ESTD 1845

QUEEN’S
UNIVERSITY
BELFAST

Cloud/ Virtualization Security

Dr. Sandra Scott-Hayward

CSC3064 Lecture 19

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- □ What is cloud computing?
- □ Cloud security threats and countermeasures
- □ Cloud Security Guidance
    - □ Virtualization and Containers
    - □ Incident Response
    - □ Security as a service (SecaaS)

References:

Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2014.

Mogull, Rich et al. "Security Guidance for critical areas of focus in Cloud Computing V4.0", CSA (Cloud Security Alliance), USA. (2017).

Brook, J-M.C, et al. "The Treacherous 12 – Top Threats to Cloud Computing + Industry Insights", CSA, USA. (2017).

QUEEN'S UNIVERSITY BELFAST

Cloud Security

“Fancy Hare” - https://www.youtube.com/watch?v=u0mzjn-D0Qo

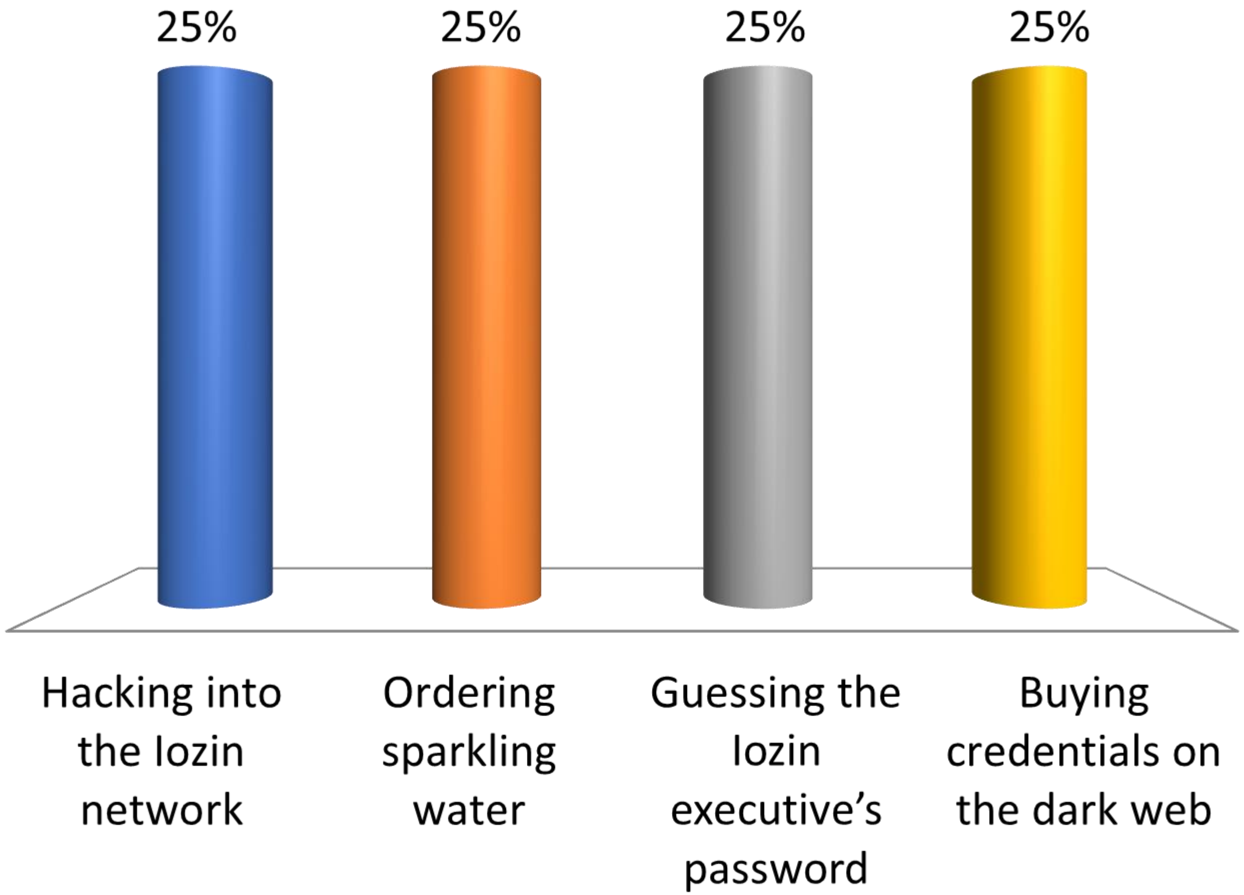
What was the first step in the attack?

A. Hacking into the Iozin network

B. Ordering sparkling water

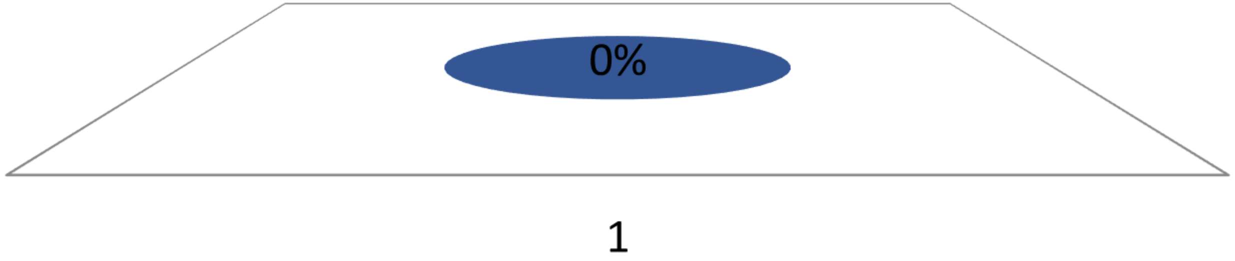
C. Guessing the Iozin executive’s password

✓ D. Buying credentials on the dark web



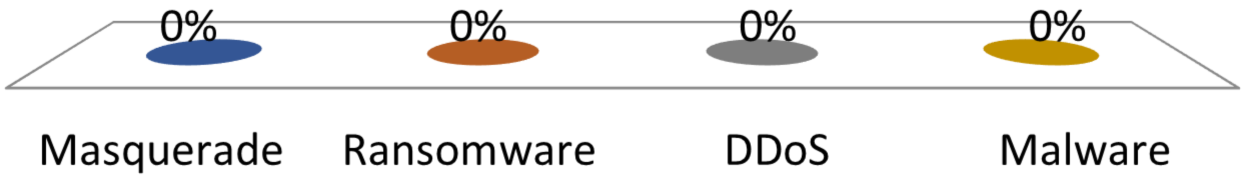
What is the Iozin cloud network security weakness?

Rank	Responses
1	
2	
3	
4	
5	
6	



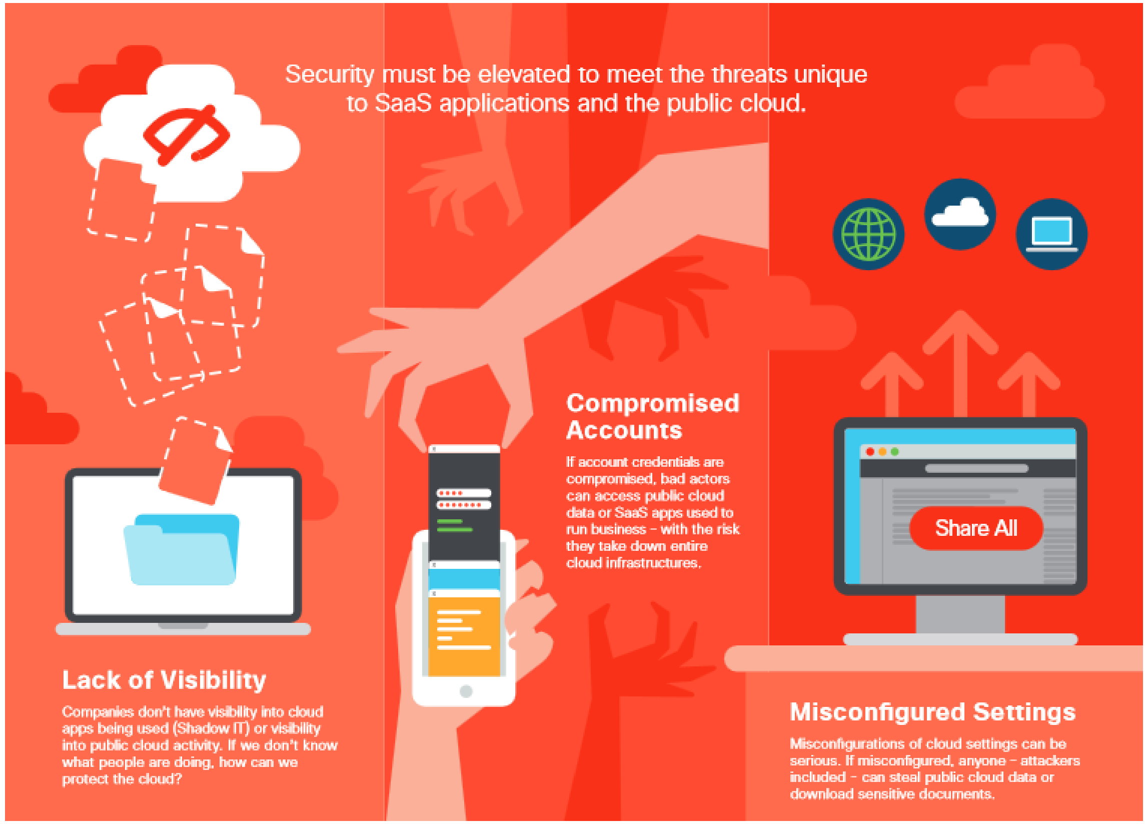
How did *Fancy Hare* access the enterprise network endpoints?

- [✓ A. Masquerade]
- B. Ransomware
- C. DDoS
- [✓ D. Malware]



Cisco - Cloud Security

“Fancy Hare” - https://www.youtube.com/watch?v=u0mzjn-D0Qo



Security must be elevated to meet the threats unique to SaaS applications and the public cloud.

Lack of Visibility

Companies don’t have visibility into cloud apps being used (Shadow IT) or visibility into public cloud activity. If we don’t know what people are doing, how can we protect the cloud?

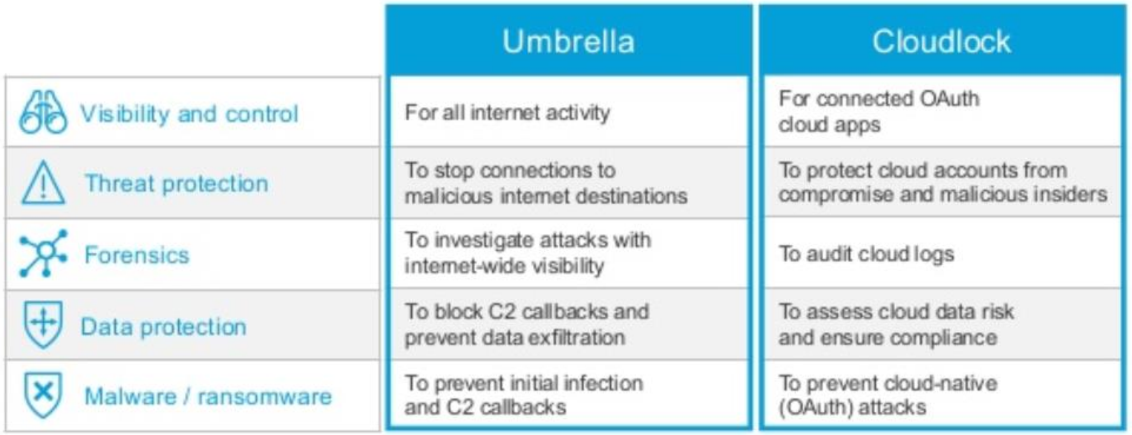
Compromised Accounts

If account credentials are compromised, bad actors can access public cloud data or SaaS apps used to run business – with the risk they take down entire cloud infrastructures.

Misconfigured Settings

Misconfigurations of cloud settings can be serious. If misconfigured, anyone – attackers included – can steal public cloud data or download sensitive documents.

- Secure access to the Internet
- Secure usage of SaaS applications



	Umbrella	Cloudlock
Visibility and control	For all internet activity	For connected OAuth cloud apps
Threat protection	To stop connections to malicious internet destinations	To protect cloud accounts from compromise and malicious insiders
Forensics	To investigate attacks with internet-wide visibility	To audit cloud logs
Data protection	To block C2 callbacks and prevent data exfiltration	To assess cloud data risk and ensure compliance
Malware / ransomware	To prevent initial infection and C2 callbacks	To prevent cloud-native (OAuth) attacks

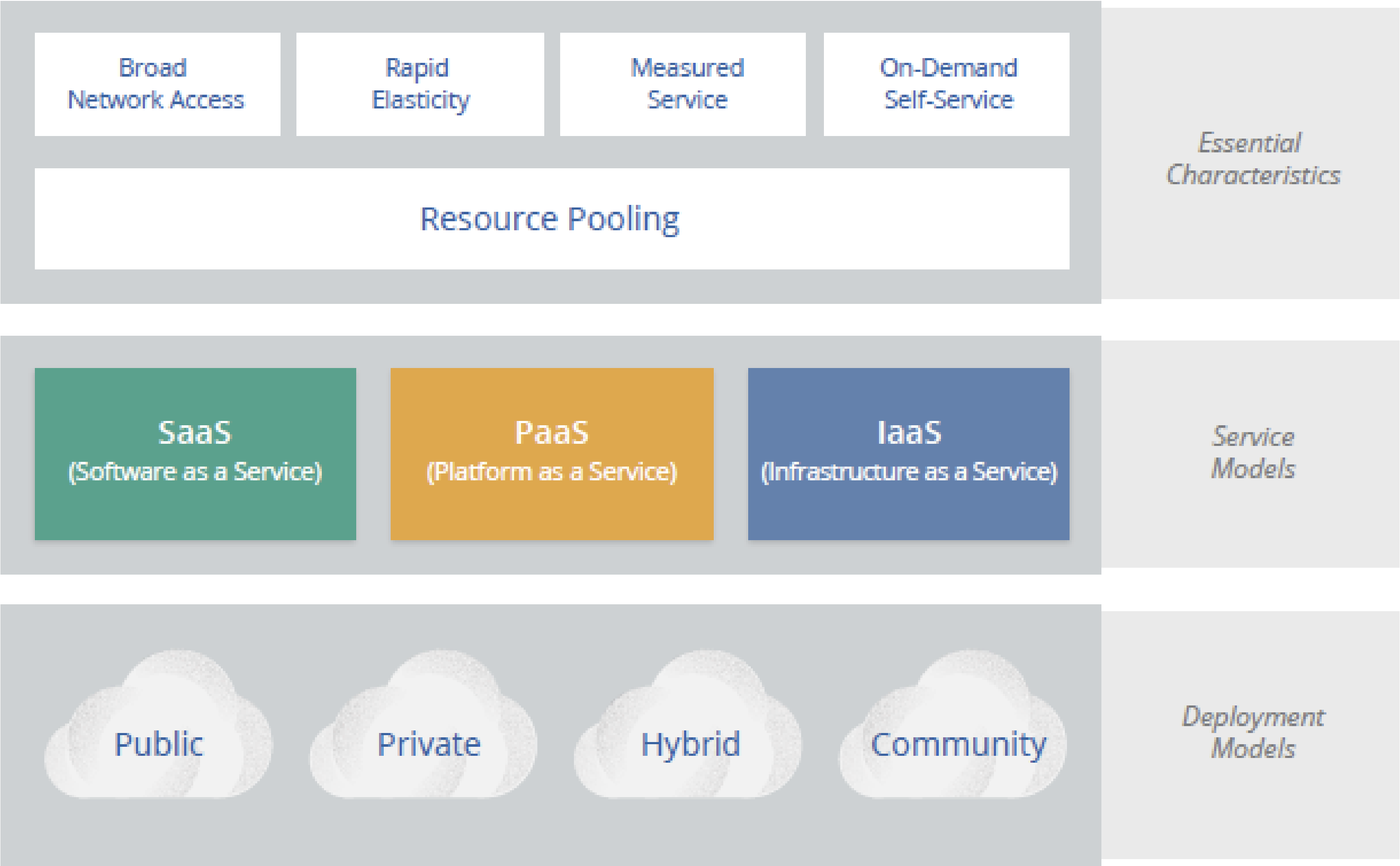
https://www.slideshare.net/Cisco/cisco-cloud-security-78092643

What is cloud computing?

NIST defines cloud computing, in NIST SP-800-145 (The NIST Definition of Cloud Computing), as follows:

“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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”

Elements of cloud computing



Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Essential Characteristics

SaaS (Software as a Service)

PaaS (Platform as a Service)

IaaS (Infrastructure as a Service)

Service Models

Public

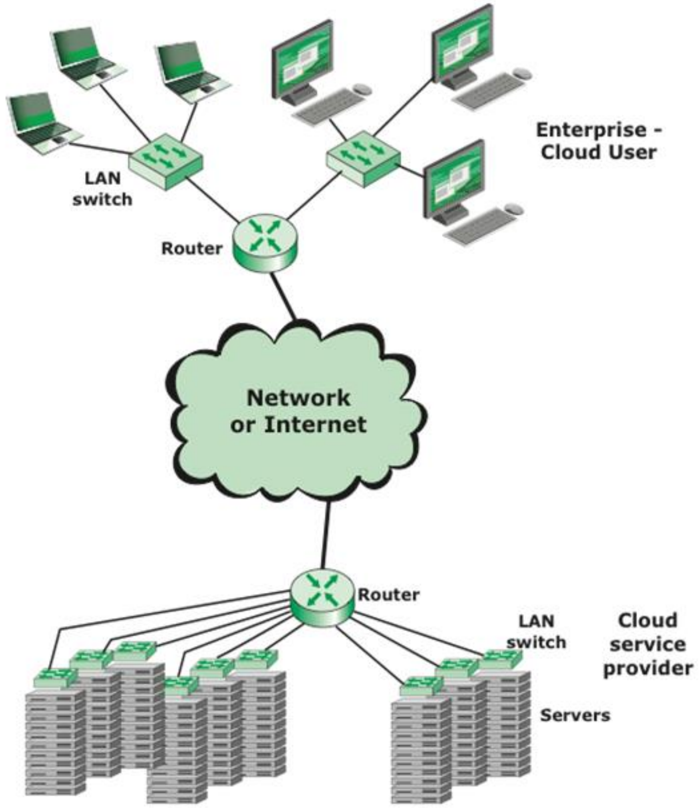
Private

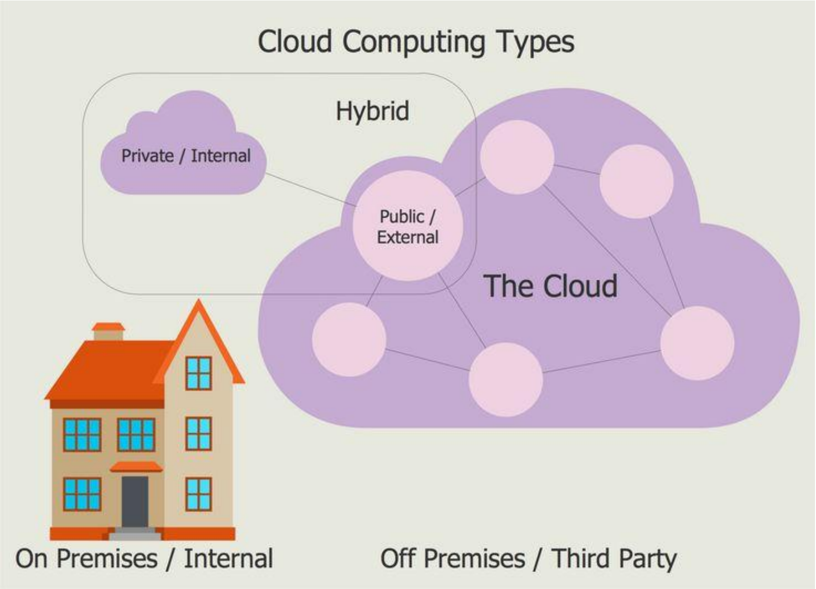
Hybrid

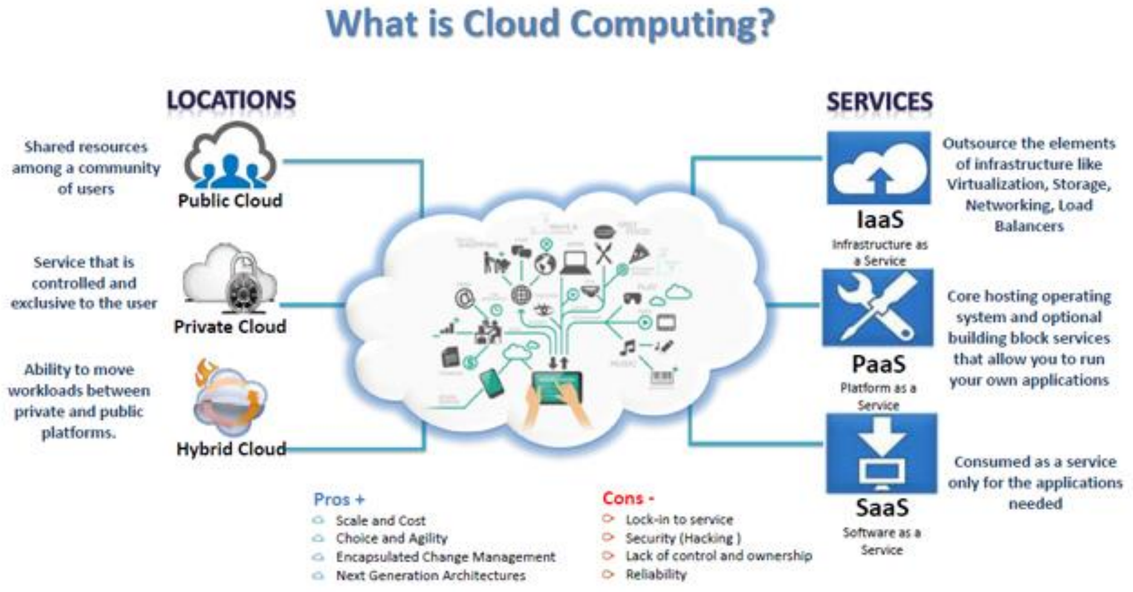
Community

Deployment Models

Typical cloud computing context







Shared resources among a community of users

Service that is controlled and exclusive to the user

Ability to move workloads between private and public platforms.

Outsource the elements of infrastructure like Virtualization, Storage, Networking, Load Balancers

Core hosting operating system and optional building block services that allow you to run your own applications

Consumed as a service only for the applications needed

Pros +

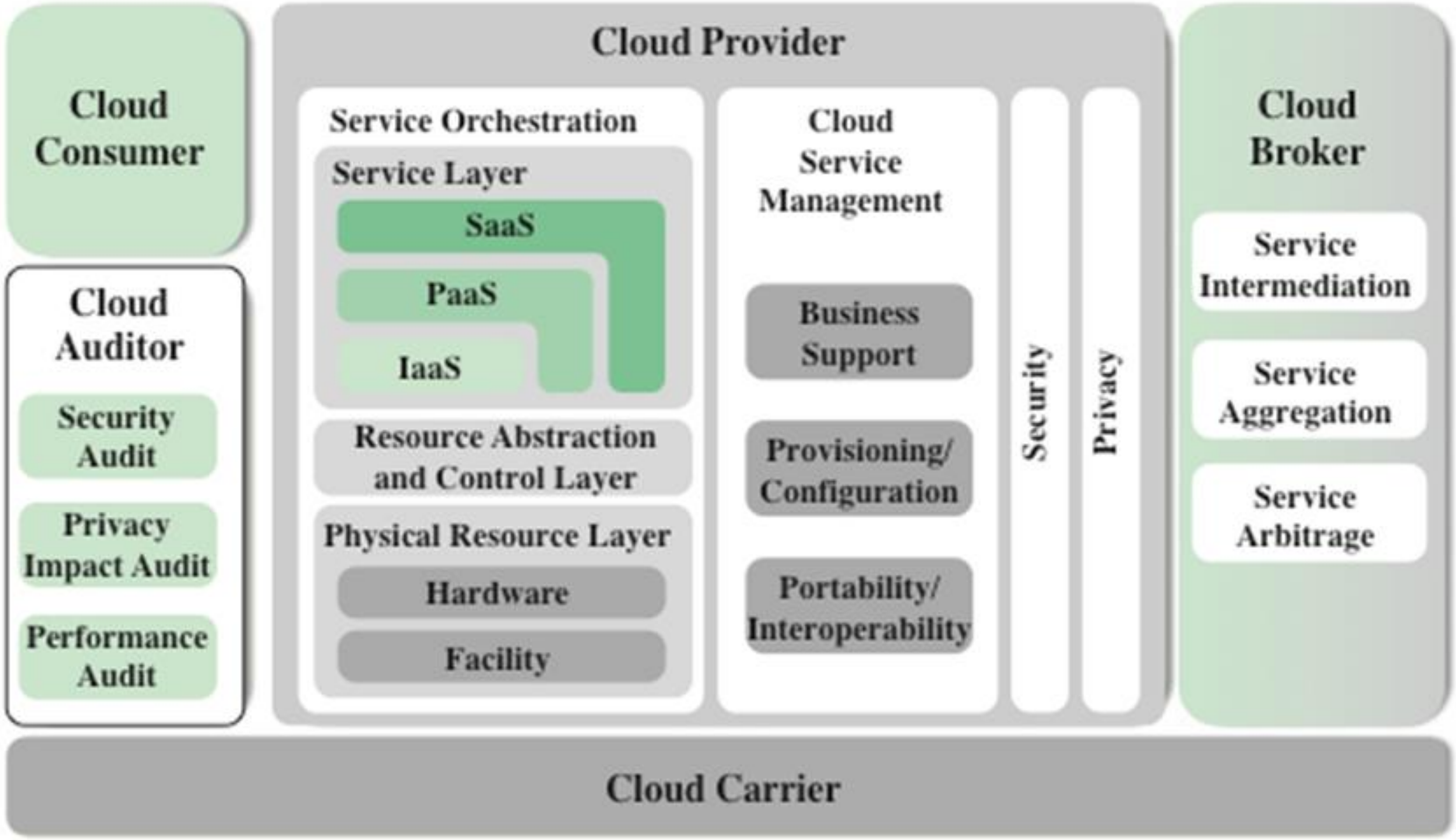
- Scale and Cost
- Choice and Agility
- Encapsulated Change Management
- Next Generation Architectures

Cons -

- Lock-in to service
- Security (Hacking)
- Lack of control and ownership
- Reliability

QUEEN'S UNIVERSITY BELFAST

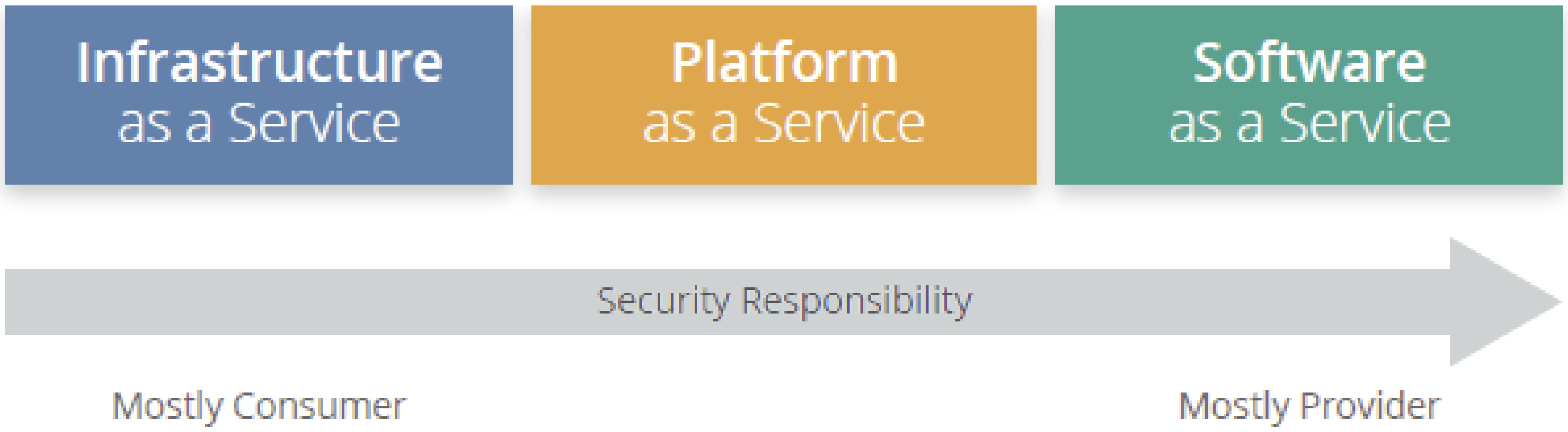
NIST Cloud Computing Reference Architecture



Cloud “actors” – Roles and Responsibilities

- *Cloud consumer:* A person or organization that maintains a business relationship with, and uses service from, cloud providers.
- *Cloud provider:* A person, organization, or entity responsible for making a service available to interested parties.
- *Cloud auditor:* A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
- *Cloud broker:* An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between CPs and cloud consumers.
- *Cloud carrier:* An intermediary that provides connectivity and transport of cloud services from CPs to cloud consumers.

Cloud Security – Security Responsibility



Infrastructure as a Service

Platform as a Service

Software as a Service

Security Responsibility

Mostly Consumer

Mostly Provider

The security responsibility for a Software as a Service cloud computing service model lies mostly with the provider. True or False?

[✓ A. True]

B. False

12 top cloud security threats for 2018

The Cloud Security Alliance list ranked in order of severity per survey results:

- Data breaches
- Insufficient identity, credential, and access management
- Insecure interfaces and APIs
- System vulnerabilities
- Account hijacking
- Malicious insiders
- Advanced persistent threats (APTs)
- Data loss
- Insufficient due diligence
- Abuse and nefarious use of cloud services
- Denial of Service
- Shared technology vulnerabilities

Cloud security threats and countermeasures

Threat	Security measure	Example
Data Breaches	Multifactor authentication, Encryption	BitDefender (AWS)
Insufficient IAM	Multifactor authentication, Key rotation	Instagram account recovery
Insecure Interfaces and APIs	Secure development lifecycle, security-specific code reviews, penetration testing	IRS breach (vulnerable API)
System vulnerabilities	Vulnerability scanning, security patches/upgrades	Heartbleed/Shellshock
Account Hijacking	Multifactor authentication, Prohibit sharing account credentials, AAA	Code Space admin console compromise (AWS)
Malicious Insiders	Control encryption process and keys, segregate duties, effective logging, monitoring, auditing	

QUEEN'S UNIVERSITY BELFAST

Cloud security threats and countermeasures

Threat	Security measure	Example
Advanced Persistent Threats	Education/Awareness of social engineering, advanced security controls, incident response plans	
Data Loss	Back up data, geographic redundancy – review contract	Amazon EC2 crash
Insufficient due diligence	Perform extensive due diligence to understand risks (commercial, technical, legal, compliance)	Nirvanix Bankruptcy
Abuse and nefarious use of cloud services	CSP detection of misuse of cloud e.g. inbound/outbound DoS attacks, workload health monitoring	
Denial of Service	DDoS detection and mitigation mechanisms	
Shared technology vulnerabilities	Multifactor authentication, HIDS, NIDS, segmentation	

What cloud security threats can be protected against by the use of Multi Factor authentication?

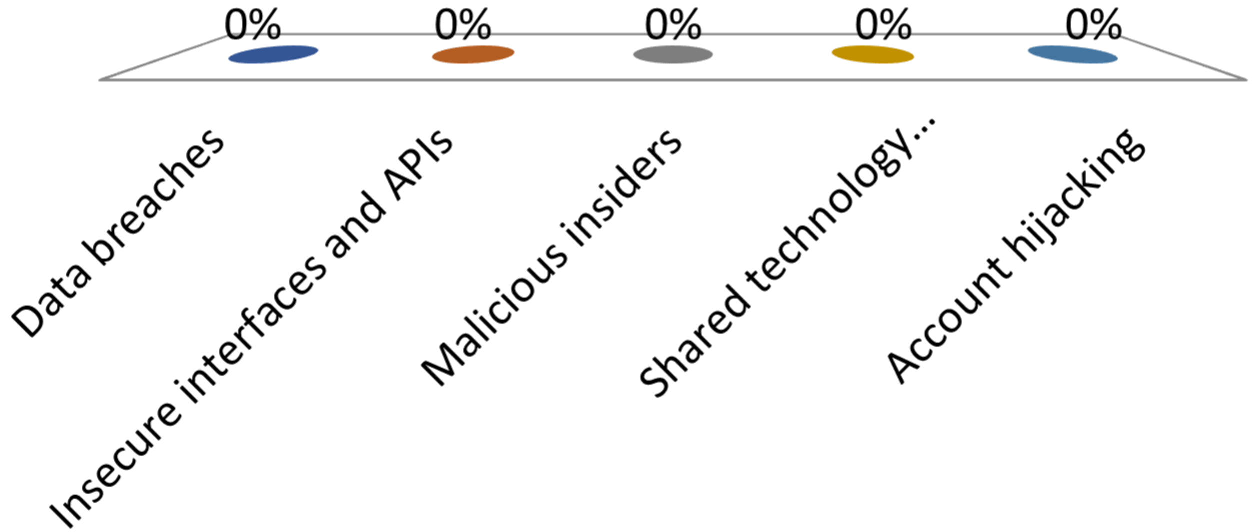
✓ A. Data breaches

B. Insecure interfaces and APIs

C. Malicious insiders

✓ D. Shared technology vulnerabilities

✓ E. Account hijacking

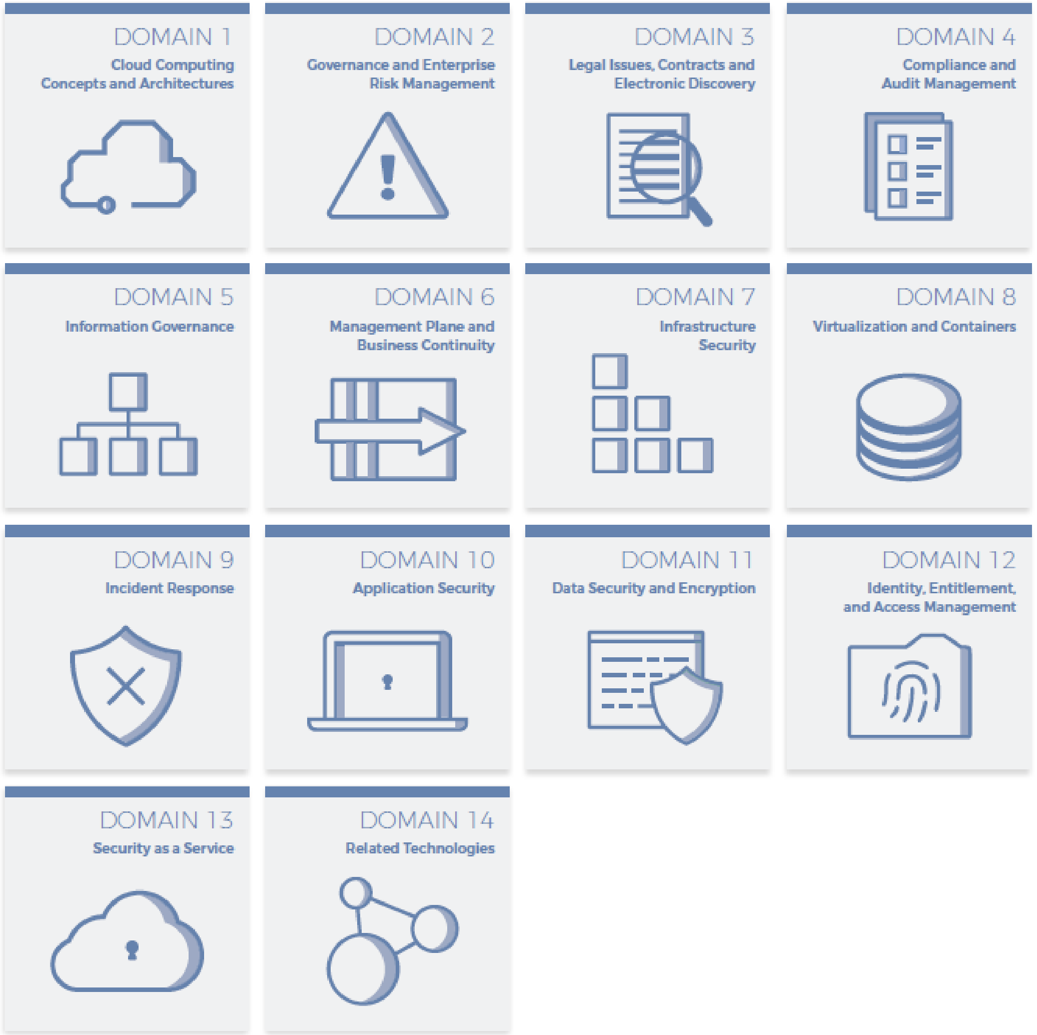


CSA Security Guidance

14 Domains

We’ll just consider:

- Virtualization and Containers
- Incident Response
- Security as a Service



DOMAIN 1
Cloud Computing Concepts and Architectures

DOMAIN 2
Governance and Enterprise Risk Management

DOMAIN 3
Legal Issues, Contracts and Electronic Discovery

DOMAIN 4
Compliance and Audit Management

DOMAIN 5
Information Governance

DOMAIN 6
Management Plane and Business Continuity

DOMAIN 7
Infrastructure Security

DOMAIN 8
Virtualization and Containers

DOMAIN 9
Incident Response

DOMAIN 10
Application Security

DOMAIN 11
Data Security and Encryption

DOMAIN 12
Identity, Entitlement, and Access Management

DOMAIN 13
Security as a Service

DOMAIN 14
Related Technologies

What is “virtualization”?

Technique for hiding the physical characteristics of computing resources from the way other systems, applications or end users interact with them.

Two common functions:

- Making multiple physical resources appear to function as a single logical resource
- Making a single physical resource appear to function as multiple logical resources

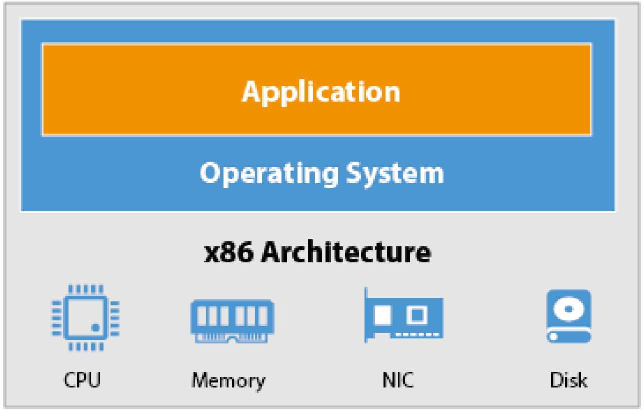
Background

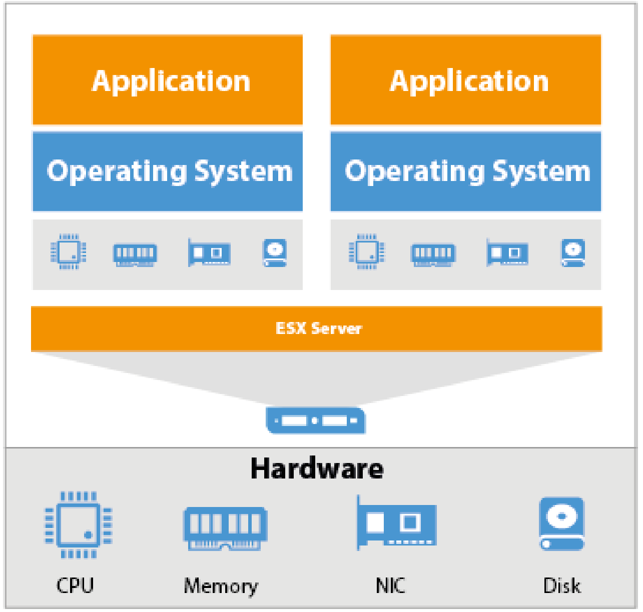
What is a “virtual machine (VM)”?

Implementation of a machine that executes programs as if it were a real machine

Two categories:

- Process virtual machine
  - Runs as a normal application inside an operating system to abstract away the details of the underlying hardware
- System virtual machine
  - Allows multiplexing (time sharing) of the underlying hardware between different operating systems





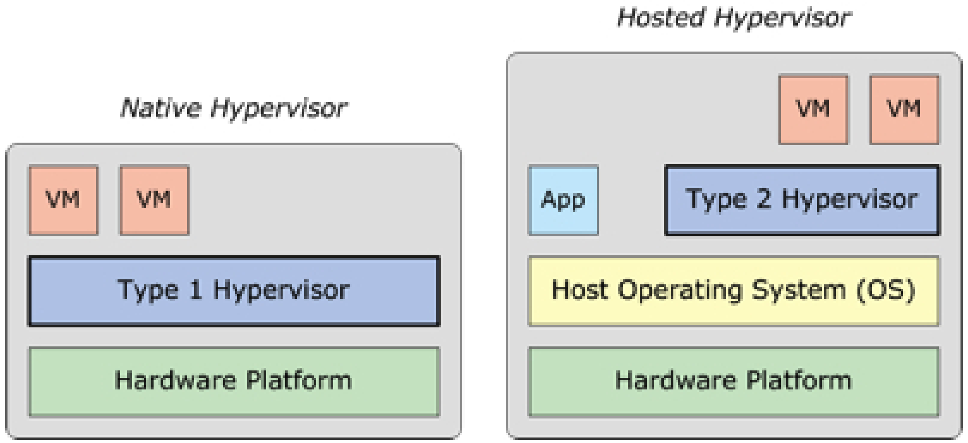
QUEEN'S UNIVERSITY BELFAST

System Virtual Machines

Implemented through the use of a Virtual Machine Monitor (VMM) also known as a Hypervisor

Two classifications of Hypervisors:

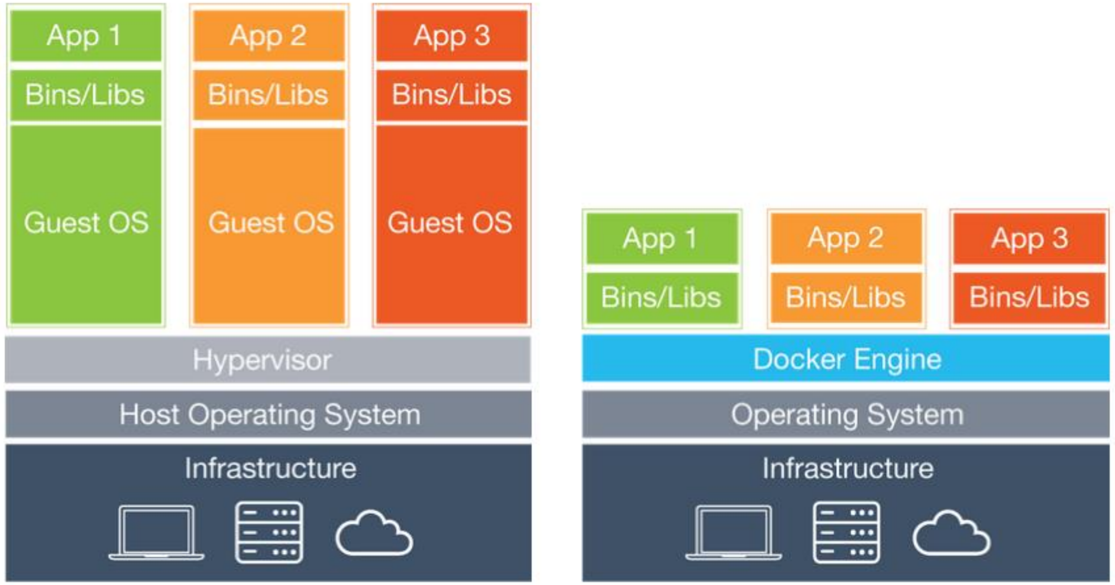
- Native (Hardware-level): software runs directly on top of a given hardware platform as a control program for operating systems (e.g. Xen, Vmware ESX)
- Hosted (OS-Level): software runs within an operating system environment as a control program for other operating systems (e.g. VMware workstation)



Containers

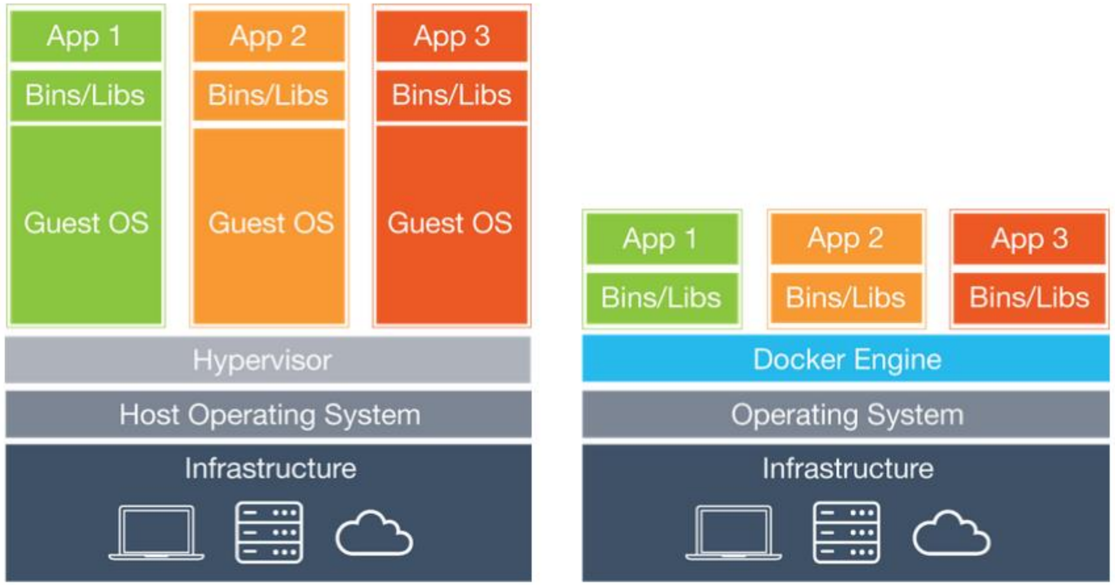
Code execution environments that run within an operating system, sharing and leveraging resources of that operating system.

- Multiple containers can run on the same VM or be implemented without the use of VMs and run directly on hardware.
- Restricted environment with only access to the processes and capabilities defined in the container configuration.



Virtualization and Containers

- Security of the virtualization technology itself e.g. securing the hypervisor
- Security controls for the virtual assets



Network security challenges in the virtualized data center

- Hypervisor integrity
  - A successful attack against a host’s hypervisor can compromise all of the workloads being delivered by the host.
- Intra-host communications
  - Communications traffic between different VMs on the same physical host is often not visible and therefore cannot be controlled by traditional physical firewalls and IPS
- VM migration
  - When VMs migrate from one physical host to another or from one physical site to another, they tend to break network security tools that rely on physical and/or network-layer attributes

Virtualization Security Recommendations:

Cloud provider responsibilities:

- Secure underlying infrastructure and virtualization technology e.g. patching/configuring hypervisors
- Assure security isolation between tenants i.e. compute processes or memory in one VM/container should not be visible to another
- Provide security capabilities for cloud users e.g. secure VM image distribution, secure boot process
- Provide attack protection mechanisms e.g. DDoS/IDS

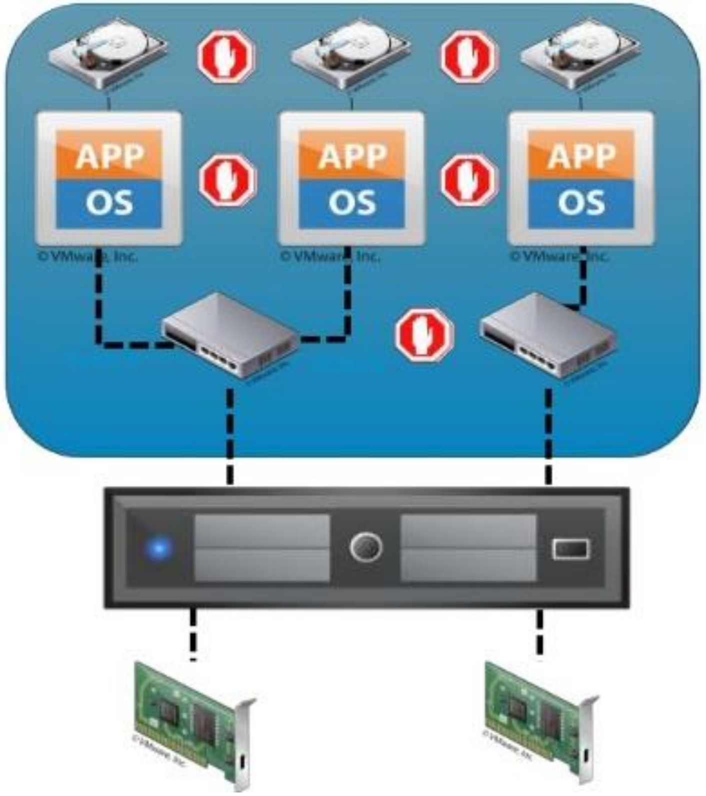
Virtualization Security Recommendations:

Cloud user responsibilities:

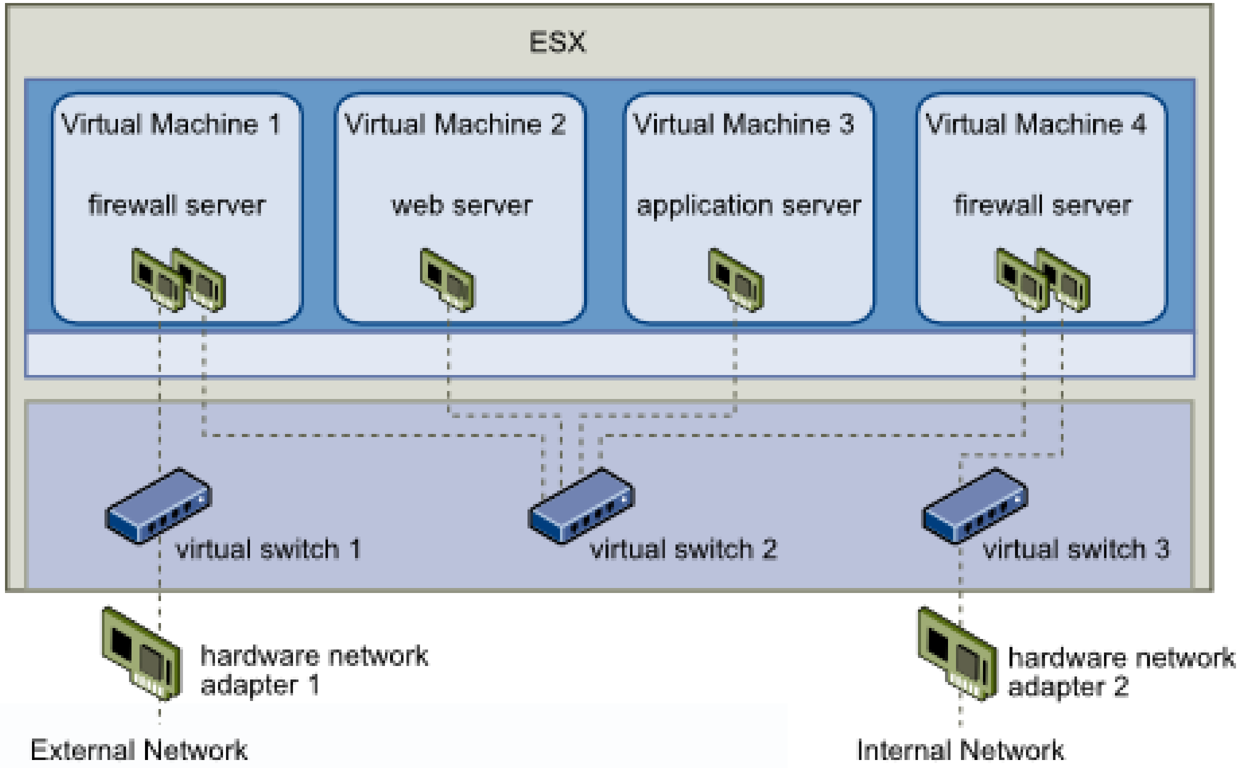
- Use the security capabilities/controls offered by the cloud provider e.g.
    - security settings, such as identity management, to the virtual resources
    - Monitoring and logging
    - Image asset management
    - Dedicated hosting (i.e. network isolation)
- Implement security controls on the virtual resource e.g. secure configuration/secure code

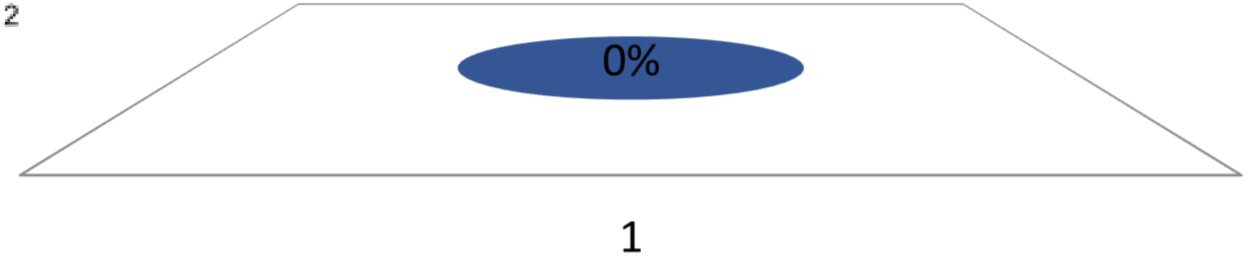
Isolation

- Assure isolation between virtual networks, even if those networks are all controlled by the same consumer.
  - Unless the consumer deliberately connects the separate virtual networks.

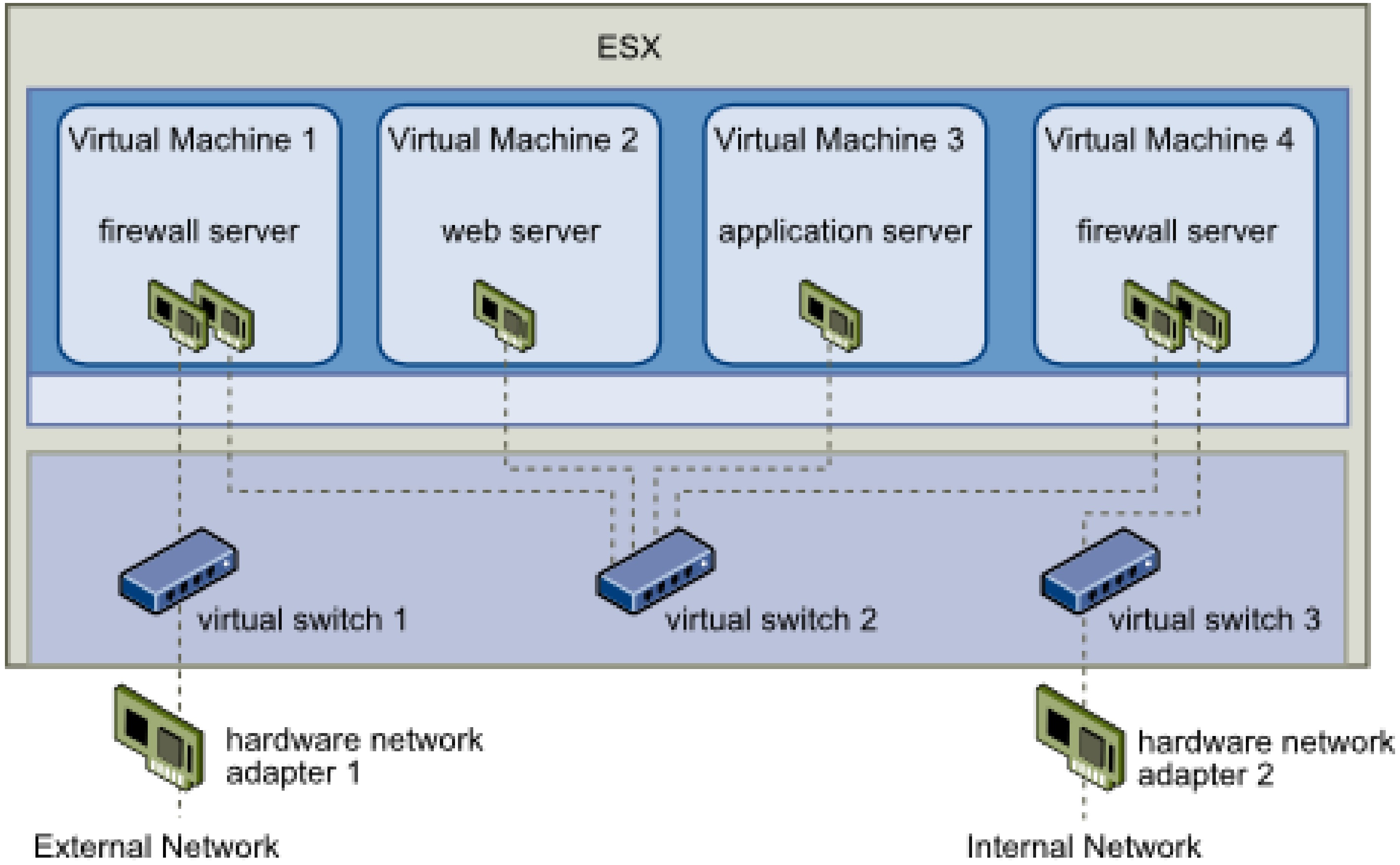


What is shown in the figure?



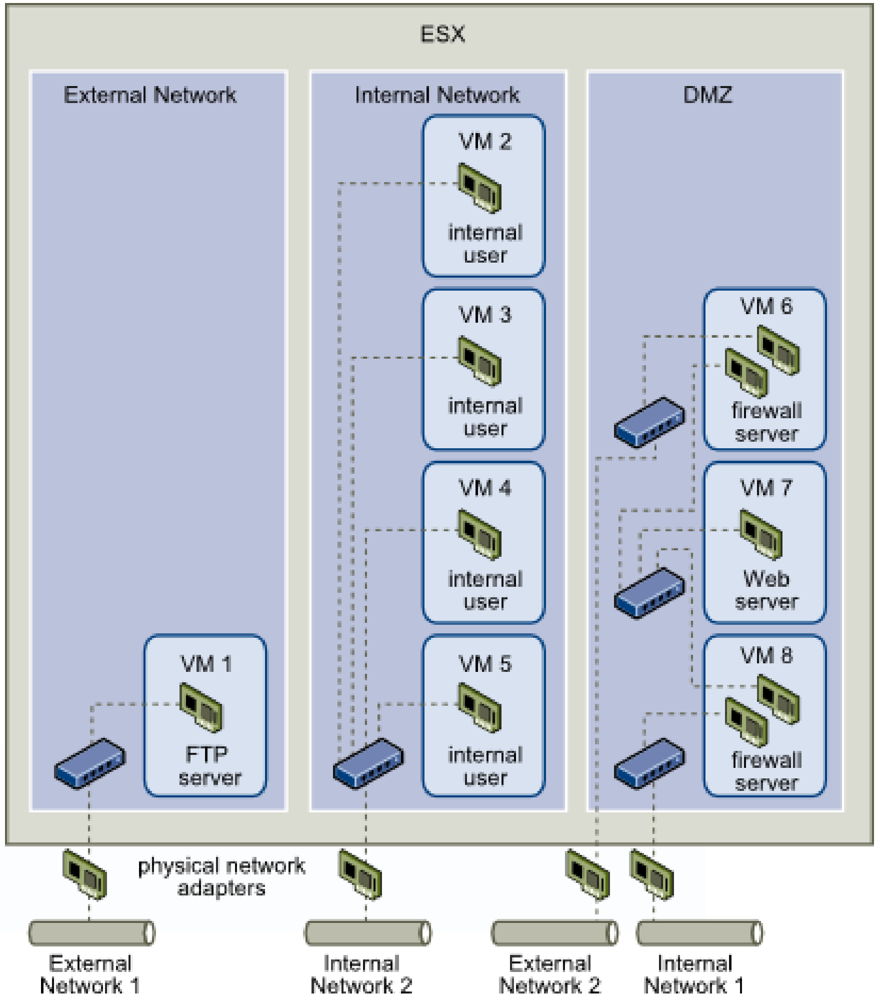


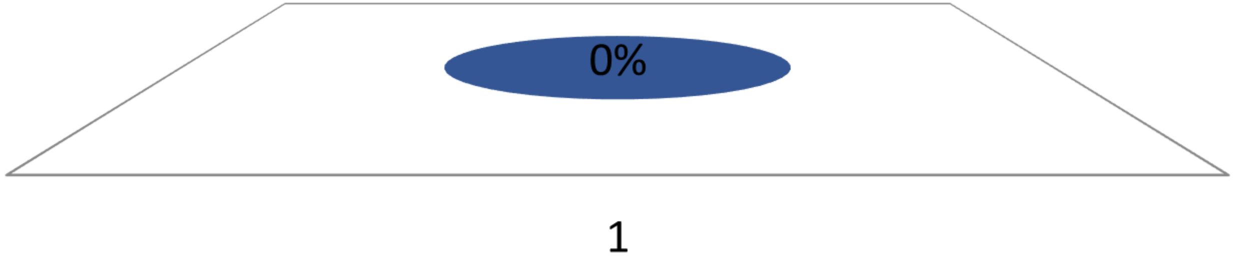
DMZ configured on a single host



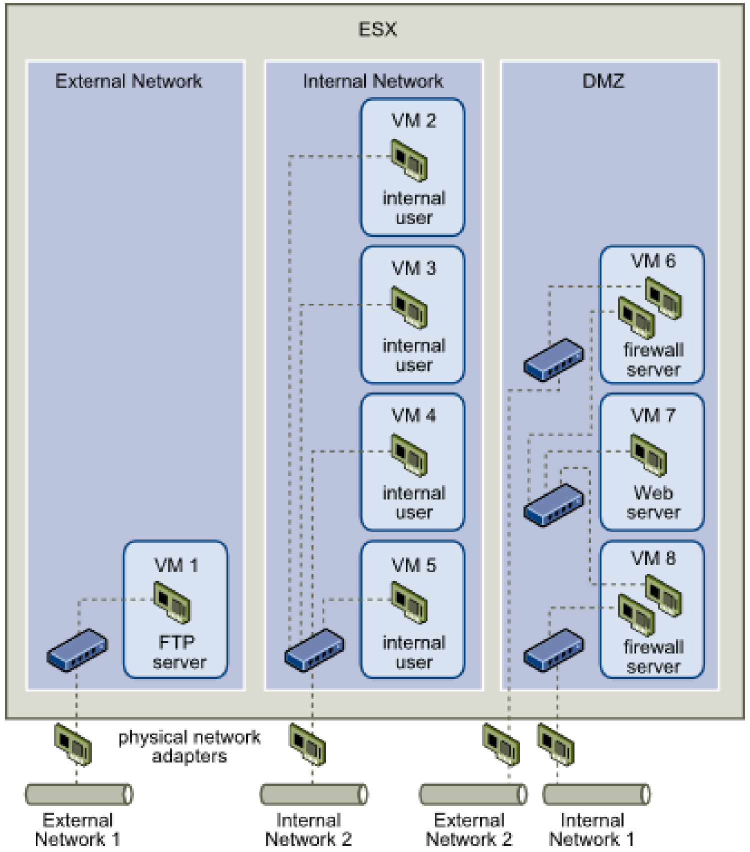
https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp#com.vmware.vsphere.server_configclassic.doc_40/esx_server_config/security_for_esx_systems/c_example_creating_a_network_dmz_on_a_single_esx_host.html

What is shown in the figure?



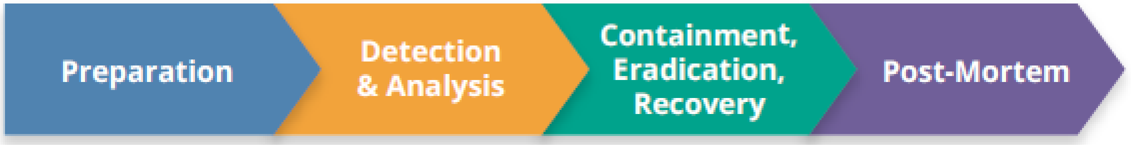


Multiple networks within a single host



https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp#com.vmware.vsphere.server_configclassic.doc_40/esx_server_config/security_for_esx_systems/c_example_creating_multiple_networks_within_a_single_esx_host.html

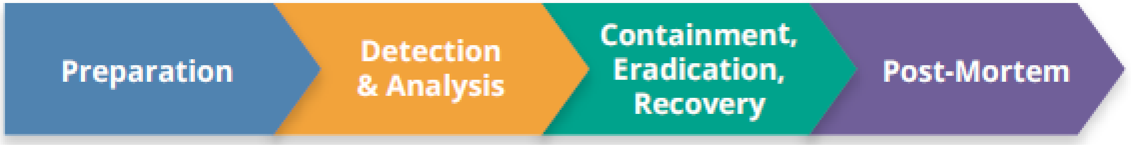
Incident Response



When preparing for cloud incident response, consider:

- SLAs and Governance:
  - What is the cloud provider responsible for?
  - Who are the points of contact?
  - What are the response time expectations?
  - Do you have out-of-band communication procedures (in case networks are impacted)?
  - What data are you going to have access to?
- IaaS/PaaS vs. SaaS:
  - In a multitenant environment, how can data specific to your cloud be provided for investigation?
- “Cloud jump kit”:
  - Do you have tools to collect logs and metadata from the cloud platform?
  - How do you obtain images of running virtual machines and what kind of data do you have access to?

Incident Response



Recommendations:

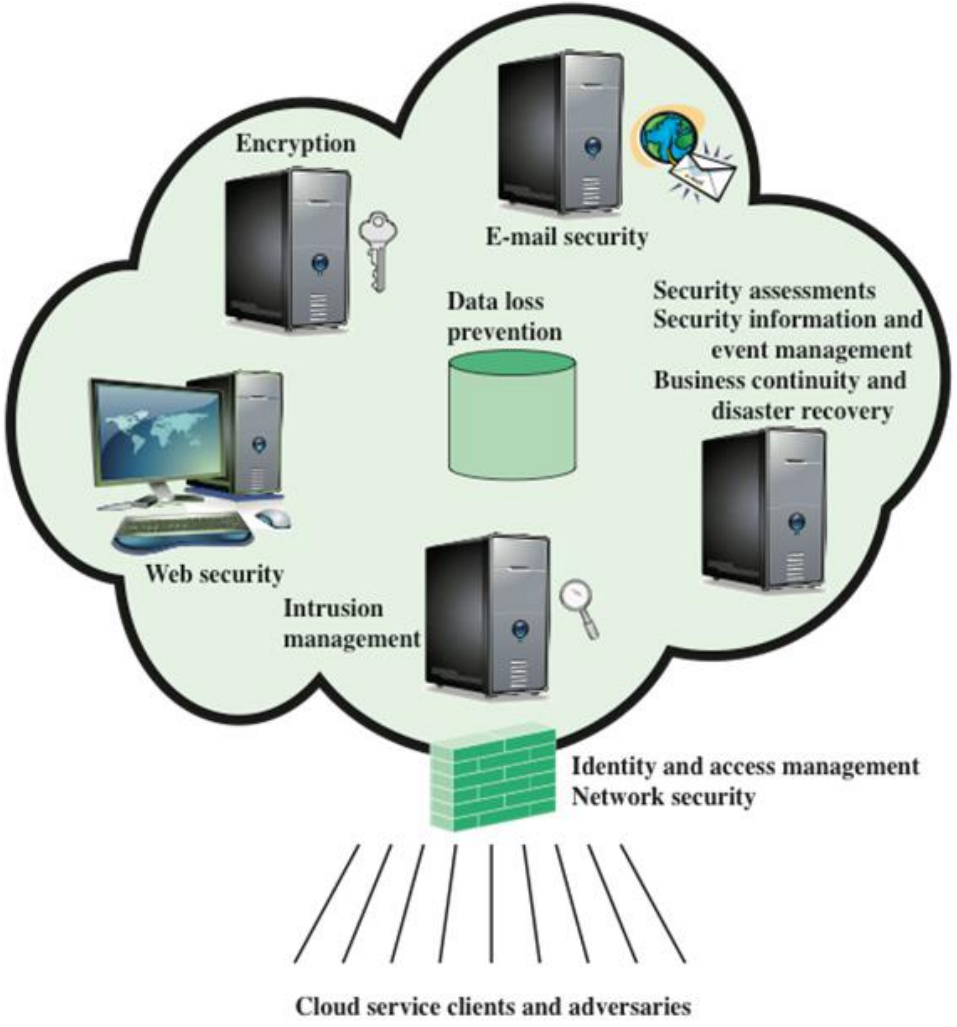
- SLAs and setting expectations around customer versus provider responsibilities
- Cloud customers must:
  - Set up proper communication paths with the provider that can be used in an incident
  - Understand the content and format of data that the CSP will supply for analysis and evaluate whether available forensic data satisfies legal chain of custody requirements
- For each CSP, the approach to detecting and handling incidents involving the resources hosted at that provider must be planned and described in the enterprise incident response plan
- The SLA with each CSP must guarantee support for the incident handling required for effective execution of the enterprise incident response plan

Cloud Security as a Service (SecaaS)

- The Cloud Security Alliance defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems

- The Cloud Security Alliance has identified the following SecaaS categories of service:
  - Identity, entitlement, and access management services
  - Cloud access and security brokers (also known as cloud security gateways)
  - Web security gateways
  - E-mail security
  - Security assessment
  - Web application firewalls
  - Intrusion Detection/Prevention (IDS/IPS)
  - Security information and event management (SIEM)
  - Encryption and key management
  - Business continuity and disaster recovery
  - Security management
  - Distributed Denial of Service Protection

Elements of Cloud Security as a Service


Encryption
E-mail security
Data loss prevention
Security assessments
Security information and event management
Business continuity and disaster recovery
Web security
Intrusion management
Identity and access management
Network security
Cloud service clients and adversaries

Cloud Security as a Service (SecaaS)

- Recommendations:
  - Before engaging a SecaaS provider, be sure to understand any security-specific requirements for data-handling (and availability), investigative, and compliance support.
  - Pay particular attention to handling of regulated data, such as PII
  - Understand data retention needs – consider standard data feeds to avoid lock-in

Summary

- Cloud Computing – Definition, Elements, Roles
- Cloud security threats and countermeasures
- Cloud Security Alliance – Security Guidance
    - Virtualization and Containers
    - Incident Response
    - Security as a Service

Questions?

Next Session: Wireless/Mobile Security

Friday, 29 March 2019