Understanding Security Concepts in an Enterprise Environment

Data Masking

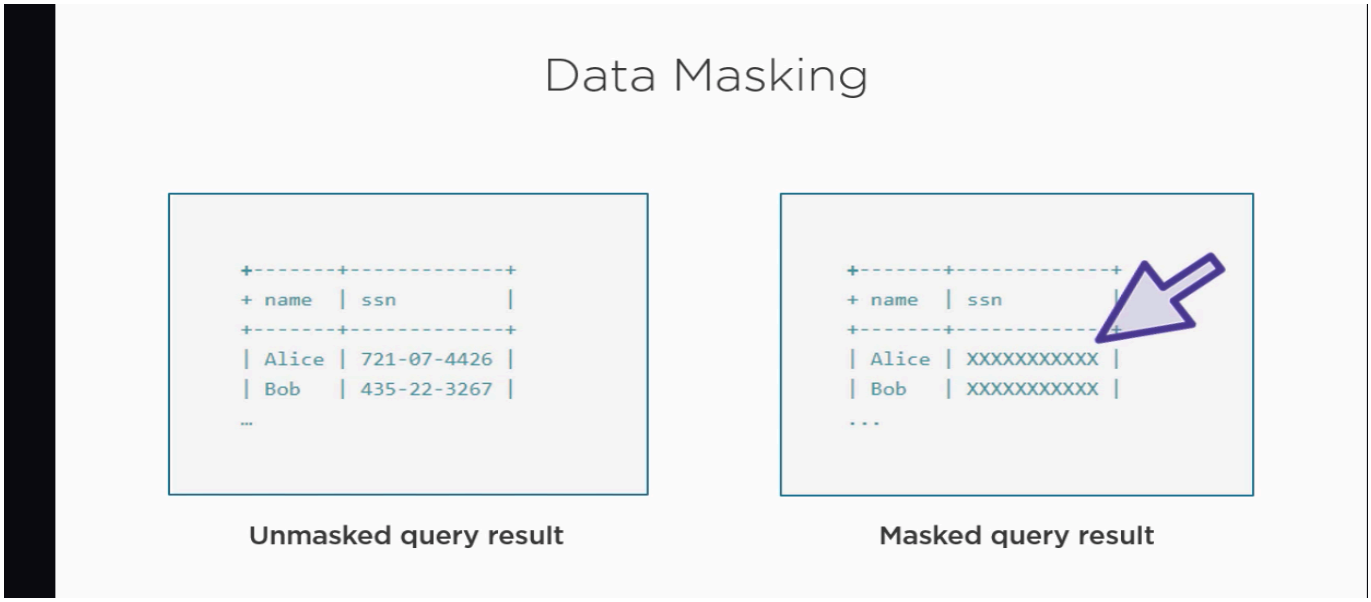
-Can be done within applications, databases, etc at the individual record, row, or table.

Intention: To hide important data from those who should not access it.

IP Address masking:

Network Address Translation (NAT) enables private IP addresses to be masked behind a proxy or firewall.

Data masking example:



Masked users social security numbers to make them not available to users who should not see it.

Tokenization:

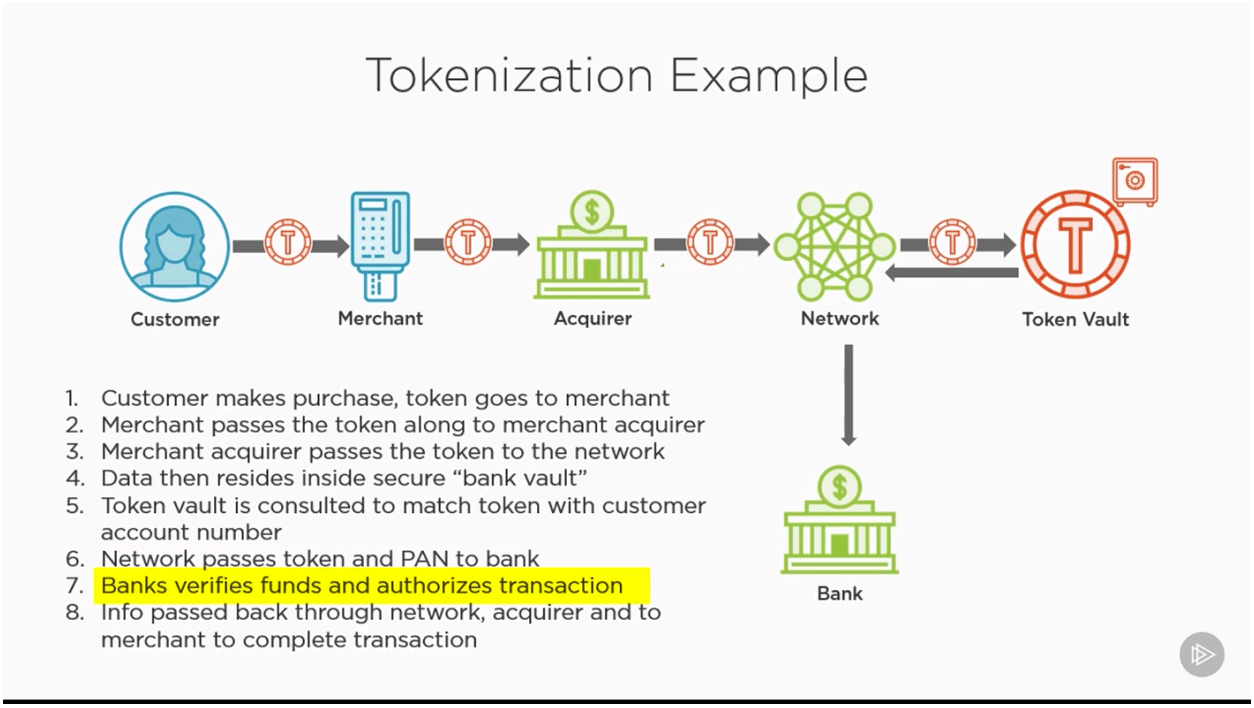
Replacing sensitive data with non sensitive equivalent.

-can be single use, multiple uses, cryptographic, or non cryptographic, irr/reversible, etc.

Examples:

- High-Value tokens (HVTs) can be used to replace things like primary account #s (PAN) on credit card transactions, can be bound to specific devices.
- Low- value tokens (LVTs) similar to HVTS but needs the underlying tokenization system to match it back to the actual PAN (primary account number)

Visualization of Tokenization:



Digital Rights Management (DRM)

Suite of tools to limit how/where content can be accessed.

Goal:

Prevent content from being copied

Restrict what devices content can be viewed on.

Examples: MP4, MP3, MOV, etc.

Hardware Based Encryption (TPM and HSM)

-TPM (Trusted Platform Module):

A hardware chip embedded on the computer's motherboard. Used to store Cryptographic keys used for encryption.

-HSM (Hardware Security Module):
Are removable or external devices that can be added later. Both are used for encryption using RSA keys.

Cloud Access Security Broker:

Security Policy Enforcement points

- Either on prem or in cloud
- Placed b/t the company (consumer) and the cloud provider.
- Ensures policies are enforced when accessing cloud based assets.

Examples of things controlled:

-Authentication/ Single sign-on
-Credential mapping
-Device profiling
-Logging

Security- as-a-Service (SECaaS)

Cloud provider that can offer security services cheaper and more effective than on-prem.

Why Cloud and not on prem:

- Authentication
- Anti-Virus/malware/Spyware
- Intrusion Detection
- Pen Testing
- SIEM (Security Incident Event Management)

Difference b/t Security as a service (SECaas)and Cloud Access Security Broker (CASB):

So What's the Difference?

SECaaS

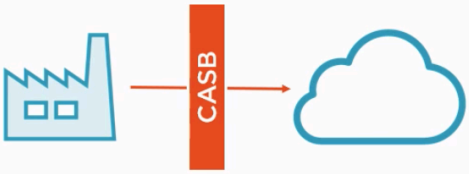
Cloud providers offer their services, infrastructure, resources, etc., to extend into a company's network

They provide the security services typically at a cheaper TCO than the customer organization can

CASB

Sits between a customer's network and the cloud, acting as a broker or services gateway

Enforces the customer organization's policies when accessing anything in the cloud



Recovery

Example: Can users recover their own passwords?

-If so: ensure security Questions are not easily discovered through social engineering.

- Policy defines if a user needs to call a help desk or have self service options.

Secure protocols:

SSL/TLS

-Secure Sockets Layer/ Transport Layer Security

- Can allow encryption or enable.

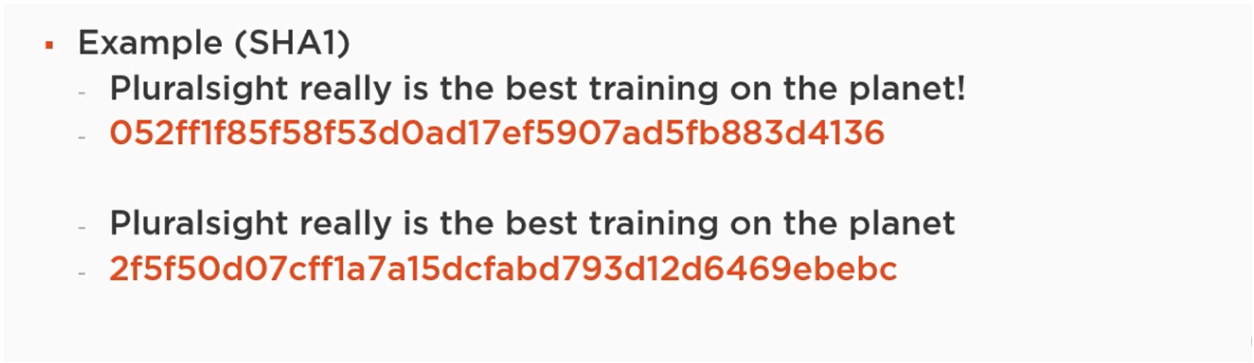
- TLS = newer + based on SSL.
- Adds confidentiality and data integrity by encapsulating other protocols.
- TLS venison 1.2+ should be used wherever possible.

Hashing

A mathematical Algorithm applied to a file before or after transmission.

-if anything within the file changes, the hash will be completely different.

Types: MD5, SHA1, SHA2.



Comparing hashes = good way to verify the integrity of something downloaded.

API (Application programming interfaces) Considerations:

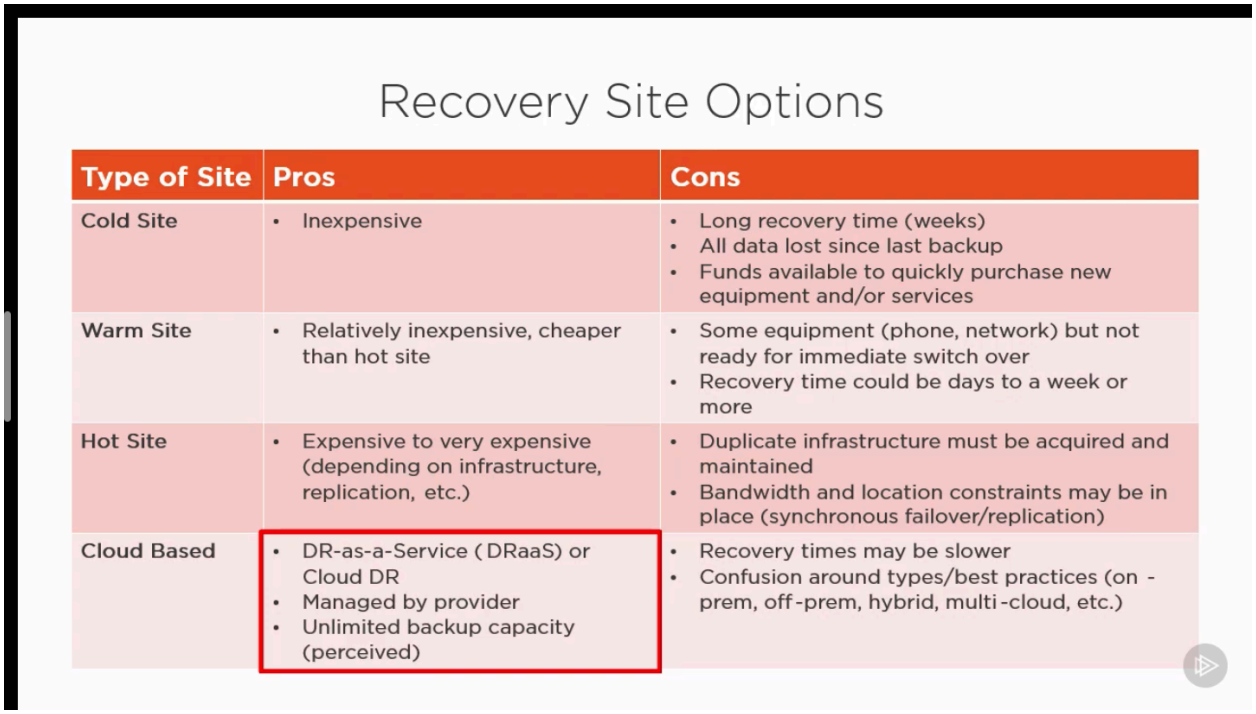
API Gateways can perform load balancing, virus scanning, orchestration, Authentication, data conversion and more.

Users do not directly interact with API. API is handled behind the scenes. What changes = interaction with API.

Examples:

- Advanced Security
- Mediation
- Custom API
- Load Balancing
- Caching
- Request Shaping
- Transport Security

Recovery Site Options



Recovery Site Options

Type of Site	Pros	Cons
Cold Site	• Inexpensive	• Long recovery time (weeks) • All data lost since last backup • Funds available to quickly purchase new equipment and/or services
Warm Site	• Relatively inexpensive, cheaper than hot site	• Some equipment (phone, network) but not ready for immediate switch over • Recovery time could be days to a week or more
Hot Site	• Expensive to very expensive (depending on infrastructure, replication, etc.)	• Duplicate infrastructure must be acquired and maintained • Bandwidth and location constraints may be in place (synchronous failover/replication)
Cloud Based	• DR-as-a-Service (DRaaS) or Cloud DR • Managed by provider • Unlimited backup capacity (perceived)	• Recovery times may be slower • Confusion around types/best practices (on-prem, off-prem, hybrid, multi-cloud, etc.)

It = important to have data centers that are dispersed in case of disaster.

Honeypots

- Computers or hosts that are set up TO become targets of attacks.
  - Appear to have sensitive info
  - Monitored to identify hackers or learn their methods and techniques.

- HoneyFiles
  -Similar but applies to individual files designed to entice bad actors and monitor their activities.

Honeynets

- Similar to Honeypots but larger in scale
- Network setup intentionally for attack so the attackers can be monitored/studied.
- Honeywall = Firewall Honeypot

Fake Telemetry:

- Applications can pretend to be useful utilities

Examples: Antivirus and antimalware fakes

Claims to find fake viruses/malware, shows report data, etc.

Tricks users into paying for premium support, virus removal.

Can install additional malware

DNS Sinkhole

- DNS server that supplies false results.

- Can be used constructively or maliciously
- Good use example: DNS sinkhole high up the DNS hierarchy to stop a botnet from operating across the internet
- Bad use: Malicious actors redirecting users to a malicious website.

Understanding Virtualization and Cloud Computing

Cloud = Storage that = external to a company's data.

- Accessible from outside network
- Can be simply storage or automation.

Cloud Storage:

- Access controls
  -Policy around who can access what data
  -Audit third party providers to ensure their security practices are at least as stringent.

- Is data copied to data centers and where are they located?

Cloud Computing:
Virtualization of infrastructure, platform and services.

-Reduced time to market
-Automation and self service
-Increased speed to develop and deliver

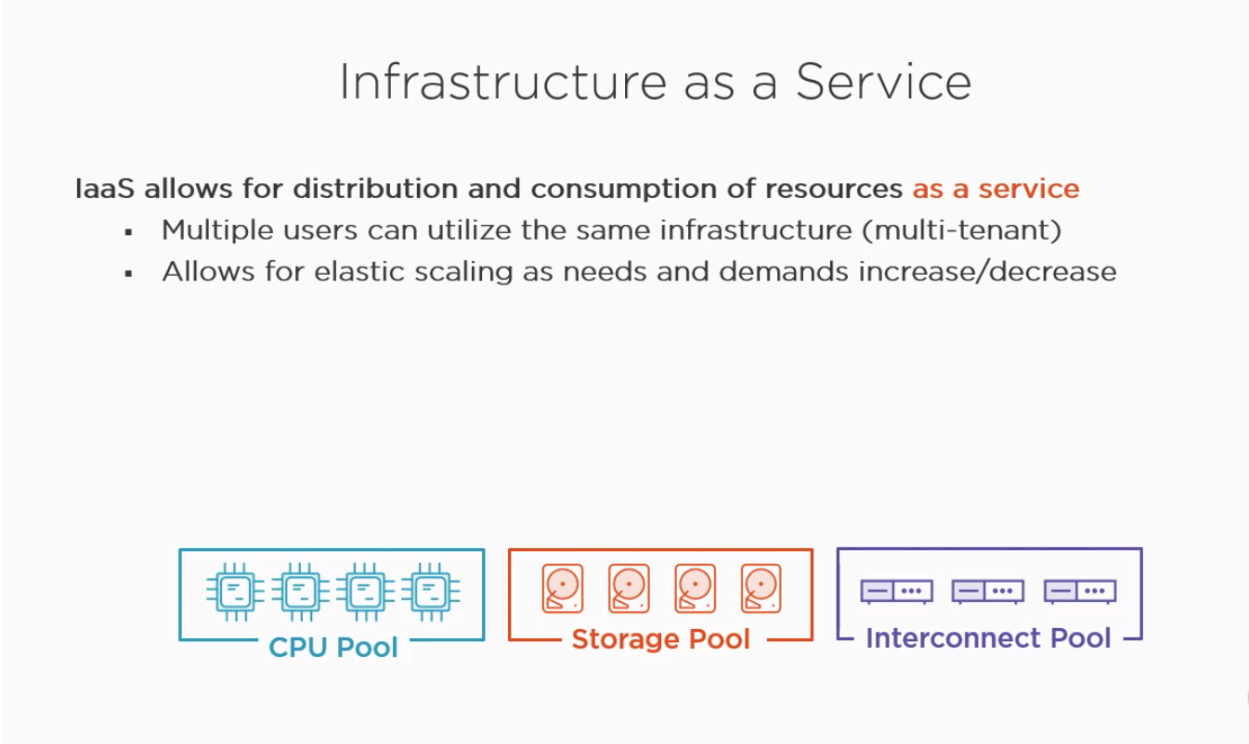
<u>Types of Cloud Computing:</u>

Infrastructure as a service (IaaS; “I-as”)
Platform as a Service (PaaS; “pass”)

Software as a Service (SaaS; “Sass like sassy”)

HA= High availability
DR= Disaster Recovery

Infrastructure as a Service (Iaas)



-Pay for only what you need and not more or less. It prices things from a utility model and shift from Capex to Opex

-IaaS and Automation is leveraged and is self service, enabling aa customer to select their hardware and software configurations.

Platform as a Service (PaaS)

A Paas environment = computational resources that can be created and configured.

Is multi tenanted.

Examples of Paas Providers:

-AWS Elastic Beanstalk
-Windows Azure
-Heroku
-Force.com
-Google App Engine
-Apache Stratos
-Openstack (redhat)
-Cloud Foundry (Pivotal)

Software as a Service

SaaS
-App that are provided on demand
-No Setup, installation, configuration required.

Examples: Salesforce, Office 365, Google Apps

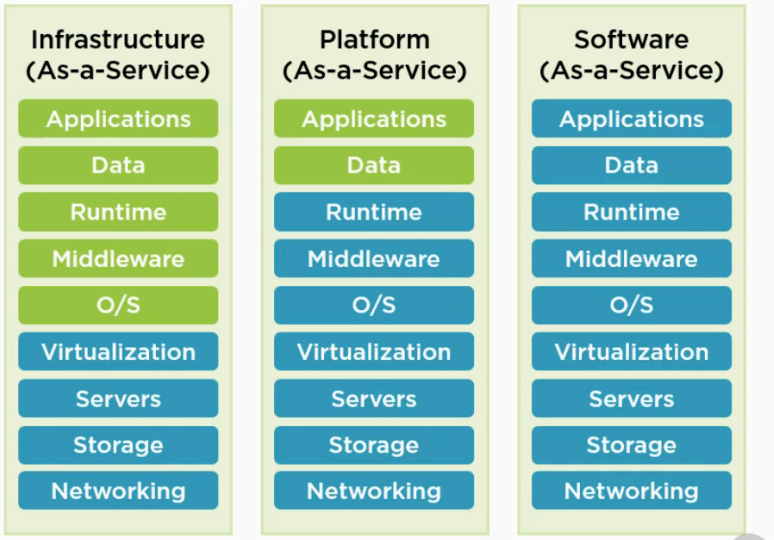
IaaS, PaaS and SaaS Differentiators

Infrastructure-as-a-Service
- You manage the OS up

Platform-as-a-Service
- You manage the DATA up

Software-as-a-Service
- You manage nothing

If you're running a Private Cloud, then you are the "vendor" and the customers are the managers



You Manage Managed by Vendor

Managed Service Provider (MSP)

MSP’s deliver Services that are either on prem at site of customer, in the MSP’s data center or in a third party data center.

-Network
-Application
-Infrastructure
-Security
-An outsource IT and provide 24/7 monitoring.

On-prem vs. Off-prem

On-prem	Off-prem
You own the infrastructure	Don't own the equipment
More control on customization and non-standard builds	Managed by provider
More direct control over policies, management, administration	Less control over customization, policies and overall administration
Continual upgrade/refresh of infrastructure	No lifecycle or maintenance activities
Capital expenditure (CAPEX) typically	Patching and security managed by provider
	Operating expense (OPEX) typically

Fog computing

Fog computing extends cloud computing to the network edge.

- Edge computing (processing data local to where it was created) = a subset
- Compromised of compute, Network, and storage

Edge Computing

- Edge + fog = sometimes interchanged
- Is a subset of fog (storage, compute, and network close to the edge)

Virtualization

Taking the capabilities and "personality" of a physical device and converting to a virtual representation

- Can perform the same functions as its physical counterpart
- Lower infrastructure costs
- Increased licensing costs (hypervisor license)

Only buy what is needed but increases licencing cost

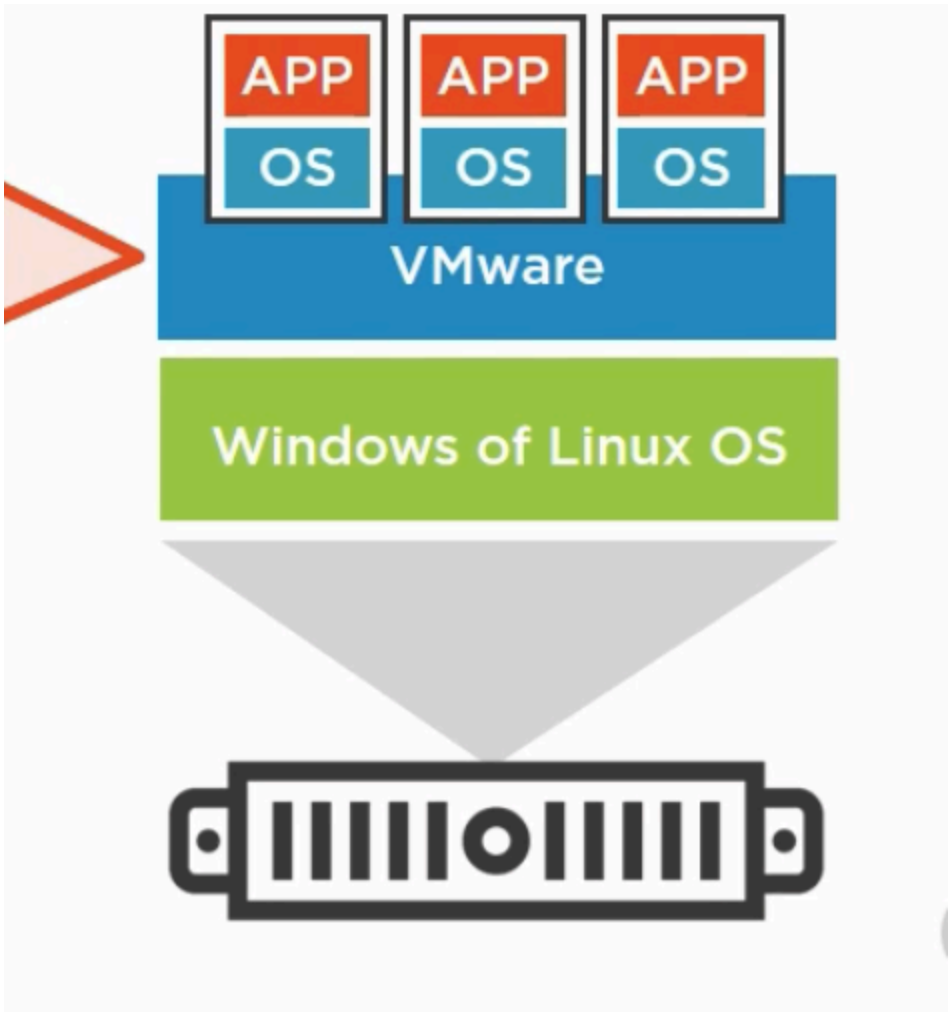
Types of virtualized servers:

Type 1:
Hosts run on bare metal servers and guests run on the host.

Example: Linux, etc,

Type 2:
Hosts run on top of the OS and guests run inside the host. (i.e. Vmware workstation or Virtual Box)

Runs at third layer above the hardware

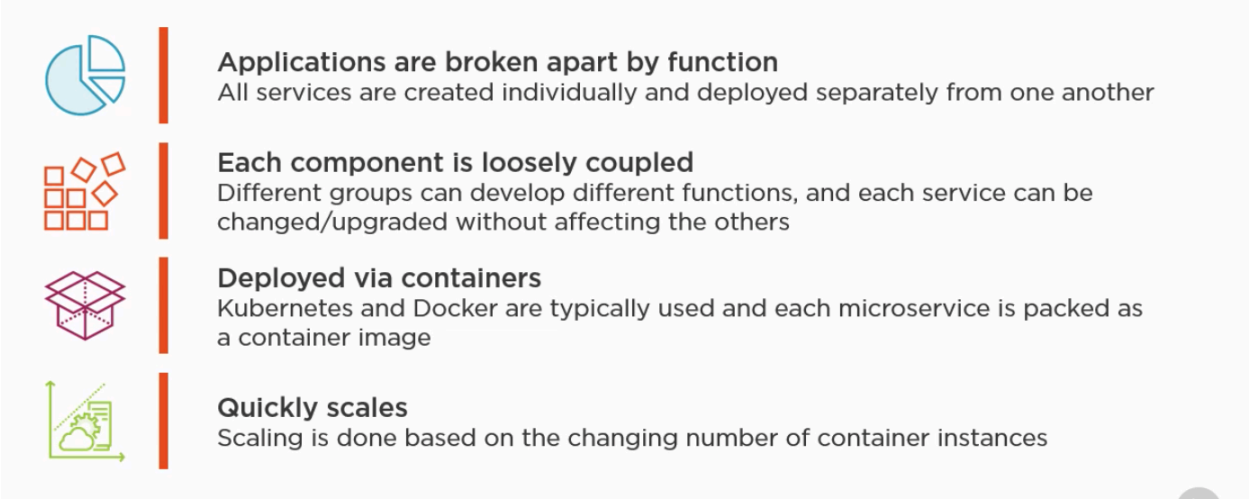

APP
OS
APP
OS
APP
OS
VMware
Windows of Linux OS

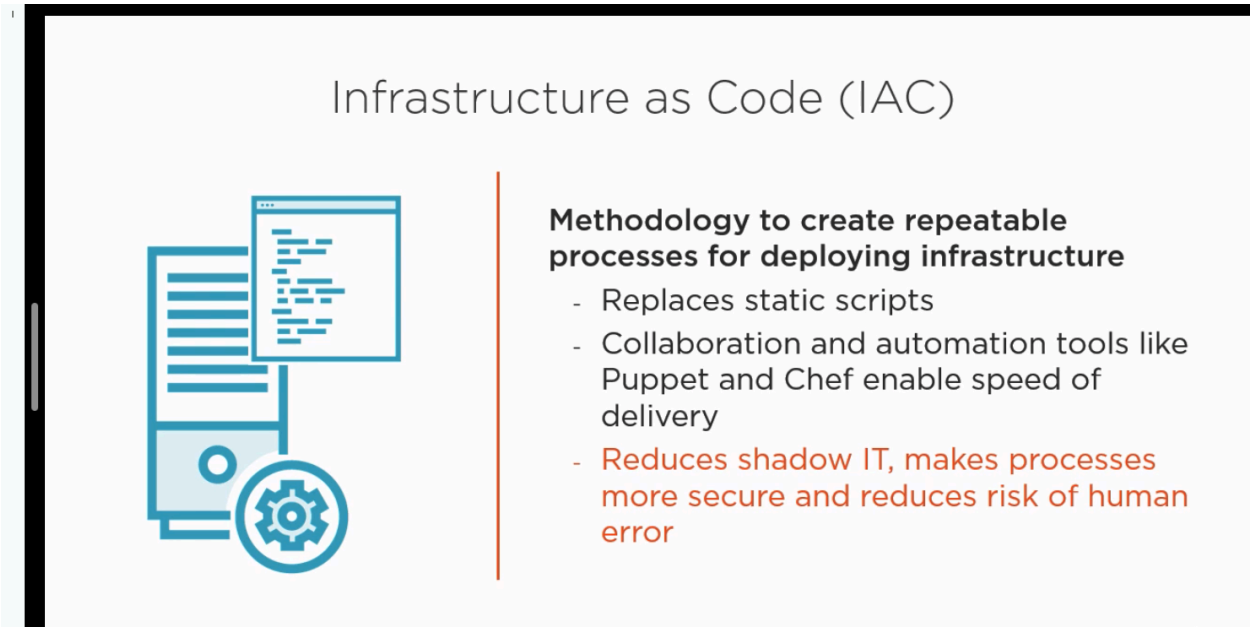
Container Based:

Operating System Virtualization:

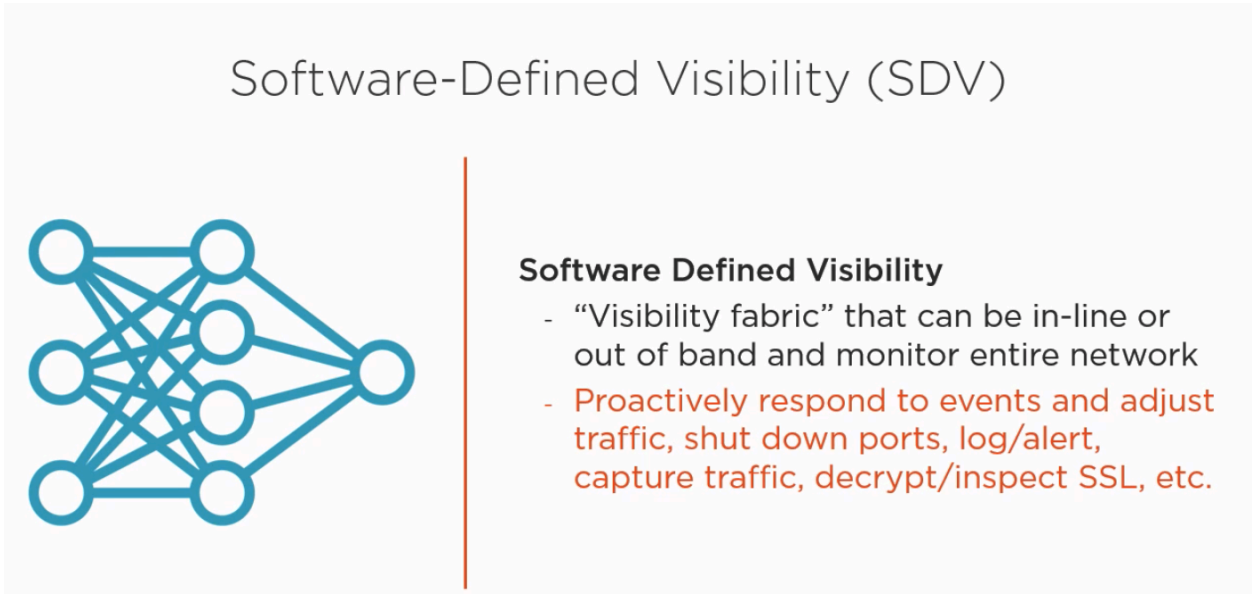
-lightweight
-containers can start in milliseconds
-Shares OS kernel
-Contains App and binaries

Microservices Key Points:





Software Defined Visibility (SDV)



Serverless architecture

- Underlying infrastructure is abstracted from user (IaaS, PaaS)
- Only the code is managed/deployed and can scale at the individual call level
- Only pay for the times the function is called vs. paying for an application to be always on and waiting for requests

Serverless providers:

- AWS Lamba, Microsoft Azure Functions and Twilio Functions