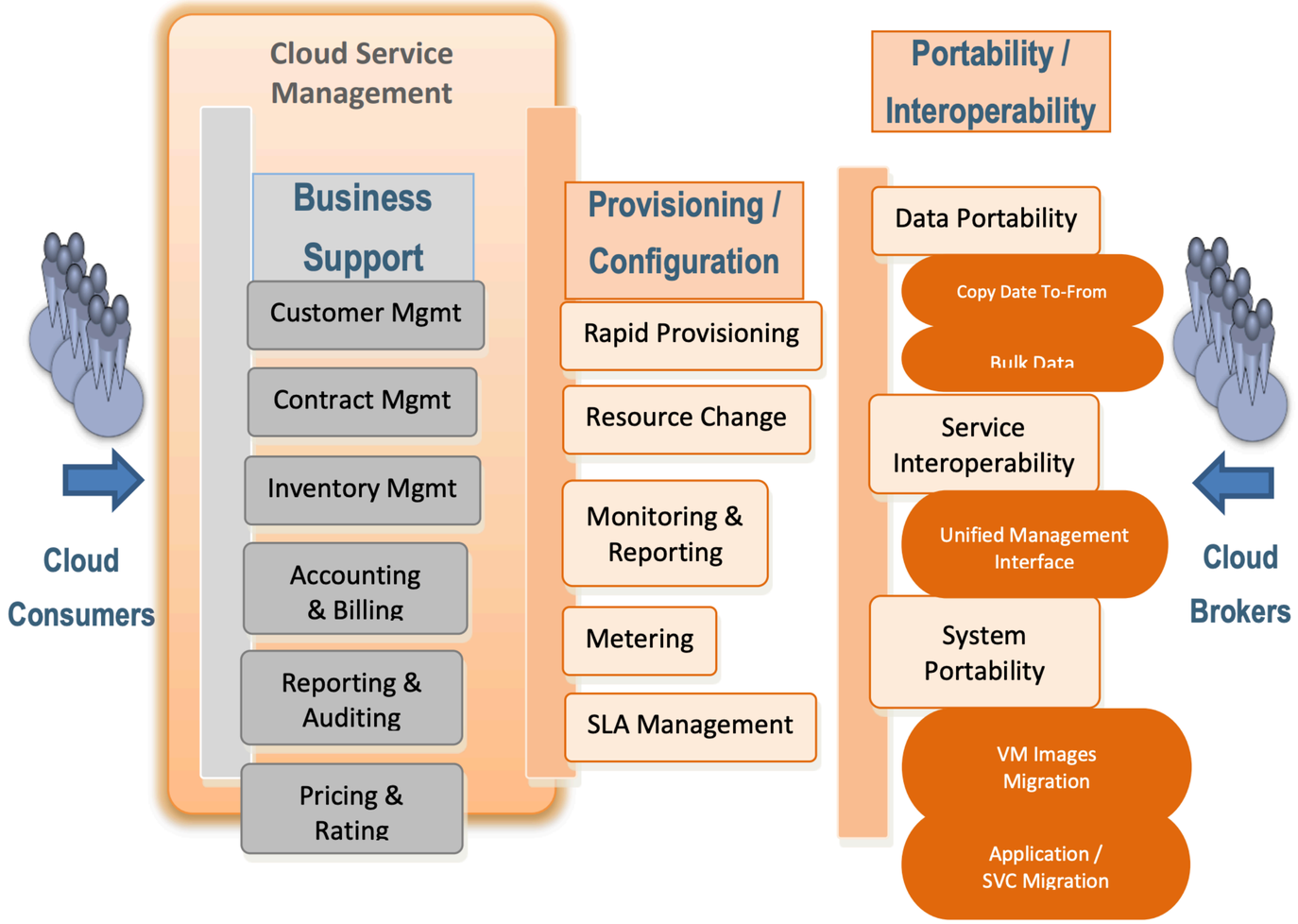
Source: *https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf*

SaaS vs. PaaS vs. IaaS



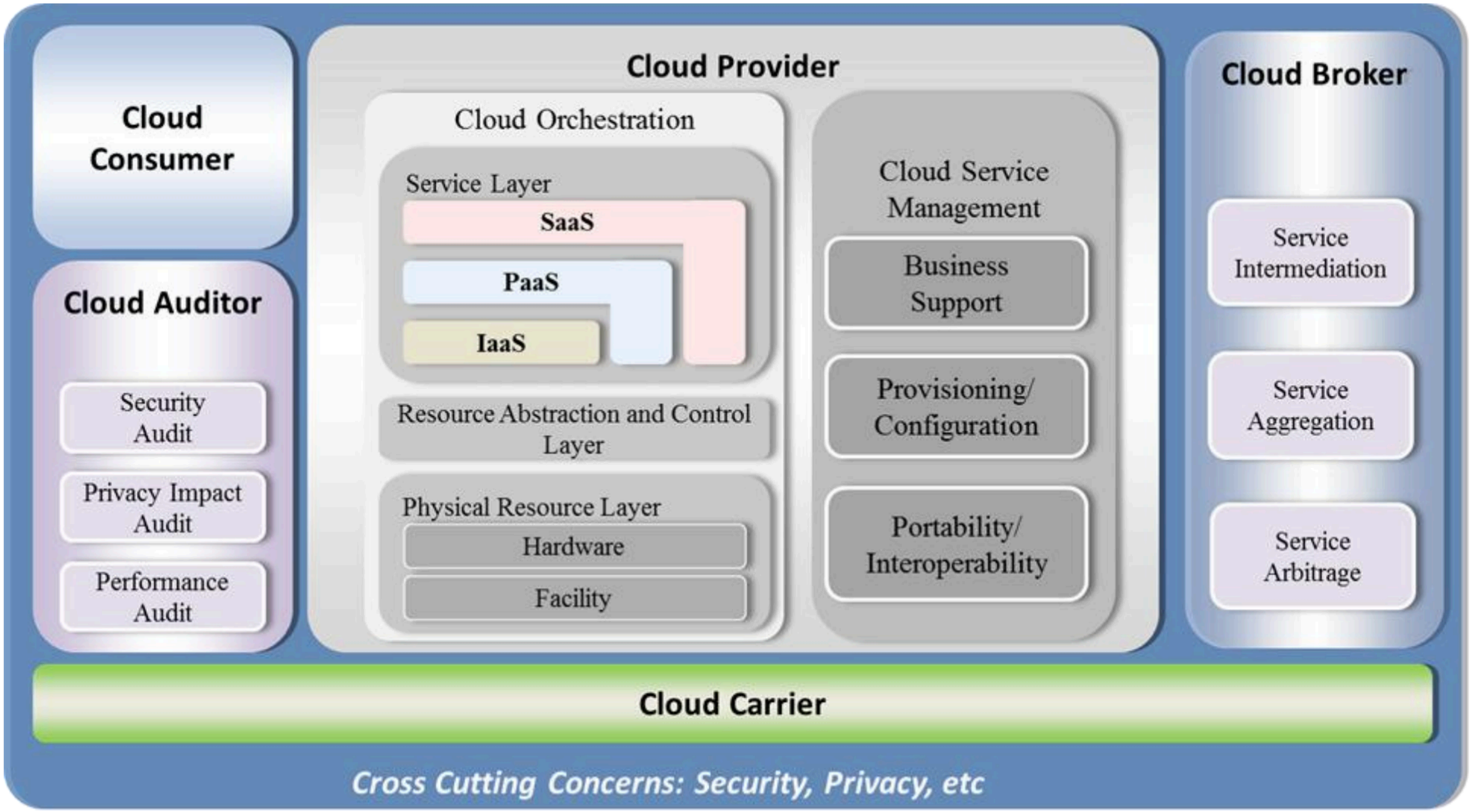
Source: *https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf*

Cloud Service Management



Source: *https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf*

Cloud Service Management



Source: *https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf*

How to make the application independent of the platform?

- There are multiple approaches. We will use the container model.
- A container embeds all the dependencies and resources.
- We will use the Docker platform as container service.

What is a Docker?

Definition by vendor:

Docker is **a software platform that allows you to build, test, and deploy applications quickly**. Docker packages software into standardized units called containers with everything the software needs to run, including libraries, system tools, code, and runtime.

Let’s get real

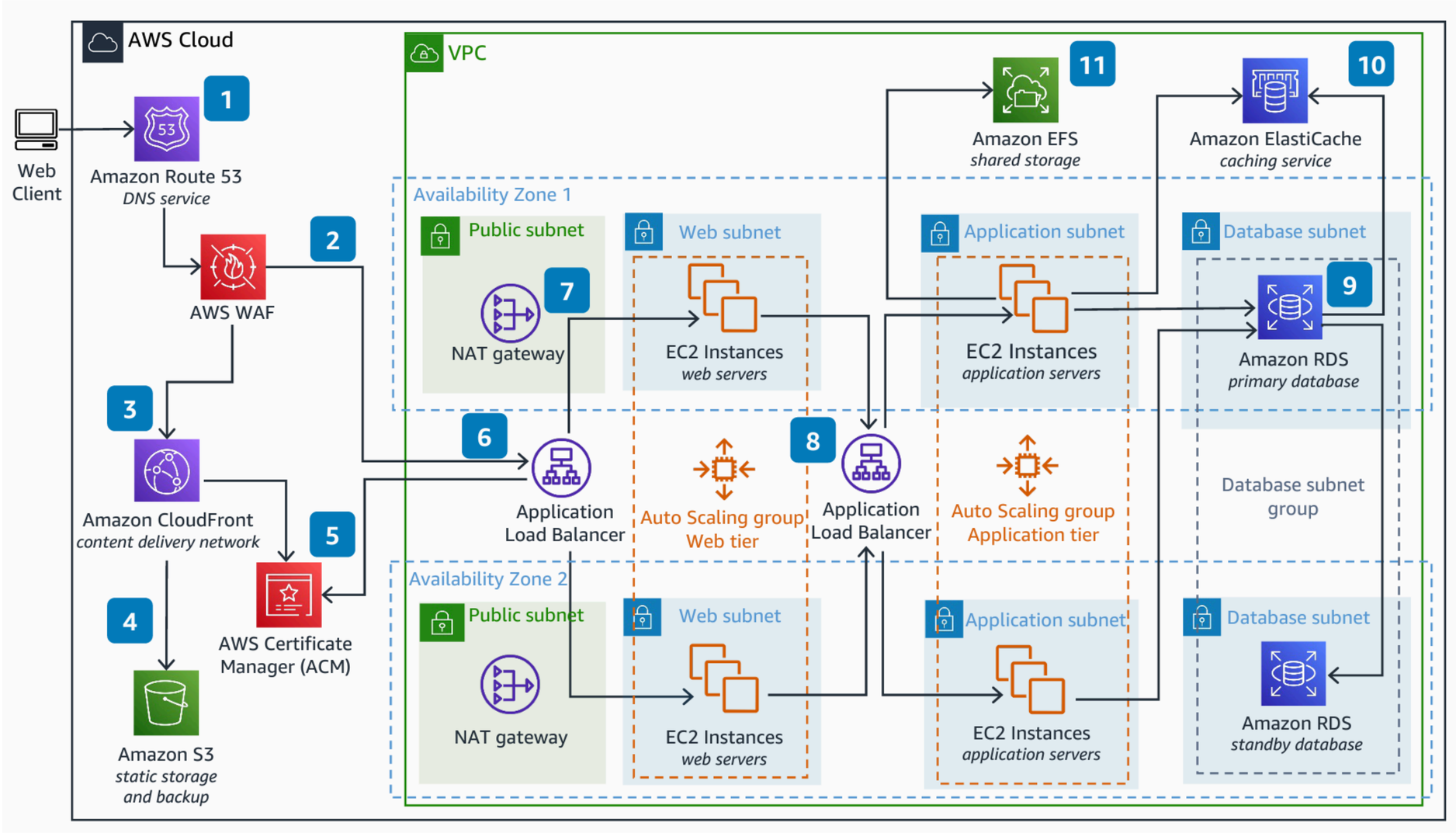
A walkthrough of deployment in AWS

Infrastructure to Security

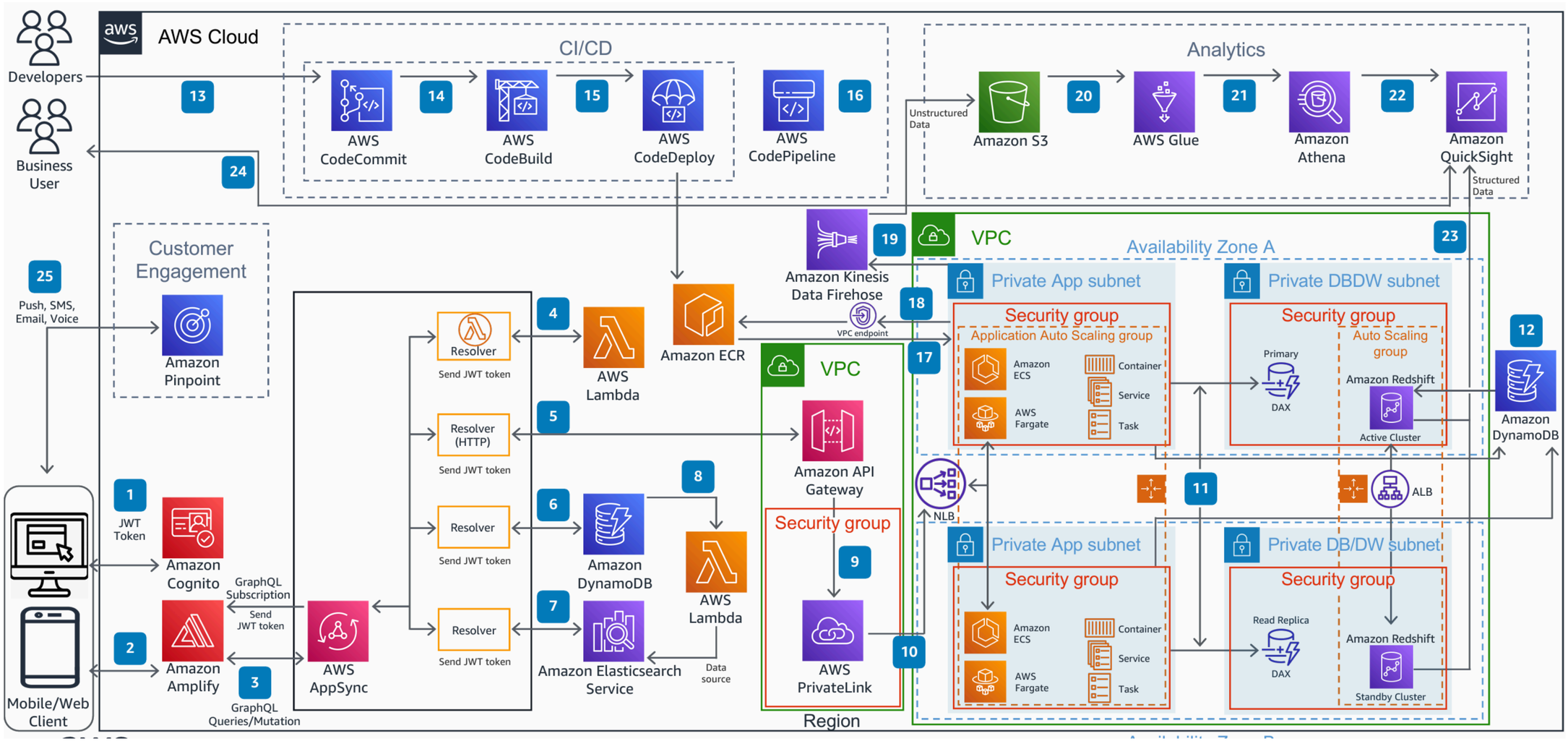
Cloud Reference Architectures

https://aws.amazon.com/architecture/reference-architecture-diagrams

Traditional Web Application in the Cloud



Modern Web Application in the Cloud



Cloud Security Framework

Initial Access	Elevated Access	Expanded Access	Public Access
Phishing	Malware	Botnet	Exfiltration over Web
Watering hole	Keylogger	Command & control	Encrypted channels
Drive-by download	Pass-the-hash	Lateral movement	Non-web exfiltration

Technique	Relation to Internet Domain-based Exploitation
Phishing	The technique uses an Internet domain link to allure victims.
Watering hole	A frequently accessed domain is infected with malware.
Drive-by download	Unintentional download from a domain due to a vulnerability.
Botnet	A network of devices communicates using the Internet.
Command & Control	Communication with attacker-controlled Internet domain.
Exfiltration over Web	Send data to Internet domain using web and email
Encrypted channels	Send data to Internet domain using encryption protocols
Non-web exfiltration	Send data to Internet domain using applications and scripts

How Secure Cloud Computing Works?

Organization	Year	Initial Access	Elevated Access	Expanded Access	Public Access
Target	2013	Phishing	Malware	Botnet	EoW
Sony	2014	Spear Phishing	Pass the Hash	Command & Control	EoW
Yahoo	2014	Spear Phishing	Malware	Lateral Movement	EoW
Anthem	2014	Spear Phishing	Malware	Lateral Movement	EoW
U.S. OPM	2014	Phishing	Malware	Command & Control	EoW
RUAG	2015	Watering Hole	Malware	Botnet	EoW
MS	2015	Insider	NA	NA	EoW
Tesla	2018	Insider	NA	NA	EoW
Apple	2018	Insider	NA	NA	EoW
Capital One	2019	Insider	NA	NA	EoW
G.E.	2020	Insider	NA	NA	EoW
SolarWinds	2020	Vulnerability	NA	C2	EoW

Take 5 to read the Terminology

Terminology

- **Assets**: These are things that an enterprise wants to protect. Generally, there are four types of assets of interest: personnel, facilities, processes, and information.

- **Vulnerability**: This is a way in which an asset can be compromised. Vulnerabilities can be further characterized in terms of the “CIA” of cybersecurity:
  - **Confidentiality**: protecting the secrecy of data
  - **Integrity**: protecting data from unauthorized changes
  - **Availability**: data and the systems are available when needed.

Terminology

- **Threats:** These are the ways in which vulnerabilities can be exploited to cause damage to the asset. Threats may be natural or man-made, accidental or deliberate, random or deterministic.

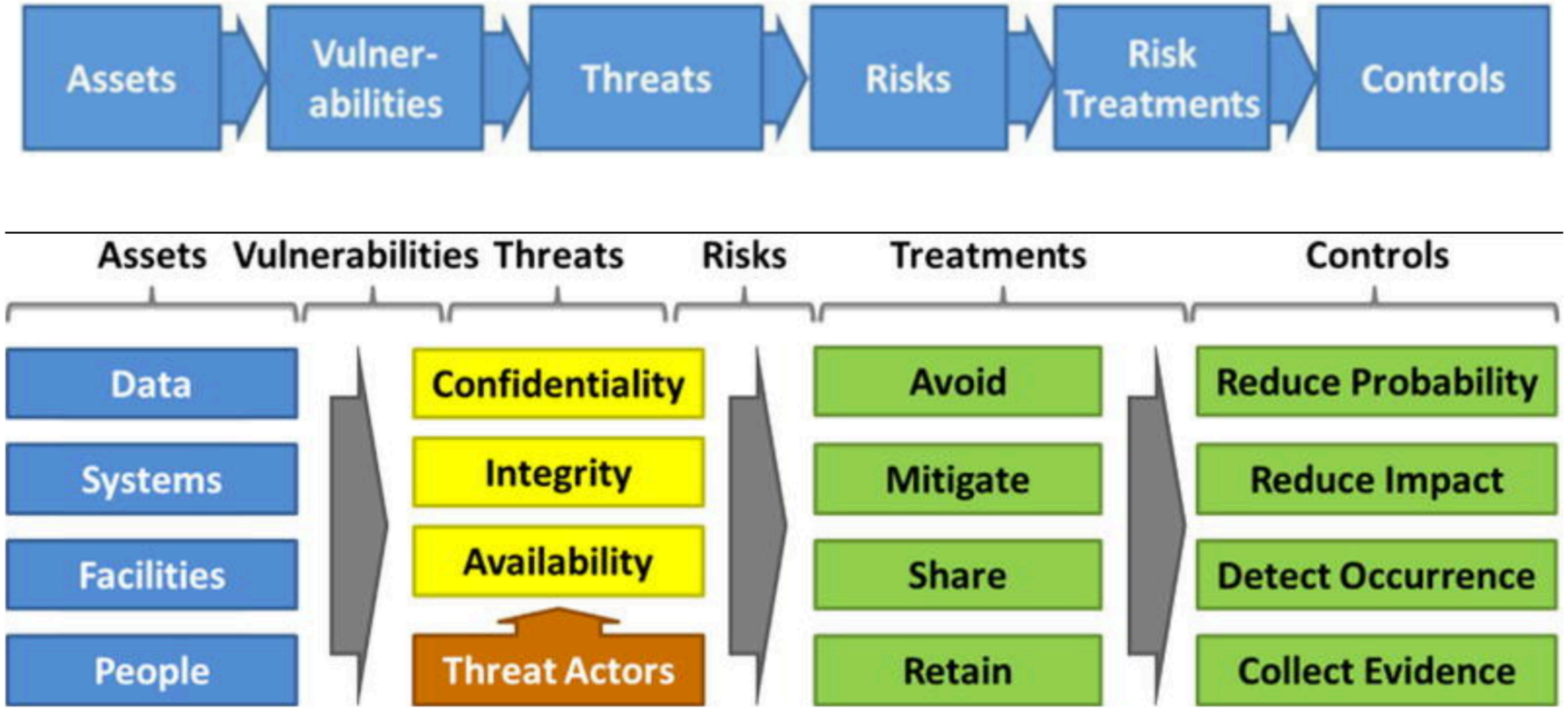
- **Risks:** The amount of exposure or loss to business due to a relevant threat is called risk. A threat against a well-protected area generally produces a low level of risk, while a threat against an area where the enterprise is not well protected produces a high level of risk that must be considered.

- **Risk treatment:** There are a number of ways to handle risk, besides just trying to prevent the bad thing from happening. The main four are (1) Avoid (2) Mitigate (3) Share and (4) Retain.

Terminology

- **Controls**: if the enterprise chooses to reduce the risk, it can apply security “controls.” Security controls can do four things.
  - Controls can decrease the probability the risk will occur or make it more challenging for attackers to execute on the risk.
  - Controls can reduce the influence when the risk does transpire, perhaps limiting the amount of damage that occurs.
  - Controls can detect the occurrence of the risk happening, allowing for active responses to restrain the damage and reduce the exposure.
  - Controls can accumulate evidence that is used to show the operation of security controls, to detect failures of the controls, or to support investigations after an incident has happened

How to secure business assets?



Controls: Different School of Thoughts

1. **Compliance-based security controls:** the origin behind this category depends on the widespread knowledge of “known risk” associated with any new technology or asset introduced into the environment. For example, adding a new operating system such as Windows 10 into the environment requires scanning through public standards and selecting the relevant ones for our corporate environment:

- STIG (https://www.stigviewer.com/stig/windows_10)
- CIS (https://www.cisecurity.org/benchmark/microsoft_windows_desktop/)
- NIST checklist (https://nvd.nist.gov/ncp/checklist/629)

Controls: Different School of Thoughts

2. **Risk-based security controls**: Business typically drives this category of risk controls on the assumption there is “unknown risk” to operating in the world of interconnected corporations and customer-facing business through the Internet.

For example, with the provision of work from anywhere, the business drove the security controls development for the following challenges:

- Users and assets can connect from anywhere. We need a way to dynamically restrict the list of services or the complete access based on location.
- SaaS services providers are growing. Corporate active directory service was not designed to expose granularly the accounts and services based on geographic location, application, environment and the present job of the user.
- Laptops and corporate enabled mobile devices leverage Identity as a service, so we need a design pattern to expose just enough identities, systems and organizational structure to induce trust and leverage existing IAM investment.

Controls: Different School of Thoughts

3. **Capability-based security controls**: A Technology savvy organization typically drives this category of security controls to ensure the cybersecurity engineers and analysts have the following capabilities (i) Incident response (ii) Forensics investigations (iii) Behavior analytics (iv) Anomaly detection. These capabilities are just a sample and they do not represent the complete list.

What are different categories of security controls?

What are different categories of security controls?

1. **Systems Administration**: A functional group that covers secure administration of enterprise infrastructure and security systems and protects system administration channels from compromise.
2. **Network Security**: covers security of enterprise networks and access to network services from the Internet and Intranet.
3. **Application Security**: a group that focuses on the security of enterprise applications using cybersecurity technologies that are appropriate to and tailored for the protection of those applications and their communications.

What are different categories of security controls?

4. Endpoint, Server, and Device Security: provides for the protection of endpoints, servers, and devices that access enterprise data, and protects them from compromise.

5. Identity, Authentication, and Access Management: covers identification, authentication, and access control throughout the identity lifecycle including provisioning, re-certification, and de-provisioning.

6. Data Protection and Cryptography: provisions for the protection of data stored in the enterprise and the use of cryptographic technologies to perform that protection, as well as to support other operations such as authentication, non-repudiation, and data integrity.

What are different categories of security controls?

7. Monitoring, Vulnerability & Patch Management: covers the regular monitoring of security infrastructure, scanning, and analysis of vulnerabilities in that infrastructure, and management of patches and workarounds to address those vulnerabilities.

8. High Availability, Disaster Recovery, and Physical Protection: provides for the protection of availability in the enterprise, including making systems highly available, recovering from disasters, and physically protecting facilities, people, systems, and data.

9. Incident Response: provides for the investigation, response, and recovery of incidents that are identified through monitoring of the enterprise.

What are different categories of security controls?

10. Asset Management and Supply Chain: covers accounting of enterprise assets, procurement information associated with them, their life cycles, changes, and ensuring orderly and secure disposal without compromise of enterprise data or security.

11. Policy, Audit, E-Discovery, and Training: focuses on policy oversight of controls and audit of their effectiveness, support for legal e-discovery activities, and training of staff in proper security policies and practices.

How to design controls by threats?

Zero Trust Architecture

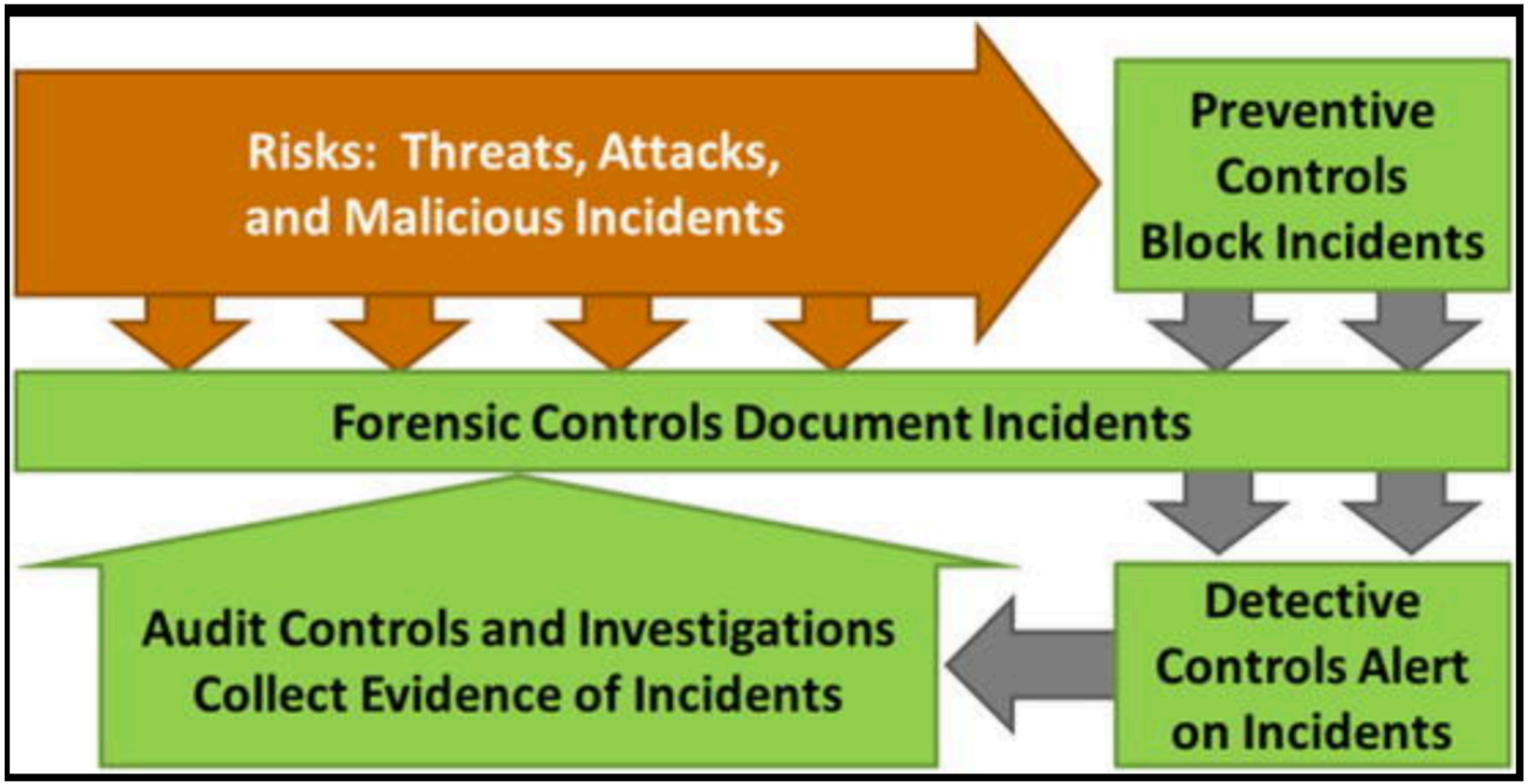
https://csrc.nist.gov/publications/detail/sp/800-207/final

MITRE Framework

https://attack.mitre.org/versions/v11/matrices/enterprise/

How to design controls by threats?

Controls by Type of Attack



Controls by Type of Attack

- **Preventive Controls** block the threat and prevent incidents from occurring altogether
- **Detective Controls** detect when the risk has transpired and generate alerts that can then be acted upon
- **Forensic Controls** collect records of activities related to the risk and can be used to produce artifacts to help the operation of detective controls, investigations of incidents, and audits of controls to verify their operation and effectiveness
- **Audit Controls** investigate for the presence of the risk, incidents associated with the risk, and the operation of controls that mitigate the risk

Impact of Controls

	Preventive	*Detective*	*Forensic*	*Audit*
Block Attacks?	Good	Medium	Poor	Poor
Detect Attacks?	Poor	Good	Poor	Medium
Operational Impact	High	Low	Low	Low
Investigate Attacks?	Poor	Medium	Good	Good
Cost to Implement	High	Medium	Medium	Low
Cost to Operate	Medium	High	Low	Medium
Flexibility	Poor	Poor	Medium	Good

What are typical web application controls?

Functional Areas	Preventive Controls	Detective Controls	Respond & Recover
Network Security	• Web Application Firewall • Intrusion prevention system	• Netflow data • Packet capture data	• Update firewall rules
Application Security	• Run-time app self-protection (RASP) • XSS protection • Static & dynamic code analysis	• Web access logs • Database access logs	• Patch vulnerabilities and republish the app
Endpoint, Server, and Device Security	• Host firewall enforcement • Host Intrusion prevention	• Systems events & logs • Endpoint detection & response	• Endpoint Detection & Response

Functional Areas	Prevent	Detect	Respond & Recover
Identity, Authentication, and Access Management	• Multi-factor authentication • Timed privilege access	• Directory service • Behavior analytics • Anomaly detection	• Change credentials • Conditional access controls
Data Protection and Cryptography	• TLS security • HTTP Strict Transport Security	• TLS mismatch detection • User-Agent inspector	• Re-encrypt the data • Change certificate key length
Monitoring Vulnerability and Patch Management	• Blackbox & white box testing • Fuzzing	• Web app security scanner	• Patch the systems

Homework

Homework - 1

Design a start-up infrastructure for running a web service with sensitive data. We will discuss various frameworks and security controls you could use during the class.

A sample reference for homework expectations:

https://blogs.lt.vt.edu/hfsecurity/