Cloud Security

- Understanding cloud security involves an overall introduction to cloud computing
- It also means understanding the steps to take in order to secure the cloud computing environment

CENGAGE

Introduction to Cloud Computing (1 of 6)

- In a *hosted services* environment, servers, storage, and the supporting networking infrastructure are shared by multiple enterprises over a remote network connection
- **Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources
  - Entities that offer cloud computing are called **cloud service providers**
- The savings available through cloud computing are due to the following factors:
  - *Elasticity and scalability*
  - *Pay-per-use*
  - *On demand*
  - *Resiliency*

Introduction to Cloud Computing (2 of 6)

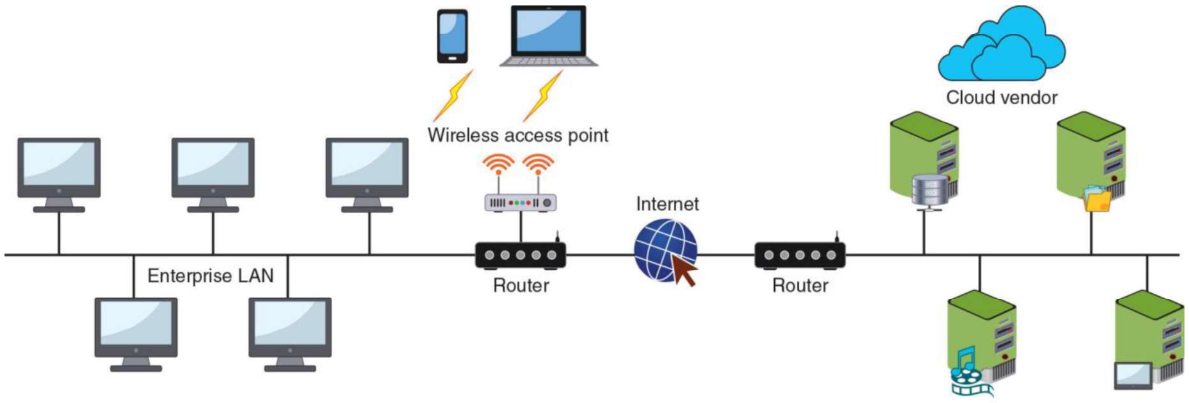

Figure 10-1 Cloud computing

Figure 10-1 Cloud computing

Introduction to Cloud Computing (3 of 6)

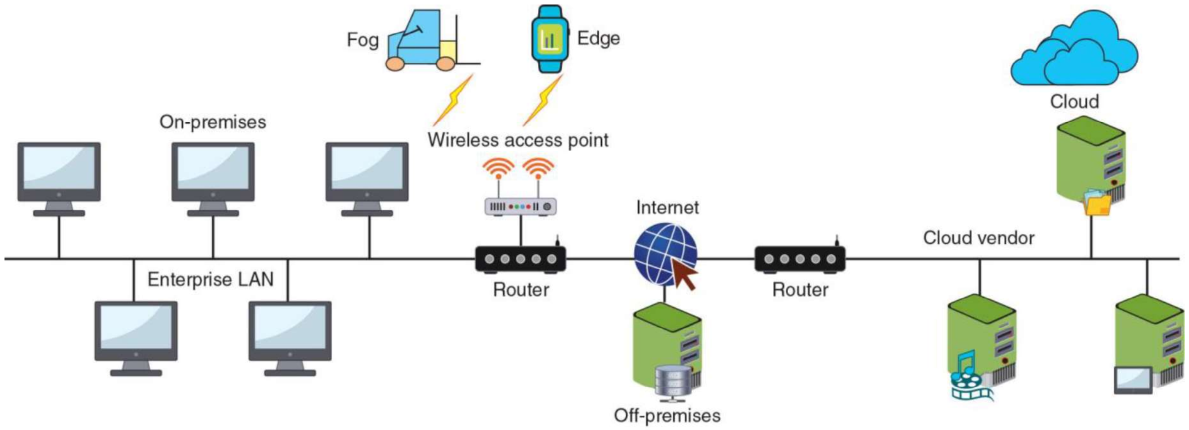

Figure 10-2 Computing locations

Figure 10-2 Computing locations

Introduction to Cloud Computing (4 of 6)

- Cloud Architecture
  - *Thin client* is a computer that runs from resources stored on a central cloud server
  - *Transit gateway* is an Amazon Web Services (AWS) technology that allows organizations to connect all existing virtual private clouds (VPCs), physical data centers, remote offices, and remote gateways into a single managed source
  - *Serverless infrastructure* is one in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider

Introduction to Cloud Computing (5 of 6)

- There are four service models in cloud computing:
  - **Software as a Service (SaaS)**
    - Vendor provides access to the vendor’s software applications running on a cloud infrastructure
  - **Platform as a Service (PaaS)**
    - Consumers install and run their own specialized applications on the cloud computing network
  - **Infrastructure as a Service (IaaS)**
    - Vendor allows customers to deploy and run their own software, including OSs and applications
  - **Anything as a Service (XaaS)**
    - A broad category of subscription services related to cloud computing

Introduction to Cloud Computing (6 of 6)

- Management
  - Cloud management can be conducted by the local organization performing the work itself or by contracting with a third-party management service provider
- **Services integration** attempts to achieve a “boundary-less” approach
  - Involves integrating all users across the enterprise who are using cloud computing
- When locally managing cloud computing, an enterprise should have written **resource policies** in place
  - They must outline who is responsible for cloud computing, what are their duties and responsibilities, how cloud computing can be used (and not used), and the processes for acquiring these resources
- A **managed service provider** (**MSP**) delivers services through ongoing and regular support as well as active administration of those resources
  - An MSP assumes the role of a traditional on-prem IT organization

Securing Cloud Computing (1 of 6)

Security issue	Description
Unauthorized access to data	Improper cloud security configurations can result in data being left exposed.
Lack of visibility	Organizations have limited or no visibility into the security mechanisms of the cloud provider and thus cannot verify the effectiveness of security controls.
Insecure application program interfaces (APIs)	While APIs help cloud customers customize their PaaS by providing data recognition, access, and effective encryption, a vulnerable API can be exploited by threat actors.
Compliance regulations	Maintaining compliance requires that an organization know where its data is, who can access it, and how it is protected, but this can be difficult in an opaque cloud system, which lacks transparency.
System vulnerabilities	A cloud infrastructure is prone to system vulnerabilities due to complex networks and multiple third-party platforms.

CENGAGE

Securing Cloud Computing (2 of 6)

- Cloud Security Controls
  - Securing cloud computing involves using controls such as the following:
    - **Conducting audits –** a **cloud security audit** is an independent examination of cloud service controls
    - **Use Regions and Zones –** reliability and resiliency are achieved through duplicating processes across one or more geographical areas (called **high availability across zones**)
    - **Secrets management –** enables strong security and improved management of a microservices-based architecture, allowing the entire cloud infrastructure to remain flexible and scalable without sacrificing security
    - **Enforce Functional Area Mitigations –** See Table 10-6

CENGAGE

Securing Cloud Computing (3 of 6)

Feature	Description
Limited and automated replication	While secret data and secret names are “project-global” resources, the secret data is stored in regions, which the user can specify or the cloud provider can designate.
Secret-specific versioning	A secret can be pinned to a specific version of the code (like “v3.2”).
Audit logging	Every interaction generates an audit entry in a log file that can be used to find abnormal access patterns that may indicate possible security breaches.
Default encryption	Data is encrypted in transit and at rest with AES-256-bit encryption keys.
Extensibility	One system is able to extend and integrate into other existing secrets management systems.

Securing Cloud Computing (4 of 6)

- Application Security
  - One of an organization’s security protections for cloud computing application security is to use a **cloud access security broker** (**CSAB**)
  - CASB is a set of software tools or services that resides between the enterprises’ on-premises infrastructure and the cloud provider’s infrastructure
  - CASB acts as a “gatekeeper”, ensuring that the security policies of the enterprise extend to its data in the cloud
- Security Virtual Device Solutions
  - A **next generation secure web gateway** (**SWG**) examines both incoming and outgoing traffic and performs basic URL and monitoring in web applications
  - A **cloud firewall** is virtual software that functions in a similar manner to a physical security appliance by examining traffic into and out of the cloud

CENGAGE

Securing Cloud Computing (5 of 6)

- Lack of a Cloud Conceptual Model
  - Physical networks use the Open Source Interconnection (OSI) seven-layer model to illustrate network functionality
  - With cloud computing, the OSI model is no longer as useful
  - The lack of a conceptual model like the OSI model makes selecting and managing security virtual devices more challenging
  - Different cloud-based conceptual models are starting to be proposed
    - However, no single model has been widely adapted
    - One model is shown in Table 10-7

Securing Cloud Computing (6 of 6)

Layer and name	Description	Party responsible
5—Application Experience	End-user facing interface	Customer
4—Native Service	Create, store, process	Customer
3—Software-Defined Datacenter	Create infrastructure	SaaS—Cloud computing provider PaaS and IaaS—Customer
2—Virtualization Software	Software that virtualizes the hardware	Cloud computing provider
1—Physical Infrastructure	Buildings, power, cables, hardware, utilities	Cloud computing provider

CENGAGE

Knowledge Check Activity 1

Which cloud security control provides reliability and resiliency through the duplication of processes across geographical areas?

a. Conducting audits

b. Implementing secrets management

c. Using regions and zones

d. Enforcing functional area mitigations

Knowledge Check Activity 1: Answer

Which cloud security control provides reliability and resiliency through the duplication of processes across geographical areas?

Answer: c. Using regions and zones

In a cloud computing environment, reliability and resiliency are achieved through duplicating processes across one or more geographical areas. This is called using regions and zones or high availability across zones.

Virtualization Security

- Virtualization security involves an understanding of the topic along with specific examples
- It includes specific steps to be taken to secure a virtualized environment

Defining Virtualization (1 of 5)

- What is Virtualization?
  - **Virtualization** is a means of managing and presenting computer resources without regard to physical layout or location
  - *Host virtualization* is a type of virtualization in which an entire operating system environment is simulated
  - A *virtual machine* (*VM*) is a simulated software-based emulation of a computer
  - The *host system* runs a hypervisor that manages the virtual operating systems and supports one or more guest systems
  - Virtualization is used to consolidate multiple physical servers into VMs that can run on a single physical computer

Defining Virtualization (2 of 5)

- The VM monitor program is called a *hypervisor*, which manages the VM operating systems
- Two types of hypervisor:
  - *Type I* – run directly on the computer’s hardware instead of the underlying OS
  - *Type II* – run on the host OS, much like an application
- A **container** holds only the necessary OS components that are needed for that specific application to run
  - Reduces the necessary hard drive storage space and RAM needed
  - Allows for containers to start more quickly because the OS does not have to be started

Defining Virtualization (3 of 5)

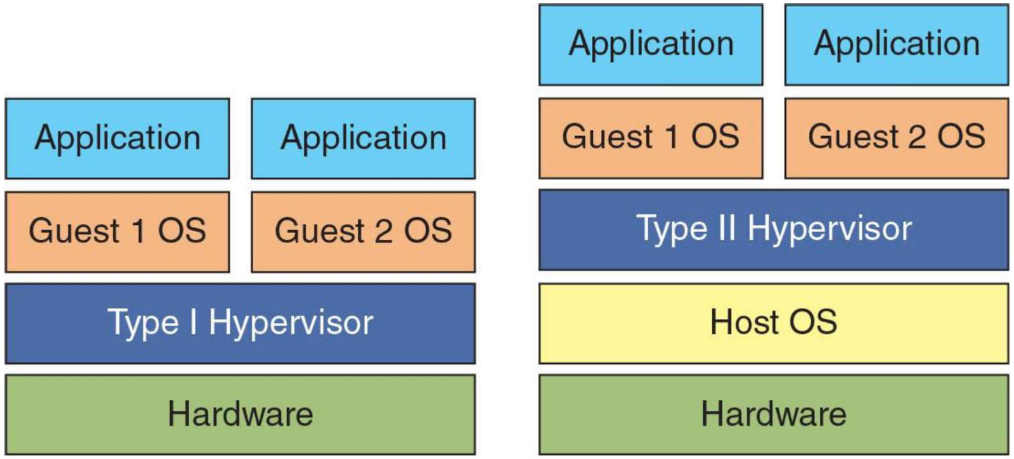

Figure 10-7 Type I and Type II hypervisors

Figure 10-7 Type I and Type II hypervisors

Defining Virtualization (4 of 5)

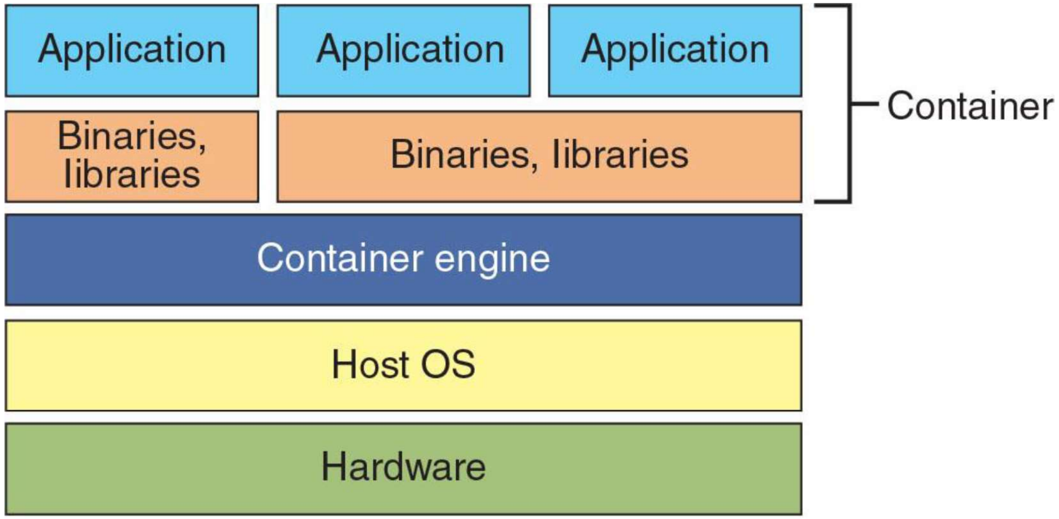

Figure 10-8 Container

Figure 10-8 Container

Defining Virtualization (5 of 5)

- Advantages of Virtualization
  - New virtual server machines can be made available (*host availability*) and resources can easily be expanded or contracted as needed (*host elasticity*)
  - Can reduce costs
    - Fewer physical computers must be purchased and maintained
  - Can provide uninterrupted server access to users
    - Supports *live migration* which allows a virtual machine to be moved to a different physical computer with no impact to users