CHƯƠNG 08
CLOUD SECURITY

ThS.Nguyễn Duy
duyn@uit.edu.vn

Module Flow

1. Introduction to Cloud Computing
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Introduction to Cloud Computing

Cloud computing is an on-demand delivery of **IT capabilities** where IT infrastructure and applications are provided to **subscribers** as a metered service over a network

Characteristics of Cloud Computing

1. On-demand self service
2. Distributed storage
3. Rapid elasticity
4. Automated management
5. Broad network access
6. Resource pooling
7. Measured service
8. Virtualization technology

Types of Cloud Computing Services

Infrastructure-as-a-Service (IaaS)

- Provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API
- E.g. Amazon EC2, Go grid, Sungrid, Windows SkyDrive, etc.

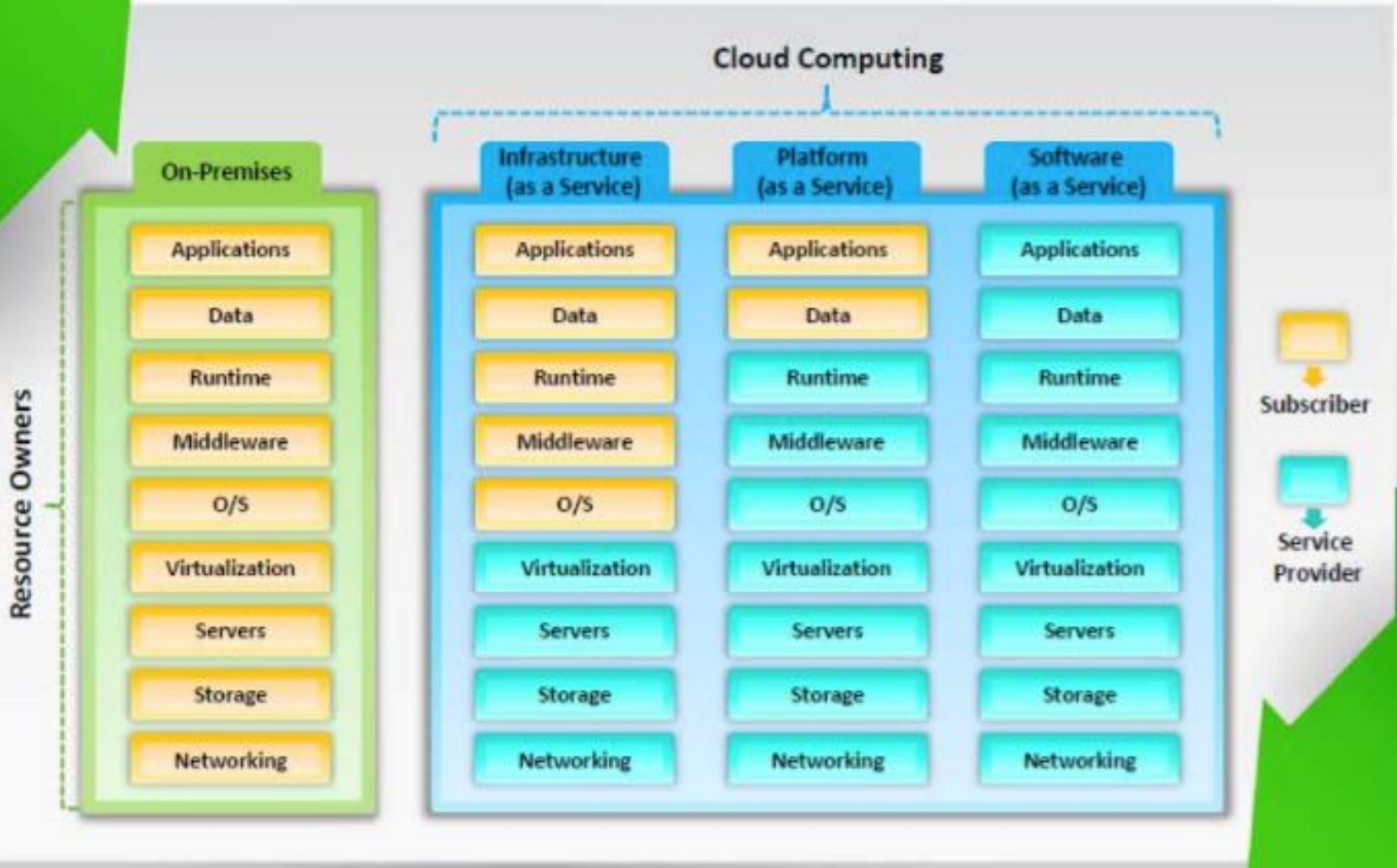
Platform-as-a-Service (PaaS)

- Offers development tools, configuration management, and deployment platforms on-demand that can be used by subscribers to develop custom applications
- E.g. Intel MashMaker, Google App Engine, Force.com, Microsoft Azure, etc.

Software-as-a-Service (SaaS)

- Offers software to subscribers on-demand over the Internet
- E.g. web-based office applications like Google Docs or Calendar, Salesforce CRM, etc.

Separation of Responsibilities in Cloud



Cloud Deployment Models

Cloud deployment model selection is based on the **enterprise requirements**

Private Cloud

Cloud infrastructure operated solely for a **single organization**

Community Cloud

Shared infrastructure between **several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)

Hybrid Cloud

Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models

Public Cloud

Services are rendered over a **network that is open for public use**

NIST Cloud Computing Reference Architecture

C|EH Certified Ethical Hacker

NIST cloud computing reference architecture defines five major factors:

Cloud Auditor

A party for making independent assessments of cloud service controls and taking an opinion thereon

Cloud Broker

An entity to manage cloud services in terms of use, performance, and delivery who also maintains relationship between cloud providers and consumers

Cloud Consumer

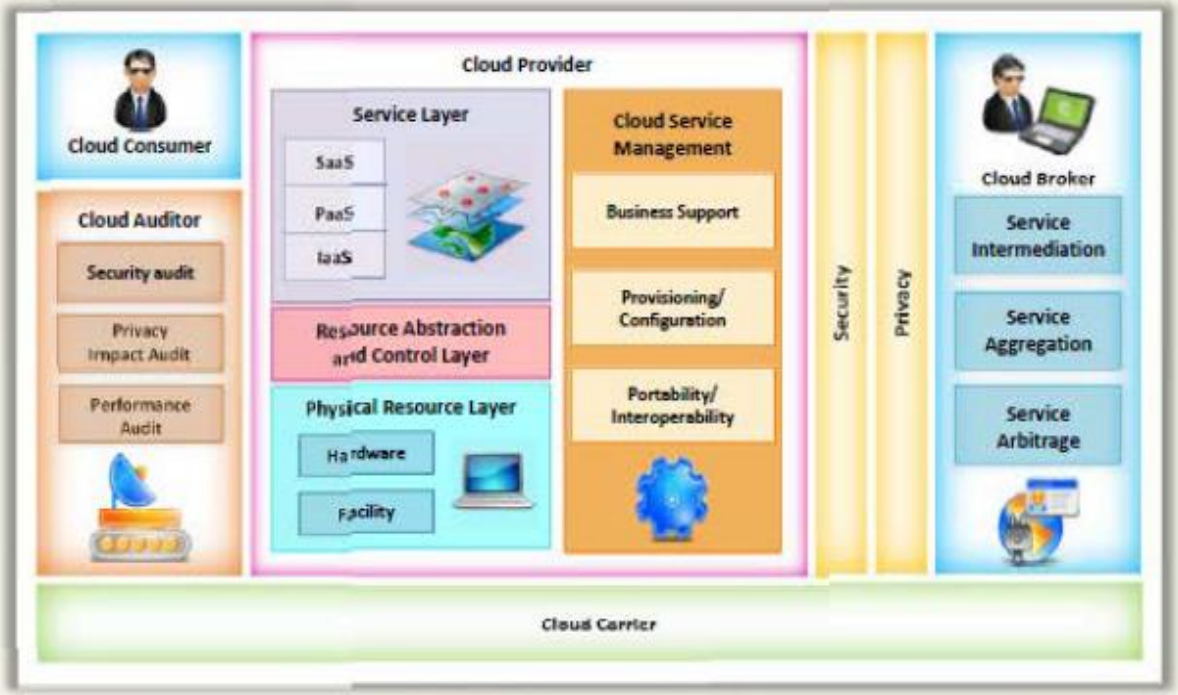
A person or organization that uses cloud computing services

Cloud Carrier

An intermediary for providing connectivity and transport services between cloud consumers and providers

Cloud Provider

A person or organization providing services to interested parties



Overview of the NIST cloud computing reference architecture

Benefits of Virtualization in Cloud

1. Increases business continuity through efficient disaster recovery
2. Reduces cost of setting cloud infrastructure (cost on hardware, servers, etc.)
3. Improves the way organizations manage IT and deliver services
4. Improves operational efficiency
5. Reduces system administration work
6. Facilitates better backup and data protection
7. Increases service levels and enable self-service provisioning
8. Helps administrators to ensure control and compliance

Module Flow

1. Introduction to Cloud Computing
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Cloud Computing Threats

C|EH Certified Ethical Hacker

1. Data breach/loss
2. Abuse of cloud services
3. Insecure interfaces and APIs
4. Insufficient due diligence
5. Shared technology issues
6. Unknown risk profile
7. Inadequate infrastructure design and planning
8. Conflicts between client hardening procedures and cloud environment
9. Loss of operational and security logs
10. Malicious insiders
11. Illegal access to cloud systems
12. Privilege escalation
13. Loss of business reputation due to co-tenant activities
14. Natural disasters
15. Hardware failure
16. Supply chain failure
17. Modifying network traffic
18. Isolation failure
19. Cloud provider acquisition
20. Management interface compromise
21. Network management failure
22. Authentication attacks
23. VM-level attacks
24. Lock-in
25. Licensing risks
26. Loss of governance
27. Loss of encryption keys
28. Risks from changes of Jurisdiction
29. Undertaking malicious probes or scans
30. Theft of computer equipment
31. Cloud service termination or failure
32. Subpoena and e-discovery
33. Improper data handling and disposal
34. Loss or modification of backup data
35. Compliance risks
36. Economic Denial of Sustainability (EDOS)

Cloud Computing Threats (Cont'd)

C|EH Certified Ethical Hacker

Data Breach/Loss

Data loss issues include:

- **Data is erased**, modified or decoupled (lost)
- **Encryption keys are lost**, misplaced or stolen
- **Illegal access to the data** in cloud due to Improper authentication, authorization, and access controls
- **Misuse of data** by CSP

Abuse of Cloud Services

Attackers **create anonymous access to cloud services** and perpetrate various attacks such as:

- **Password** and **key** cracking
- Building rainbow tables
- **CAPTCHA**-solving farms
- Launching **dynamic attack points**
- Hosting **exploits** on cloud platforms
- Hosting **malicious data**
- **Botnet** command or control
- **DDoS**

Insecure Interfaces and APIs

Insecure interfaces and APIs related risks:

- Circumvents **user defined polices**
- Is not credential leak proof
- Breach in **logging and monitoring facilities**
- Unknown API dependencies
- Reusable **passwords/tokens**
- Insufficient input-data validation

Cloud Computing Threats (Cont'd)

C|EH Certified Ethical Hacker

Insufficient Due Diligence

Ignorance of CSP's cloud environment pose risks in **operational responsibilities** such as security, encryption, incident response, and more issues such as contractual issues, design and architectural issues, etc.

Shared Technology Issues

Most underlying components that make up the cloud infrastructure (ex: GPU, CPU caches, etc.) **does not offer strong isolation properties** in a multi-tenant environment which enables attackers to attack other machines if they are able to exploit vulnerabilities in one client's applications

Unknown Risk Profile

Client organizations are unable to get a clear picture of internal security procedures, security compliance, configuration hardening, patching, auditing and logging, etc. as they are less involved with **hardware** and **software ownership** and maintenance in the cloud

Cloud Computing Threats (Cont'd)

C|EH Certified Ethical Hacker

Illegal Access to the Cloud

Weak authentication and authorization controls could lead to illegal access thereby compromising confidential and critical data stored in the cloud

Loss of Business Reputation due to Co-tenant Activities

Resources are shared in the cloud, thus malicious activity of one co-tenant might affect the reputation of the other, resulting in poor service delivery, data loss, etc. that bring down organization's reputation

Privilege Escalation

A mistake in the access allocation system causes a customer, third party, or employee to get more access rights than needed

Natural Disasters

Based on geographic location and climate, data centers may be exposed to natural disasters such as floods, lightening, earthquakes, etc. that can affect the cloud services

Hardware Failure

Hardware failure such as switches, servers, etc. in data centers can make the cloud data inaccessible

Cloud Computing Threats (Cont'd)

Supply Chain Failure

- Cloud providers outsource certain tasks to third parties. Thus the security of the **cloud is directly proportional to security of each link** and the extent of dependency on third parties
- A disruption in the chain may lead to **loss of data privacy** and **integrity**, **services unavailability**, **violation of SLA**, **economic** and **reputational losses** resulting in failure to meet customer demand, and cascading failure

Modifying Network Traffic

- In cloud, the network traffic may be modified due to flaws while provisioning or de-provisioning network, or **vulnerabilities in communication encryption**
- Modification of network traffic may cause **loss**, **alteration**, or **theft of confidential data** and communications

Isolation Failure

- Due to the **isolation failure**, attackers try to **control operations** of other cloud customers **to gain illegal access** to the data

Module Flow

1. Introduction to Cloud Computing
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Cloud Computing Attacks

C|EH Certified Ethical Hacker

1. Service Hijacking using Social Engineering Attacks
2. Session Hijacking using XSS Attack
3. Domain Name System (DNS) Attacks
4. SQL Injection Attacks
5. Wrapping Attack
6. Service Hijacking using Network Sniffing
7. Session Hijacking using Session Riding
8. Side Channel Attacks or Cross-guest VM Breaches
9. Cryptanalysis Attacks
10. DoS and DDoS Attacks

Service Hijacking using Social Engineering Attacks

C|EH Certified Ethical Hacker

01 Social engineering is a non-technical kind of **intrusion that relies heavily on human interaction** and often involves tricking other people to break normal security procedures

02 Attacker might target the cloud service provider to **reset the password** or **IT staff accessing the cloud services to reveal passwords**

03 Other ways to obtain passwords include: **password guessing**, using **keylogging malware**, implementing **password cracking techniques**, sending **phishing mails**, etc.

04 Social engineering attack results in **exposing customer data**, credit card data, **personal information**, **business plans**, staff data, identity theft, etc.

Service Hijacking using Network Sniffing

Network sniffing involves **interception and monitoring of network traffic** which is being sent between the two cloud nodes

Attacker uses packet sniffers to capture sensitive data such as **passwords**, **session cookies**, and other web service related security configuration such as the **UDDI** (Universal Description Discovery and Integrity), **SOAP** (Simple Object Access Protocol) and **WSDL** (Web Service Description Language) files

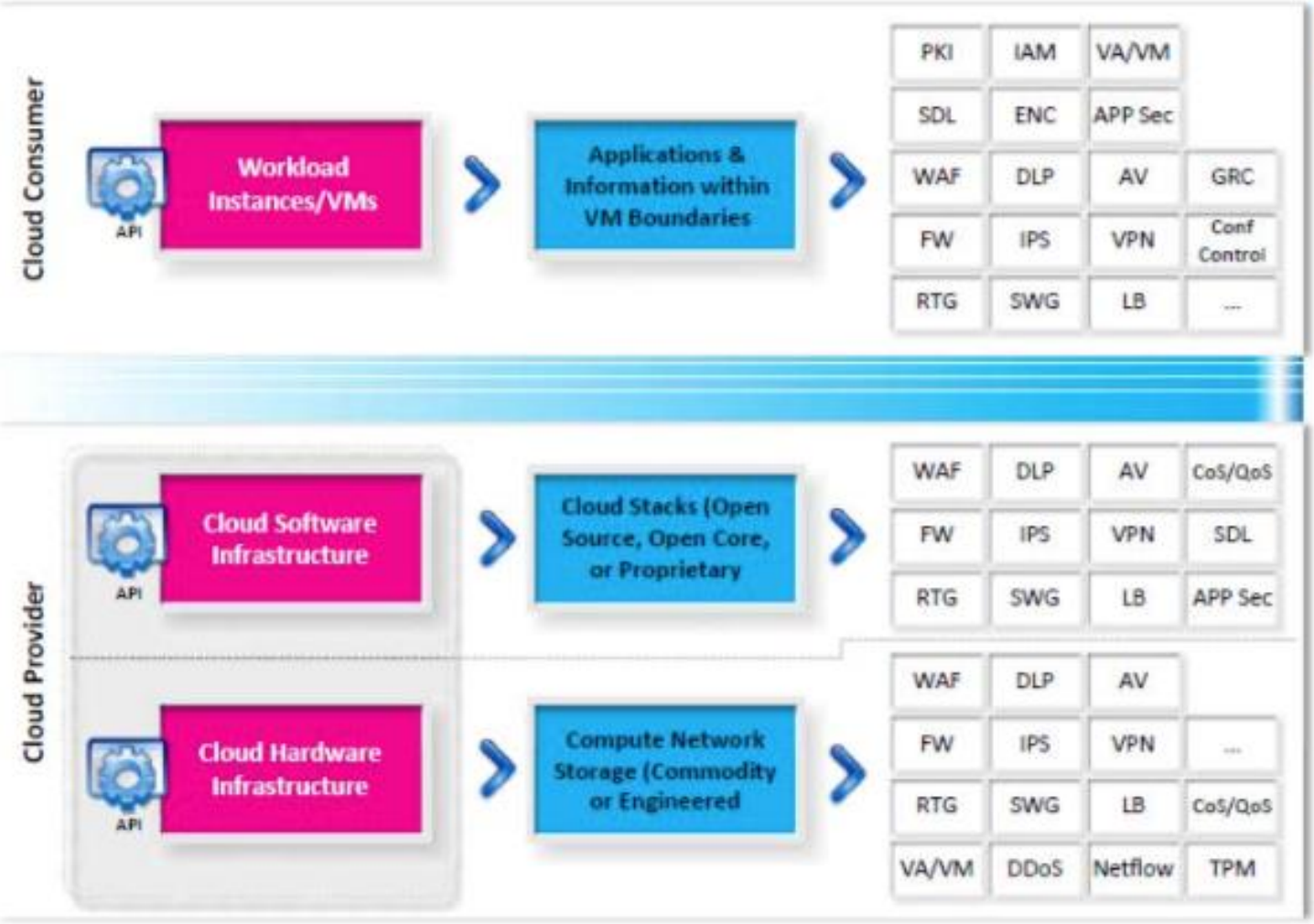
Module Flow

1. Introduction to Cloud Computing
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Cloud Security Control Layers

01	**Applications**	SDLC. Binary Analysis, Scanners, Web App Firewalls, Transactional Sec	
02	**Information**	DLP, CMF, Database Activity, Monitoring, Encryption	
03	**Management**	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring	
04	**Network**	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth	
05	**Trusted Computing**	Hardware & software RoT & API's	
06	**Computer and Storage**	Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking	
07	**Physical**	Physical Plant Security, CCTV, Guards	

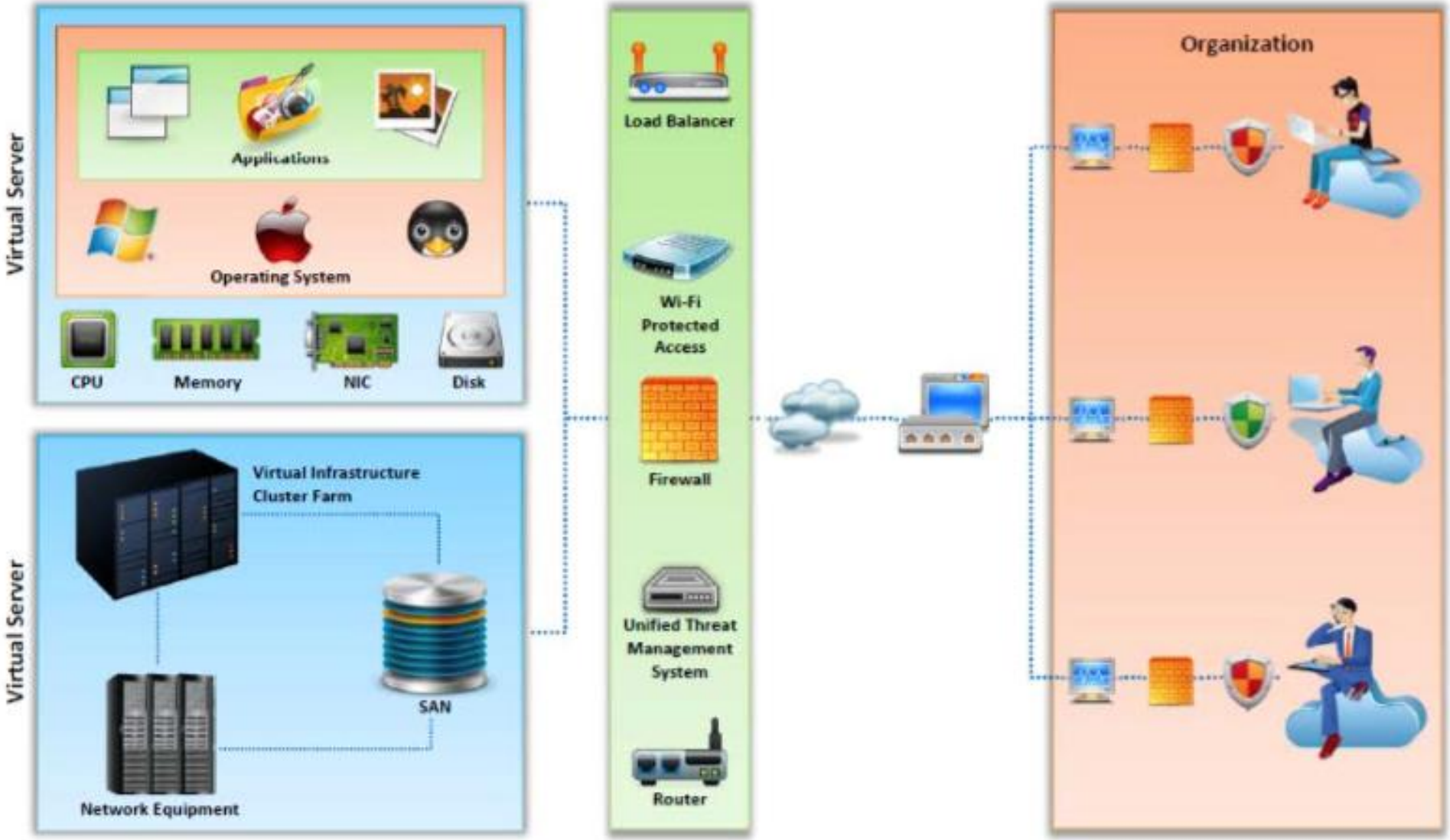
Cloud Security is the Responsibility of both Cloud Provider and Consumer



Security Controls

- PKI: Public Key Infrastructure
- SDL: Security Development Lifecycle
- WAF: Web Application Firewall
- FW: Firewall
- RTG: Real Traffic Grabber
- IAM: Identity and Access Management
- ENC: Encryption
- DLP: Data loss prevention
- IPS: Intrusion Prevention System
- SWG: Secure Web Gateway
- VA/VM: Virtual Application/Virtual Machine
- App Sec: Application security
- AV: Anti-virus
- VPN: Virtual Private Network
- LB: Load Balancer
- GRC: Governance, Risk, and Compliance
- Config Control: Configuration Control
- CoS/QoS: Class of Service/ Quality of Service
- DDoS: Distributed denial of service
- TPM: Trusted Platform Module
- Netflow: Network protocol by Cisco

Placement of Security Controls in the Cloud



Best Practices for Securing Cloud (Cont'd)

- Analyze **cloud provider security policies** and SLAs
- Assess security of **cloud APIs** and also log customer **network traffic**
- Ensure that cloud undergoes regular **security checks and updates**
- Ensure that physical security is a **24 x 7 x 365** affair
- Enforce **security standards** in installation/ configuration
- Ensure that the memory, storage, and network access is **isolated**
- Leverage strong **two-factor authentication** techniques where possible
- Baseline **security breach notification** process
- Analyze **API dependency chain software** modules
- Enforce stringent **registration and validation process**
- Perform vulnerability and configuration **risk assessment**
- Disclose infrastructure information, **security patching**, and firewall details

Best Practices for Securing Cloud (Cont'd)

1. Enforce stringent **cloud security compliance**, SCM (Software Configuration Management), and management practice transparency
2. Employ security devices such as IDS, IPS, firewall, etc. to guard and stop **unauthorized access** to the data stored in the cloud
3. Enforce strict **supply chain** management and conduct a comprehensive supplier assessment
4. Enforce stringent **security policies and procedures** like access control policy, information security management policy and contract policy
5. Ensure **infrastructure security** through proper management and monitoring , availability, secure VM separation and service assurance
6. Use **VPNs** to secure the clients data and ensure that data is **completely deleted** from the main servers along with its replicas when requested for data disposal
7. Ensure **Secure Sockets Layer** (SSL) is used for sensitive and confidential data transmission
8. Analyze the **security model** of cloud provider interfaces
9. Understand terms and conditions in **SLA** like **minimum level of uptime** and **penalties** in case of failure to adhere to the agreed level
10. Enforce basic information security practices namely strong **password policy**, **physical security**, device security, **encryption**, data security, network security, etc.

Module Flow

1. Introduction to Cloud Computing
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

Cloud Security Tools

Alert Logic
https://www.alertlogic.com

SecludIT
http://secludit.com

Dell Cloud Manager
http://www.enstratius.com

Nessus Enterprise for AWS
http://www.tenable.com

Qualys Cloud Suite
https://www.qualys.com

Trend Micro's Instant-On Cloud Security
http://www.trendmicro.com

Symantec O3
http://www.symantec.com

Cloud Application Visibility
http://www.zscaler.com

Porticor
http://www.porticor.com

Panda Cloud Office Protection
http://www.cloudantivirus.com

Module Flow

1. Introduction to Cloud Computing
2. Cloud Computing Threats
3. Cloud Computing Attacks
4. Cloud Security
5. Cloud Security Tools
6. Cloud Penetration Testing

What is Cloud Pen Testing?

Cloud pen testing is a method of actively evaluating the security of a cloud system by **simulating an attack from a malicious source**

Security posture of cloud should be monitored regularly to determine the presence of **vulnerabilities** and the **risks** they pose

Cloud security is based on the shared responsibility of both **cloud provider** and the **client**

Type of cloud as well as the type of cloud provider determines if pen testing is allowed or not

- If it is **SaaS**, pen testing is **not allowed** by providers as it might impact their infrastructure
- If it is **PaaS** or **IaaS**, pen testing is **allowed** but coordination is required

The contract and SLA made with cloud provider states if pen testing is allowed, if so **what kinds of tests** are allowed and **how frequently** can it be done

Key Considerations for Pen Testing in the Cloud

- Determine the **type of cloud**; PaaS, IaaS or SaaS
- Obtain **written consents** for performing pen testing
- Ensure every aspect of the Infrastructure (IaaS), Platform (PaaS), or Software (SaaS) are included in the **scope of testing** and **generated reports**
- Determine **what kind of testing** is permitted by Cloud Service Provider (CSP) and **how often**
- Prepare **legal** and **contractual** documents
- Perform both **internal** and **external pen testing**
- Perform pen tests on the **web apps/services** in the cloud without web application firewall (WAF) or reverse proxy
- Perform **vulnerability scans on host** available in the cloud
- Determine how to coordinate with the CSP for **scheduling** and **performing the test**

Scope of Cloud Pen Testing

1. Pen testing **web applications** includes mobile applications
2. Pen testing network or host includes **systems**, **firewalls**, **IDS**, **databases**, etc., available in cloud
3. Pen testing **web services** includes mobile back-end services